



## **Cisco Embedded Wireless Controller on Catalyst Access Points Configuration Guide, IOS XE Amsterdam 17.1.x**

**First Published:** 2020-02-22

### **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).

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 standards documentation, or language that is used by a referenced third-party product.

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)

© 2020 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### PREFACE

<b>Preface</b>	<b>xxxiii</b>
Document Conventions	xxxiii
Related Documentation	xxxv
Communications, Services, and Additional Information	xxxv
Cisco Bug Search Tool	xxxv
Documentation Feedback	xxxv

---

### CHAPTER 1

<b>Overview of Cisco Embedded Wireless Controller on Catalyst Access Points</b>	<b>1</b>
Elements of the New Configuration Model	1
Configuration Workflow	2
Initial Setup	3

---

### PART I

<b>System Configuration</b>	<b>5</b>
-----------------------------	----------

---

### CHAPTER 2

<b>System Configuration</b>	<b>7</b>
Information About New Configuration Model	7
Configuring a Wireless Profile Policy (GUI)	9
Configuring a Wireless Profile Policy (CLI)	10
Configuring a Flex Profile	11
Configuring an AP Profile (GUI)	12
Configuring an AP Profile (CLI)	15
Configuring an RF Profile (GUI)	15
Configuring an RF Profile (CLI)	16
Configuring Policy Tag (GUI)	17
Configuring a Policy Tag (CLI)	17
Configuring Wireless RF Tag (GUI)	18

Configuring Wireless RF Tag (CLI)	19
Attaching a Policy Tag and Site Tag to an AP (GUI)	20
Attaching Policy Tag and Site Tag to an AP (CLI)	20
AP Filter	21
Introduction to AP Filter	21
Set Tag Priority (GUI)	22
Set Tag Priority	22
Create an AP Filter (GUI)	23
Create an AP Filter (CLI)	23
Set Up and Update Filter Priority (GUI)	24
Set Up and Update Filter Priority	24
Verify AP Filter Configuration	24

**CHAPTER 3****Smart Licensing 27**

Information About Cisco Smart Licensing	27
Creating a Smart Account	29
Using Smart Licensing	30
Using Specified License Reservation (SLR)	30
Enabling Specified License Reservation in CSSM	31
Enabling Smart Software Licensing	32
Registering for Smart License (Connected Mode)	33
Enabling Smart License Reservation	33
Enabling Smart Call Home Reporting	34
Configuring AIR License Level (GUI)	35
Configuring AIR License Level (CLI)	35
Configuring AIR Network Essentials License Level	36
Configuring AIR Network Advantage License Level	36
Verifying Smart Licensing Configurations	37

**CHAPTER 4****Conversion and Migration 39**

Conversion and Migration in Embedded Wireless Controller Capable APs	39
Types of Conversion	39
Access Point Conversion	40
Converting a CAPWAP AP to an Embedded Wireless Controller Capable AP	40

	Converting an Embedded Wireless Controller Capable AP to a CAPWAP AP	40
	Converting a Single AP to CAPWAP or Embedded Wireless Controller Capable AP (CLI)	40
	AP Conversion Deployment Scenarios	41
	Network Conversion	43
	Converting the Network (CLI)	43
	Network Conversion Deployment Scenarios	44
	SKU Conversion Scenarios	45
	Converting AireOS Mobility Express Network to Embedded Wireless Controller Network	46
<hr/>		
<b>CHAPTER 5</b>	<b>Best Practices</b>	<b>47</b>
	Introduction	47
<hr/>		
<b>PART II</b>	<b>Lightweight Access Points</b>	<b>49</b>
<hr/>		
<b>CHAPTER 6</b>	<b>Country Codes</b>	<b>51</b>
	Information About Country Codes	51
	Prerequisites for Configuring Country Codes	51
	Configuring Country Codes (GUI)	52
	How to Configure Country Codes	52
	Configuration Examples for Configuring Country Codes	54
	Viewing Channel List for Country Codes	54
<hr/>		
<b>CHAPTER 7</b>	<b>AP Priority</b>	<b>55</b>
	Failover Priority for Access Points	55
	Setting AP Priority (GUI)	55
	Setting AP Priority	56
<hr/>		
<b>CHAPTER 8</b>	<b>Rogue per AP</b>	<b>57</b>
	Rogue per AP	57
	Enabling Rogue Detection	58
	Configuring an AP Profile (GUI)	58
	Configure an AP Profile	61
	Define a Wireless Site Tag and Assign an AP Profile (GUI)	62
	Define a Wireless Site Tag and Assign an AP Profile (CLI)	63

Associating Wireless Tag to an AP (GUI) 63

Associate Wireless Tag to an AP (CLI) 64

---

**CHAPTER 9**

**802.11 Parameters for Cisco Access Points 65**

2.4-GHz Radio Support 65

Configuring 2.4-GHz Radio Support for the Specified Slot Number 65

5-GHz Radio Support 67

Configuring 5-GHz Radio Support for the Specified Slot Number 67

Information About Dual-Band Radio Support 69

Configuring Default XOR Radio Support 70

Configuring XOR Radio Support for the Specified Slot Number (GUI) 72

Configuring XOR Radio Support for the Specified Slot Number 72

Receiver Only Dual-Band Radio Support 74

Information About Receiver Only Dual-Band Radio Support 74

Configuring Receiver Only Dual-Band Parameters for Access Points 74

Enabling CleanAir with Receiver Only Dual-Band Radio on a Cisco Access Point (GUI) 74

Enabling CleanAir with Receiver Only Dual-Band Radio on a Cisco Access Point 75

Disabling Receiver Only Dual-Band Radio on a Cisco Access Point (GUI) 75

Disabling Receiver Only Dual-Band Radio on a Cisco Access Point 75

Configuring Client Steering (CLI) 76

Verifying Cisco Access Points with Dual-Band Radios 77

---

**CHAPTER 10**

**802.1x Support 79**

Introduction to the 802.1X Authentication 79

EAP-FAST Protocol 79

EAP-TLS/EAP-PEAP Protocol 80

Limitations of the 802.1X Authentication 80

Topology - Overview 80

Configuring 802.1X Authentication Type and LSC AP Authentication Type (GUI) 81

Configuring 802.1X Authentication Type and LSC AP Authentication Type 81

Configuring the 802.1X Username and Password (GUI) 82

Configuring the 802.1X Username and Password (CLI) 83

Enabling 802.1X on the Switch Port 84

Verifying 802.1X on the Switch Port 85

Verifying the Authentication Type 86

---

**CHAPTER 11**

**Information About NAT Support 87**

Restrictions for NAT Support 87

Enabling Centralized NAT on a VLAN 88

Verifying NAT Support 88

---

**PART III**

**Radio Resource Management 91**

---

**CHAPTER 12**

**Radio Resource Management 93**

Information About Radio Resource Management 93

Radio Resource Monitoring 94

Transmit Power Control 94

Overriding the TPC Algorithm with Minimum and Maximum Transmit Power Settings 94

Dynamic Channel Assignment 95

Coverage Hole Detection and Correction 97

Restrictions for Radio Resource Management 97

How to Configure RRM 97

Configuring Neighbor Discovery Type (CLI) 97

Configuring Transmit Power Control 98

Configuring the Tx-Power Control Threshold (CLI) 98

Configuring the Tx-Power Level (CLI) 98

Configuring 802.11 RRM Parameters 99

Configuring Advanced 802.11 Channel Assignment Parameters (CLI) 99

Configuring 802.11 Coverage Hole Detection (CLI) 101

Configuring 802.11 Event Logging (CLI) 102

Configuring 802.11 Statistics Monitoring (CLI) 103

Configuring the 802.11 Performance Profile (CLI) 104

Configuring Advanced 802.11 RRM 105

Enabling Channel Assignment (CLI) 105

Restarting DCA Operation 106

Updating Power Assignment Parameters (CLI) 106

Configuring Rogue Access Point Detection in RF Groups 106

Configuring Rogue Access Point Detection in RF Groups (CLI) 106

Monitoring RRM Parameters and RF Group Status **108**

- Monitoring RRM Parameters **108**
- Verifying RF Group Status (CLI) **108**

Examples: RF Group Configuration **109**

Information About ED-RRM **109**

- Configuring ED-RRM on the Cisco Wireless LAN Controller (CLI) **109**

---

**CHAPTER 13 Coverage Hole Detection 111**

Coverage Hole Detection and Correction **111**

- Configuring Coverage Hole Detection (GUI) **111**
- Configuring Coverage Hole Detection (CLI) **112**
- Configuring CHD for RF Tag Profile (GUI) **113**
- Configuring CHD for RF Profile (CLI) **114**

---

**CHAPTER 14 Cisco Flexible Radio Assignment 115**

Information About Flexible Radio Assignment **115**

- Benefits of the FRA **116**
- Configuring an FRA Radio (CLI) **116**
- Configuring an FRA Radio (GUI) **118**

---

**CHAPTER 15 XOR Radio Support 121**

Information About Dual-Band Radio Support **121**

- Configuring Default XOR Radio Support **122**
- Configuring XOR Radio Support for the Specified Slot Number (GUI) **124**
- Configuring XOR Radio Support for the Specified Slot Number **124**

---

**CHAPTER 16 Cisco Receiver Start of Packet 127**

Information About Receiver Start of Packet Detection Threshold **127**

- Restrictions for Rx SOP **127**
- Configuring Rx SOP (CLI) **128**
- Customizing RF Profile (CLI) **128**

---

**CHAPTER 17 Client Limit 131**



Information About Client Limit	131
Configuring Client Limit Per WLAN (GUI)	131
Configuring Client Limit Per WLAN (CLI)	131

---

**CHAPTER 18**     **IP Theft**    **133**

Introduction to IP Theft	133
Configuring IP Theft (GUI)	134
Configuring IP Theft	134
Configuring the IP Theft Exclusion Timer	134
Verifying IP Theft Configuration	135

---

**CHAPTER 19**     **Unscheduled Automatic Power Save Delivery**    **137**

Information About Unscheduled Automatic Power Save Delivery	137
Viewing Unscheduled Automatic Power Save Delivery (CLI)	137

---

**CHAPTER 20**     **Enabling USB Port on Access Points**    **139**

USB Port as Power Source for Access Points	139
Configuring an AP Profile (CLI)	140
Configuring USB Settings for an Access Point (CLI)	140
Monitoring USB Configurations for Access Points (CLI)	141

---

**PART IV**            **Network Management**    **143**

---

**CHAPTER 21**     **DHCP Option82**    **145**

Information About DHCP Option 82	145
Configuring DHCP Option 82 Global Interface	146
Configuring DHCP Option 82 Globally Through Server Override (CLI)	146
Configuring DHCP Option 82 Globally Through Different SVIs (GUI)	147
Configuring DHCP Option 82 Globally Through Different SVIs (CLI)	147
Configuring DHCP Option 82 Format	148
Configuring DHCP Option82 Through a VLAN Interface	149
Configuring DHCP Option 82 Through Option-Insert Command (CLI)	149
Configuring DHCP Option 82 Through the server-ID-override Command (CLI)	150
Configuring DHCP Option 82 Through a Subscriber-ID (CLI)	151

Configuring DHCP Option 82 Through server-ID-override and subscriber-ID Commands (CLI)	152
Configuring DHCP Option 82 Through Different SVIs (CLI)	153

---

<b>CHAPTER 22</b>	<b>RADIUS Realm</b>	<b>155</b>
	Information About RADIUS Realm	155
	Enabling RADIUS Realm	156
	Configuring Realm to Match the RADIUS Server for Authentication and Accounting	156
	Configuring the AAA Policy for a WLAN	157
	Verifying the RADIUS-Realm Configuration	159

---

<b>CHAPTER 23</b>	<b>Persistent SSID Broadcast</b>	<b>161</b>
	Persistent SSID Broadcast	161
	Configuring Persistent SSID Broadcast	161
	Verifying Persistent SSID Broadcast	162

---

<b>CHAPTER 24</b>	<b>Network Monitoring</b>	<b>163</b>
	Network Monitoring	163
	Status Information Received Synchronously - Configuration Examples	163
	Alarm and Event Information Received Asynchronously - Configuration Examples	165

---

<b>PART V</b>	<b>System Management</b>	<b>167</b>
---------------	--------------------------	------------

---

<b>CHAPTER 25</b>	<b>Network Mobility Services Protocol</b>	<b>169</b>
	Information About Network Mobility Services Protocol	169
	Enabling NMSP On-Premises Services	170
	Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues	170
	Modifying the NMSP Notification Threshold for Clients, and Tags	171
	Configuring NMSP Strong Cipher	171
	Verifying NMSP Settings	172
	Examples: NMSP Settings Configuration	174
	Probe RSSI Location	174
	Configuring Probe RSSI	175
	Verifying Probe RSSI	176
	RFID Tag Support	176

Configuring RFID Tag Support 177

Verifying RFID Tag Support 177

---

**CHAPTER 26**

**Application Visibility and Control 181**

Information About Application Visibility and Control 181

Prerequisites for Application Visibility and Control 182

Restrictions for Application Visibility and Control 182

AVC Configuration Overview 183

Create a Flow Monitor 183

Configuring a Flow Monitor (GUI) 184

Create a Flow Exporter 184

Configure a WLAN for AVC 185

Configuring a Policy Tag 186

Attaching a Policy Profile to a WLAN Interface (GUI) 186

Attaching a Policy Profile to a WLAN Interface (CLI) 186

Attaching a Policy Profile to an AP 188

Verify the AVC Configuration 188

AVC-Based Selective Reanchoring 189

Restrictions for AVC-Based Selective Reanchoring 189

Configuring the Flow Exporter 189

Configuring the Flow Monitor 190

Configuring the AVC Reanchoring Profile 191

Configuring the Wireless WLAN Profile Policy 191

Verifying AVC Reanchoring 192

---

**CHAPTER 27**

**Cisco Connected Mobile Experiences Cloud 197**

Configuring Cisco CMX Cloud 197

Verifying Cisco CMX Cloud Configuration 198

---

**CHAPTER 28**

**EDCA Parameters 201**

Enhanced Distributed Channel Access Parameters 201

Configuring EDCA Parameters (GUI) 201

Configuring EDCA Parameters (CLI) 202

---

**CHAPTER 29****802.11 parameters and Band Selection 205**

Information About Configuring Band Selection, 802.11 Bands, and Parameters 205

Band Select 205

802.11 Bands 206

802.11n Parameters 206

802.11h Parameters 206

Restrictions for Band Selection, 802.11 Bands, and Parameters 206

How to Configure 802.11 Bands and Parameters 207

Configuring Band Selection (GUI) 207

Configuring Band Selection (CLI) 208

Configuring the 802.11 Bands (GUI) 209

Configuring the 802.11 Bands (CLI) 209

Configuring a Band-Select RF Profile (GUI) 212

Configuring 802.11n Parameters (GUI) 212

Configuring 802.11n Parameters (CLI) 213

Configuring 802.11h Parameters (CLI) 215

Monitoring Configuration Settings for Band Selection, 802.11 Bands, and Parameters 216

Verifying Configuration Settings Using Band Selection and 802.11 Bands Commands 216

Example: Viewing the Configuration Settings for the 5-GHz Band 216

Example: Viewing the Configuration Settings for the 2.4-GHz Band 218

Example: Viewing the status of 802.11h Parameters 219

Example: Verifying the Band-Selection Settings 220

Configuration Examples for Band Selection, 802.11 Bands, and Parameters 220

Examples: Band Selection Configuration 220

Examples: 802.11 Bands Configuration 221

Examples: 802.11n Configuration 221

Examples: 802.11h Configuration 222

---

**CHAPTER 30****Image Download 223**

Information About Image Download 223

Updates to the AP Image Predownload Status (GUI) 223

Image Download Scenarios 224

Image Download During AP Join 224

Network Software Upgrade (Pre-Download)	225
Methods Supported for Image Download	225
TFTP Image Download Method	226
SFTP Image Download Method	226
Desktop (HTTP) Image Download Method	226
Prerequisites for Image Download	226
Configuring Image Download Profile	227
Configuring TFTP Image Download (GUI)	227
Configuring TFTP Image Download (CLI)	228
Configuring SFTP Image Download (GUI)	229
Configuring SFTP Image Download (CLI)	229
Configuring CCO Mode for Software Upgrade (GUI)	230
Configuring CCO Image Download (CLI)	232
Troubleshooting - CCO Image Download Error Messages	234
Configuring Desktop (HTTP) Image Download (GUI)	234
Initiating Pre-Download (CLI)	235
Verifying Image Download	236

---

**CHAPTER 31**

<b>Conditional Debug and Radioactive Tracing</b>	<b>239</b>
Introduction to Conditional Debugging	239
Introduction to Radioactive Tracing	239
Conditional Debugging and Radioactive Tracing	240
Location of Tracefiles	240
Configuring Conditional Debugging (GUI)	241
Configuring Conditional Debugging	241
Recommended Workflow for Trace files	242
Copying Tracefiles Off the Box	243
Configuration Examples for Conditional Debugging	244
Verifying Conditional Debugging	244
Example: Verifying Radioactive Tracing Log for SISF	244

---

**CHAPTER 32**

<b>Aggressive Client Load Balancing</b>	<b>247</b>
Information About Aggressive Client Load Balancing	247
Enabling Aggressive Client Load Balancing (GUI)	248

Configuring Aggressive Client Load Balancing (GUI) 248  
 Configuring Aggressive Client Load Balancing (CLI) 249

---

**CHAPTER 33**

**Accounting Identity List 251**

Configuring Accounting Identity List (GUI) 251  
 Configuring Accounting Identity List (CLI) 251  
 Configuring Client Accounting (GUI) 252  
 Configuring Client Accounting (CLI) 252

---

**CHAPTER 34**

**Volume Metering 255**

Configuring Volume Metering 255

---

**CHAPTER 35**

**Enabling Syslog Messages in Access Points and Controller for Syslog Server 257**

Information About Enabling Syslog Messages in Access Points and Embedded Wireless Controller for Syslog Server 257  
 Configuring Syslog Server for an AP Profile 258  
 Configuring Syslog Server for the Controller (GUI) 260  
 Configuring Syslog Server for the Embedded Wireless Controller 261  
 Verifying Syslog Server Configurations 262

---

**CHAPTER 36**

**Introduction to Software Maintenance Upgrade 267**

Overview of Controller SMUs 268  
 Managing Controller Hot or Cold SMU Package 269  
 Creating SMU Files (GUI) 270  
 Configuration Examples for SMU 271  
 Rolling AP Upgrade 273  
     Rolling AP Upgrade Process 273  
     Verifying AP Upgrade on the Controller 274  
 AP Device Pack (APDP) and AP Service Pack (APSP) 275  
     APSP and APDP 275  
     Managing APSP and APDP 276  
         Configuring the APSP and APDP Files (GUI) 276  
         Configuring the TFTP Server Directory 276  
         Configuring the SFTP Server Directory 277

Positive Workflow - APSP and APDP	279
Rollback and Cancel	280
Verifying APDP on the Embedded Wireless Controller	281

---

**PART VI**      **Security**    **283**

---

**CHAPTER 37**    **IPv4 ACLs**    **285**

Information about Network Security with ACLs	285
ACL Overview	285
Access Control Entries	285
ACL Supported Types	286
Supported ACLs	286
ACL Precedence	286
Port ACLs	286
Router ACLs	287
ACEs and Fragmented and Unfragmented Traffic	288
ACEs and Fragmented and Unfragmented Traffic Examples	288
Standard and Extended IPv4 ACLs	289
IPv4 ACL Switch Unsupported Features	289
Access List Numbers	289
Numbered Standard IPv4 ACLs	290
Numbered Extended IPv4 ACLs	291
Named IPv4 ACLs	291
ACL Logging	292
Hardware and Software Treatment of IP ACLs	292
IPv4 ACL Interface Considerations	293
Restrictions for Configuring IPv4 Access Control Lists	293
How to Configure ACLs	294
Configuring IPv4 ACLs (GUI)	294
Configuring IPv4 ACLs	294
Creating a Numbered Standard ACL (GUI)	295
Creating a Numbered Standard ACL (CLI)	295
Creating a Numbered Extended ACL (GUI)	297
Creating a Numbered Extended ACL (CLI)	297

Creating Named Standard ACLs (GUI)	301
Creating Named Standard ACLs	301
Creating Extended Named ACLs (GUI)	303
Creating Extended Named ACLs	303
Applying an IPv4 ACL to an Interface (GUI)	305
Applying an IPv4 ACL to an Interface (CLI)	305
Applying ACL to Policy Profile (GUI)	306
Applying ACL to Policy Profile	306
Configuration Examples for ACLs	307
Examples: Including Comments in ACLs	307
IPv4 ACL Configuration Examples	307
ACLs in a Small Networked Office	308
Examples: ACLs in a Small Networked Office	308
Example: Numbered ACLs	309
Examples: Extended ACLs	309
Examples: Named ACLs	310
Monitoring IPv4 ACLs	310
<hr/>	
<b>CHAPTER 38</b>	<b>DNS-Based Access Control Lists 313</b>
Information About DNS-Based Access Control Lists	313
FlexConnect in Embedded Wireless Controller	314
Roaming	315
Restrictions on DNS-Based Access Control Lists	315
Flex Mode	316
Configuring the URL Filter List (CLI)	316
Configuring the URL Filter List (GUI)	316
Applying Custom Pre-Auth DNS ACL on WLAN	317
Applying Custom Post-Auth DNS ACL on Policy Profile	317
Configuring ISE for Central Web Authentication (GUI)	318
Viewing DNS-Based Access Control Lists	318
<hr/>	
<b>CHAPTER 39</b>	<b>Allowed List of Specific URLs 323</b>
Allowed List of Specific URLs	323
Adding URL to Allowed List	323



Verifying URLs on the Allowed List 324

---

**CHAPTER 40**

**Web-Based Authentication 327**

Authentication Overview 327

Device Roles 329

Authentication Process 329

Local Web Authentication Banner 330

Customized Local Web Authentication 333

Guidelines 333

Redirection URL for Successful Login Guidelines 335

How to Configure Local Web Authentication 335

Configuring Default Local Web Authentication 335

Configuring AAA Authentication (GUI) 335

Configuring AAA Authentication (CLI) 336

Configuring the HTTP/HTTPS Server (GUI) 337

Configuring the HTTP Server (CLI) 337

Creating a Parameter Map (GUI) 338

Configuring the Maximum Web Authentication Request Retries 338

Configuring a Local Banner in Web Authentication Page (GUI) 339

Configuring a Local Banner in Web Authentication Page (CLI) 339

Configuration Examples for Local Web Authentication 340

Example: Obtaining Web Authentication Certificate 340

Example: Displaying a Web Authentication Certificate 341

Example: Choosing the Default Web Authentication Login Page 342

Example: Choosing a Customized Web Authentication Login Page from an IPv4 External Web Server 343

Example: Choosing a Customized Web Authentication Login Page from an IPv6 External Web Server 343

Example: Assigning Login, Login Failure, and Logout Pages per WLAN 343

Example: Configuring Preauthentication ACL 344

Example: Configuring Webpassthrough 344

Verifying Web Authentication Type 344

Authentication for Sleeping Clients 345

Information About Authenticating Sleeping Clients 345

Restrictions on Authenticating Sleeping Clients	346
Configuring Authentication for Sleeping Clients (GUI)	346
Configuring Authentication for Sleeping Clients (CLI)	347

**CHAPTER 41****Central Web Authentication 349**

Information About Central Web Authentication	349
Prerequisites for Central Web Authentication	350
How to Configure ISE	350
Creating an Authorization Profile	350
Creating an Authentication Rule	350
Creating an Authorization Rule	351
How to Configure Central Web Authentication on the Controller	352
Configuring WLAN (GUI)	352
Configuring WLAN (CLI)	353
Configuring Policy Profile (CLI)	354
Configuring a Policy Profile (GUI)	356
Creating Redirect ACL	356
Configuring AAA for Central Web Authentication	357
Configuring Redirect ACL in Flex Profile (GUI)	358
Configuring Redirect ACL in Flex Profile (CLI)	359
Authentication for Sleeping Clients	359
Information About Authenticating Sleeping Clients	359
Restrictions on Authenticating Sleeping Clients	360
Configuring Authentication for Sleeping Clients (GUI)	361
Configuring Authentication for Sleeping Clients (CLI)	361

**CHAPTER 42****ISE Simplification and Enhancements 363**

Utilities for Configuring Security	363
Configuring Multiple Radius Servers	364
Verifying AAA and Radius Server Configurations	365
Configuring Captive Portal Bypassing for Local and Central Web Authentication	365
Information About Captive Bypassing	365
Configuring Captive Bypassing for WLAN in LWA and CWA (GUI)	366
Configuring Captive Bypassing for WLAN in LWA and CWA (CLI)	367

Sending DHCP Options 55 and 77 to ISE	368
Information about DHCP Option 55 and 77	368
Configuration to Send DHCP Options 55 and 77 to ISE (GUI)	368
Configuration to Send DHCP Options 55 and 77 to ISE (CLI)	368
Configuring EAP Request Timeout (GUI)	369
Configuring EAP Request Timeout	370
Configuring EAP Request Timeout in Wireless Security (CLI)	370
Captive Portal	371
Captive Portal Configuration	371
Configuring Captive Portal (GUI)	371
Configuring Captive Portal	372
Captive Portal Configuration - Example	374

**CHAPTER 43****Authentication and Authorization Between Multiple RADIUS Servers 377**

Information About Authentication and Authorization Between Multiple RADIUS Servers	377
Configuring 802.1X Security for WLAN with Split Authentication and Authorization Servers	378
Configuring Explicit Authentication and Authorization Server List (GUI)	378
Configuring Explicit Authentication Server List (GUI)	379
Configuring Explicit Authentication Server List (CLI)	379
Configuring Explicit Authorization Server List (GUI)	380
Configuring Explicit Authorization Server List (CLI)	381
Configuring Authentication and Authorization List for 802.1X Security (GUI)	382
Configuring Authentication and Authorization List for 802.1X Security	382
Configuring Web Authentication for WLAN with Split Authentication and Authorization Servers	383
Configuring Authentication and Authorization List for Web Authentication (GUI)	383
Configuring Authentication and Authorization List for Web Authentication	383
Verifying Split Authentication and Authorization Configuration	385
Configuration Examples	385

**CHAPTER 44****Secure LDAP 387**

Information About SLDAP	387
Prerequisite for Configuring SLDAP	389
Restrictions for Configuring SLDAP	389
Configuring SLDAP	389

Configuring an AAA Server Group (GUI)	390
Configuring a AAA Server Group	391
Configuring Search and Bind Operations for an Authentication Request	392
Configuring a Dynamic Attribute Map on an SLDAP Server	393
Verifying the SLDAP Configuration	393

**CHAPTER 45****RADIUS DTLS 395**

Information About RADIUS DTLS	395
Prerequisites	397
Configuring RADIUS DTLS Server	397
Configuring RADIUS DTLS Connection Timeout	398
Configuring RADIUS DTLS Idle Timeout	398
Configuring Source Interface for RADIUS DTLS Server	399
Configuring RADIUS DTLS Port Number	400
Configuring RADIUS DTLS Connection Retries	400
Configuring RADIUS DTLS Trustpoint	401
Configuring DTLS Dynamic Author	402
Enabling DTLS for Client	402
Configuring Client Trustpoint for DTLS	403
Configuring DTLS Idle Timeout	404
Configuring Server Trustpoint for DTLS	404
Verifying the RADIUS DTLS Server Configuration	405
Clearing RADIUS DTLS Specific Statistics	405

**CHAPTER 46****MAC Authentication Bypass 407**

MAC Authentication Bypass	407
MAB Configuration Guidelines	407
Configuring 802.11 Security for WLAN (GUI)	409
Configuring 802.11 Security for WLAN (CLI)	410
Configuring AAA for External Authentication	410
Configuring AAA for Local Authentication (GUI)	412
Configuring AAA for Local Authentication (CLI)	412
Configuring MAB for Local Authentication	413
Configuring MAB for External Authentication (GUI)	414

Configuring MAB for External Authentication (CLI) 414

---

**CHAPTER 47**

**Dynamic Frequency Selection 417**

Information About Dynamic Frequency Selection 417

Configuring Dynamic Frequency Selection (GUI) 417

Configuring Dynamic Frequency Selection 417

Verifying DFS 418

---

**CHAPTER 48**

**Managing Rogue Devices 419**

Rogue Detection 419

Rogue Devices 419

AP Impersonation Detection 420

Configuring Rogue Detection (GUI) 421

Configuring Rogue Detection (CLI) 421

Configuring RSSI Deviation Notification Threshold for Rogue APs (CLI) 422

Configuring Management Frame Protection (GUI) 423

Configuring Management Frame Protection (CLI) 423

Verifying Management Frame Protection 424

Verifying Rogue Events 424

Verifying Rogue Detection 425

Examples: Rogue Detection Configuration 427

Configuring Rogue Policies (GUI) 427

Configuring Rogue Policies (CLI) 428

Rogue Location Discovery Protocol (RLDP) 429

Rogue Location Discovery Protocol 429

Configuring RLDP for Generating Alarms (GUI) 431

Configuring an RLDP for Generating Alarms (CLI) 431

Configuring a Schedule for RLDP (GUI) 432

Configuring a Schedule for RLDP (CLI) 432

Configuring an RLDP for Auto-Contain (GUI) 433

Configuring an RLDP for Auto-Contain (CLI) 433

Configuring RLDP Retry Times on Rogue Access Points (GUI) 434

Configuring RLDP Retry Times on Rogue Access Points (CLI) 434

Verifying Rogue AP RLDP 434

Rogue Detection Security Level	435
Setting Rogue Detection Security-level	436
Wireless Service Assurance Rogue Events	437
Monitoring Wireless Service Assurance Rogue Events	437

**CHAPTER 49****Classifying Rogue Access Points 439**

Information About Classifying Rogue Access Points	439
Guidelines and Restrictions for Classifying Rogue Access Points	440
How to Classify Rogue Access Points	441
Classifying Rogue Access Points and Clients Manually (GUI)	441
Classifying Rogue Access Points and Clients Manually (CLI)	441
Configuring Rogue Classification Rules (GUI)	443
Configuring Rogue Classification Rules (CLI)	444
Monitoring Rogue Classification Rules	446
Examples: Classifying Rogue Access Points	447

**CHAPTER 50****Configuring Secure Shell 449**

Information About Configuring Secure Shell	449
SSH and Device Access	449
SSH Servers, Integrated Clients, and Supported Versions	449
SSH Configuration Guidelines	450
Secure Copy Protocol Overview	450
Secure Copy Protocol	451
SFTP Support	451
Prerequisites for Configuring Secure Shell	451
Restrictions for Configuring Secure Shell	452
How to Configure SSH	452
Setting Up the Device to Run SSH	452
Configuring the SSH Server	453
Monitoring the SSH Configuration and Status	455

**CHAPTER 51****Private Shared Key 457**

Information About Private Preshared Key	457
Configuring a PSK in a WLAN (CLI)	458

Configuring a PSK in a WLAN (GUI)	459
Applying a Policy Profile to a WLAN (GUI)	460
Applying a Policy Profile to a WLAN (CLI)	460
Verifying a Private PSK	460

**CHAPTER 52****Multi-Preshared Key 465**

Information About Multi-Preshared Key	465
Restrictions on Multi-PSK	466
Configuring Multi-Preshared Key (GUI)	466
Configuring Multi-Preshared Key (CLI)	469
Verifying Multi-PSK Configurations	470

**CHAPTER 53****Multiple Authentications for a Client 473**

Information About Multiple Authentications for a Client	473
Information About Supported Combination of Authentications for a Client	473
Configuring Multiple Authentications for a Client	474
Configuring WLAN for 802.1X and Local Web Authentication (GUI)	474
Configuring WLAN for 802.1X and Local Web Authentication (CLI)	474
Configuring WLAN for Preshared Key (PSK) and Local Web Authentication (GUI)	476
Configuring WLAN for Preshared Key (PSK) and Local Web Authentication	476
Configuring WLAN for PSK or Identity Preshared Key (iPSK) and Central Web Authentication (GUI)	478
Configuring WLAN for PSK or Identity Preshared Key (iPSK) and Central Web Authentication	478
Configuring WLAN	478
Applying Policy Profile to a WLAN	479
Verifying Multiple Authentication Configurations	480

**CHAPTER 54****Information About Cisco Umbrella WLAN 485**

Registering Embedded Wireless Controller to Cisco Umbrella Account	486
Configuring Cisco Umbrella WLAN	487
Importing CA Certificate to the Trust Pool	487
Creating a Local Domain RegEx Parameter Map	488
Configuring Parameter Map Name in WLAN (GUI)	489
Configuring the Umbrella Parameter Map	490

Enabling or Disabling DNScrypt (GUI)	490
Enabling or Disabling DNScrypt	491
Configuring Timeout for UDP Sessions	491
Configuring Parameter Map Name in WLAN (GUI)	492
Configuring Parameter Map Name in WLAN	492
Verifying the Cisco Umbrella Configuration	493

**CHAPTER 55****Locally Significant Certificates 495**

Information About Locally Significant Certificates	495
Certificate Provisioning in Controllers	496
Device Certificate Enrollment Operation	496
Certificate Provisioning on Lightweight Access Point	496
Restrictions for Locally Significant Certificates	496
Provisioning Locally Significant Certificates	497
Configuring RSA Key for PKI Trustpoint	497
Configuring PKI Trustpoint Parameters	497
Authenticating and Enrolling a PKI Trustpoint (GUI)	498
Authenticating and Enrolling the PKI Trustpoint with CA Server (CLI)	499
Configuring AP Join Attempts with LSC Certificate (GUI)	500
Configuring AP Join Attempts with LSC Certificate (CLI)	501
Configuring Subject-Name Parameters in LSC Certificate	501
Configuring Key Size for LSC Certificate	502
Configuring Trustpoint for LSC Provisioning on an Access Point	502
Configuring an AP LSC Provision List (GUI)	502
Configuring an AP LSC Provision List (CLI)	503
Configuring LSC Provisioning for all the APs (GUI)	504
Configuring LSC Provisioning for All APs (CLI)	505
Configuring LSC Provisioning for the APs in the Provision List	505
Verifying LSC Configuration	505
Configuring Management Trustpoint to LSC (GUI)	506
Configuring Management Trustpoint to LSC (CLI)	506

**PART VII****Quality of Service 509**



**CHAPTER 56****Quality of Service 511**

- Wireless QoS Overview 511
- Wireless QoS Targets 511
  - SSID Policies 511
  - Client Policies 512
  - Supported QoS Features on Wireless Targets 512
- Precious Metal Policies for Wireless QoS 512
- Prerequisites for Wireless QoS 513
- Restrictions for QoS on Wireless Targets 513
- Metal Policy Format 514
  - Metal Policy Format 514
  - Auto QoS Policy Format 518
  - Architecture for Voice, Video and Integrated Data (AVVID) 520
- How to apply Bi-Directional Rate Limiting 521
  - Information about Bi-Directional Rate Limiting 521
  - Prerequisites for Bi-Directional Rate Limiting 522
  - Configure Metal Policy on SSID 522
  - Configure Metal Policy on Client 523
  - Configure Bi-Directional Rate Limiting for All Traffic 524
  - Configure Bi-Directional Rate Limiting Based on Traffic Classification 524
  - Apply Bi-Directional Rate Limiting Policy Map to Policy Profile 526
  - Apply Metal Policy with Bi-Directional Rate Limiting 527
- How to apply Per Client Bi-Directional Rate Limiting 528
  - Information About Per Client Bi-Directional Rate Limiting 528
  - Prerequisites for Per Client Bi-Directional Rate Limiting 529
  - Restrictions on Per Client Bi-Directional Rate Limiting 529
  - Configuring Per Client Bi-Directional Rate Limiting (GUI) 529
  - Verifying Per Client Bi-Directional Rate Limiting 530
  - Configuring BDRL Using AAA Override 530
  - Verifying Bi-Directional Rate-Limit 531
- How to Configure Wireless QoS 532
  - Configuring a Policy Map with Class Map (GUI) 532
  - Configuring a Class Map (CLI) 533

Configuring Policy Profile to Apply QoS Policy (GUI)	534
Configuring Policy Profile to Apply QoS Policy (CLI)	534
Applying Policy Profile to Policy Tag (GUI)	535
Applying Policy Profile to Policy Tag (CLI)	535
Attaching Policy Tag to an AP	536

---

**CHAPTER 57****Wireless Auto-QoS 539**

Information About Auto QoS	539
How to Configure Wireless AutoQoS	540
Configuring Wireless AutoQoS on Profile Policy	540
Disabling Wireless AutoQoS	541
Rollback AutoQoS Configuration (GUI)	541
Rollback AutoQoS Configuration	541
Clearing Wireless AutoQoS Policy Profile (GUI)	542
Clearing Wireless AutoQoS Policy Profile	542
Viewing AutoQoS on policy profile	543

---

**CHAPTER 58****Native Profiling 545**

Information About Native Profiling	545
Creating a Class Map (GUI)	546
Creating a Class Map (CLI)	546
Creating a Service Template (GUI)	548
Creating a Service Template (CLI)	549
Creating a Parameter Map	550
Creating a Policy Map (GUI)	550
Creating a Policy Map (CLI)	551
Configuring Native Profiling in Local Mode	553
Verifying Native Profile Configuration	553

---

**PART VIII****IPv6 555**

---

**CHAPTER 59****Information About IPv6 Client Address Learning 557**

Address Assignment Using SLAAC	557
Stateful DHCPv6 Address Assignment	558

Static IP Address Assignment	559
Router Solicitation	559
Router Advertisement	559
Neighbor Discovery	559
Neighbor Discovery Suppression	560
Router Advertisement Guard	560
Router Advertisement Throttling	560
Prerequisites for IPv6 Client Address Learning	561
Configuring IPv6 on Embedded Wireless Controller Interface	561
Native IPv6	562
Information About IPv6	562
Configuring IPv6 Addressing	562
Creating an AP Join Profile (GUI)	564
Creating an AP Join Profile (CLI)	564
Configuring the Primary and Backup Embedded Wireless Controller (GUI)	565
Configuring Primary and Backup Controller (CLI)	565
Verifying IPv6 Configuration	566

**CHAPTER 60**

<b>Information About IPv6 ACL</b>	<b>567</b>
Understanding IPv6 ACLs	567
Types of ACL	567
Per User IPv6 ACL	567
Filter ID IPv6 ACL	568
Downloadable IPv6 ACL	568
Prerequisites for Configuring IPv6 ACL	568
Restrictions for Configuring IPv6 ACL	568
Configuring IPv6 ACLs	569
Default IPv6 ACL Configuration	569
Interaction with Other Features and Switches	569
How To Configure an IPv6 ACL	570
Creating an IPv6 ACL	570
Creating WLAN IPv6 ACL	573
Verifying IPv6 ACL	573
Displaying IPv6 ACLs	573

Configuration Examples for IPv6 ACL 574

Example: Creating an IPv6 ACL 574

Example: Displaying IPv6 ACLs 574

---

**PART IX**

**CleanAir 577**

---

**CHAPTER 61**

**Cisco CleanAir 579**

Information About Cisco CleanAir 579

Cisco CleanAir-Related Terms 580

Cisco CleanAir Components 580

Interference Types that Cisco CleanAir can Detect 581

EDRRM and AQR Update Mode 582

Prerequisites for CleanAir 582

Restrictions for CleanAir 582

How to Configure CleanAir 583

Enabling CleanAir for the 2.4-GHz Band (GUI) 583

Enabling CleanAir for the 2.4-GHz Band (CLI) 583

Configuring Interference Reporting for a 2.4-GHz Device (GUI) 583

Configuring Interference Reporting for a 2.4-GHz Device (CLI) 584

Enabling CleanAir for the 5-GHz Band (GUI) 586

Enabling CleanAir for the 5-GHz Band (CLI) 586

Configuring Interference Reporting for a 5-GHz Device (GUI) 587

Configuring Interference Reporting for a 5-GHz Device (CLI) 587

Configuring Event Driven RRM for a CleanAir Event (GUI) 589

Configuring EDRRM for a CleanAir Event (CLI) 589

Verifying CleanAir Parameters 590

Monitoring Interference Devices 591

Configuration Examples for CleanAir 591

CleanAir FAQs 592

---

**CHAPTER 62**

**Spectrum Intelligence 593**

Spectrum Intelligence 593

Configuring Spectrum Intelligence 594

Verifying Spectrum Intelligence Information 594

---

**PART X****WLAN 597**

---

**CHAPTER 63****WLANs 599**

- Information About WLANs 599
  - Band Selection 599
  - Off-Channel Scanning Deferral 599
  - DTIM Period 600
  - Session Timeouts 600
  - Cisco Client Extensions 601
  - Peer-to-Peer Blocking 601
  - Diagnostic Channel 601
- Prerequisites for WLANs 602
- Restrictions for WLANs 602
- How to Configure WLANs 603
  - Creating WLANs (GUI) 603
  - Creating WLANs (CLI) 603
  - Deleting WLANs (GUI) 604
  - Deleting WLANs 605
  - Searching WLANs (CLI) 605
  - Enabling WLANs (GUI) 605
  - Enabling WLANs (CLI) 606
  - Disabling WLANs (GUI) 606
  - Disabling WLANs (CLI) 606
  - Configuring General WLAN Properties (CLI) 607
  - Configuring Advanced WLAN Properties (CLI) 608
  - Configuring Advanced WLAN Properties (GUI) 610
- Verifying WLAN Properties (CLI) 611

---

**CHAPTER 64****Network Access Server Identifier 613**

- Information About Network Access Server Identifier 613
- Creating a NAS ID Policy(GUI) 614
- Creating a NAS ID Policy 614
- Attaching a Policy to a Tag (GUI) 615

Attaching a Policy to a Tag (CLI) 615  
 Verifying the NAS ID Configuration 616

---

**CHAPTER 65 DHCP for WLANs 619**

DHCP for WLANs 619

---

**CHAPTER 66 WLAN Security 621**

Information About AAA Override 621  
 Prerequisites for Layer 2 Security 621  
 How to Configure WLAN Security 622  
     Configuring Static WEP Layer 2 Security Parameters (CLI) 622  
     Configuring WPA + WPA2 Layer 2 Security Parameters (CLI) 622

---

**CHAPTER 67 Peer-to-Peer Client Support 625**

Information About Peer-to-Peer Client Support 625  
 Configure Peer-to-Peer Client Support 625

---

**CHAPTER 68 802.11r BSS Fast Transition 627**

Information About 802.11r Fast Transition 627  
 Restrictions for 802.11r Fast Transition 628  
 Monitoring 802.11r Fast Transition (CLI) 629  
 Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI) 630  
 Configuring 802.11r Fast Transition in an Open WLAN (GUI) 631  
 Configuring 802.11r Fast Transition in an Open WLAN (CLI) 632  
 Configuring 802.11r Fast Transition on a PSK Security–Enabled WLAN (CLI) 633  
 Disabling 802.11r Fast Transition (GUI) 634  
 Disabling 802.11r Fast Transition (CLI) 634

---

**CHAPTER 69 Assisted Roaming 637**

802.11k Neighbor List and Assisted Roaming 637  
 Restrictions for Assisted Roaming 638  
 How to Configure Assisted Roaming 638  
     Configuring Assisted Roaming (CLI) 638

Verifying Assisted Roaming	639
Configuration Examples for Assisted Roaming	639

---

<b>CHAPTER 70</b>	<b>802.11v</b>	<b>641</b>
	Information About 802.11v	641
	Enabling 802.11v Network Assisted Power Savings	641
	Prerequisites for Configuring 802.11v	642
	Restrictions for 802.11v	642
	Enabling 802.11v BSS Transition Management	642
	Configuring 802.11v BSS Transition Management (GUI)	643
	Configuring 802.11v BSS Transition Management (CLI)	643

---

<b>CHAPTER 71</b>	<b>802.11w</b>	<b>645</b>
	Information About 802.11w	645
	Prerequisites for 802.11w	648
	Restrictions for 802.11w	648
	How to Configure 802.11w	649
	Configuring 802.11w (GUI)	649
	Configuring 802.11w (CLI)	649
	Disabling 802.11w	650
	Monitoring 802.11w	651

---

<b>CHAPTER 72</b>	<b>Deny Wireless Client Session Establishment Using Calendar Profiles</b>	<b>653</b>
	Information About Denial of Wireless Client Session Establishment	653
	Configuring Daily Calendar Profile	654
	Configuring Weekly Calendar Profile	655
	Configuring Monthly Calendar Profile	656
	Mapping a Daily Calendar Profile to a Policy Profile	657
	Mapping a Weekly Calendar Profile to a Policy Profile	658
	Mapping a Monthly Calendar Profile to a Policy Profile	659
	Verifying Calendar Profile Configuration	660
	Verifying Policy Profile Configuration	661

---

<b>CHAPTER 73</b>	<b>Introduction to EoGRE</b>	<b>663</b>
-------------------	------------------------------	------------

EoGRE Configuration Overview **664**

Create a Tunnel Gateway **665**

Configuring a Tunnel Domain **666**

Configuring EoGRE Global Parameters **667**

Configuring a Tunnel Profile **667**

Associating WLAN to a Wireless Policy Profile **669**

Attaching a Policy Tag and a Site Tag to an AP **669**

Verifying the EoGRE Tunnel Configuration **670**





## Preface

This preface describes the conventions of this document and information on how to obtain other documentation. It also provides information on what's new in Cisco product documentation.

- [Document Conventions](#) , on page xxxiii
- [Related Documentation](#), on page xxxv
- [Communications, Services, and Additional Information](#), on page xxxv

## 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.

Convention	Description
{x   y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[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

Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Read the installation instructions before using, installing, or connecting the system to the power source. Use the statement number provided at the end of each warning statement to locate its translation in the translated safety warnings for 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.

---

## Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit [Cisco DevNet](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

## Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

## Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.





## CHAPTER 1

# Overview of Cisco Embedded Wireless Controller on Catalyst Access Points

---

Cisco Embedded Wireless Controller on Catalyst Access Points are the next generation of wireless controllers built for the Intent-based networking. The Cisco controllers are IOS XE based and integrates the RF Excellence from Aironet with Intent-based Networking capabilities of IOS XE to create the best-in-class wireless experience for your evolving and growing organization.

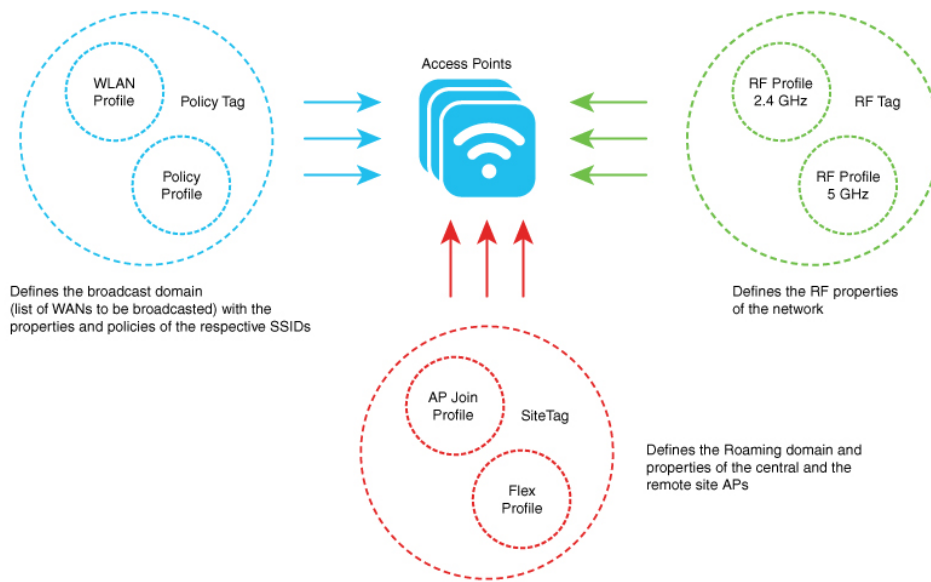
The controllers are deployable in physical form factors and can be managed using Cisco DNA Center, Netconf/YANG, web-based GUI, or CLI.

The configuration data model is based on design principles of reusability, simplified provisioning, enhanced flexibility and modularization to help manage networks as they scale up and simplify the management of dynamically changing business and IT requirements.

- [Elements of the New Configuration Model, on page 1](#)
- [Configuration Workflow, on page 2](#)
- [Initial Setup, on page 3](#)

## Elements of the New Configuration Model

The following diagram depicts the elements of the new configuration model.



### Tags

The property of a tag is defined by the property of the policies associated to it, which in turn is inherited by an associated client or an AP. There are various type of tags, each of which is associated to different profiles. Every tag has a default that is created when the system boots up.

### Profiles

Profiles represent a set of attributes that are applied to the clients associated to the APs or the APs themselves. Profiles are reusable entities that can be used across tags.

## Configuration Workflow

The following set of steps defines the logical order of configuration. Apart from the WLAN profile, all the profiles and tags have a default object associated with it.

#### 1. Create the following profiles:

- WLAN
- Policy
- AP Join
- Flex
- RF

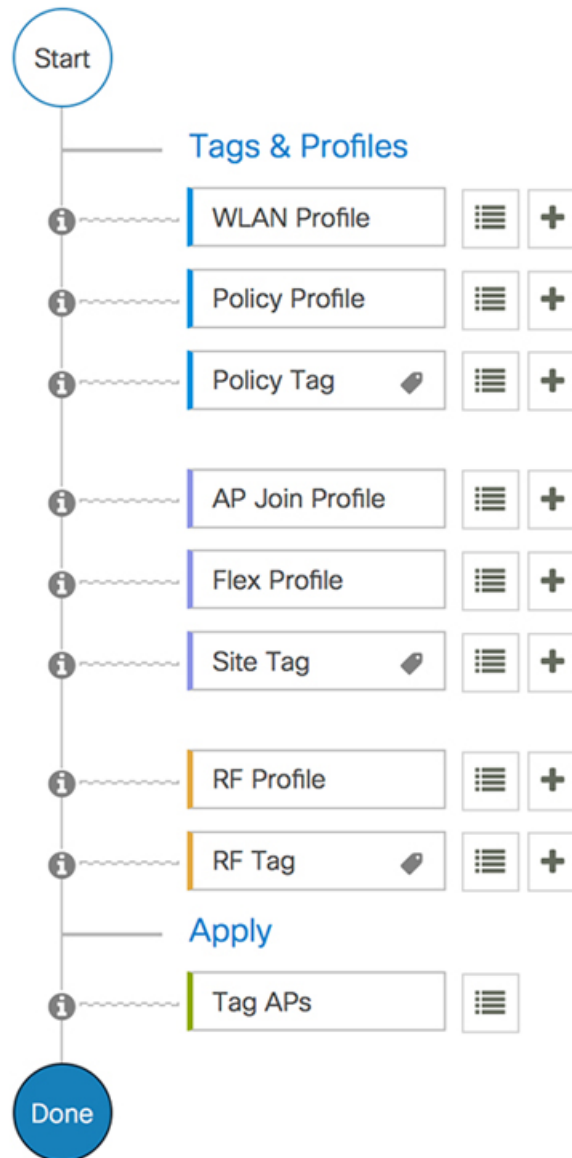
#### 2. Create the following tags:

- Policy
- Site

- RF

3. Associate tags to an AP.

Figure 1: Configuration Workflow



365513

# Initial Setup

## Setting up the Controller

The initial configuration wizard in Cisco Embedded Wireless Controller on Catalyst Access Points is a simplified, out-of-the-box installation and configuration interface for controller. This section provides

instructions to set up a controller to operate in a small, medium, or large network wireless environment, where access points can join and together as a simple solution provide various services, such as corporate employee or guest wireless access on the network.



---

**Note** From Cisco IOS XE Amsterdam 17.1.x onwards, date and time will not reflect in the web UI unless it is synched with Network Time Protocol (NTP).

---



---

**Note** When the AP has rebooted in the EWC mode, it broadcasts a provisioning SSID ending with the last digits of the MAC address. You can connect to the provisioning SSID using the PSK **password**.

You can then open a browser and you are redirected to [mywifi.cisco.com](http://mywifi.cisco.com) which takes you to the AP web UI. Enter the username as **webui** and password as **cisco**.

---



---

**Note** We recommend that you use the **wireless ewc-ap factory-reset** command to reset the EWC device to Day0 state (with the configuration wizard). This command also resets all the APs and EWC-APs in the network to Day0 state. You can use the **erase startup-config** command to remove the configuration from the device. However, this is not synched to other devices in the network.

---



---

**Note** After completing the Day0 wizard, the internal AP disjoins, and rejoins after one minute.

---



---

**Note** The wireless management must be the AP Gigabit port and you cannot have several SVIs configured in IOS-XE.

---





## PART I

# System Configuration

- [System Configuration](#), on page 7
- [Smart Licensing](#), on page 27
- [Conversion and Migration](#), on page 39
- [Best Practices](#), on page 47





## CHAPTER 2

# System Configuration

---

- [Information About New Configuration Model, on page 7](#)
- [Configuring a Wireless Profile Policy \(GUI\), on page 9](#)
- [Configuring a Wireless Profile Policy \(CLI\), on page 10](#)
- [Configuring a Flex Profile, on page 11](#)
- [Configuring an AP Profile \(GUI\), on page 12](#)
- [Configuring an AP Profile \(CLI\), on page 15](#)
- [Configuring an RF Profile \(GUI\), on page 15](#)
- [Configuring an RF Profile \(CLI\), on page 16](#)
- [Configuring Policy Tag \(GUI\), on page 17](#)
- [Configuring a Policy Tag \(CLI\), on page 17](#)
- [Configuring Wireless RF Tag \(GUI\), on page 18](#)
- [Configuring Wireless RF Tag \(CLI\), on page 19](#)
- [Attaching a Policy Tag and Site Tag to an AP \(GUI\), on page 20](#)
- [Attaching Policy Tag and Site Tag to an AP \(CLI\), on page 20](#)
- [AP Filter, on page 21](#)

## Information About New Configuration Model

The configuration of Cisco Embedded Wireless Controller on Catalyst Access Points is simplified using different tags, namely rf-tag, policy-tag, and site-tag. The access points would derive their configuration from the profiles that are contained within the tags.

Profiles are a collection of feature-specific attributes and parameters applied to tags. The rf-tag contains the radio profiles, the policy-tag contains the WLAN profile and policy profile, and the site-tag contains the flex profile and ap-join profile.

### Policy Tag

The policy tag constitutes mapping of the WLAN profile to the policy profile. The WLAN profile defines the wireless characteristics of the WLAN. The policy profile defines the network policies and the switching policies for the client (Quality of Service [QoS] is an exception which constitutes AP policies as well).

The policy tag contains the map of WLAN policy profile. There can be a maximum of 16 such entries per policy tag. Changes to the map entries are effected based on the status of the WLAN profile and policy profile. For example, if a map (WLAN1 and Policy1) is added to the policy tag, and both the WLAN profile and the policy profile are enabled, the definitions are pushed to the APs using the policy tag. However, if one of them

is in disabled state, the definition is not pushed to the AP. Similarly, if a WLAN profile is already being broadcast by an AP, it can be deleted using the no form of the command in the policy tag.

### Site Tag

The site tag defines the properties of a site and contains the flex profile and the AP join profile. The attributes that are specific to the corresponding flex or remote site are part of the flex profile. Apart from the flex profile, the site tag also comprises attributes that are specific to the physical site (and hence cannot be a part of the profile that is a reusable entity). For example, the list of primary APs for efficient upgrade is a part of a site tag rather than that of a flex profile.

If a flex profile name or an AP profile name is changed in the site tag, the AP is forced to rejoin the controller by disconnecting the Datagram Transport Layer Security (DTLS) session. When a site tag is created, the AP and flex profiles are set to default values (default-ap-profile and default-flex-profile).

### RF Tag

The RF tag contains the 2.4 GHz and 5 GHz RF profiles. The default RF tag contains the global configuration. Both these profiles contain the same default values for global RF profiles for the respective radios.

### Profiles

Profiles are a collection of feature-specific attributes and parameters applied to tags. Profiles are reusable entities that can be used across tags. Profiles (used by tags) define the properties of the APs or its associated clients.

### WLAN Profile

WLAN profiles are configured with same or different service set identifiers (SSIDs). An SSID identifies the specific wireless network for the controller to access. Creating WLANs with the same SSID allows to assign different Layer 2 security policies within the same wireless LAN.

To distinguish WLANs having the same SSID, create a unique profile name for each WLAN. WLANs with the same SSID must have unique Layer 2 security policies so that clients can select a WLAN based on the information advertised in the beacon and probe responses. The switching and network policies are not part of the WLAN definition.

### Policy Profile

Policy profile broadly consists of network and switching policies. Policy profile is a reusable entity across tags. Anything that is a policy for a client that is applied on an AP or controller is moved to the policy profile, for example, VLAN, ACL, QoS, session timeout, idle timeout, AVC profile, bonjour profile, local profiling, device classification, BSSID QoS, and so on. However, all the wireless-related security attributes and features on the WLAN are grouped under the WLAN profile.

### Flex Profile

Flex profile contains policy attributes and remote site-specific parameters. For example, the EAP profiles that can be used when the AP acts as an authentication server for local RADIUS server information, VLAN-ACL mapping, VLAN name-to-ID mapping, and so on.

### AP Join Profile

The default AP join profile values will have the global AP parameters and the AP group parameters. The AP join profile contains attributes that are specific to AP, such as CAPWAP, IPv4 and IPv6, UDP Lite, High Availability, Retransmit config parameters, Global AP failover, Hyperlocation config parameters, Telnet and SSH, 11u parameters, and so on.



---

**Note** Telnet is not supported for the following Cisco AP models: 1542D, 1542I, 1562D, 1562E, 1562I, 1562PS, 1800S, 1800T, 1810T, 1810W, 1815M, 1815STAR, 1815TSN, 1815T, 1815T, 1815W, 1832I, 1840I, 1852E, 1852I, 2802E, 2802I, 2802H, 3700C, 3800, 3802E, 3802I, 3802P, 4800, IW6300, ESW6300, 9105AXI, 9105AXW, 9115AXI, 9115AXE, 9117I, APVIRTUAL, 9120AXI, 9120AXE, 9130AXI, and 9130AXE.

---

### RF Profile

RF profile contains the common radio configuration for the APs. RF profiles are applied to all the APs that belong to an AP group, where all the APs in that group have the same profile settings.

### Association of APs

APs can be associated using different ways. The default option is by using Ethernet MAC address, where the MAC is associated with policy-tag, site tag, and RF tag.

In filter-based association, APs are mapped using regular expressions. A regular expression (regex) is a pattern to match against an input string. Any number of APs matching that regex will have policy-tag, site tag, and RF tag mapped to them, which is created as part of the AP filter.

In AP-based association, tag names are configured at the PnP server and the AP stores them and sends the tag name as part of discovery process.

In location-based association, tags are mapped as per location and are pushed to any AP Ethernet MAC address mapped to that location.

### Modifying AP Tags

Modifying an AP tag results in DTLS connection reset, forcing the AP to rejoin the controller. If only one tag is specified in the configuration, default tags are used for other types, for example, if only policy tag is specified, the default-site-tag and default-rf-tag will be used for site tag and RF tag.

## Configuring a Wireless Profile Policy (GUI)

### Procedure

---

- Step 1** Choose **Configuration** > **Tags & Profiles** > **Policy**.
- Step 2** On the **Policy Profile** page, click **Add**.
- Step 3** In the **Add Policy Profile** window, in **General** tab, enter a name and description for the policy profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces. Do not use spaces as it causes system instability.

**Step 4** To enable the policy profile, set **Status** as **Enabled**.

**Step 5** In the WLAN Switching Policy section, choose the following, as required:

- No Central Switching: Tunnels both the wireless user traffic and all control traffic via CAPWAP to the centralized controller where the user traffic is mapped to a dynamic interface/VLAN on the controller. This is the normal CAPWAP mode of operation.
- Central Authentication: Tunnels client data to the controller, as the controller handles client authentication.
- No Central DHCP: The DHCP packets received from AP are centrally switched to the controller and then forwarded to the corresponding VLAN based on the AP and the SSID.
- Central Association Enable: When central association is enabled, all switching is done on the controller.
- Flex NAT/PAT: Enables Network Address Translation(NAT) and Port Address Translation (PAT) mode.

**Step 6** Click **Save & Apply to Device**.

## Configuring a Wireless Profile Policy (CLI)

Follow the procedure given below to configure a wireless profile policy:



**Note** When a client moves from an old controller to a new controller (managed by Cisco Prime Infrastructure), the old IP address of the client is retained, if the IP address is learned by ARP or data gleaned. To avoid this scenario, ensure that you enable **ipv4 dhcp required** command in the policy profile. Otherwise, the IP address gets refreshed only after a period of 24 hours.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile policy <i>profile-policy</i></b>  <b>Example:</b> Device(config)# wireless profile policy rr-xyz-policy-1	Configures WLAN policy profile and enters wireless policy configuration mode.
<b>Step 3</b>	<b>idle-timeout <i>timeout</i></b>  <b>Example:</b> Device(config-wireless-policy)# idle-timeout 1000	(Optional) Configures the duration of idle timeout, in seconds.

	Command or Action	Purpose
<b>Step 4</b>	<b>vlan <i>vlan-id</i></b> <b>Example:</b> Device(config-wireless-policy)# vlan 24	Configures VLAN name or VLAN ID.
<b>Step 5</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wireless-policy)# no shutdown	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.
<b>Step 6</b>	<b>show wireless profile policy summary</b> <b>Example:</b> Device# show wireless profile policy summary	Displays the configured policy profiles. <b>Note</b> (Optional) To view detailed information about a policy profile, use the <b>show wireless profile policy detailed <i>policy-profile-name</i></b> command.

## Configuring a Flex Profile

Follow the procedure given below to set a flex profile:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile flex <i>flex-profile</i></b> <b>Example:</b> Device(config)# wireless profile flex rr-xyz-flex-profile	Configures a Flex profile and enters Flex profile configuration mode.
<b>Step 3</b>	<b>description</b> <b>Example:</b> Device(config-wireless-flex-profile)# description xyz-default-flex-profile	(Optional) Enables default parameters for the flex profile.
<b>Step 4</b>	<b>arp-caching</b> <b>Example:</b> Device(config-wireless-flex-profile)# arp-caching	(Optional) Enables ARP caching.
<b>Step 5</b>	<b>end</b> <b>Example:</b>	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	Device(config-wireless-flex-profile)# end	
<b>Step 6</b>	<b>show wireless profile flex summary</b>  <b>Example:</b> Device# show wireless profile flex summary	(Optional) Displays the flex-profile parameters.  <b>Note</b> To view detailed parameters about the flex profile, use the <b>show wireless profile flex detailed flex-profile-name</b> command.

## Configuring an AP Profile (GUI)

### Before you begin

The default AP join profile values will have the global AP parameters and the AP group parameters. The AP join profile contains attributes that are specific to AP, such as CAPWAP, IPv4/IPv6, UDP Lite, High Availability, retransmit configuration parameters, global AP failover, Hyperlocation configuration parameters, Telnet/SSH, 11u parameters, and so on.

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > AP Join**.
- Step 2** On the **AP Join Profile** page, click **Add**.  
The **Add AP Join Profile** page is displayed.
- Step 3** In the **General** tab, enter a name and description for the AP join profile.
- Step 4** Check the **LED State** check box to set the LED state of all APs connected to the device to blink so that the APs are easily located.
- Step 5** In the **Client** tab and **Statistics Timer** section, enter the time in seconds that the AP sends its 802.11 statistics to the controller.
- Step 6** In the **TCP MSS Configuration** section, check the **Adjust MSS Enable** check box to enter value for Adjust MSS. You can enter or update the maximum segment size (MSS) for transient packets that traverse a router. TCP MSS adjustment enables the configuration of the maximum segment size (MSS) for transient packets that traverse a router, specifically TCP segments with the SYN bit set.
- In a CAPWAP environment, a lightweight access point discovers a device by using CAPWAP discovery mechanisms, and then sends a CAPWAP join request to the device. The device sends a CAPWAP join response to the access point that allows the access point to join the device.
- When the access point joins the device, the device manages its configuration, firmware, control transactions, and data transactions.
- Step 7** In the **AP** tab, you can configure the following:
- General
    - a) In the **General** tab, check the **Switch Flag** check box to enable switches.



- b) Check the **Power Injector State** check box if power injector is being used. Power Injector increases wireless LAN deployment flexibility of APs by providing an alternative powering option to local power, inline power-capable multiport switches, and multiport power patch panels.
- c) From the **Power Injector Type** drop-down list, choose power injector type from the following options:
  - Installed: If you want the AP to examine and remember the MAC address of the currently connected switch port. (This selection assumes that a power injector is connected.)
  - Override: To enable the AP to operate in high-power mode without first verifying a matching MAC address.
- d) In the **Injector Switch MAC** field, enter the MAC address of the switch.
- e) From the **EAP Type** drop-down list, choose the EAP type as *EAP-FAST*, *EAP-TLS*, or *EAP-PEAP*.
- f) From the **AP Authorization Type** drop-down list, choose the type as either *CAPWAP DTLS +* or *CAPWAP DTLS*.
- g) In the **Client Statistics Reporting Interval** section, enter the interval for 5 GHz and 2.4 GHz radios in seconds.
- h) Check the **Enable** check box to enable extended module.
- i) From the **Profile Name** drop-down list, choose a profile name.
- j) Click **Save & Apply to Device**.
  - Hyperlocation: Cisco Hyperlocation is a location solution that allows to track the location of wireless clients with the accuracy of one meter. Selecting this option disables all other fields in the screen, except NTP Server.
- a) In the **Hyperlocation** tab, check the **Enable Hyperlocation** check box.
- b) Enter the **Detection Threshold** value to filter out packets with low RSSI. The valid range is –100 dBm to –50 dBm.
- c) Enter the **Trigger Threshold** value to set the number of scan cycles before sending a BAR to clients. The valid range is 0 to 99.
- d) Enter the **Reset Threshold** value to reset value in scan cycles after trigger. The valid range is 0 to 99.
- e) Enter the **NTP Server** IP address.
- f) Click **Save & Apply to Device**.
  - BLE: If your APs are Bluetooth Low Energy (BLE) enabled, they can transmit beacon messages that are packets of data or attributes transmitted over a low energy link. These BLE beacons are frequently used for health monitoring, proximity detection, asset tracking, and in-store navigation. For each AP, you can customize BLE Beacon settings configured globally for all APs.
- a) In the **BLE** tab, enter a value in the **Beacon Interval** field to indicate how often you want your APs to send out beacon advertisements to nearby devices. The range is from 1 to 10, with a default of 1.
- b) In the **Advertised Attenuation Level** field, enter the attenuation level. The range is from 40 to 100, with a default of 59.
- c) Click **Save & Apply to Device**.

**Step 8**

In the **Management** tab, you can configure the following:

- Device

- a) In the **Device** tab, enter the **IPv4/IPv6 Address** of the TFTP server, **TFTP Downgrade** section.
- b) In the **Image File Name** field, enter the name of the software image file.
- c) From the **Facility Value** drop-down list, choose the appropriate facility.

- d) Enter the IPv4 or IPv6 address of the host.
- e) Choose the appropriate **Log Trap Value**.
- f) Enable Telnet and/or SSH configuration, if required.
- g) Enable core dump, if required.
- h) Click **Save & Apply to Device**.

- User

- a) In the **User** tab, enter username and password details.
- b) Choose the appropriate password type.
- c) In the **Secret** field, enter a custom secret code.
- d) Choose the appropriate secret type.
- e) Choose the appropriate encryption type.
- f) Click **Save & Apply to Device**.

- Credentials

- a) In the **Credentials** tab, enter local username and password details.
- b) Choose the appropriate local password type.
- c) Enter 802.1x username and password details.
- d) Choose the appropriate 802.1x password type.
- e) Enter the time in seconds after which the session should expire.
- f) Enable local credentials and/or 802.1x credentials as required.
- g) Click **Save & Apply to Device**.
- a) In the **CDP Interface** tab, enable the CDP state, if required.
- b) Click **Save & Apply to Device**.

**Step 9** In the **Rogue AP** tab, check the **Rogue Detection** check box to enable rogue detection.

**Step 10** In the **Rogue Detection Minimum RSSI** field, enter the RSSI value.

This field specifies the minimum RSSI value for which a Rogue AP should be reported. All Rogue APs with RSSI lower than what is configured will not be reported to controller.

**Step 11** In the **Rogue Detection Transient Interval** field, enter the transient interval value.

This field indicates how long the Rogue AP should be seen before reporting the controller.

**Step 12** In the **Rogue Detection Report Interval** field, enter the report interval value.

This field indicates the frequency (in seconds) of Rogue reports sent from AP to controller.

**Step 13** Check the **Rogue Containment Automatic Rate Selection** check box to enable rogue containment automatic rate selection.

Here, the AP selects the best rate for the target Rogue, based on its RSSI.

**Step 14** Check the **Auto Containment on FlexConnect Standalone** check box to enable the feature.

Here, the AP will continue containment in case it moves to flexconnect standalone mode.

**Step 15** Click **Save & Apply to Device**.

---

## Configuring an AP Profile (CLI)

Follow the procedure given below to configure and AP profile:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ap profile <i>ap-profile</i></b> <b>Example:</b> Device(config)# ap profile xyz-ap-profile	Configures an AP profile and enters AP profile configuration mode. <b>Note</b> In an AP profile, the <b>EAP-FAST</b> is the default EAP type. <b>Note</b> When you delete a named profile, the APs associated with that profile will not revert to the default profile.
<b>Step 3</b>	<b>description <i>ap-profile-name</i></b> <b>Example:</b> Device(config-ap-profile)# description "xyz ap profile"	Adds a description for the ap profile.
<b>Step 4</b>	<b>cdp</b> <b>Example:</b> Device(config-ap-profile)# cdp	Enables CDP for all Cisco APs.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config-ap-profile)# end	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.
<b>Step 6</b>	<b>show ap profile name <i>profile-name</i> detailed</b> <b>Example:</b> Device# show ap profile name xyz-ap-profile detailed	(Optional) Displays detailed information about an AP join profile.

## Configuring an RF Profile (GUI)

### Procedure

**Step 1** Choose **Configuration > Tags & Profiles > RF**.

- Step 2** On the **RF Profile** page, click **Add**.
- Step 3** In the **General** tab, enter a name for the RF profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.
- Step 4** Choose the appropriate **Radio Band**.
- Step 5** To enable the profile, set the status as **Enable**.
- Step 6** Enter a **Description** for the RF profile.
- Step 7** Click **Save & Apply to Device**.

## Configuring an RF Profile (CLI)

Follow the procedure given below to configure an RF profile:

### Before you begin

Ensure that you use the same RF profile name that you create here, when configuring the wireless RF tag too. If there is a mismatch in the RF profile name (for example, if the RF tag contains an RF profile that does not exist), the corresponding radios will not come up.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ap dot11 24ghz rf-profile <i>rf-profile</i></b>  <b>Example:</b> Device(config)# ap dot11 24ghz rf-profile rfprof24_1	Configures an RF profile and enters RF profile configuration mode.  <b>Note</b> Use the <b>24ghz</b> command to configure the 802.11b parameters. Use the <b>5ghz</b> command to configure the 802.11a parameters.
<b>Step 3</b>	<b>default</b>  <b>Example:</b> Device(config-rf-profile)# default	(Optional) Enables default parameters for the RF profile.
<b>Step 4</b>	<b>no shutdown</b>  <b>Example:</b> Device(config-rf-profile)# no shutdown	Enables the RF profile on the device.
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Device(config-rf-profile)# end	Exits configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
<b>Step 6</b>	<b>show ap rf-profile summary</b> <b>Example:</b> Device# show ap rf-profile summary	(Optional) Displays the summary of the available RF profiles.
<b>Step 7</b>	<b>show ap rf-profile name <i>rf-profile</i> detail</b> <b>Example:</b> Device# show ap rf-profile name rfprof24_1 detail	(Optional) Displays detailed information about a particular RF profile.

## Configuring Policy Tag (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Tags > Policy**.
  - Step 2** Click **Add** to view the **Add Policy Tag** window.
  - Step 3** Enter a name and description for the policy tag. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.
  - Step 4** Click **Add** to map WLAN and policy.
  - Step 5** Choose the WLAN profile to map with the appropriate policy profile, and click the tick icon.
  - Step 6** Click **Save & Apply to Device**.
- 

## Configuring a Policy Tag (CLI)

Follow the procedure given below to configure a policy tag:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>wireless tag policy <i>policy-tag-name</i></b> <b>Example:</b>	Configures policy tag and enters policy tag configuration mode.

	Command or Action	Purpose
	<pre>Device(config-policy-tag)# wireless tag policy default-policy-tag</pre>	<p><b>Note</b> When performing LWA, the clients connected to a controller gets disconnected intermittently before session timeout.</p> <p>As a workaround it is recommended to include all policy profiles with central association or no central association under a given policy tag.</p>
<b>Step 4</b>	<p><b>description</b> <i>description</i></p> <p><b>Example:</b></p> <pre>Device(config-policy-tag)# description "default-policy-tag"</pre>	Adds a description to a policy tag.
<b>Step 5</b>	<p><b>remote-lan</b> <i>name</i> <b>policy</b> <i>profile-policy-name</i> {<b>ext-module</b>  <b>port-id</b> }</p> <p><b>Example:</b></p> <pre>Device(config-policy-tag)# remote-lan rr-xyz-rlan-aa policy rr-xyz-rlan-policy1 port-id 2</pre>	Maps a remote-LAN profile to a policy profile.
<b>Step 6</b>	<p><b>wlan</b> <i>wlan-name</i> <b>policy</b> <i>profile-policy-name</i></p> <p><b>Example:</b></p> <pre>Device(config-policy-tag)# wlan rr-xyz-wlan-aa policy rr-xyz-policy-1</pre>	Maps a policy profile to a WLAN profile.
<b>Step 7</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-policy-tag)# end</pre>	Exits policy tag configuration mode, and returns to privileged EXEC mode.
<b>Step 8</b>	<p><b>show wireless tag policy summary</b></p> <p><b>Example:</b></p> <pre>Device# show wireless tag policy summary</pre>	<p>(Optional) Displays the configured policy tags.</p> <p><b>Note</b> To view detailed information about a policy tag, use the <b>show wireless tag policy detailed</b> <i>policy-tag-name</i> command.</p>

## Configuring Wireless RF Tag (GUI)

### Procedure

- 
- Step 1** a) Choose **Configuration > Tags & Profiles > Tags > RF**.
- Step 2** Click **Add** to view the **Add RF Tag** window.

- Step 3** Enter a name and description for the RF tag. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.
- Step 4** Choose the required **5 GHz Band RF Profile** and **2.4 GHz Band RF Profile** to be associated with the RF tag.
- Step 5** Click **Update & Apply to Device**.

## Configuring Wireless RF Tag (CLI)

Follow the procedure given below to configure a wireless RF tag:

### Before you begin

- You can use only two profiles (2.4-GHz and 5-GHz band RF profiles) in an RF tag.
- Ensure that you use the same AP tag name that you created when configuring the AP tag task too.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless tag rf rf-tag</b> <b>Example:</b> Device(config)# wireless tag rf rftag1	Creates an RF tag and enters wireless RF tag configuration mode.
<b>Step 3</b>	<b>24ghz-rf-policy rf-policy</b> <b>Example:</b> Device(config-wireless-rf-tag)# 24ghz-rf-policy rfprof24_1	Attaches an IEEE 802.11b RF policy to the RF tag.  To configure a dot11a policy, use the <b>5ghz-rf-policy</b> command.
<b>Step 4</b>	<b>description policy-description</b> <b>Example:</b> Device(config-wireless-rf-tag)# description Test	Adds a description for the RF tag.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config-wireless-rf-tag)# end	Exits configuration mode and returns to privileged EXEC mode.
<b>Step 6</b>	<b>show wireless tag rf summary</b> <b>Example:</b> Device# show wireless tag rf summary	Displays the available RF tags.

	Command or Action	Purpose
<b>Step 7</b>	<b>show wireless tag rf detailed</b> <i>rf-tag</i> <b>Example:</b> Device# show wireless tag rf detailed rftag1	Displays detailed information of a particular RF tag.

## Attaching a Policy Tag and Site Tag to an AP (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Wireless > Access Points**.
- The **All Access Points** section displays details of all the APs on your network.
- Step 2** To edit the configuration details of an AP, select the row for that AP.
- The **Edit AP** window is displayed.
- Step 3** In the **General** tab and **Tags** section, specify the appropriate policy, site, and RF tags, that you created on the **Configuration > Tags & Profiles > Tags** page.
- Step 4** Click **Update & Apply to Device**.
- 

## Attaching Policy Tag and Site Tag to an AP (CLI)

Follow the procedure given below to attach a policy tag and a site tag to an AP:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ap</b> <i>mac-address</i> <b>Example:</b> Device(config)# ap F866.F267.7DFB	Configures a Cisco AP and enters AP profile configuration mode. <b>Note</b> The <i>mac-address</i> should be a wired mac address.
<b>Step 3</b>	<b>policy-tag</b> <i>policy-tag-name</i> <b>Example:</b> Device(config-ap-tag)# policy-tag rr-xyz-policy-tag	Maps a policy tag to the AP.



	Command or Action	Purpose
<b>Step 4</b>	<b>site-tag</b> <i>site-tag-name</i> <b>Example:</b> Device(config-ap-tag)# site-tag rr-xyz-site	Maps a site tag to the AP.
<b>Step 5</b>	<b>rf-tag</b> <i>rf-tag-name</i> <b>Example:</b>	Associates the RF tag.
<b>Step 6</b>	<b>end</b> <b>Example:</b> Device(config-ap-tag)# end	Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.
<b>Step 7</b>	<b>show ap tag summary</b> <b>Example:</b> Device# show ap tag summary	(Optional) Displays AP details and the tags associated to it.
<b>Step 8</b>	<b>show ap name</b> <i>&lt;ap-name&gt;</i> <b>tag info</b> <b>Example:</b> Device# show ap name <i>ap-name</i> tag info	(Optional) Displays the AP name with tag information.
<b>Step 9</b>	<b>show ap name</b> <i>&lt;ap-name&gt;</i> <b>tag detail</b> <b>Example:</b> Device# show ap name <i>ap-name</i> tag detail	(Optional) Displays the AP name with tag details.

## AP Filter

### Introduction to AP Filter

The introduction of tags in the new configuration model in the Cisco Embedded Wireless Controller on Catalyst Access Points has created multiple sources for tags to be associated with access points (APs). Tag sources can be static configuration, AP filter engine, per-AP PNP, or default tag sources. In addition to this, the precedence of the tags also plays an important role. The AP filter feature addresses these challenges in a seamless and intuitive manner.

AP filters are similar to the access control lists (ACLs) used in the controller and are applied at the global level. You can add AP names as filters, and other attributes can be added as required. Add the filter criteria as part of the discovery requests.

The AP Filter feature organizes tag sources with the right priority, based on the configuration.

You cannot disable the AP filter feature. However, the relative priority of a tag source can be configured using **ap filter-priority** *priority filter-name* command.



**Note** You can configure tag names at the PnP server (similar to the Flex group and AP group) and the AP stores and send the tag name as part of discovery and join requests.

## Set Tag Priority (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Tags > AP > Tag Source**.
- Step 2** Drag and Drop the Tag Sources to change priorities.
- 

## Set Tag Priority

Multiple tag sources might result in ambiguity for network administrators. To address this, you can define priority for tags. When an AP joins the controller, the tags are picked based on priority. If precedence is not set, the defaults are used.

Use the following procedure to set tag priority:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters the global configuration mode.
<b>Step 2</b>	<b>ap tag-source-priority source-priority source {filter   pnp}</b>  <b>Example:</b> Device(config)# ap tag-source-priority 2 source pnp	Configures AP tag source priority.  <b>Note</b> It is not mandatory to configure AP filter. It comes with default priorities for Static, Filter, and PnP.
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Device(config)# end	Exits configuration mode and returns to privileged EXEC mode.
<b>Step 4</b>	<b>ap tag-sources revalidate</b>  <b>Example:</b> Device# ap tag-sources revalidate	Revalidates AP tag sources. The priorities become active only after this command is run.  <b>Note</b> If you change the priorities for Filter and PnP, and want to evaluate them, run the <b>revalidate</b> command.

## Create an AP Filter (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Tags > AP > Filter**.
- Step 2** Click **Add**.
- Step 3** In the **Associate Tags to AP** dialog box which is displayed, enter the **Rule Name**, the **AP name regex** and the **Priority**. Optionally, you can also choose the policy tag from the **Policy Tag Name** drop-down list, the site tag from the **Site Tag Name** drop-down list and the RF tag from the **RF Tag Name** drop-down list.
- Step 4** Click **Apply to Device**.
- 

## Create an AP Filter (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters the global configuration mode.
<b>Step 2</b>	<b>ap filter name</b> <i>filter_name</i>  <b>Example:</b> Device(config)# ap filter filter-1	Configures an AP filter.
<b>Step 3</b>	<b>ap name-regex</b> <i>regular-expression</i>  <b>Example:</b> Device(config-ap-filter)# ap name-regex testany	Configures the AP filter based on regular expression.  For example, if you have named an AP as <b>ap-1ab-12</b> , then you can configure the filter with a regular expression, such as <b>ap-1ab-\d+</b> , to match the AP name.
<b>Step 4</b>	<b>tag policy</b> <i>policy-tag</i>  <b>Example:</b> Device(config-ap-filter)# tag policy pol-tag1	Configures a policy tag for this filter.
<b>Step 5</b>	<b>tag rf</b> <i>rf-tag</i>  <b>Example:</b> Device(config-ap-filter)# tag rf rf-tag1	Configures an RF tag for this filter.
<b>Step 6</b>	<b>tag site</b> <i>site-tag</i>  <b>Example:</b> Device(config-ap-filter)# tag site sitel	Configures a site tag for this filter.

	Command or Action	Purpose
<b>Step 7</b>	<b>end</b> <b>Example:</b> Device(config-ap-filter)# end	Exits configuration mode and returns to privileged EXEC mode.

## Set Up and Update Filter Priority (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Tags > AP > Filter**.
- Step 2**
- If you want to setup a new AP filter, then click **Add**. In the **Associate Tags to AP** dialog box which is displayed, enter the **Rule Name**, the **AP name regex** and the **Priority**. Optionally, you can also select the **Policy Tag Name**, the **Site Tag Name** and the **RF Tag Name**. Click **Apply to Device**.
  - If you want to update the priority of an existing AP filter, click on the Filter and in the **Edit Tags** dialog box and change the **Priority**. In case the Filter is Inactive, no priority can be set to it. Click **Update and Apply to Device**.
- 

## Set Up and Update Filter Priority

Follow the procedure given below to set and update filter priority:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ap filter priority <i>priority</i> filter-name</b> <i>filter-name</i> <b>Example:</b> Device(config)# ap filter priority 10 filter-name test1	Configure AP filter priority. <b>Note</b> A filter without a priority is not active. Similarly, you cannot set a filter priority without a filter.
<b>Step 3</b>	<b>end</b> <b>Example:</b> Device(config-ap)# end	Exits configuration mode and returns to privileged EXEC mode.

## Verify AP Filter Configuration

The following **show** commands are used to display tag sources and filters, and their priorities.

To view the tag source priorities, use the following command:

```
Device# show ap tag sources
```

```
Priority Tag source
-----
0 Static
1 Filter
2 AP
3 Default
```

To view the available filters, use the following command:

```
Device# show ap filter all
```

Filter Name Tag	regex	Policy Tag	RF Tag	Site
first	abcd	pol-tag1	rf-tag1	
site-tag1				
test1	testany			site1
filter1	testany			

To view the list of active filters, use the following command:

```
Device# show ap filters active
```

Priority Site Tag	Filter Name	regex	Policy Tag	RF Tag
10	test1	testany		
site1				

To view the source of an AP tag, use the following command:

```
Device# show ap tag summary
```

```
Number of APs: 4
```

AP Name	AP Mac	Site Tag Name	Policy Tag Name	RF Tag Name	Misconfigured Tag Source
AP002A.1034.CA78	002a.1034.ca78	named-site-tag	named-policy-tag	named-rf-tag	No Filter
AP00A2.891C.2480	00a2.891c.2480	named-site-tag	named-policy-tag	named-rf-tag	No Filter
AP58AC.78DE.9946	58ac.78de.9946	default-site-tag	default-policy-tag	default-rf-tag	No AP
AP0081.C4F4.1F34	0081.c4f4.1f34	default-site-tag	default-policy-tag	default-rf-tag	No Default





## CHAPTER 3

# Smart Licensing

---

- Information About Cisco Smart Licensing, on page 27
- Creating a Smart Account, on page 29
- Using Smart Licensing, on page 30
- Using Specified License Reservation (SLR), on page 30
- Enabling Specified License Reservation in CSSM, on page 31
- Enabling Smart Software Licensing, on page 32
- Registering for Smart License (Connected Mode), on page 33
- Enabling Smart License Reservation, on page 33
- Enabling Smart Call Home Reporting, on page 34
- Configuring AIR License Level (GUI), on page 35
- Configuring AIR License Level (CLI), on page 35
- Configuring AIR Network Essentials License Level, on page 36
- Configuring AIR Network Advantage License Level, on page 36
- Verifying Smart Licensing Configurations, on page 37

## Information About Cisco Smart Licensing

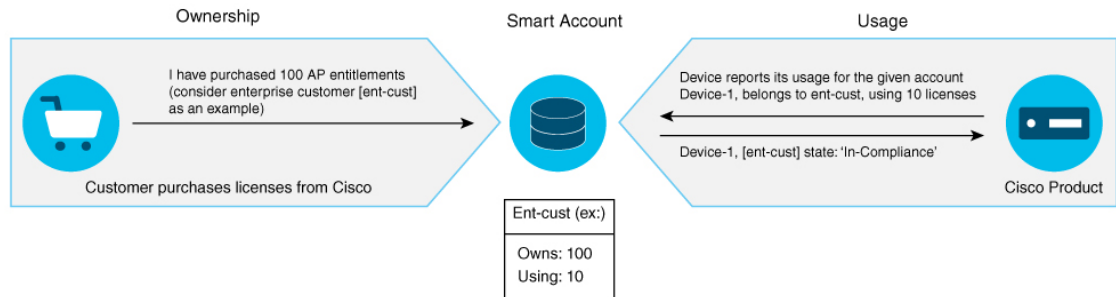
Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure – you control what users can access. With Smart Licensing you get:

- **Easy Activation:** Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- **Unified Management:** My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- **License Flexibility:** Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central ([software.cisco.com](https://software.cisco.com)).

For a more detailed overview on Cisco Licensing, go to [cisco.com/go/licensingguide](https://cisco.com/go/licensingguide).

Figure 2: Relationship Between Ownership, Smart Account, and Usage



**Note** As a prerequisite, register your controller with the satellite SSM (VM on customer premises) or CSSM (Cisco Cloud) using the Smart Call Home HTTPS server.

Once your product is registered in CSSM, you will be able to view the license usage using your Smart Account or Virtual Account for every eight hours.



- Note**
- Smart Licensing registration is lost when the device switches from controller to autonomous mode and back. In such instances, you should re-register the controller to CSSM to restore licenses authorization.
  - After adding new license in the Cisco Smart Software Manager (CSSM) for customer virtual account, run the **license smart renew auth** command on the controller to get the license status changed from Out OF Compliance to Authorised.

Access points support the following AIR licensing levels:

- AIR Network Essential (AIR-NE)
- AIR Network Advantage (AIR-NA)
- AIR DNA Essential (AIR-DNA-E)
- AIR DNA Advantage (AIR-DNA-A)



**Note** The *AIR-DNA-A* and *AIR-DNA-E* are the available license levels on the controller.

The *AIR-DNA-A* is the default mode.

You can configure as *AIR-DNA-A* or *AIR-DNA-E* 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.

### Smart Licensing Reservation Types

License reservation is a mechanism to reserve node locked licenses and install them on the controller.



The following are the license reservation types:

- Permanent License Reservation (PLR)—All licenses are reserved.
- Specified License Reservation (SLR)—Only specific licenses are reserved. Supports term licenses.

The controller supports four different entitlement registration or reporting on Smart Licensing or service reservation. Every connecting AP requires a Cisco DNA Center License to leverage the unique value properties of the controller.



---

**Note** The controller boots up with *AIR-DNA-A* as the default. Any change in the license level requires a reboot.

---

### Entitlement Reporting

Entitlement reporting is nothing but reporting the number of access points on the controller to the Cisco Smart Software Manager (CSSM).

The entitlement reporting is based on the configured AIR license level on the controller.



---

**Note** Two types of entitlement reporting occurs when you are in *AIR-DNA-E* and *AIR-DNA-A* levels. For instance, if your controller reports 100 APs as count, your entitlement reporting displays *100 AIR-NE* and *100 AIR-DNA-E*. Similarly, it also displays *100 AIR-NA* and *100 AIR-DNA-A* to CSSM.

---

## Creating a Smart Account

### Procedure

---

**Step 1** Navigate to the Cisco Software Central web page:

<https://software.cisco.com/#>

The Cisco Software Central page is displayed.

**Step 2** From the **Important News** pop-up window, click **Get a Smart Account**.

(Or)

From the **Administration** area, click **Request a Smart Account**.

Follow the process to create a Smart Account.

**Note** You need to have a Smart Account to use Smart Licensing.

---

# Using Smart Licensing

## Before you begin

Follow the procedure given below to cover the high-level steps on how to use smart licensing:

## Procedure

---

- Step 1** Configure your device for smart licensing.
- Step 2** Login to CSSM customer **Smart Account** > **Virtual Account** to generate a token.
- Step 3** Execute the following command on your device:

```
Device# license smart register idtoken <token-id>
```

**Note** You can get the *token-id* from the CSSM web portal.

**Note** You can use the **license smart register idtoken *token-id* force** command to register the device again even if the same device was registered with CSSM earlier.

---

# Using Specified License Reservation (SLR)

## Procedure

---

- Step 1** **configure terminal**

**Example:**

```
Device# configure terminal
```

Enters global configuration mode.

- Step 2** **license smart reservation**

**Example:**

```
Device(config)# license smart reservation
```

Enables specified license reservation mode on the controller.

- Step 3** **license smart reservation request local**

**Example:**

```
Device(config)# license smart reservation request local
```

Generates a request code.

**Note** Enter this request code in the Cisco Smart Software Manager portal:

```
CB-ZL-AIR-9500C-K9:9J4FVHMBXCO-BjSeUVwmn-D8
```

**Step 4**     **end**

**Example:**

```
Device(config)# end
```

Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

---

## Enabling Specified License Reservation in CSSM

### Before you begin

You should have a smart account and virtual account to generate the authorization code for the controller.

### Procedure

---

**Step 1**     Login to CSSM.

**Step 2**     De-register the smart license, if the controller is reporting to a satellite server.

```
Device(config)# license smart deregister
```

**Step 3**     Enable Specified License Reservation in the controller.

```
Device(config)# license smart reservation
```

**Step 4**     Verify the license reservation status on your controller using the following command:

```
Device# show license reservation
```

```
License reservation: ENABLED
```

```
Overall status:
```

```
  Active: PID:C9800-CL-K9,SN:9PQFKND9ZR8
           Reservation status: NOT INSTALLED
           Export-Controlled Functionality: NOT ALLOWED
  Standby: PID:C9800-CL-K9,SN:9UD8BBTHL1S
           Reservation status: NOT INSTALLED
           Export-Controlled Functionality: NOT ALLOWED
```

**Step 5**     Generate *request code* on your controller using the following command:

```
Device(config)# license smart reservation request all
```

```
Request code for active : CG-ZC9800-CL-K9:9PQFKND9ZR8-BjSeUVwmn-8E
Request code for standby : CG-ZC9800-CL-K9:9PQFKND9ZR8-BjSeUVwmn-8E
```

Option *all* will generate the request code for both active and stand-by, if the controller is in HA pair.

Option *local* will generate the request code for active or standalone controller.

**Step 6**     Generate *authorization code*, using the *request code*, for each controller separately in CSSM and install both the codes in the controller. You can install the *authorization code* of standby controller through active controller.

a) Go to CSSM and navigate to your Smart Account and Virtual Account:

<https://software.cisco.com/software/cs/ws/platform/home#SmartLicensing-Inventory>

- b) Click **Licenses** tab.
- c) Click **License Reservation** button and enter the request code obtained from the previous step in to the **Reservation Request Code** field.
- d) Click **Next**.
- e) In the **Select Licenses** tab, select the **Reserve a specific license** radio button and enter the number of licenses required to reserve in the **Reserve** text box.
- f) Click **Next**.
- g) In the **Review and Confirm** tab, check the quantity and license type, and click **Generate Authorization Code** button.
- h) From the **Authorization Code** tab, select **Download as File** option to download the **authorization code**.

**Note** Repeat **Step b** to **Step h** to generate *authorization code* for the standby controller.

**Step 7** Upload the *authorization code* file to the controller bootflash: directory.

```
Device# copy ftp://<ip-address>authorization-code.txt bootflash:
Destination filename [authorization-code.txt]
```

**Step 8** Install the *authorization code* file in the controller using the following command.

```
Device# license smart reservation install file authorization-code.txt
```

**Note** Use the same command to install the *authorization code* for stand-by controller also using active controller in case of HA.

**Step 9** Verify the license summary after installing the *authorization code* on your controller using the following command:

```
Device# show license summary
```

## Enabling Smart Software Licensing

### Procedure

**Step 1** Navigate to the Cisco Software Central web page using the following link:

<https://software.cisco.com/#>

The Cisco Software Central page is displayed.

**Step 2** From the **License** tab, click **Smart Software Licensing**.

The Smart Software Licensing page is displayed.

**Step 3** Click the **Inventory** tab to view **Virtual Account: Accounting** page details.

**Step 4** Click **New Token** to register the product instances to this virtual account.

The Create Registration Token page is displayed.

**Step 5** In the **Description** field, enter a description for the ID token.

**Step 6** Check the **Allow export-controlled functionality on the products registered with this token** checkbox to enable export-controlled functionality.

**Step 7** Click **Create Token**.

**Note** Licenses cannot be purchased with the wireless controller. All licenses can be purchased with access points.

## Registering for Smart License (Connected Mode)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	Copy the token generated in <i>Enabling Smart Software Licensing</i> .	
<b>Step 2</b>	On Catalyst ME, use this token to register to Smart License.	
<b>Step 3</b>	<b>license smart register idtoken</b> <i>token</i>  <b>Example:</b> Device(config)# <b>license smart register idtoken</b> <i>CB-ZL-AIR-9500C-K9:9J4FVHMBXCO-BjSeUVwmn-D8</i>	Registers for Smart License using the token number.
<b>Step 4</b>	<b>license smart register idtoken</b> <i>token</i> [ <b>force</b> ]  <b>Example:</b> Device(config)# <b>license smart register</b> <i>CB-ZL-AIR-9500C-K9:9J4FVHMBXCO-BjSeUVwmn-D8</i> <b>force</b>	Enables registering for Smart License with force if normal registering does not take place.
<b>Step 5</b>	<b>license smart deregister</b>  <b>Example:</b> Device(config)# <b>license smart deregister</b>	De-registers the smart license.

## Enabling Smart License Reservation

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>license smart reservation</b>	Enables Smart License Reservation on ME. Request code is generated.

	Command or Action	Purpose
<b>Step 2</b>	Navigate to the Cisco Software Central web page using the following link:	<a href="https://software.cisco.com/#">https://software.cisco.com/#</a> The Cisco Software Central page is displayed.
<b>Step 3</b>	From the <b>License</b> tab, click <b>Smart Software Licensing</b> .	The Smart Software Licensing page is displayed.
<b>Step 4</b>	Click the <b>Inventory</b> tab and then click <b>Licenses &gt; License Reservation</b> .	Follow steps 1-4 to <b>Enter Request Code, Select Licenses, Review and Confirm</b> , and to generate an <b>Authorization Code</b> .
<b>Step 5</b>	After generating the Authorization Code, Click <b>Download as File</b> option to save to <code>AuthorizationCode.txt</code> .	The Authorization Code is saved as a text file.
<b>Step 6</b>	On Catalyast ME, copy the authorization file to flash ( <code>/bootflash/AutorizationCode.txt</code> ).	
<b>Step 7</b>	<b>license smart reservation install file <i>filename</i></b> <b>Example:</b> <pre>Device(config)# license smart reservation install file <i>AuthorizationCode.txt</i></pre>	Installs the reserved licenses using the Authorization Code file..
<b>Step 8</b>	<b>license smart reservation return</b>	Returns the reserved licenses.
<b>Step 9</b>	<b>no license smart reservation</b>	Exits from the SLR mode.

## Enabling Smart Call Home Reporting

### Procedure

**Step 1** **configure terminal**

**Example:**

```
Device# configure terminal
```

Enters global configuration mode.

**Step 2** **call-home reporting contact-email-addr *email-address* http-proxy *proxy-server* *port-number***

**Example:**

```
Device(config)# call-home reporting contact-email-addr sample@cisco.com http-proxy 120.20.2.2
5
```

Enables Call Home reporting.

- *port-number*—The valid range is from 1 to 65535.

**Step 3** **end**

**Example:**

```
Device(config)# end
```

Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

For more information on Smart Call Home, see:

[https://www.cisco.com/c/en/us/td/docs/switches/lan/smart\\_call\\_home/book/SCH31\\_Ch3.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/smart_call_home/book/SCH31_Ch3.html)

## Configuring AIR License Level (GUI)

### Procedure

- Step 1** Choose **Administration > Licensing**.
- Step 2** Click **Change Wireless License Level**. The **Change Wireless License Level** dialog box is displayed.
- Step 3** Select the License Level using the drop-downs.
- Step 4** After changing the **New Level** values, click **Save & Reload** (Or) **Save without Reload**. Alternatively, you can click **Reload** to reload the device. During this time, you will lose network connectivity to the device. If you wish to continue, click **Yes**.
- Step 5** Click refresh icon to refresh the device.

## Configuring AIR License Level (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>license air level {air-network-advantage   air-network-essentials}</b>  <b>Example:</b> Device(config)# license air level air-network-advantage  Device(config)# license air level air-network-essentials	Configures AIR license level. <ul style="list-style-type: none"> <li>• air-network-advantage—Is the AIR network advantage license level.</li> <li>• air-network-essentials—Is the AIR network essential license level.</li> </ul>
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Device(config)# end	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring AIR Network Essentials License Level

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>license air level network-essentials addon air-dna-essentials</b>  <b>Example:</b> Device(config)# <code>license air level network-essentials addon air-dna-essentials</code>	Configures AIR network essentials license level.
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Device(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring AIR Network Advantage License Level

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>license air level air-network-advantage addon air-dna-advantage</b>  <b>Example:</b> Device(config)# <code>license air level air-network-advantage addon air-dna-advantage</code>	Configures AIR network advantage license level.
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Device(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.



# Verifying Smart Licensing Configurations

To verify the smart licensing status and license usage, use the following command:

```
Device# show license all
Smart Licensing Status

=====
Smart Licensing is ENABLED
Registration:
  Status: REGISTERED
  Smart Account: BU Production Test
  Virtual Account: MEWLC-DE
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Nov 19 15:36:51 2018 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: May 18 15:36:50 2019 UTC
  Registration Expires: Nov 19 15:31:24 2019 UTC

License Authorization:
  Status: AUTHORIZED on Nov 20 07:46:48 2018 UTC
  Last Communication Attempt: SUCCEEDED on Nov 20 07:46:48 2018 UTC
  Next Communication Attempt: Dec 20 07:46:48 2018 UTC
  Communication Deadline: Feb 18 07:40:49 2019 UTC

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: Callhome

License Usage
=====
AP Perpetual Networkstack Essentials (DNA_NWSTACK_E):
  Description: AP Perpetual Network Stack entitled with DNA-E
  Count: 2
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED

Product Information
=====
UDI: PID:AIR-AP1900I-B-K9,SN:9ICMGRNU4U0

Agent Version
=====
Smart Agent for Licensing: 4.6.0_rel/2
Component Versions: SA:(1_3_dev)1.0.15, SI:(dev22)1.2.1, CH:(rel5)1.0.3, PK:(dev18)1.0.3

Reservation Info
```

```
=====
```

```
License reservation: DISABLED
```

To verify the smart licensing status, use the following command:

```
Device# show license status  
Smart Licensing is ENABLED
```

```
Utility:  
Status: DISABLED  
Data Privacy:  
Sending Hostname: yes  
Callhome hostname privacy: DISABLED  
Smart Licensing hostname privacy: DISABLED  
    Version privacy: DISABLED
```

```
Transport:  
Type: Callhome
```

```
Registration:  
Status: REGISTERED  
Smart Account: BU Production Test  
Virtual Account: MEWLC-DE  
    Export-Controlled Functionality: Allowed
```

```
Initial Registration: SUCCEEDED on Nov 19 15:36:51 2018 UTC  
Last Renewal Attempt: None  
Next Renewal Attempt: May 18 15:36:51 2019 UTC  
Registration Expires: Nov 19 15:31:25 2019 UTC
```

```
License Authorization:  
Status: AUTHORIZED on Nov 19 16:23:42 2018 UTC  
Last Communication Attempt: SUCCEEDED on Nov 19 16:23:42 2018 UTC  
Next Communication Attempt: Dec 19 16:23:42 2018 UTC  
Communication Deadline: Feb 17 16:18:17 2019 UTC
```

```
Export Authorization Key:  
Features Authorized:  
<none>
```

To verify the air license level and smart licensing status, use the following command:

```
Device# show version  
AIR License Level: AIR DNA Advantage  
Next reload AIR license Level: AIR DNA Advantage  
Smart Licensing Status: REGISTERED/AUTHORIZED  
    cisco AIR-AP1900I-B-K9 (VXE) processor (revision VXE) with 322620K bytes of memory.
```



## CHAPTER 4

# Conversion and Migration

---

- [Conversion and Migration in Embedded Wireless Controller Capable APs](#) , on page 39
- [Types of Conversion](#), on page 39
- [Access Point Conversion](#), on page 40
- [Network Conversion](#), on page 43
- [SKU Conversion Scenarios](#), on page 45
- [Converting AireOS Mobility Express Network to Embedded Wireless Controller Network](#) , on page 46

## Conversion and Migration in Embedded Wireless Controller Capable APs

The Cisco Embedded Wireless Controller on Catalyst Access Points is not supported on any non-802.11ax (non-11ax) based access points (AP). It is only supported on 802.11ax (11ax) based APs. The embedded wireless controller is the only supported form of Cisco Mobility Express on 11ax based APs.

The conversion enables you to convert the 11ax APs running CAPWAP to embedded wireless controller and vice-versa.

## Types of Conversion

The types of conversion scenarios supported are:

- AP Conversion – The following AP conversions are supported:
  - Converting a CAPWAP AP to Embedded Wireless Controller - This conversion is required when you have an AP with a CAPWAP image, and you want to use the AP to deploy a embedded wireless controller based network. In order to do this, you must convert the CAPWAP AP to a embedded wireless controller.
  - Converting an Embedded Wireless Controller AP to a CAPWAP AP – This conversion is required if you want to migrate the APs from an embedded wireless controller network to a non-embedded wireless controller network; or if you do not want the APs to participate in the primary AP election process.
- Network Conversion

- SKU Conversion

## Access Point Conversion

This section gives the details of converting a CAPWAP access point to an embedded wireless controller.

### Converting a CAPWAP AP to an Embedded Wireless Controller Capable AP



**Note** Before converting from CAPWAP to embedded wireless controller (EWC), ensure that you upgrade the corresponding AP with the CAPWAP image in Cisco AireOS Release 8.10.105.0. If this upgrade is not performed, the conversion will fail.

To convert an 802.11ax AP with a CAPWAP image to an embedded wireless controller capable image, either download the controller image based on the automated image download process, use the conversion command, or convert through the WebUI.



**Note** When the AP is embedded wireless controller capable, the AP can participate in the primary AP election process. Only if the AP is elected as a primary, can it perform the controller functionality.

### Converting an Embedded Wireless Controller Capable AP to a CAPWAP AP

To convert an 802.11ax AP from the embedded wireless controller network to a non-embedded wireless controller network, set the AP type to CAPWAP using the conversion command or the WebUI, respectively, and then plug it on to the controller network so that it joins the controller. If the image on the controller is different from the image on the AP, a new CAPWAP image is requested from the controller.

### Converting a Single AP to CAPWAP or Embedded Wireless Controller Capable AP (CLI)

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> >enable	Enters privileged EXEC mode.
<b>Step 2</b>	<b>wireless ewc ap ap-type ap-name</b> { capwap   ewc }  <b>Example:</b>	Changes the AP to CAPWAP type or to the embedded controller type.

	Command or Action	Purpose
	Device#wireless ewc-ap ap ap-type ap-name capwap	

**Example**

```
wireless ewc-ap ap ap-type ap-name {capwap | ewc}
```

## AP Conversion Deployment Scenarios

1. Standalone 802.11ax CAPWAP AP to start an embedded wireless controller network:

802.11ax AP	Embedded Wireless Controller Capable APs	Use-Case	Automatic Conversion
Standalone 802.11ax CAPWAP AP	Network does not exist.	To use a the standalone 802.11ax CAPWAP AP as the first AP for setting up the embedded wireless controller network.	Automatic conversion is not possible. You must download both the controller and the AP image using the supported image transfer protocols with AP command:  <pre>ap-type {capwap   ewc-ap} [&lt;sftp/tftp&gt;://&lt;server ip&gt;/&lt;AP imagepath&gt; &lt;sftp/tftp&gt;://&lt;server ip&gt; Controller ImagePath]</pre>

2. Non-802.11ax CAPWAP AP joining an existing embedded wireless controller network:

CAPWAP AP	Embedded Wireless Controller Capable APs	Use-Case	Automatic Conversion
CAPWAP AP - Neither AireOS-Mobility Express capable, or, embedded wireless controller capable AP, or, AireOS-Mobility Express capable Wave 2 APs.	Existing network	To bring in a CAPWAP AP which is not embedded wireless controller capable, into an existing embedded wireless controller network, to add one more AP to the existing network.	Yes, automatic conversion is possible. This is automatically taken care through the AP Join image download process.

3. 802.11ax AP joining an existing embedded wireless controller network:

Embedded Wireless Controller Capable AP	Embedded Wireless Controller Network	Use-Case	Automatic Conversion
802.11ax AireOS-CAPWAP AP or 802.11ax Catalyst CAPWAP AP or 802.11ax embedded wireless controller capable AP	Existing network	To bring in an 802.11ax AP from an AireOS-CAPWAP network, or a CAPWAP network, or, from another embedded wireless controller network into an existing embedded wireless controller network, to add one more AP to the existing network.	<p>Yes, automatic conversion takes place.</p> <p>This is automatically taken care through the AP Join image download process.</p> <p>If the AP type is explicitly set to CAPWAP, then the AP continues to act as a CAPWAP AP unless it is converted back again to embedded wireless controller AP using the AP command, Controller command, or the WebUI.</p> <p>The following command is used for conversion as well as AP image download:</p> <pre>ap-type {capwap   ewc-ap} [&lt;sftp/tftp&gt;://&lt;server ip&gt;/&lt;AP imagepath&gt; &lt;sftp/tftp&gt;://&lt;server ip&gt;Controller ImagePath&gt;]</pre> <p>The following command is used to convert a specific AP to CAPWAP or embedded wireless controller:</p> <pre>wireless ewc-ap ap ap-type   ap-name {capwap   ewc-ap}</pre>

4. 802.11ax embedded wireless controller AP joining an AireOS CAPWAP network or a CAPWAP network:

802.11 AX Embedded Wireless Controller Capable AP	Embedded Wireless Controller Network	Use-Case	Automatic Conversion
802.11ax AP which was earlier an embedded wireless controller AP	Existing network	To bring an existing 802.11ax embedded wireless controller AP and add it to the CAPWAP network or the AireOS-CAPWAP network to add one more AP to the existing network.	<p>It is recommended to convert the AP to CAPWAP type before bringing it to the CAPWAP network. This conversion can be done manually by using the AP command, the Controller command, Controller WebUI, or by using the DHCP option.</p> <p>After conversion, the normal image download process should be followed.</p> <pre> ap-type {capwap   ewc-ap} [&lt;sftp/tftp&gt;://&lt;server ip&gt;/&lt;AP imagepath&gt; &lt;sftp/tftp&gt;://&lt;server ip&gt;Controller ImagePath]  wireless ewc-ap ap ap-type   ap-name {capwap   ewc-ap} </pre>

## Network Conversion

This section describes network conversion through the conversion command and the network conversion deployment scenarios.

### Converting the Network (CLI)

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> >enable	Enters privileged EXEC mode.

	Command or Action	Purpose
<b>Step 2</b>	<b>Wireless ewc-ap ap capwap</b> <i>primary-controller-name</i> {A:B:C:D   X:X:X:X::X}  <b>Example:</b> Device#wireless ewc-ap ap capwap wlc-name 10.0.0.0	Specifies the wireless controller name and IP address to which all the APs currently connected to the embedded wireless controller network should join.

## Network Conversion Deployment Scenarios

1. Converting an existing centralized CAPWAP network or AireOS CAPWAP network to the embedded wireless controller network

Existing Network	Embedded Wireless Controller Network	Use-Case	Automatic Conversion
CAPWAP Network: Centralized CAPWAP network or AireOS-CAPWAP network with at least one 802.11ax AP.	Network does not exist.	To convert the existing centralized CAPWAP network or the AireOS-CAPWAP network to the embedded wireless controller network.	<p>No, automatic conversion does not take place.</p> <p>You need to pick one 802.11ax AP to download both the controller and AP image using the supported image transfer protocols with the AP command.</p> <pre>ap-type {capwap   ewc-ap} &lt;sftp/tftp&gt;://&lt;server ip&gt;/&lt;AP imagepath&gt; &lt;sftp/tftp&gt;://&lt;server ip&gt; Controller ImagePath&gt;]</pre>

2. Converting an existing embedded wireless controller network to an AireOS CAPWAP network or to a centralized CAPWAP network



Existing Network	Embedded Wireless Controller Network	Use-Case	Automatic Conversion
Embedded wireless controller network with many APs.	Existing network	To convert the existing embedded wireless controller network to an AireOS-CAPWAP network or to a centralized CAPWAP network.	<p>No automatic conversion.</p> <p>You must convert all the APs or one AP at a time using the controller command to specify the IP address of the controller to which the AP has to join.</p> <p>You can also use the WebUI to convert the selected APs or all the APs by specifying the IP address of the controller to which the AP has to join.</p>

## SKU Conversion Scenarios

### 1. 802.11ax Embedded Wireless Controller SKU instead of CAPWAP SKU

SKU	Network	Use-Case	Automatic Conversion
802.11ax embedded wireless controller SKU instead of CAPWAP SKU	Network does not exist.	For an order placed for 802.11ax embedded wireless controller SKU instead of CAPWAP SKU, it should be converted to CAPWAP SKU.	<p>No automatic conversion available.</p> <p>You can use <b>DHCP option 43</b> to point to the Catalyst 9800 controller so that the APs join the Catalyst 9800 controller as a CAPWAP AP.</p>

SKU	Network	Use-Case	Automatic Conversion
2. 802.11ax CAPWAP SKU instead of the embedded wireless controller SKU.	Network does not exist.	For an order placed for the 802.11ax CAPWAP SKU instead of the embedded wireless controller SKU and now would like to convert it to embedded wireless controller SKU.	No automatic conversion available.  You should pick one 802.11ax AP to download both the controller and AP image using the supported image transfer protocols with AP command.ap-type ewc-ap <sftp/tftp>://<server ip>/<AP imagepath> <sftp/tftp>://<server ip> Controller ImagePath>

## Converting AireOS Mobility Express Network to Embedded Wireless Controller Network

### Procedure

- 
- Step 1** Remove the **Next Preferred Master** configuration from the existing AireOS Mobility Express network and save the configuration.
  - Step 2** Power down all the APs in the AireOS Mobility Express network including the primary AP.
  - Step 3** Power-on the 11 AX AP with the embedded wireless controller SKU so that it launches the controller.
  - Step 4** Provision the 11 AX AP with the required configuration (if the box is in Day-0, provision the mandatory configuration to get to Day-1).
  - Step 5** Copy, Translate, and Apply all the AireOS Mobility Express configurations to the 11 AX embedded wireless controller AP, add image download configuration.
  - Step 6** Power-on all the APs in the AireOS Mobility Express network. All the APs from the earlier AireOS Mobility Express network will join as regular APs in the embedded wireless controller network.
-



## CHAPTER 5

# Best Practices

---

- [Introduction, on page 47](#)

## Introduction

This chapter covers the best practices recommended for configuring a typical Cisco Catalyst 9800 Series wireless infrastructure. The objective is to provide common settings that you can apply to most wireless network implementations. However, not all networks are the same. Therefore, some of the tips might not be applicable to your installation. Always verify them before you perform any changes on a live network.

For more information, see [Cisco Catalyst 9800 Series Configuration Best Practices](#) guide.





## PART II

# Lightweight Access Points

- [Country Codes, on page 51](#)
- [AP Priority, on page 55](#)
- [Rogue per AP, on page 57](#)
- [802.11 Parameters for Cisco Access Points, on page 65](#)
- [802.1x Support, on page 79](#)
- [Information About NAT Support, on page 87](#)





## CHAPTER 6

# Country Codes

- [Information About Country Codes](#), on page 51
- [Prerequisites for Configuring Country Codes](#), on page 51
- [Configuring Country Codes \(GUI\)](#), on page 52
- [How to Configure Country Codes](#), on page 52
- [Configuration Examples for Configuring Country Codes](#), on page 54

## Information About Country Codes

Controllers and access points are designed for use in many countries with varying regulatory requirements. The radios within the access points are assigned to a specific regulatory domain at the factory (such as -E for Europe), but the country code enables you to specify a particular country of operation within that regulatory domain (such as FR for France or ES for Spain). Configuring a country code ensures that each radio's broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations.

### Information About Japanese Country Codes

Country codes define the channels that can be used legally in each country. These country codes are available for Japan:

- JP: Allows only -J radios to join the controller
- J2: Allows only -P radios to join the controller
- J3: Uses the -U frequencies, but allows -U, -P, and -Q radios to join the controller
- J4: Allows 2.4G JPQU and 5G PQU to join the controller.

See the [Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points](#) document for the list of channels and power levels supported by access points in the Japanese regulatory domains.

## Prerequisites for Configuring Country Codes

- Generally, you should configure one country code per device; you configure one code that matches the physical location of the device and its access points. You can configure up to 20 country codes per device. This multiple-country support enables you to manage access points in various countries from a single device.

- When the multiple-country feature is used, all the devices that are going to join the same RF group must be configured with the same set of countries, configured in the same order.
- Access points are capable of using all the available legal frequencies. However, access points are assigned to the frequencies that are supported in their relevant domains.
- The country list configured on the RF group leader determines which channels the members will operate on. This list is independent of which countries have been configured on the RF group members.
- For devices in the Japan regulatory domain, you must have at least one access point with a -J regulatory domain joined to your device.
- You cannot delete any country code using the configuration command **wireless country country-code** if the specified country was configured using the **ap country list** command and vice-versa.

## Configuring Country Codes (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Wireless > Access Points > Country**.
- Step 2** On the **Country** page, select the check box for each country where your access points are installed. If you selected more than one check box, a message is displayed indicating that RRM channels and power levels are limited to common channels and power levels.
- Step 3** Click **Apply**.
- 

## How to Configure Country Codes

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device# enable	Enters privileged EXEC mode.
<b>Step 2</b>	<b>show wireless country supported</b>  <b>Example:</b> Device# show wireless country supported	Displays a list of all the available country codes.
<b>Step 3</b>	<b>configure terminal</b>  <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.



	Command or Action	Purpose
<b>Step 4</b>	<b>ap dot11 24ghz shutdown</b> <b>Example:</b> Device(config)# ap dot11 24ghz shutdown	Disables the 802.11b/g network.
<b>Step 5</b>	<b>ap dot11 5ghz shutdown</b> <b>Example:</b> Device(config)# ap dot11 5ghz shutdown	Disables the 802.11a network.
<b>Step 6</b>	<b>ap country <i>country_code</i></b> <b>Example:</b> Device(config)# ap country IN	
<b>Step 7</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.
<b>Step 8</b>	<b>show wireless country channels</b> <b>Example:</b> Device# show wireless country channels	Displays the list of available channels for the country codes configured on your device. <b>Note</b> Perform Steps 9 through 17 only if you have configured multiple country codes in Step 6.
<b>Step 9</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 10</b>	<b>no ap dot11 5ghz shutdown</b> <b>Example:</b> Device(config)# no ap dot11 5ghz shutdown	Enables the 802.11a network.
<b>Step 11</b>	<b>no ap dot11 24ghz shutdown</b> <b>Example:</b> Device(config)# no ap dot11 24ghz shutdown	Enables the 802.11b/g network.
<b>Step 12</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.
<b>Step 13</b>	<b>ap name <i>cisco-ap</i> shutdown</b> <b>Example:</b> Device# ap name AP02 shutdown	Disables the access point. <b>Note</b> Ensure that you disable only the access point for which you are configuring country codes.

	Command or Action	Purpose
<b>Step 14</b>	<b>ap name <i>cisco-ap</i> no shutdown</b>  <b>Example:</b> Device# ap name AP02 no shutdown	Enables the access point.

# Configuration Examples for Configuring Country Codes

## Viewing Channel List for Country Codes

These examples show how to display the list of available channels for the country codes on your device:

Device# **show wireless country channels**

```
Configured Country.....: US - United States
KEY: * = Channel is legal in this country and may be configured manually.
     A = Channel is the Auto-RF default in this country.
     . = Channel is not legal in this country.
     C = Channel has been configured for use by Auto-RF.
     x = Channel is available to be configured for use by Auto-RF.
     (-,-) = (indoor, outdoor) regulatory domain 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
-----:+++++-----
(-A ,-AB ) US : A * * * * A * * * * A . . .
Auto-RF       : . . . . .
-----:+++++-----
802.11a      :          1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels      : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
               4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
-----:+++++-----
(-A ,-AB ) US : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
Auto-RF       : . . . . .
-----:+++++-----
4.9GHz 802.11a :
Channels      :          1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
               1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
-----:+++++-----
US (-A ,-AB ) : * * * * * * * * * * * * * * * * A * * * * * A
Auto-RF       : . . . . .
```

Device# **show wireless country configured**

```
Configured Country..... US - United States
Configured Country Codes
US - United States 802.11a Indoor,Outdoor/ 802.11b Indoor,Outdoor/ 802.11g Indoor,Outdoor
```



## CHAPTER 7

# AP Priority

---

- [Failover Priority for Access Points, on page 55](#)
- [Setting AP Priority \(GUI\), on page 55](#)
- [Setting AP Priority, on page 56](#)

## Failover Priority for Access Points

Each controller has a defined number of communication ports for access points. When multiple controllers with unused access point ports are deployed on the same network and one controller fails, the dropped access points automatically poll for unused controller ports and associate with them.

The following are some guidelines for configuring failover priority for access points:

- You can configure your wireless network so that the backup controller recognizes a join request from a higher-priority access point, and if necessary, disassociates a lower-priority access point as a means to provide an available port.
- Failover priority is not in effect during the regular operation of your wireless network. It takes effect only if there are more associations requests to controller than the available AP capacity on the controller.
- AP priority is checked while connecting to the controller when the controller is in full scale or the primary controller fails, the APs fallback to the secondary controller.
- You can enable failover priority on your network and assign priorities to the individual access points.
- By default, all access points are set to priority level 1, which is the lowest priority level. Therefore, you need to assign a priority level only to those access points that warrant a higher priority.

## Setting AP Priority (GUI)

### Procedure

---

- Step 1** Choose **Configuration > Wireless > Access Points**.
- Step 2** Click the Access Point.
- Step 3** In the **Edit AP** dialog box, go to **High Availability** tab.

- Step 4** Choose the priority from the **AP failover priority** drop-down list.
- Step 5** Click **Update and Apply to Device**.

## Setting AP Priority



**Note** Priority of access points ranges from 1 to 4, with 4 being the highest.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>ap name</b> <i>ap-name</i> <b>priority</b> <i>priority</i> <b>Example:</b> Device# ap name AP44d3.ca52.48b5 priority 1	Specifies the priority of an access point.
<b>Step 2</b>	<b>show ap config general</b> <b>Example:</b> Device# show ap config general	Displays common information for all access points.
<b>Step 3</b>	<b>show ap name</b> <i>ap-name</i> <b>config general</b> <b>Example:</b> Device# show ap name AP44d3.ca52.48b5 config general	Displays the configuration of a particular access point.



## CHAPTER 8

# Rogue per AP

---

- [Rogue per AP, on page 57](#)
- [Enabling Rogue Detection, on page 58](#)

## Rogue per AP

Rogue detection is configured per AP or for a group of APs. The rogue AP detection is configured under the AP profile. The rogue AP detection configuration is enabled by default and is part of the default AP profile.

The following commands are deprecated from this release:

- **wireless wps rogue detection enable**
- **wireless wps rogue detection report-interval** *interval*
- **wireless wps rogue detection min-rssi** *rssi*
- **wireless wps rogue detection min-transient-time** *transtime*
- **wireless wps rogue detection containment flex-connect**
- **wireless wps rogue detection containment auto-rate**

### Enabling Rogue Detection

The following are the high-level steps to enable rogue detection:

- Configure an AP Profile
- Define a Wireless Site Tag and Assign the AP Profile
- Associate the Wireless Site Tag to an AP



---

**Note** The controller may not report the original min-rssi value due to conversions made by the AP and the controller. Hence, the reported min-rssi may be different from the original value.

---

# Enabling Rogue Detection

## Configuring an AP Profile (GUI)

### Before you begin

The default AP join profile values will have the global AP parameters and the AP group parameters. The AP join profile contains attributes that are specific to AP, such as CAPWAP, IPv4/IPv6, UDP Lite, High Availability, retransmit configuration parameters, global AP failover, Hyperlocation configuration parameters, Telnet/SSH, 11u parameters, and so on.

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > AP Join**.
- Step 2** On the **AP Join Profile** page, click **Add**.  
The **Add AP Join Profile** page is displayed.
- Step 3** In the **General** tab, enter a name and description for the AP join profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.
- Step 4** Check the **LED State** check box to set the LED state of all APs connected to the device to blink so that the APs are easily located.
- Step 5** In the **Client** tab and **Statistics Timer** section, enter the time in seconds that the AP sends its 802.11 statistics to the controller.
- Step 6** In the **TCP MSS Configuration** section, check the **Adjust MSS Enable** check box to enter value for Adjust MSS. You can enter or update the maximum segment size (MSS) for transient packets that traverse a router. TCP MSS adjustment enables the configuration of the maximum segment size (MSS) for transient packets that traverse a router, specifically TCP segments with the SYN bit set.
- In a CAPWAP environment, a lightweight access point discovers a device by using CAPWAP discovery mechanisms, and then sends a CAPWAP join request to the device. The device sends a CAPWAP join response to the access point that allows the access point to join the device.
- When the access point joins the device, the device manages its configuration, firmware, control transactions, and data transactions.
- Step 7** In the **AP** tab, you can configure the following:
- General
    - a) In the **General** tab, check the **Switch Flag** check box to enable switches.
    - b) Check the **Power Injector State** check box if power injector is being used. Power Injector increases wireless LAN deployment flexibility of APs by providing an alternative powering option to local power, inline power-capable multiport switches, and multiport power patch panels.  
  
Power Injector Selection parameter enables you to protect your switch port from an accidental overload if the power injector is inadvertently bypassed.
    - c) From the **Power Injector Type** drop-down list, choose power injector type from the following options:

- **Installed**—This option examines and remembers the MAC address of the currently connected switch port and assumes that a power injector is connected. Choose this option if your network contains older Cisco 6-Watt switches and you want to avoid possible overloads by forcing a double-check of any relocated access points.

If you want to configure the switch MAC address, enter the MAC address in the **Injector Switch MAC Address** text box. If you want the access point to find the switch MAC address, leave the **Injector Switch MAC Address** text box blank.

**Note** Each time an access point is relocated, the MAC address of the new switch port fails to match the remembered MAC address, and the access point remains in low-power mode. You must then physically verify the existence of a power injector and reselect this option to cause the new MAC address to be remembered.

- **Override**—This option allows the access point to operate in high-power mode without first verifying a matching MAC address. You can use this option if your network does not contain any older Cisco 6-W switches that could be overloaded if connected directly to a 12-W access point. The advantage of this option is that if you relocate the access point, it continues to operate in high-power mode without any further configuration. The disadvantage of this option is that if the access point is connected directly to a 6-W switch, an overload occurs.

- In the **Injector Switch MAC** field, enter the MAC address of the switch.
  - From the **EAP Type** drop-down list, choose the EAP type as *EAP-FAST*, *EAP-TLS*, or *EAP-PEAP*.
  - From the **AP Authorization Type** drop-down list, choose the type as either *CAPWAP DTLS +* or *CAPWAP DTLS*.
  - In the **Client Statistics Reporting Interval** section, enter the interval for 5 GHz and 2.4 GHz radios in seconds.
  - Check the **Enable** check box to enable extended module.
  - From the **Profile Name** drop-down list, choose a profile name.
  - Click **Save & Apply to Device**.
- **Hyperlocation**: Cisco Hyperlocation is a location solution that allows to track the location of wireless clients with the accuracy of one meter. Selecting this option disables all other fields in the screen, except NTP Server.
    - In the **Hyperlocation** tab, check the **Enable Hyperlocation** check box.
    - Enter the **Detection Threshold** value to filter out packets with low RSSI. The valid range is –100 dBm to –50 dBm.
    - Enter the **Trigger Threshold** value to set the number of scan cycles before sending a BAR to clients. The valid range is 0 to 99.
    - Enter the **Reset Threshold** value to reset value in scan cycles after trigger. The valid range is 0 to 99.
    - Enter the **NTP Server** IP address.
    - Click **Save & Apply to Device**.
  - **BLE**: If your APs are Bluetooth Low Energy (BLE) enabled, they can transmit beacon messages that are packets of data or attributes transmitted over a low energy link. These BLE beacons are frequently used for health monitoring, proximity detection, asset tracking, and in-store navigation. For each AP, you can customize BLE Beacon settings configured globally for all APs.
    - In the **BLE** tab, enter a value in the **Beacon Interval** field to indicate how often you want your APs to send out beacon advertisements to nearby devices. The range is from 1 to 10, with a default of 1.

- b) In the **Advertised Attenuation Level** field, enter the attenuation level. The range is from 40 to 100, with a default of 59.
- c) Click **Save & Apply to Device**.
  - **Packet Capture:** Packet Capture feature allows to capture the packets on the AP for the wireless client troubleshooting. The packet capture operation is performed on the AP by the radio drivers on the current channel on which it is operational, based on the specified packet capture filter.
- a) In the **Packet Capture** tab, choose an **AP Packet Capture Profile** from the drop-down list.
- b) You can also create a new profile by clicking the + sign.
- c) Enter a name and description for the AP packet capture profile.
- d) Enter the **Buffer Size**.
- e) Enter the **Duration**.
- f) Enter the **Truncate Length** information.
- g) In the **Server IP** field, enter the IP address of the TFTP server.
- h) In the **File Path** field, enter the directory path.
- i) Enter the username and password details.
- j) From the **Password Type** drop-down list, choose the type.
- k) In the **Packet Classifiers** section, use the option to select or enter the packets to be captured.
- l) Click **Save**.
- m) Click **Save & Apply to Device**.

**Step 8**

In the **Management** tab, you can configure the following:

- **Device**

- a) In the **Device** tab, enter the **IPv4/IPv6 Address** of the TFTP server, **TFTP Downgrade** section.
- b) In the **Image File Name** field, enter the name of the software image file.
- c) From the **Facility Value** drop-down list, choose the appropriate facility.
- d) Enter the IPv4 or IPv6 address of the host.
- e) Choose the appropriate **Log Trap Value**.
- f) Enable Telnet and/or SSH configuration, if required.
- g) Enable core dump, if required.
- h) Click **Save & Apply to Device**.

- **User**

- a) In the **User** tab, enter username and password details.
- b) Choose the appropriate password type.
- c) In the **Secret** field, enter a custom secret code.
- d) Choose the appropriate secret type.
- e) Choose the appropriate encryption type.
- f) Click **Save & Apply to Device**.

- **Credentials**

- a) In the **Credentials** tab, enter local username and password details.
- b) Choose the appropriate local password type.
- c) Enter 802.1x username and password details.
- d) Choose the appropriate 802.1x password type.



- e) Enter the time in seconds after which the session should expire.
- f) Enable local credentials and/or 802.1x credentials as required.
- g) Click **Save & Apply to Device**.
- a) In the **CDP Interface** tab, enable the CDP state, if required.
- b) Click **Save & Apply to Device**.

**Step 9** In the **Rogue AP** tab, check the **Rogue Detection** check box to enable rogue detection.

**Step 10** In the **Rogue Detection Minimum RSSI** field, enter the RSSI value.

This field specifies the minimum RSSI value for which a Rogue AP should be reported. All Rogue APs with RSSI lower than what is configured will not be reported to controller.

**Step 11** In the **Rogue Detection Transient Interval** field, enter the transient interval value.

This field indicates how long the Rogue AP should be seen before reporting the controller.

**Step 12** In the **Rogue Detection Report Interval** field, enter the report interval value.

This field indicates the frequency (in seconds) of Rogue reports sent from AP to controller.

**Step 13** Check the **Rogue Containment Automatic Rate Selection** check box to enable rogue containment automatic rate selection.

Here, the AP selects the best rate for the target Rogue, based on its RSSI.

**Step 14** Check the **Auto Containment on FlexConnect Standalone** check box to enable the feature.

Here, the AP will continue containment in case it moves to flexconnect standalone mode.

**Step 15** Click **Save & Apply to Device**.

## Configure an AP Profile

Follow the procedure given below to configure an AP profile:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters the global configuration mode.
<b>Step 2</b>	<b>ap profile <i>ap-profile</i></b> <b>Example:</b> Device(config)# ap profile xyz-ap-profile	Configures an AP profile and enters the ap profile configuration mode.
<b>Step 3</b>	<b>description <i>ap-profile-name</i></b> <b>Example:</b> Device(config-ap-profile)# description "xyz ap profile"	Adds a description for the ap profile.

	Command or Action	Purpose
<b>Step 4</b>	<b>rogue detection enable</b> <b>Example:</b> Device(config-ap-profile)# rogue detection enable	Enables rogue detection for individual access points.  Rogue detection is enabled by default. Use this command if rogue detection is disabled.
<b>Step 5</b>	<b>rogue detection report-interval interval</b> <b>Example:</b> Device(config-ap-profile)# rogue detection report-interval 12	Specifies the time interval, in seconds, at which APs should send the rogue detection report to the embedded controller.  The default value for <i>interval</i> is 10.
<b>Step 6</b>	<b>rogue detection min-rssi rssi</b> <b>Example:</b> Device(config-ap-profile)# rogue detection min-rssi -128	Specifies the minimum RSSI value that rogues should have for APs to detect them.  The minimum RSSI value is -128.
<b>Step 7</b>	<b>rogue detection min-transient-time transtime</b> <b>Example:</b> Device(config-ap-profile)# rogue detection min-transient-time 120	Specifies the time interval at which rogues have to be consistently scanned for by APs after the first time the rogues are scanned.  The lowest value for minimum transient time is 0.
<b>Step 8</b>	<b>rogue detection containment flex-connect</b> <b>Example:</b> Device(config-ap-profile)# rogue detection containment flex-connect	Sets the auto containment options for standalone FlexConnect access points.  By default, this option is disabled.
<b>Step 9</b>	<b>rogue detection containment auto-rate</b> <b>Example:</b> Device(config-ap-profile)# rogue detection containment auto-rate	Sets the auto rate for containment of rogues.  By default, auto-rate is disabled.

## Define a Wireless Site Tag and Assign an AP Profile (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Tags**.
  - Step 2** On the **Tags** page, click the **Site** tab and click **Add**.
  - Step 3** In the **Add Site Tag** window, enter the name in the **name** field.
  - Step 4** Choose the AP profile from the **AP Join Profile** drop-down list.
  - Step 5** Click **Save & Apply to Device**.
-

## Define a Wireless Site Tag and Assign an AP Profile (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters the global configuration mode.
<b>Step 2</b>	<b>wireless tag site</b> <i>site-tag</i> <b>Example:</b> Device(config)# wireless tag site default-site-tag	Enters the wireless site tag configuration mode.
<b>Step 3</b>	<b>ap-profile</b> <i>ap-profile</i> <b>Example:</b> Device(config-site-tag)# ap-profile xyz-ap-profile	Assigns an AP profile to the wireless site.
<b>Step 4</b>	<b>exit</b> <b>Example:</b> Device(config-site-tag)# exit	Returns to the global configuration mode.

## Associating Wireless Tag to an AP (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Tags**.
- Step 2** Click **AP** tab to configure the following:
- Tag Source
  - Static
  - Filter
- Step 3** In the **Static** tab, click **Add** to perform the following:
- a) Enter a MAC address.
  - b) Choose the appropriate **Policy Tag Name**, **Site Tag Name**, and **RF Tag Name**.
  - c) Click **Save & Apply to Device**.
- Step 4** In the **Filter** tab, click **Add** to perform the following:
- a) Enter a rule and AP name.
  - b) Use the slider to enable **Active**.
  - c) Enter the priority. The valid range is from 0 to 127.
  - d) Choose the appropriate **Policy Tag Name**, **Site Tag Name**, and **RF Tag Name**.

- e) Click **Save & Apply to Device**.

## Associate Wireless Tag to an AP (CLI)

Follow the procedure given below to apply the rogue configuration defined under ap profile to the AP.



**Note** If the AP is not explicitly associated to a non-default site tag, it will be associated to default-site-tag and resultantly the default-ap-profile rogue configuration will be used.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters the global configuration mode.
<b>Step 2</b>	<b>ap mac-address</b> <b>Example:</b> Device(config)# ap F866.F267.7DFB	Configures Cisco APs and enters the ap configuration mode.
<b>Step 3</b>	<b>site-tag site-tag-name</b> <b>Example:</b> Device(config-ap-tag)# site-tag sitetag1	Maps a wireless site tag to the AP.



## CHAPTER 9

# 802.11 Parameters for Cisco Access Points

- [2.4-GHz Radio Support, on page 65](#)
- [5-GHz Radio Support, on page 67](#)
- [Information About Dual-Band Radio Support , on page 69](#)
- [Configuring Default XOR Radio Support, on page 70](#)
- [Configuring XOR Radio Support for the Specified Slot Number \(GUI\), on page 72](#)
- [Configuring XOR Radio Support for the Specified Slot Number, on page 72](#)
- [Receiver Only Dual-Band Radio Support, on page 74](#)
- [Configuring Client Steering \(CLI\), on page 76](#)
- [Verifying Cisco Access Points with Dual-Band Radios, on page 77](#)

## 2.4-GHz Radio Support

### Configuring 2.4-GHz Radio Support for the Specified Slot Number

#### Before you begin



**Note** The term *802.11b radio* or *2.4-GHz radio* will be used interchangeably.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device# enable	Enters privileged EXEC mode.
<b>Step 2</b>	<b>ap name <i>ap-name</i> dot11 24ghz slot 0 SI</b>  <b>Example:</b> Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 SI	Enables Spectrum Intelligence (SI) for the dedicated 2.4-GHz radio hosted on slot 0 for a specific access point. For more information, see the <i>Spectrum Intelligence</i> section in this guide.

	Command or Action	Purpose
		Here, <b>0</b> refers to the Slot ID.
<b>Step 3</b>	<p><b>ap name</b> <i>ap-name</i> <b>dot11 24ghz slot 0 antenna</b> {<b>ext-ant-gain</b> <i>antenna_gain_value</i>   <b>selection</b> [<b>internal</b>   <b>external</b>]}</p> <p><b>Example:</b></p> <pre>Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 antenna selection internal</pre>	<p>Configures 802.11b antenna hosted on slot 0 for a specific access point.</p> <ul style="list-style-type: none"> <li>• <b>ext-ant-gain:</b> Configures the 802.11b external antenna gain. <i>antenna_gain_value</i>- Refers to the external antenna gain value in multiples of .5 dBi units. The valid range is from 0 to 4294967295.</li> <li>• <b>selection:</b> Configures the 802.11b antenna selection (internal or external).</li> </ul>
<b>Step 4</b>	<p><b>ap name</b> <i>ap-name</i> <b>dot11 24ghz slot 0 beamforming</b></p> <p><b>Example:</b></p> <pre>Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 beamforming</pre>	Configures beamforming for the 2.4-GHz radio hosted on slot 0 for a specific access point.
<b>Step 5</b>	<p><b>ap name</b> <i>ap-name</i> <b>dot11 24ghz slot 0 channel</b> {<i>channel_number</i>   <b>auto</b>}</p> <p><b>Example:</b></p> <pre>Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 channel auto</pre>	Configures advanced 802.11 channel assignment parameters for the 2.4-GHz radio hosted on slot 0 for a specific access point.
<b>Step 6</b>	<p><b>ap name</b> <i>ap-name</i> <b>dot11 24ghz slot 0 cleanair</b></p> <p><b>Example:</b></p> <pre>Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 cleanair</pre>	Enables CleanAir for 802.11b radio hosted on slot 0 for a specific access point.
<b>Step 7</b>	<p><b>ap name</b> <i>ap-name</i> <b>dot11 24ghz slot 0 dot11n antenna</b> {<b>A</b>   <b>B</b>   <b>C</b>   <b>D</b>}</p> <p><b>Example:</b></p> <pre>Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 dot11n antenna A</pre>	<p>Configures 802.11n antenna for 2.4-GHz radio hosted on slot 0 for a specific access point.</p> <p>Here,</p> <p><b>A:</b> Is the antenna port A. <b>B:</b> Is the antenna port B. <b>C:</b> Is the antenna port C. <b>D:</b> Is the antenna port D.</p>
<b>Step 8</b>	<p><b>ap name</b> <i>ap-name</i> <b>dot11 24ghz slot 0 shutdown</b></p> <p><b>Example:</b></p> <pre>Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 shutdown</pre>	Disables 802.11b radio hosted on slot 0 for a specific access point.

	Command or Action	Purpose
<b>Step 9</b>	<b>ap name</b> <i>ap-name</i> <b>dot11 24ghz slot 0 txpower</b> <i>{tx_power_level   auto}</i>  <b>Example:</b> Device# <b>ap name AP-SIDD-A06 dot11 24ghz slot 0 txpower auto</b>	Configures transmit power level for 802.11b radio hosted on slot 0 for a specific access point. <ul style="list-style-type: none"> <li>• <i>tx_power_level</i>: Is the transmit power level in dBm. The valid range is from 1 to 8.</li> <li>• <b>auto</b>: Enables auto-RF.</li> </ul>

## 5-GHz Radio Support

### Configuring 5-GHz Radio Support for the Specified Slot Number

#### Before you begin



**Note** The term *802.11a radio* or *5-GHz radio* will be used interchangeably in this document.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device# <b>enable</b>	Enters privileged EXEC mode.
<b>Step 2</b>	<b>ap name</b> <i>ap-name</i> <b>dot11 5ghz slot 1 SI</b>  <b>Example:</b> Device# <b>ap name AP-SIDD-A06 dot11 5ghz slot 1 SI</b>	Enables Spectrum Intelligence (SI) for the dedicated 5-GHz radio hosted on slot 1 for a specific access point.  Here, <b>1</b> refers to the Slot ID.
<b>Step 3</b>	<b>ap name</b> <i>ap-name</i> <b>dot11 5ghz slot 1 antenna</b> <b>ext-ant-gain</b> <i>antenna_gain_value</i>  <b>Example:</b> Device# <b>ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna ext-ant-gain</b>	Configures external antenna gain for 802.11a radios for a specific access point hosted on slot 1.  <i>antenna_gain_value</i> —Refers to the external antenna gain value in multiples of .5 dBi units. The valid range is from 0 to 4294967295.
<b>Step 4</b>	<b>ap name</b> <i>ap-name</i> <b>dot11 5ghz slot 1 antenna</b> <b>mode</b> [ <b>omni</b>   <b>sectorA</b>   <b>sectorB</b> ]  <b>Example:</b> Device# <b>ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna mode sectorA</b>	Configures the antenna mode for 802.11a radios for a specific access point hosted on slot 1.

	Command or Action	Purpose
<b>Step 5</b>	<b>ap name <i>ap-name</i> dot11 5ghz slot 1 antenna selection [internal   external]</b>  <b>Example:</b> Device# <b>ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna selection internal</b>	Configures the antenna selection for 802.11a radios for a specific access point hosted on slot 1.
<b>Step 6</b>	<b>ap name <i>ap-name</i> dot11 5ghz slot 1 beamforming</b>  <b>Example:</b> Device# <b>ap name AP-SIDD-A06 dot11 5ghz slot 1 beamforming</b>	Configures beamforming for the 5-GHz radio hosted on slot 1 for a specific access point.
<b>Step 7</b>	<b>ap name <i>ap-name</i> dot11 5ghz slot 1 channel {<i>channel_number</i>   auto   width [20   40   80   160]}</b>  <b>Example:</b> Device# <b>ap name AP-SIDD-A06 dot11 5ghz slot 1 channel auto</b>	Configures advanced 802.11 channel assignment parameters for the 5-GHz radio hosted on slot 1 for a specific access point.  Here, <i>channel_number</i> - Refers to the channel number. The valid range is from 1 to 173.
<b>Step 8</b>	<b>ap name <i>ap-name</i> dot11 5ghz slot 1 cleanair</b>  <b>Example:</b> Device# <b>ap name AP-SIDD-A06 dot11 5ghz slot 1 cleanair</b>	Enables CleanAir for 802.11a radio hosted on slot 1 for a given or specific access point.
<b>Step 9</b>	<b>ap name <i>ap-name</i> dot11 5ghz slot 1 dot11n antenna {<b>A</b>   <b>B</b>   <b>C</b>   <b>D</b>}</b>  <b>Example:</b> Device# <b>ap name AP-SIDD-A06 dot11 5ghz slot 1 dot11n antenna A</b>	Configures 802.11n for 5-GHz radio hosted on slot 1 for a specific access point.  Here, <b>A</b> - Is the antenna port A. <b>B</b> - Is the antenna port B. <b>C</b> - Is the antenna port C. <b>D</b> - Is the antenna port D.
<b>Step 10</b>	<b>ap name <i>ap-name</i> dot11 5ghz slot 1 rrm channel <i>channel</i></b>  <b>Example:</b> Device# <b>ap name AP-SIDD-A06 dot11 5ghz slot 1 rrm channel 2</b>	Is another way of changing the channel hosted on slot 1 for a specific access point.  Here, <i>channel</i> - Refers to the new channel created using 802.11h channel announcement. The valid range is from 1 to 173, provided 173 is a valid channel in the country where the access point is deployed.
<b>Step 11</b>	<b>ap name <i>ap-name</i> dot11 5ghz slot 1 shutdown</b>  <b>Example:</b>	Disables 802.11a radio hosted on slot 1 for a specific access point.



	Command or Action	Purpose
	Device# <b>ap name AP-SIDD-A06 dot11 5ghz slot 1 shutdown</b>	
<b>Step 12</b>	<b>ap name <i>ap-name</i> dot11 5ghz slot 1 txpower {<i>tx_power_level</i>   auto}</b>  <b>Example:</b> Device# <b>ap name AP-SIDD-A06 dot11 5ghz slot 1 txpower auto</b>	Configures 802.11a radio hosted on slot 1 for a specific access point. <ul style="list-style-type: none"> <li>• <i>tx_power_level</i>- Is the transmit power level in dBm. The valid range is from 1 to 8.</li> <li>• <b>auto</b>- Enables auto-RF.</li> </ul>

## Information About Dual-Band Radio Support

The Dual-Band (XOR) radio in Cisco 2800, 3800, 4800, and the 9120 series AP models offer the ability to serve 2.4-GHz or 5-GHz bands or passively monitor both the bands on the same AP. These APs can be configured to serve clients in 2.4-GHz and 5-GHz bands, or serially scan both 2.4-GHz and 5-GHz bands on the flexible radio while the main 5-GHz radio serves clients.

Cisco APs models up and through the Cisco 9120 APs are designed to support dual 5-GHz band operations with the *i* model supporting a dedicated Macro/Micro architecture and the *e* and *p* models supporting Macro/Macro. The Cisco 9130AXI APs and the Cisco 9136 APs support dual 5-GHz operations as Micro/Messo cell.

When a radio moves between bands (from 2.4-GHz to 5-GHz and vice versa), clients need to be steered to get an optimal distribution across radios. When an AP has two radios in the 5-GHz band, client steering algorithms contained in the Flexible Radio Assignment (FRA) algorithm are used to steer a client between the same band co-resident radios.

The XOR radio support can be steered manually or automatically:

- Manual steering of a band on a radio—The band on the XOR radio can only be changed manually.
- Automatic client and band steering on the radios is managed by the FRA feature that monitors and changes the band configurations as per site requirements.



**Note** RF measurement will not run when a static channel is configured on slot 1. Due to this, the dual band radio slot 0 will move only with 5-GHz radio and not to the monitor mode.

When slot 1 radio is disabled, RF measurement will not run, and the dual band radio slot 0 will be only on 2.4-GHz radio.

# Configuring Default XOR Radio Support

## Before you begin



**Note** The default radio points to the XOR radio hosted on slot 0.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# <b>enable</b>	Enters privileged EXEC mode.
<b>Step 2</b>	<b>ap name <i>ap-name</i> dot11 dual-band antenna ext-ant-gain <i>antenna_gain_value</i></b> <b>Example:</b> Device# ap name <i>ap-name</i> dot11 dual-band antenna ext-ant-gain 2	Configures the 802.11 dual-band antenna on a specific Cisco access point.  <i>antenna_gain_value</i> : The valid range is from 0 to 40.
<b>Step 3</b>	<b>ap name <i>ap-name</i> [no] dot11 dual-band shutdown</b> <b>Example:</b> Device# ap name <i>ap-name</i> dot11 dual-band shutdown	Shuts down the default dual-band radio on a specific Cisco access point.  Use the <b>no</b> form of the command to enable the radio.
<b>Step 4</b>	<b>ap name <i>ap-name</i> dot11 dual-band role manual client-serving</b> <b>Example:</b> Device# ap name <i>ap-name</i> dot11 dual-band role manual client-serving	Switchs to client-serving mode on the Cisco access point.
<b>Step 5</b>	<b>ap name <i>ap-name</i> dot11 dual-band band 24ghz</b> <b>Example:</b> Device# ap name <i>ap-name</i> dot11 dual-band band 24ghz	Switchs to 2.4-GHz radio band.
<b>Step 6</b>	<b>ap name <i>ap-name</i> dot11 dual-band txpower {<i>transmit_power_level</i>   auto}</b> <b>Example:</b>	Configures the transmit power for the radio on a specific Cisco access point.

	Command or Action	Purpose
	<pre>Device# ap name <i>ap-name</i> dot11 dual-band txpower 2</pre>	<p><b>Note</b> When an FRA-capable radio (slot 0 on 9120 AP[for instance]) is set to Auto, you cannot configure static channel and Txpower on this radio.</p> <p>If you want to configure static channel and Txpower on this radio, you will need to change the radio role to Manual Client-Serving mode.</p>
<b>Step 7</b>	<p><b>ap name <i>ap-name</i> dot11 dual-band channel <i>channel-number</i></b></p> <p><b>Example:</b></p> <pre>Device# ap name <i>ap-name</i> dot11 dual-band channel 2</pre>	<p>Enters the channel for the dual band.</p> <p><i>channel-number</i>—The valid range is from 1 to 173.</p>
<b>Step 8</b>	<p><b>ap name <i>ap-name</i> dot11 dual-band channel auto</b></p> <p><b>Example:</b></p> <pre>Device# ap name <i>ap-name</i> dot11 dual-band channel auto</pre>	<p>Enables the auto channel assignment for the dual-band.</p>
<b>Step 9</b>	<p><b>ap name <i>ap-name</i> dot11 dual-band channel width {20 MHz   40 MHz   80 MHz   160 MHz}</b></p> <p><b>Example:</b></p> <pre>Device# ap name <i>ap-name</i> dot11 dual-band channel width 20 MHz</pre>	<p>Chooses the channel width for the dual band.</p>
<b>Step 10</b>	<p><b>ap name <i>ap-name</i> dot11 dual-band cleanair</b></p> <p><b>Example:</b></p> <pre>Device# ap name <i>ap-name</i> dot11 dual-band cleanair</pre>	<p>Enables the Cisco CleanAir feature on the dual-band radio.</p>
<b>Step 11</b>	<p><b>ap name <i>ap-name</i> dot11 dual-band cleanair band {24 GHz   5 GMHz}</b></p> <p><b>Example:</b></p> <pre>Device# ap name <i>ap-name</i> dot11 dual-band cleanair band 5 GHz  Device# ap name <i>ap-name</i> [no] dot11 dual-band cleanair band 5 GHz</pre>	<p>Selects a band for the Cisco CleanAir feature.</p> <p>Use the <b>no</b> form of this command to disable the Cisco CleanAir feature.</p>
<b>Step 12</b>	<p><b>ap name <i>ap-name</i> dot11 dual-band dot11n antenna {A   B   C   D}</b></p> <p><b>Example:</b></p> <pre>Device# ap name <i>ap-name</i> dot11 dual-band dot11n antenna A</pre>	<p>Configures the 802.11n dual-band parameters for a specific access point.</p>

	Command or Action	Purpose
<b>Step 13</b>	<b>show ap name <i>ap-name</i> auto-rf dot11 dual-band</b>  <b>Example:</b> <pre>Device# show ap name <i>ap-name</i> auto-rf dot11 dual-band</pre>	Displays the auto-RF information for the Cisco access point.
<b>Step 14</b>	<b>show ap name <i>ap-name</i> wlan dot11 dual-band</b>  <b>Example:</b> <pre>Device# show ap name <i>ap-name</i> wlan dot11 dual-band</pre>	Displays the list of BSSIDs for the Cisco access point.

## Configuring XOR Radio Support for the Specified Slot Number (GUI)

### Procedure

- 
- Step 1** Click **Configuration > Wireless > Access Points**.
- Step 2** In the **Dual-Band Radios** section, select the AP for which you want to configure dual-band radios.
- The AP name, MAC address, CleanAir capability and slot information for the AP are displayed. If the Hyperlocation method is HALO, the antenna PID and antenna design information are also displayed.
- Step 3** Click **Configure**.
- Step 4** In the **General** tab, set the **Admin Status** as required.
- Step 5** Set the **CleanAir Admin Status** field to Enable or Disable.
- Step 6** Click **Update & Apply to Device**.
- 

## Configuring XOR Radio Support for the Specified Slot Number

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> <pre>Device# enable</pre>	Enters privileged EXEC mode.

	Command or Action	Purpose
Step 2	<b>ap name</b> <i>ap-name</i> <b>dot11 dual-band slot 0 antenna ext-ant-gain</b> <i>external_antenna_gain_value</i>  <b>Example:</b> Device# <b>ap name AP-SIDD-A06 dot11 dual-band slot 0 antenna ext-ant-gain 2</b>	Configures dual-band antenna for the XOR radio hosted on slot 0 for a specific access point.  <i>external_antenna_gain_value</i> - Is the external antenna gain value in multiples of .5 dBi unit. The valid range is from 0 to 40.
Step 3	<b>ap name</b> <i>ap-name</i> <b>dot11 dual-band slot 0 band {24ghz   5ghz}</b>  <b>Example:</b> Device# <b>ap name AP-SIDD-A06 dot11 dual-band slot 0 band 24ghz</b>	Configures current band for the XOR radio hosted on slot 0 for a specific access point.
Step 4	<b>ap name</b> <i>ap-name</i> <b>dot11 dual-band slot 0 channel {channel_number   auto   width [160   20   40   80]}</b>  <b>Example:</b> Device# <b>ap name AP-SIDD-A06 dot11 dual-band slot 0 channel 3</b>	Configures dual-band channel for the XOR radio hosted on slot 0 for a specific access point.  <i>channel_number</i> - The valid range is from 1 to 165.
Step 5	<b>ap name</b> <i>ap-name</i> <b>dot11 dual-band slot 0 cleanair band {24Ghz   5Ghz}</b>  <b>Example:</b> Device# <b>ap name AP-SIDD-A06 dot11 dual-band slot 0 cleanair band 24Ghz</b>	Enables CleanAir features for dual-band radios hosted on slot 0 for a specific access point.
Step 6	<b>ap name</b> <i>ap-name</i> <b>dot11 dual-band slot 0 dot11n antenna {A   B   C   D}</b>  <b>Example:</b> Device# <b>ap name AP-SIDD-A06 dot11 dual-band slot 0 dot11n antenna A</b>	Configures 802.11n dual-band parameters hosted on slot 0 for a specific access point.  Here, <b>A</b> - Enables antenna port A. <b>B</b> - Enables antenna port B. <b>C</b> - Enables antenna port C. <b>D</b> - Enables antenna port D.
Step 7	<b>ap name</b> <i>ap-name</i> <b>dot11 dual-band slot 0 role {auto   manual [client-serving   monitor]}</b>  <b>Example:</b> Device# <b>ap name AP-SIDD-A06 dot11 dual-band slot 0 role auto</b>	Configures dual-band role for the XOR radio hosted on slot 0 for a specific access point.  The following are the dual-band roles: <ul style="list-style-type: none"> <li>• <b>auto</b>- Refers to the automatic radio role selection.</li> <li>• <b>manual</b>- Refers to the manual radio role selection.</li> </ul>
Step 8	<b>ap name</b> <i>ap-name</i> <b>dot11 dual-band slot 0 shutdown</b>	Disables dual-band radio hosted on slot 0 for a specific access point.

	Command or Action	Purpose
	<b>Example:</b> Device# <code>ap name AP-SIDD-A06 dot11 dual-band slot 0 shutdown</code>  Device# <code>ap name AP-SIDD-A06 [no] dot11 dual-band slot 0 shutdown</code>	Use the <b>no</b> form of this command to enable the dual-band radio.
<b>Step 9</b>	<b>ap name</b> <i>ap-name</i> <b>dot11 dual-band slot 0 txpower</b> { <i>tx_power_level</i>   <b>auto</b> }  <b>Example:</b> Device# <code>ap name AP-SIDD-A06 dot11 dual-band slot 0 txpower 2</code>	Configures dual-band transmit power for XOR radio hosted on slot 0 for a specific access point. <ul style="list-style-type: none"> <li>• <i>tx_power_level</i>- Is the transmit power level in dBm. The valid range is from 1 to 8.</li> <li>• <b>auto</b>- Enables auto-RF.</li> </ul>

## Receiver Only Dual-Band Radio Support

### Information About Receiver Only Dual-Band Radio Support

This feature configures the dual-band Rx-only radio features for an access point with dual-band radios.

This dual-band Rx-only radio is dedicated for Analytics, Hyperlocation, Wireless Security Monitoring, and BLE AoA\*.

This radio will always continue to serve in monitor mode, therefore, you will not be able to make any channel and *tx-rx* configurations on the 3rd radio.

### Configuring Receiver Only Dual-Band Parameters for Access Points

#### Enabling CleanAir with Receiver Only Dual-Band Radio on a Cisco Access Point (GUI)

##### Procedure

- 
- Step 1** Choose **Configuration > Wireless > Access Points**.
  - Step 2** In the **Dual-Band Radios** settings, click the AP for which you want to configure the dual-band radios.
  - Step 3** In the **General** tab, enable the **CleanAir** toggle button.
  - Step 4** Click **Update & Apply to Device**.
-

## Enabling CleanAir with Receiver Only Dual-Band Radio on a Cisco Access Point

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device# enable	Enters privileged EXEC mode.
<b>Step 2</b>	<b>ap name <i>ap-name</i> dot11 rx-dual-band slot 2 cleanair band {24Ghz   5Ghz}</b>  <b>Example:</b> Device# ap name AP-SIDD-A06 dot11 rx-dual-band slot 2 cleanair band 24Ghz  Device# ap name AP-SIDD-A06 [no] dot11 rx-dual-band slot 2 cleanair band 24Ghz	Enables CleanAir with receiver only (Rx-only) dual-band radio on a specific access point.  Here, 2 refers to the slot ID.  Use the <b>no</b> form of this command to disable CleanAir.

## Disabling Receiver Only Dual-Band Radio on a Cisco Access Point (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Wireless > Access Points**.
  - Step 2** In the **Dual-Band Radios** settings, click the AP for which you want to configure the dual-band radios.
  - Step 3** In the **General** tab, disable the **CleanAir Status** toggle button.
  - Step 4** Click **Update & Apply to Device**.
- 

## Disabling Receiver Only Dual-Band Radio on a Cisco Access Point

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device# enable	Enters privileged EXEC mode.
<b>Step 2</b>	<b>ap name <i>ap-name</i> dot11 rx-dual-band slot 2 shutdown</b>  <b>Example:</b> Device# ap name AP-SIDD-A06 dot11 rx-dual-band slot 2 shutdown  Device# ap name AP-SIDD-A06 [no] dot11 rx-dual-band slot 2 shutdown	Disables receiver only dual-band radio on a specific Cisco access point.  Here, 2 refers to the slot ID.  Use the <b>no</b> form of this command to enable receiver only dual-band radio.

# Configuring Client Steering (CLI)

## Before you begin

Enable Cisco CleanAir on the corresponding dual-band radio.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device# <b>enable</b>	Enters privileged EXEC mode.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>wireless macro-micro steering transition-threshold balancing-window number-of-clients(0-65535)</b>  <b>Example:</b> Device(config)# wireless macro-micro steering transition-threshold balancing-window 10	Configures the micro-macro client load-balancing window for a set number of clients.
<b>Step 4</b>	<b>wireless macro-micro steering transition-threshold client count number-of-clients(0-65535)</b>  <b>Example:</b> Device(config)# wireless macro-micro steering transition-threshold client count 10	Configures the macro-micro client parameters for a minimum client count for transition.
<b>Step 5</b>	<b>wireless macro-micro steering transition-threshold macro-to-micro RSSI-in-dBm(-128-0)</b>  <b>Example:</b> Device(config)# wireless macro-micro steering transition-threshold macro-to-micro -100	Configures the macro-to-micro transition RSSI.
<b>Step 6</b>	<b>wireless macro-micro steering transition-threshold micro-to-macro RSSI-in-dBm(-128-0)</b>  <b>Example:</b> Device(config)# wireless macro-micro steering transition-threshold micro-to-macro -110	Configures the micro-to-macro transition RSSI.



	Command or Action	Purpose
<b>Step 7</b>	<b>wireless macro-micro steering probe-suppression aggressiveness</b> <i>number-of-cycles(-128—0)</i>  <b>Example:</b> Device(config)# wireless macro-micro steering probe-suppression aggressiveness -110	Configures the number of probe cycles to be suppressed.
<b>Step 8</b>	<b>wireless macro-micro steering probe-suppression hysteresis</b> <i>RSSI-in-dBm</i>  <b>Example:</b> Device(config)# wireless macro-micro steering probe-suppression hysteresis -5	Configures the macro-to-micro probe in RSSI. The range is between -6 to -3.
<b>Step 9</b>	<b>wireless macro-micro steering probe-suppression probe-only</b>  <b>Example:</b> Device(config)# wireless macro-micro steering probe-suppression probe-only	Enables probe suppression mode.
<b>Step 10</b>	<b>wireless macro-micro steering probe-suppression probe-auth</b>  <b>Example:</b> Device(config)# wireless macro-micro steering probe-suppression probe-auth	Enables probe and single authentication suppression mode.
<b>Step 11</b>	<b>show wireless client steering</b>  <b>Example:</b> Device# show wireless client steering	Displays the wireless client steering information.

## Verifying Cisco Access Points with Dual-Band Radios

To verify the access points with dual-band radios, use the following command:

```
Device# show ap dot11 dual-band summary
```

```
AP Name Subband Radio      Mac      Status Channel Power Level Slot ID Mode
-----
4800    All 3890.a5e6.f360 Enabled (40)* *1/8    (22 dBm)    0  Sensor
4800    All 3890.a5e6.f360 Enabled N/A    N/A        2          Monitor
```





# CHAPTER 10

## 802.1x Support

---

- [Introduction to the 802.1X Authentication, on page 79](#)
- [Limitations of the 802.1X Authentication, on page 80](#)
- [Topology - Overview, on page 80](#)
- [Configuring 802.1X Authentication Type and LSC AP Authentication Type \(GUI\), on page 81](#)
- [Configuring 802.1X Authentication Type and LSC AP Authentication Type, on page 81](#)
- [Enabling 802.1X on the Switch Port, on page 84](#)
- [Verifying 802.1X on the Switch Port, on page 85](#)
- [Verifying the Authentication Type, on page 86](#)

## Introduction to the 802.1X Authentication

IEEE 802.1X port-based authentication is configured on a device to prevent unauthorized devices from gaining access to the network. The device can combine the function of a router, switch, and access point, depending on the fixed configuration. Any device connecting to a switch port where 802.1X authentication is enabled must go through relevant EAP authentication model to start exchanging traffic.

Currently, the Cisco Wave 2 and Wi-Fi 6 (802.11AX) APs support 802.1X authentication with switch port for EAP-FAST, EAP-TLS and EAP-PEAP methods. Now, you can enable configurations and provide credentials to the AP from the embedded controller.

## EAP-FAST Protocol

In the EAP-FAST protocol developed by Cisco, in order to establish a secured TLS tunnel with RADIUS, the AP requires a strong shared key (PAC), either provided via in-band provisioning (in a secured channel) or via out-band provisioning (manual).



---

**Note** The EAP-FAST type configuration requires Dot1x credentials configuration for AP, since AP will use EAP-FAST with MSCHAP Version 2 method.

---



---

**Note** Local EAP is not supported on the Cisco 7925 phones.

---

## EAP-TLS/EAP-PEAP Protocol

The EAP-TLS protocol or EAP-PEAP protocol provides certificate based mutual EAP authentication.

In EAP-TLS, both the server and the client side certificates are required, where the secured shared key is derived for the particular session to encrypt or decrypt data. Whereas, in EAP-PEAP, only the server side certificate is required, where the client authenticates using password based protocol in a secured channel.



---

**Note** The EAP-PEAP type configuration requires Dot1x credentials configuration for AP; and the AP also needs to go through LSC provisioning. AP uses the PEAP protocol with MSCHAP Version 2 method.

---

## Limitations of the 802.1X Authentication

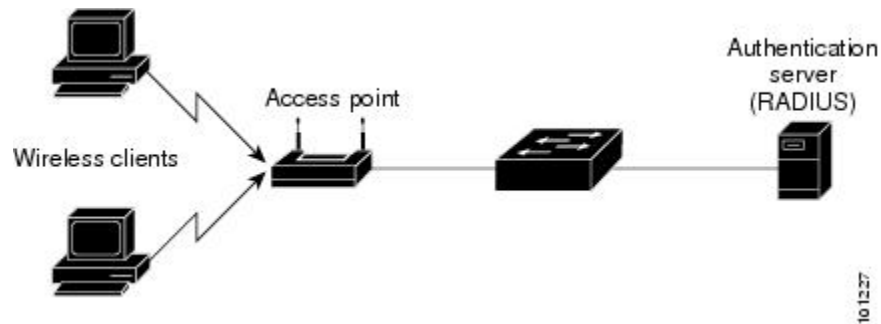
- 802.1X is not supported on dynamic ports or Ethernet Channel ports.
- 802.1X is not supported in a mesh AP scenario.
- There is no recovery from the embedded controller on credential mismatch or the expiry/invalidity of the certificate on AP. The 802.1X authentication has to be disabled on the switch port to connect the AP back to fix the configurations.
- There are no certificate revocation checks implemented on the certificates installed in AP.
- Only one Locally Significant Certificates (LSC) can be provisioned on the AP and the same certificate must be used for CAPWAP DTLS session establishment with embedded controller and the 802.1X authentication with the switch. If global LSC configuration on the embedded controller is disabled; AP deletes LSC which is already provisioned.
- If clear configurations are applied on the AP, then the AP will lose the 802.1X EAP type configuration and the LSC certificates. AP should again go through staging process if 802.1X is required.
- 802.1X for trunk port APs on multi-host authentication mode is supported. Network Edge Authentication Topology (NEAT) is not supported on COS APs.

## Topology - Overview

The 802.1X authentication events are as follows:

1. The AP acts as the 802.1X supplicant and is authenticated by the switch against the RADIUS server which supports EAP-FAST along with EAP-TLS and EAP-PEAP. When dot1x authentication is enabled on a switch port, the device connected to it authenticates itself to receive and forward data other than 802.1X traffic.
2. In order to authenticate with EAP-FAST method, the AP requires the credentials of the RADIUS server. It can be configured at the embedded controller, from where it will be passed on to the AP via configuration update request. For, EAP-TLS or EAP-PEAP the APs use the certificates (device/ID and CA) made significant by the local CA server.

Figure 3: Figure 1 Topology for 802.1X Authentication



10 1227

## Configuring 802.1X Authentication Type and LSC AP Authentication Type (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > AP Join**.
- Step 2** On the **AP Join Profile** page, click **Add**.  
The **Add AP Join Profile** page is displayed.
- Step 3** In the **AP > General** tab, navigate to the **AP EAP Auth Configuration** section.
- Step 4** From the **EAP Type** drop-down list, choose the EAP type as *EAP-FAST*, *EAP-TLS*, or *EAP-PEAP* to configure the dot1x authentication type.
- Step 5** From the **AP Authorization Type** drop-down list, choose the type as either *CAPWAP DTLS +* or *CAPWAP DTLS*.
- Step 6** Click **Save & Apply to Device**.
- 

## Configuring 802.1X Authentication Type and LSC AP Authentication Type

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  Enter your password if prompted.

	Command or Action	Purpose
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enables privileged EXEC mode. Enters global configuration mode.
<b>Step 3</b>	<b>ap profile &lt;profile-name&gt;</b> <b>Example:</b> Device(config)# ap profile new-profile	Specify a profile name.
<b>Step 4</b>	<b>dot1x {max-sessions   username   eap-type   lsc-ap-auth-state}</b> <b>Example:</b> Device(config-ap-profile)# dot1x eap-type	Configures the dot1x authentication type. <b>max-sessions:</b> Configures the maximum 802.1X sessions initiated per AP. <b>username:</b> Configures the 802.1X username for all Aps. <b>eap-type:</b> Configures the dot1x authentication type with the switch port. <b>lsc-ap-auth-state:</b> Configures the LSC authentication state on the AP.
<b>Step 5</b>	<b>dot1x eap-type {EAP-FAST   EAP-TLS   EAP-PEAP}</b> <b>Example:</b> Device(config-ap-profile)# dot1x eap-type	Configures the dot1x authentication type: EAP-FAST, EAP-TLS, or EAP-PEAP.
<b>Step 6</b>	<b>dot1x lsc-ap-auth-state {CAPWAP-DTLS   Dot1x-port-auth   Both}</b> <b>Example:</b> Device(config-ap-profile)# dot1x lsc-ap-auth-state Dot1x-port-auth	Configures the LSC authentication state on the AP. <b>CAPWAP-DTLS:</b> Uses LSC only for CAPWAP DTLS. <b>Dot1x-port-auth:</b> Uses LSC only for dot1x authentication with port. <b>Both:</b> Uses LSC for both CAPWAP-DTLS and Dot1x authentication with port.
<b>Step 7</b>	<b>end</b> <b>Example:</b> Device(config-ap-profile)# end	Exits the AP profile configuration mode and enters privileged EXEC mode.

## Configuring the 802.1X Username and Password (GUI)

### Procedure

**Step 1** Choose **Configuration > Tags & Profiles > AP Join**.

- Step 2** On the **AP Join** page, click the name of the AP Join profile or click **Add** to create a new one.
- Step 3** Click the **Management** tab and then click the **Credentials** tab.
- Step 4** Enter the local username and password details.
- Step 5** Choose the appropriate local password type.
- Step 6** Enter 802.1X username and password details.
- Step 7** Choose the appropriate 802.1X password type.
- Step 8** Enter the time in seconds after which the session should expire.
- Step 9** Enable local credentials and/or 802.1X credentials as required.
- Step 10** Click **Update & Apply to Device**.

## Configuring the 802.1X Username and Password (CLI)

The following procedure configures the 802.1X password for all the APs:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enables privileged EXEC mode. Enters global configuration mode.
<b>Step 3</b>	<b>ap profile &lt;profile-name&gt;</b> <b>Example:</b> Device(config)# ap profile new-profile	Specify a profile name.
<b>Step 4</b>	<b>dot1x {max-sessions   username   eap-type   lsc-ap-auth-state}</b> <b>Example:</b> Device(config-ap-profile)# dot1x eap-type	Configures the dot1x authentication type. <b>max-sessions:</b> Configures the maximum 802.1X sessions initiated per AP. <b>username:</b> Configures the 802.1X username for all Aps. <b>eap-type:</b> Configures the dot1x authentication type with the switch port. <b>lsc-ap-auth-state:</b> Configures the LSC authentication state on the AP.
<b>Step 5</b>	<b>dot1x username &lt;username&gt; password {0   8} &lt;password&gt;</b> <b>Example:</b>	Configures the dot1x password for all the APs. 0: Specifies an unencrypted password will follow.

	Command or Action	Purpose
	<code>Device(config-ap-profile)#dot1x username username password 0 password</code>	8: Specifies an AES encrypted password will follow.

## Enabling 802.1X on the Switch Port

The following procedure enables 802.1X on the switch port:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> <code>Device&gt; enable</code>	Enables privileged EXEC mode.  Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> <code>Device# configure terminal</code>	Enables privileged EXEC mode. Enters global configuration mode.
<b>Step 3</b>	<b>aaa new-model</b>  <b>Example:</b> <code>Device(config)# aaa new-model</code>	Enables AAA.
<b>Step 4</b>	<b>aaa authentication dot1x {default   listname} method1[method2...]</b>  <b>Example:</b> <code>Device(config)# aaa authentication dot1x default group radius</code>	Creates a series of authentication methods that are used to determine user privilege to access the privileged command level so that the device can communicate with the AAA server.
<b>Step 5</b>	<b>aaa authourization network group</b>  <b>Example:</b> <code>aaa authourization network group</code>	Enables AAA authorization for network services on 802.1X.
<b>Step 6</b>	<b>dot1x system-auth-control</b>  <b>Example:</b> <code>Device(config)# dot1x system-auth-control</code>	Globally enables 802.1X port-based authentication.
<b>Step 7</b>	<b>interface type slot/port</b>  <b>Example:</b> <code>Device(config)# interface fastethernet2/1</code>	Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.
<b>Step 8</b>	<b>authentication port-control {auto   force-authorized   force-unauthorized}</b>	Enables 802.1X port-based authentication on the interface.



	Command or Action	Purpose
	<b>Example:</b> <pre>Device(config-if)# authentication port-control auto</pre>	<p>auto—Enables IEEE 802.1X authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL-start frame is received. The Device requests the identity of the supplicant and begins relaying authentication messages between the supplicant and the authentication server. Each supplicant attempting to access the network is uniquely identified by the Device by using the supplicant MAC address.</p> <p>force-authorized—Disables IEEE 802.1X authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without IEEE 802.1X-based authentication of the client. This is the default setting.</p> <p>force-unauthorized—Causes the port to remain in the unauthorized state, ignoring all attempts by the supplicant to authenticate. The Device cannot provide authentication services to the supplicant through the port.</p>
<b>Step 9</b>	<b>dot1x pae [supplicant   authenticator   both]</b>  <b>Example:</b> <pre>Device(config-if)# dot1x pae authenticator</pre>	
<b>Step 10</b>	<b>end</b>  <b>Example:</b> <pre>Device(config-if)# end</pre>	Exits interface configuration mode and enters privileged EXEC mode.

## Verifying 802.1X on the Switch Port

The following show command displays the authentication state of 802.1X on the switch port:

```
Device# show dot1x all
Sysauthcontrol           Enabled
Dot1x Protocol Version   2
Dot1x Info for FastEthernet1
-----
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection         = Both
```

```

HostMode                = MULTI_HOST
ReAuthentication        = Disabled
QuietPeriod             = 60
ServerTimeout           = 30
SuppTimeout             = 30
ReAuthPeriod            = 3600 (Locally configured)
ReAuthMax               = 2
MaxReq                  = 2
TxPeriod                = 30
RateLimitPeriod         = 0
Device#

```

## Verifying the Authentication Type

The following show command displays the authentication state of an AP profile:

```

Device#show ap profile <profile-name> detailed ?
chassis Chassis
|          Output modifiers
<cr>

Device#show ap profile <profile-name> detailed

AP Profile Name          : default-ap-profile
Description               : default ap profile
...
Dot1x EAP Method         : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
LSC AP AUTH STATE        : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port auth

```



## CHAPTER 11

# Information About NAT Support

Network Address Translation (NAT) allows a device to act as an agent between the Internet (public) and a local network (private). It maps the controller's intranet IP addresses to a corresponding external address. The AP-manager interface of the controller must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.

The master AP in an Embedded Wireless Controller (EWC) network performs NAT on the wireless client traffic. This is achieved by translating the public and private IP addresses of the clients. Depending on the placement and number of NATs, the translation may be required at one or both ends of the tunnel.

The master AP performs NAT for the guest WLAN. However, this is not required for the employee WLAN. The IP address for the clients connected to the guest WLAN is provided by the internal DHCP server running on the master AP, whereas the clients connected to the employee WLAN gets the IP address from an external DHCP server.

The master AP acts as a gateway to the traffic coming from the clients connected to the NAT-ed WLAN and performs address translation. The clients connected to the non NAT-ed WLAN uses the gateway provided by the external DHCP server to send the traffic.

For centralized NAT WLANs, the controller provisions the VLAN mapping to the specific WLAN. When performing NAT, both the private IP address (address in the network before the NAT device) and the public IP address (address in the public network) has to be configured.

The external DHCP server provides the IP addresses for the APs. The master AP requires two IP addresses, one for the internal AP and one for when it is acting as a wireless controller. The internal DHCP server is not used to assign IP addresses to the APs connected to the network. The external DHCP server is used to provide the IP address to the clients on non- NAT-ed WLANs.

- [Restrictions for NAT Support](#) , on page 87
- [Enabling Centralized NAT on a VLAN](#), on page 88
- [Verifying NAT Support](#), on page 88

## Restrictions for NAT Support

- When centralized NAT is enabled, wired to wireless client traffic on the same VLAN is not supported.
- The WLAN, where centralized NAT is enabled, must also be provisioned on the master AP.
- Client DHCP server must run on the EWC for centralized NAT to work. External DHCP servers are not supported.

## Enabling Centralized NAT on a VLAN

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless ewc-ap centralized-nat vlan <i>vlan-id</i></b>  <b>Example:</b> Device(config)# wireless ewc-ap centralized-nat test-vlan 10	Enables centralized NAT on a VLAN.
<b>Step 3</b>	(Optional) <b>wireless ewc-ap centralized-nat vlan <i>vlan-id</i> peer-blocking</b>  <b>Example:</b> Device(config)# wireless ewc-ap centralized-nat test-vlan 10 peer-blocking	Configures peer to peer blocking.
<b>Step 4</b>	<b>end</b>  <b>Example:</b> Device(config)# end	Returns to privileged EXEC mode.

## Verifying NAT Support

To view the history of the AP datapath programming for centralized NAT, use the below command:

```
Device# show wireless mob-exp centralized-nat history
```

```
Centralized NAT Global event history:
Timestamp Event RC Context
-----
06/17/2019 05:28:39.962760 Route add 0 100.100.100.0/255.255.255.0 0.0.0.0 2
06/17/2019 05:28:39.961794 VLAN update 0 0-4095 0,10 1,100 1
06/17/2019 05:28:39.961162 Route add 0 10.10.10.0/255.255.255.0 0.0.0.0 1
Centralized NAT AP DP plumbing client event history:
Timestamp Event RC Context
-----
06/17/2019 05:37:55.827602 Client del 0 10.10.10.3
06/17/2019 05:37:55.826296 Client del 0 10.10.10.3
06/17/2019 05:37:32.160737 Client add 0 MAC b8:27:eb:27:f3:f6, IP 10.10.10.4, WLAN 2
06/17/2019 05:37:31.454851 Client del 0 10.10.10.4
06/17/2019 05:37:31.453479 Client del 0 10.10.10.4
06/17/2019 05:36:25.659639 Client add 0 MAC b8:27:eb:27:f3:f6, IP 10.10.10.4, WLAN 1
06/17/2019 05:35:52.513500 Client add 0 MAC b8:27:eb:be:08:ea, IP 10.10.10.3, WLAN 1
```

To view the NAT status, use the below command on the AP:

```
Device# show flexconnect ewc-ap nat status
Programmed WLC IP
9.9.71.50
Programmed Vlan Config
output 0: vlan 0-9,11-4095
output 1: vlan 10
Programmed Route Table
0.0.0.0/0 1.1.1.1          0
10.10.10.0/24 -          2
NAT and P2P Block Status:
WLAN    NAT-Enabled    P2P-Block
  0      false         false
  1      true          false
```





## PART III

# Radio Resource Management

- [Radio Resource Management, on page 93](#)
- [Coverage Hole Detection, on page 111](#)
- [Cisco Flexible Radio Assignment, on page 115](#)
- [XOR Radio Support, on page 121](#)
- [Cisco Receiver Start of Packet, on page 127](#)
- [Client Limit, on page 131](#)
- [IP Theft, on page 133](#)
- [Unscheduled Automatic Power Save Delivery, on page 137](#)
- [Enabling USB Port on Access Points, on page 139](#)







## CHAPTER 12

# Radio Resource Management

---

- [Information About Radio Resource Management, on page 93](#)
- [Restrictions for Radio Resource Management, on page 97](#)
- [How to Configure RRM, on page 97](#)
- [Monitoring RRM Parameters and RF Group Status, on page 108](#)
- [Examples: RF Group Configuration, on page 109](#)
- [Information About ED-RRM, on page 109](#)

## Information About Radio Resource Management

The Radio Resource Management (RRM) software that is embedded in the device acts as a built-in Radio Frequency (RF) engineer to consistently provide real-time RF management of your wireless network. RRM enables devices to continually monitor their associated lightweight access points for the following information:

- **Traffic load**—The total bandwidth used for transmitting and receiving traffic. It enables wireless LAN managers to track and plan network growth ahead of client demand.
- **Interference**—The amount of traffic coming from other 802.11 sources.
- **Noise**—The amount of non-802.11 traffic that is interfering with the currently assigned channel.
- **Coverage**—The Received Signal Strength (RSSI) and signal-to-noise ratio (SNR) for all connected clients.
- **Other** —The number of nearby access points.

RRM performs these functions:

- Radio resource monitoring
- Power control transmission
- Dynamic channel assignment
- Coverage hole detection and correction
- RF grouping



---

**Note** RRM grouping does not occur when an AP operates in a static channel that is not in the DCA channel list. The Neighbor Discovery Protocol (NDP) is sent only on DCA channels; therefore, when a radio operates on a non-DCA channel, it does not receive NDP on the channel.

---

## Radio Resource Monitoring

RRM automatically detects and configures new devices and lightweight access points as they are added to the network. It then automatically adjusts the associated and nearby lightweight access points to optimize coverage and capacity.

Lightweight access points can scan all the valid channels for the country of operation as well as for channels available in other locations. The access points in local mode go *offchannel* for a period not greater than 70 ms to monitor these channels for noise and interference. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and interfering access points.



---

**Note** In the presence of voice traffic or other critical traffic (in the last 100 ms), access points can defer off-channel measurements. The access points also defer off-channel measurements based on the WLAN scan priority configurations.

---

Each access point spends only 0.2 percent of its time off channel. This activity is distributed across all the access points so that adjacent access points are not scanning at the same time, which could adversely affect wireless LAN performance.

## Transmit Power Control

The device dynamically controls access point transmit power based on the real-time wireless LAN conditions.

The Transmit Power Control (TPC) algorithm increases and decreases an access point's power in response to changes in the RF environment. In most instances, TPC seeks to lower an access point's power to reduce interference, but in the case of a sudden change in the RF coverage, for example, if an access point fails or becomes disabled, TPC can also increase power on the surrounding access points. This feature is different from coverage hole detection, which is primarily concerned with clients. TPC provides enough RF power to achieve the required coverage levels while avoiding channel interference between access points. We recommend that you select TPCv1; TPCv2 option is deprecated. With TPCv1, you can select the channel aware mode; we recommend that you select this option for 5 GHz, and leave it unchecked for 2.4 GHz.

## Overriding the TPC Algorithm with Minimum and Maximum Transmit Power Settings

The TPC algorithm balances RF power in many diverse RF environments. However, it is possible that automatic power control will not be able to resolve some scenarios in which an adequate RF design was not possible to implement due to architectural restrictions or site restrictions, for example, when all the access points must be mounted in a central hallway, placing the access points close together, but requiring coverage to the edge of the building.

In these scenarios, you can configure maximum and minimum transmit power limits to override TPC recommendations. The maximum and minimum TPC power settings apply to all the access points through RF profiles in a RF network.

To set the Maximum Power Level Assignment and Minimum Power Level Assignment, enter the maximum and minimum transmit power used by RRM in the fields in the **Tx Power Control** window. The range for these parameters is -10 to 30 dBm. The minimum value cannot be greater than the maximum value; the maximum value cannot be less than the minimum value.

If you configure a maximum transmit power, RRM does not allow any access point attached to the controller, to exceed this transmit power level (whether the power is set by RRM TPC or by coverage hole detection). For example, if you configure a maximum transmit power of 11 dBm, no access point will transmit above 11 dBm, unless the access point is configured manually.

## Dynamic Channel Assignment

Two adjacent access points on the same channel can cause either signal contention or signal collision. In a collision, data is not received by the access point. This functionality can become a problem, for example, when someone reading an e-mail in a café affects the performance of the access point in a neighboring business. Even though these are separate networks, someone sending traffic to the café on channel 1 can disrupt communication in an enterprise using the same channel. Devices can dynamically allocate access point channel assignments to avoid conflict and increase capacity and performance. Channels are *reused* to avoid wasting scarce RF resources. In other words, channel 1 is allocated to a different access point far from the café, which is more effective than not using channel 1 altogether.

The device's Dynamic Channel Assignment (DCA) capabilities are also useful in minimizing adjacent channel interference between access points. For example, two overlapping channels in the 802.11b/g band, such as 1 and 2, cannot simultaneously use 11 or 54 Mbps. By effectively reassigning channels, the device keeps adjacent channels that are separated.




---

**Note** We recommend that you use only nonoverlapping channels (1, 6, 11, and so on).

---




---

**Note** Channel change does not require you to shut down the radio.

---

The device examines a variety of real-time RF characteristics to efficiently handle channel assignments as follows:

- Access point received energy: The received signal strength measured between each access point and its nearby neighboring access points. Channels are optimized for the highest network capacity.
- Noise: Noise can limit signal quality at the client and access point. An increase in noise reduces the effective cell size and degrades user experience. By optimizing channels to avoid noise sources, the device can optimize coverage while maintaining system capacity. If a channel is unusable due to excessive noise, that channel can be avoided.
- 802.11 interference: Interference is any 802.11 traffic that is not a part of your wireless LAN, including rogue access points and neighboring wireless networks. Lightweight access points constantly scan all the channels looking for sources of interference. If the amount of 802.11 interference exceeds a predefined configurable threshold (the default is 10 percent), the access point sends an alert to the device. Using the

RRM algorithms, the device may then dynamically rearrange channel assignments to increase system performance in the presence of the interference. Such an adjustment could result in adjacent lightweight access points being on the same channel, but this setup is preferable to having the access points remain on a channel that is unusable due to an interfering foreign access point.

In addition, if other wireless networks are present, the device shifts the usage of channels to complement the other networks. For example, if one network is on channel 6, an adjacent wireless LAN is assigned to channel 1 or 11. This arrangement increases the capacity of the network by limiting the sharing of frequencies. If a channel has virtually no capacity remaining, the device may choose to avoid this channel. In huge deployments in which all nonoverlapping channels are occupied, the device does its best, but you must consider RF density when setting expectations.

- **Load and utilization:** When utilization monitoring is enabled, capacity calculations can consider that some access points are deployed in ways that carry more traffic than other access points, for example, a lobby versus an engineering area. The device can then assign channels to improve the access point that has performed the worst. The load is taken into account when changing the channel structure to minimize the impact on the clients that are currently in the wireless LAN. This metric keeps track of every access point's transmitted and received packet counts to determine how busy the access points are. New clients avoid an overloaded access point and associate to a new access point. This *Load and utilization* parameter is disabled by default.

The device combines this RF characteristic information with RRM algorithms to make system-wide decisions. Conflicting demands are resolved using soft-decision metrics that guarantee the best choice for minimizing network interference. The end result is optimal channel configuration in a three-dimensional space, where access points on the floor above and below play a major factor in an overall wireless LAN configuration.




---

**Note** In a Dynamic Frequency Selection (DFS) enabled AP environment, ensure that you enable the UNII2 channels option under the DCA channel to allow 100-MHz separation for the dual 5-GHz radios.

---

The RRM startup mode is invoked in the following conditions:

- In a single-device environment, the RRM startup mode is invoked after the device is upgraded and rebooted.
- In a multiple-device environment, the RRM startup mode is invoked after an RF Group leader is elected.
- You can trigger the RRM startup mode from the CLI.

The RRM startup mode runs for 100 minutes (10 iterations at 10-minute intervals). The duration of the RRM startup mode is independent of the DCA interval, sensitivity, and network size. The startup mode consists of 10 DCA runs with high sensitivity (making channel changes easy and sensitive to the environment) to converge to a steady-state channel plan. After the startup mode is finished, DCA continues to run at the specified interval and sensitivity.




---

**Note** DCA algorithm interval is set to 1 hour, but DCA algorithm always runs in default interval of 10 min, channel allocation occurs at 10-min intervals for the first 10 cycles, and channel changes occur as per the DCA algorithm every 10 min. After that the DCA algorithm goes back to the configured time interval. This is common for both DCA interval and anchor time because it follows the steady state.

---



**Note** If Dynamic Channel Assignment (DCA)/Transmit Power Control (TPC) is turned off on the RF group member, and auto is set on RF group leader, the channel or TX power on a member gets changed as per the algorithm that is run on the RF group leader.

## Coverage Hole Detection and Correction

The RRM coverage hole detection algorithm can detect areas of radio coverage in a wireless LAN that are below the level needed for robust radio performance. This feature can alert you to the need for an additional (or relocated) lightweight access point.

If clients on a lightweight access point are detected at threshold levels (RSSI, failed client count, percentage of failed packets, and number of failed packets) lower than those specified in the RRM configuration, the access point sends a “coverage hole” alert to the device. The alert indicates the existence of an area where clients are continually experiencing poor signal coverage, without having a viable access point to which to roam. The device discriminates between coverage holes that can and cannot be corrected. For coverage holes that can be corrected, the device mitigates the coverage hole by increasing the transmit power level for that specific access point. The device does not mitigate coverage holes caused by clients that are unable to increase their transmit power or are statically set to a power level because increasing their downstream transmit power might increase interference in the network.

## Restrictions for Radio Resource Management

- If an AP tries to join the RF-group that already holds the maximum number of APs it can support, the device rejects the application and throws an error.

## How to Configure RRM

### Configuring Neighbor Discovery Type (CLI)

#### Procedure

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
Step 2	<b>ap dot11 {24ghz   5ghz} rrm ndp-type {protected   transparent}</b>  <b>Example:</b> Device(config)# <code>ap dot11 24ghz rrm</code>	Configures the neighbor discovery type. By default, the mode is set to “transparent”. <ul style="list-style-type: none"> <li>• <b>protected:</b> Sets the neighbor discover type to protected. Packets are encrypted.</li> </ul>

	Command or Action	Purpose
	<pre>ndp-type protected  Device(config)#ap dot11 24ghz rrm ndp-type transparent</pre>	<ul style="list-style-type: none"> <li>• <b>transparent:</b> Sets the neighbor discover type to transparent. Packets are sent as is.</li> </ul>
<b>Step 3</b>	<pre>end  Example: Device(config)# end</pre>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring Transmit Power Control

### Configuring the Tx-Power Control Threshold (CLI)

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<pre>configure terminal  Example: Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 2</b>	<pre>ap dot11 {24ghz   5ghz} rrm tpc-threshold threshold_value  Example: Device(config)#ap dot11 24ghz rrm tpc-threshold -60</pre>	Configures the Tx-power control threshold used by RRM for auto power assignment. The range is from -80 to -50.
<b>Step 3</b>	<pre>end  Example: Device(config)# end</pre>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

### Configuring the Tx-Power Level (CLI)

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<pre>configure terminal  Example: Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 2</b>	<pre>ap dot11 {24ghz   5ghz} rrm txpower {trans_power_level   auto   max   min   once}  Example:</pre>	Configures the 802.11 tx-power level <ul style="list-style-type: none"> <li>• <b>trans_power_level</b>—Sets the transmit power level.</li> </ul>

	Command or Action	Purpose
	<pre>Device(config)#ap dot11 24ghz rrm txpower auto</pre>	<ul style="list-style-type: none"> <li>• <b>auto</b>—Enables auto-RF.</li> <li>• <b>max</b>—Configures the maximum auto-RF tx-power.</li> <li>• <b>min</b>—Configures the minimum auto-RF tx-power.</li> <li>• <b>once</b>—Enables one-time auto-RF.</li> </ul>
<b>Step 3</b>	<pre>end</pre> <p><b>Example:</b></p> <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.

## Configuring 802.11 RRM Parameters

### Configuring Advanced 802.11 Channel Assignment Parameters (CLI)

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<pre>configure terminal</pre> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 2</b>	<pre>ap dot11 {24ghz   5ghz} rrm channel cleanair-event sensitivity {high   low   medium}</pre> <p><b>Example:</b></p> <pre>Device(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high</pre>	<p>Configures CleanAir event-driven RRM parameters.</p> <ul style="list-style-type: none"> <li>• <b>High</b>—Specifies the most sensitivity to non-Wi-Fi interference as indicated by the air quality (AQ) value.</li> <li>• <b>Low</b>—Specifies the least sensitivity to non-Wi-Fi interference as indicated by the AQ value.</li> <li>• <b>Medium</b>—Specifies medium sensitivity to non-Wi-Fi interference as indicated by the AQ value.</li> </ul>
<b>Step 3</b>	<pre>ap dot11 {24ghz   5ghz} rrm channel dca {   anchor-time   global {auto   once}   interval   min-metric   sensitivity {high   low   medium}}</pre> <p><b>Example:</b></p> <pre>Device(config)#ap dot11 24ghz rrm channel</pre>	<p>Configures Dynamic Channel Assignment (DCA) algorithm parameters for the 802.11 band.</p> <ul style="list-style-type: none"> <li>• –Enter a channel number to be added to the DCA list.</li> </ul>

	Command or Action	Purpose
	<pre>dca interval 2</pre>	<ul style="list-style-type: none"> <li>• <b>anchor-time</b>—Configures the anchor time for the DCA. The range is between 0 and 23 hours.</li> <li>• <b>global</b>—Configures the DCA mode for all 802.11 Cisco APs. <ul style="list-style-type: none"> <li>• <b>auto</b>—Enables auto-RF.</li> <li>• <b>once</b>—Enables auto-RF only once.</li> </ul> </li> <li>• <b>interval</b>—Configures the DCA interval value. The values are 1, 2, 3, 4, 6, 8, 12 and 24 hours and the default value 0 denotes 10 minutes.</li> <li>• <b>min-metric</b>—Configures the DCA minimum RSSI energy metric. The range is between -100 and -60.</li> <li>• <b>sensitivity</b>—Configures the DCA sensitivity level to changes in the environment. <ul style="list-style-type: none"> <li>• <b>high</b>—Specifies the most sensitivity.</li> <li>• <b>low</b>—Specifies the least sensitivity.</li> <li>• <b>medium</b>—Specifies medium sensitivity.</li> </ul> </li> </ul>
<b>Step 4</b>	<pre>ap dot11 5ghz rrm channel dca chan-width {20   40   80}</pre> <p><b>Example:</b></p> <pre>Device(config)#ap dot11 5ghz rrm channel dca chan-width best</pre>	Configures the DCA channel bandwidth for all 802.11 radios in the 5-GHz band. Sets the channel bandwidth to 20 MHz, 40 MHz, or 80 MHz, ; 20 MHz is the default value for channel bandwidth. 80 MHz is the default value for best. Set the channel bandwidth to best before configuring the constraints.
<b>Step 5</b>	<pre>ap dot11 {24ghz   5ghz} rrm channel device</pre> <p><b>Example:</b></p> <pre>Device(config)#ap dot11 24ghz rrm channel device</pre>	Configures the persistent non-Wi-Fi device avoidance in the 802.11 channel assignment.
<b>Step 6</b>	<pre>ap dot11 {24ghz   5ghz} rrm channel foreign</pre> <p><b>Example:</b></p> <pre>Device(config)#ap dot11 24ghz rrm channel foreign</pre>	Configures the foreign AP 802.11 interference avoidance in the channel assignment.



	Command or Action	Purpose
<b>Step 7</b>	<b>ap dot11 {24ghz   5ghz} rrm channel load</b> <b>Example:</b> <pre>Device(config)#ap dot11 24ghz rrm channel load</pre>	Configures the Cisco AP 802.11 load avoidance in the channel assignment.
<b>Step 8</b>	<b>ap dot11 {24ghz   5ghz} rrm channel noise</b> <b>Example:</b> <pre>Device(config)#ap dot11 24ghz rrm channel noise</pre>	Configures the 802.11 noise avoidance in the channel assignment.
<b>Step 9</b>	<b>end</b> <b>Example:</b> <pre>Device(config)# end</pre>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring 802.11 Coverage Hole Detection (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>ap dot11 {24ghz   5ghz} rrm coverage data {fail-percentage   packet-count   rssi-threshold}</b> <b>Example:</b> <pre>Device(config)#ap dot11 24ghz rrm coverage data fail-percentage 60</pre>	Configures the 802.11 coverage hole detection for data packets. <ul style="list-style-type: none"> <li>• <b>fail-percentage:</b> Configures the 802.11 coverage failure-rate threshold for uplink data packets as a percentage that ranges from 1 to 100%.</li> <li>• <b>packet-count:</b> Configures the 802.11 coverage minimum failure count threshold for uplink data packets that ranges from 1 to 255.</li> <li>• <b>rssi-threshold:</b> Configures the 802.11 minimum receive coverage level for data packets that range from -90 to -60 dBm.</li> </ul>
<b>Step 3</b>	<b>ap dot11 {24ghz   5ghz} rrm coverage exception global <i>exception level</i></b> <b>Example:</b> <pre>Device(config)#ap dot11 24ghz rrm</pre>	Configures the 802.11 Cisco AP coverage exception level as a percentage that ranges from 0 to 100%.

	Command or Action	Purpose
	<pre>coverage exception global 50</pre>	
<b>Step 4</b>	<p><b>ap dot11 {24ghz   5ghz} rrm coverage level global <i>cli_min exception level</i></b></p> <p><b>Example:</b></p> <pre>Device(config)#ap dot11 24ghz rrm coverage level global 10</pre>	Configures the 802.11 Cisco AP client minimum exception level that ranges from 1 to 75 clients.
<b>Step 5</b>	<p><b>ap dot11 {24ghz   5ghz} rrm coverage voice {fail-percentage   packet-count   rssi-threshold}</b></p> <p><b>Example:</b></p> <pre>Device(config)#ap dot11 24ghz rrm coverage voice packet-count 10</pre>	<p>Configures the 802.11 coverage hole detection for voice packets.</p> <ul style="list-style-type: none"> <li>• <b>fail-percentage:</b> Configures the 802.11 coverage failure-rate threshold for uplink voice packets as a percentage that ranges from 1 to 100%.</li> <li>• <b>packet-count:</b> Configures the 802.11 coverage minimum failure count threshold for uplink voice packets that ranges from 1 to 255.</li> <li>• <b>rssi-threshold:</b> Configures the 802.11 minimum receive coverage level for voice packets that range from -90 to -60 dBm.</li> </ul>
<b>Step 6</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config)# end</pre>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring 802.11 Event Logging (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 2</b>	<p><b>ap dot11 24ghz   5ghz rrm logging {channel   coverage   foreign   load   noise   performance   txpower}</b></p> <p><b>Example:</b></p> <pre>Device(config)#ap dot11 24ghz rrm logging channel</pre>	<p>Configures event-logging for various parameters.</p> <ul style="list-style-type: none"> <li>• <b>channel</b>—Configures the 802.11 channel change logging mode.</li> <li>• <b>coverage</b>—Configures the 802.11 coverage profile logging mode.</li> </ul>

	Command or Action	Purpose
	<pre>Device(config)#ap dot11 24ghz rrm logging coverage</pre> <pre>Device(config)#ap dot11 24ghz rrm logging foreign</pre> <pre>Device(config)#ap dot11 24ghz rrm logging load</pre> <pre>Device(config)#ap dot11 24ghz rrm logging noise</pre> <pre>Device(config)#ap dot11 24ghz rrm logging performance</pre> <pre>Device(config)#ap dot11 24ghz rrm logging txpower</pre>	<ul style="list-style-type: none"> <li>• <b>foreign</b>—Configures the 802.11 foreign interference profile logging mode.</li> <li>• <b>load</b>—Configures the 802.11 load profile logging mode.</li> <li>• <b>noise</b>—Configures the 802.11 noise profile logging mode.</li> <li>• <b>performance</b>—Configures the 802.11 performance profile logging mode.</li> <li>• <b>txpower</b>—Configures the 802.11 transmit power change logging mode.</li> </ul>
<b>Step 3</b>	<pre>end</pre> <p><b>Example:</b></p> <pre>Device(config)# end</pre>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring 802.11 Statistics Monitoring (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<pre>configure terminal</pre> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 2</b>	<pre>ap dot11 24ghz   5ghz rrm monitor channel-list {all   country   dca}</pre> <p><b>Example:</b></p> <pre>Device(config)#ap dot11 24ghz rrm monitor channel-list all</pre>	<p>Sets the 802.11 monitoring channel-list for parameters such as noise/interference/rogue.</p> <ul style="list-style-type: none"> <li>• <b>all</b>— Monitors all channels.</li> <li>• <b>country</b>— Monitor channels used in configured country code.</li> <li>• <b>dca</b>— Monitor channels used by dynamic channel assignment.</li> </ul>
<b>Step 3</b>	<pre>ap dot11 24ghz   5ghz rrm monitor coverage interval</pre> <p><b>Example:</b></p> <pre>Device(config)#ap dot11 24ghz rrm monitor coverage 600</pre>	Configures the 802.11 coverage measurement interval in seconds that ranges from 60 to 3600.

	Command or Action	Purpose
<b>Step 4</b>	<b>ap dot11 24ghz   5ghz rrm monitor load interval</b> <b>Example:</b> Device (config) #ap dot11 24ghz rrm monitor load 180	Configures the 802.11 load measurement interval in seconds that ranges from 60 to 3600.
<b>Step 5</b>	<b>ap dot11 24ghz   5ghz rrm monitor noise interval</b> <b>Example:</b> Device (config) #ap dot11 24ghz rrm monitor noise 360	Configures the 802.11 noise measurement interval (channel scan interval) in seconds that ranges from 60 to 3600.
<b>Step 6</b>	<b>ap dot11 24ghz   5ghz rrm monitor signal interval</b> <b>Example:</b> Device (config) #ap dot11 24ghz rrm monitor signal 480	Configures the 802.11 signal measurement interval (neighbor packet frequency) in seconds that ranges from 60 to 3600.
<b>Step 7</b>	<b>end</b> <b>Example:</b> Device (config) # end	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring the 802.11 Performance Profile (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ap dot11 {24ghz   5ghz} rrm profile clients cli_threshold_value</b> <b>Example:</b> Device (config) #ap dot11 24ghz rrm profile clients 20	Sets the threshold value for 802.11 Cisco AP clients that range between 1 and 75 clients.
<b>Step 3</b>	<b>ap dot11 {24ghz   5ghz} rrm profile foreign int_threshold_value</b> <b>Example:</b>	Sets the threshold value for 802.11 foreign interference that ranges between 0 and 100%.

	Command or Action	Purpose
	Device(config)#ap dot11 24ghz rrm profile foreign 50	
<b>Step 4</b>	<b>ap dot11 {24ghz   5ghz} rrm profile noise for_noise_threshold_value</b>  <b>Example:</b>  Device(config)#ap dot11 24ghz rrm profile noise -65	Sets the threshold value for 802.11 foreign noise ranges between -127 and 0 dBm.
<b>Step 5</b>	<b>ap dot11 {24ghz   5ghz} rrm profile throughput throughput_threshold_value</b>  <b>Example:</b>  Device(config)#ap dot11 24ghz rrm profile throughput 10000	Sets the threshold value for 802.11 Cisco AP throughput that ranges between 1000 and 10000000 bytes per second.
<b>Step 6</b>	<b>ap dot11 {24ghz   5ghz} rrm profile utilization rf_util_threshold_value</b>  <b>Example:</b>  Device(config)#ap dot11 24ghz rrm profile utilization 75	Sets the threshold value for 802.11 RF utilization that ranges between 0 to 100%.
<b>Step 7</b>	<b>end</b>  <b>Example:</b>  Device(config)# end	Returns to privileged EXEC mode.

## Configuring Advanced 802.11 RRM

### Enabling Channel Assignment (CLI)

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device# enable	Enters privileged EXEC mode.
<b>Step 2</b>	<b>ap dot11 {24ghz   5ghz} rrm channel-update</b>  <b>Example:</b>  Device# ap dot11 24ghz rrm channel-update	Enables the 802.11 channel selection update for each of the Cisco access points.  <b>Note</b> After you enable <b>ap dot11 {24ghz   5ghz} rrm channel-update</b> , a token is assigned for channel assignment in the DCA algorithm.

## Restarting DCA Operation

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# <code>enable</code>	Enters privileged EXEC mode.
<b>Step 2</b>	<b>ap dot11 {24ghz   5ghz} rrm dca restart</b> <b>Example:</b> Device# <code>ap dot11 24ghz rrm dca restart</code>	Restarts the DCA cycle for 802.11 radio.

## Updating Power Assignment Parameters (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# <code>enable</code>	Enters privileged EXEC mode.
<b>Step 2</b>	<b>ap dot11 {24ghz   5ghz} rrm txpower update</b> <b>Example:</b> Device# <code>ap dot11 24ghz rrm txpower update</code>	Updates the 802.11 transmit power for each of the Cisco access points.

## Configuring Rogue Access Point Detection in RF Groups

### Configuring Rogue Access Point Detection in RF Groups (CLI)

#### Before you begin

Ensure that each embedded controller in the RF group has been configured with the same RF group name.



**Note** The name is used to verify the authentication IE in all beacon frames. If the embedded controller have different names, false alarms will occur.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>Example:</b> Device#	Perform this step for every access point connected to the embedded controller. <ul style="list-style-type: none"> <li>• <b>monitor:</b> Sets the AP mode to monitor mode.</li> <li>• <b>clear:</b> Resets AP mode to local or remote based on the site.</li> <li>• <b>sensor:</b> Sets the AP mode to sensor mode.</li> <li>• <b>sniffer:</b> Sets the AP mode to wireless sniffer mode.</li> </ul>
<b>Step 2</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.
<b>Step 3</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 4</b>	<b>wireless wps ap-authentication</b> <b>Example:</b> Device (config)# <b>wireless wps ap-authentication</b>	Enables rogue access point detection.
<b>Step 5</b>	<b>wireless wps ap-authentication threshold value</b> <b>Example:</b> Device (config)# <b>wireless wps ap-authentication threshold 50</b>	<p>Specifies when a rogue access point alarm is generated. An alarm occurs when the threshold value (which specifies the number of access point frames with an invalid authentication IE) is met or exceeded within the detection period.</p> <p>The valid threshold range is from 1 to 255, and the default threshold value is 1. To avoid false alarms, you may want to set the threshold to a higher value.</p> <p><b>Note</b> Enable rogue access point detection and threshold value on every embedded controller in the RF group.</p> <p><b>Note</b> If rogue access point detection is not enabled on every embedded controller in the RF group, the access points on the embedded controller with this feature disabled are reported as rogues.</p>

# Monitoring RRM Parameters and RF Group Status

## Monitoring RRM Parameters

*Table 1: Commands for monitoring Radio Resource Management*

Commands	Description
<b>show ap dot11 24ghz channel</b>	Displays the configuration and statistics of the 802.11b channel assignment.
<b>show ap dot11 24ghz coverage</b>	Displays the configuration and statistics of the 802.11b coverage.
<b>show ap dot11 24ghz group</b>	Displays the configuration and statistics of the 802.11b grouping.
<b>show ap dot11 24ghz logging</b>	Displays the configuration and statistics of the 802.11b event logging.
<b>show ap dot11 24ghz monitor</b>	Displays the configuration and statistics of the 802.11b monitoring.
<b>show ap dot11 24ghz profile</b>	Displays 802.11b profiling information for all Cisco APs.
<b>show ap dot11 24ghz summary</b>	Displays the configuration and statistics of the 802.11b Cisco APs.
<b>show ap dot11 24ghz txpower</b>	Displays the configuration and statistics of the 802.11b transmit power control.
<b>show ap dot11 5ghz channel</b>	Displays the configuration and statistics of the 802.11a channel assignment.
<b>show ap dot11 5ghz coverage</b>	Displays the configuration and statistics of the 802.11a coverage.
<b>show ap dot11 5ghz group</b>	Displays the configuration and statistics of the 802.11a grouping.
<b>show ap dot11 5ghz logging</b>	Displays the configuration and statistics of the 802.11a event logging.
<b>show ap dot11 5ghz monitor</b>	Displays the configuration and statistics of the 802.11a monitoring.
<b>show ap dot11 5ghz profile</b>	Displays 802.11a profiling information for all Cisco APs.
<b>show ap dot11 5ghz summary</b>	Displays the configuration and statistics of the 802.11a Cisco APs.
<b>show ap dot11 5ghz txpower</b>	Displays the configuration and statistics of the 802.11a transmit power control.

## Verifying RF Group Status (CLI)

This section describes the new commands for RF group status.

The following commands can be used to verify RF group status on the .

*Table 2: Verifying Aggressive Load Balancing Command*

Command	Purpose



<b>show ap dot11 5ghz group</b>	Displays the controller name which is the RF group leader for the 802.11a RF network.
<b>show ap dot11 24ghz group</b>	Displays the controller name which is the RF group leader for the 802.11b/g RF network.

## Examples: RF Group Configuration

This example shows how to configure RF group name:

```
Device# configure terminal
Device(config)# wireless rf-network test1
Device(config)# ap dot11 24ghz shutdown
Device(config)# end
Device # show network profile 5
```

This example shows how to configure rogue access point detection in RF groups:

```
Device#
Device# end
Device# configure terminal
Device(config)# wireless wps ap-authentication
Device(config)# wireless wps ap-authentication threshold 50
Device(config)# end
```

## Information About ED-RRM

Spontaneous interference is interference that appears suddenly on a network, perhaps jamming a channel or a range of channels completely. The Cisco CleanAir spectrum event-driven RRM feature allows you to set a threshold for air quality (AQ) that, if exceeded, triggers an immediate channel change for the affected access point. Most RF management systems can avoid interference, but this information takes time to propagate through the system. Cisco CleanAir relies on AQ measurements to continuously evaluate the spectrum and can trigger a move within 30 seconds. For example, if an access point detects interference from a video camera, it can recover by changing channels within 30 seconds of the camera becoming active.

## Configuring ED-RRM on the Cisco Wireless LAN Controller (CLI)

### Procedure

- Step 1** Trigger spectrum event-driven radio resource management (RRM) to run when a Cisco CleanAir-enabled access point detects a significant level of interference by entering these commands:
- ap dot11 {24ghz | 5ghz} rrm channel cleanair-event** —Configures CleanAir driven RRM parameters for the 802.11 Cisco lightweight access points.

**ap dot11 {24ghz | 5ghz} rrm channel cleanair-event sensitivity {low | medium | high | custom}**—Configures CleanAir driven RRM sensitivity for the 802.11 Cisco lightweight access points. Default selection is Medium.

**ap dot11 {24ghz | 5ghz} rrm channel cleanair-event rogue-contribution**—Enables rogue contribution.

**ap dot11 {24ghz | 5ghz} rrm channel cleanair-event rogue-contribution duty-cycle thresholdvalue**—Configures threshold value for rogue contribution. The valid range is from 1 to 99, with 80 as the default.

**Step 2** Save your changes by entering this command:

**write memory**

**Step 3** See the CleanAir configuration for the 802.11a/n/ac or 802.11b/g/n network by entering this command:

**show ap dot11 {24ghz | 5ghz} cleanair config**

Information similar to the following appears:

---



## CHAPTER 13

# Coverage Hole Detection

---

- [Coverage Hole Detection and Correction, on page 111](#)

## Coverage Hole Detection and Correction

The RRM coverage hole detection algorithm can detect areas of radio coverage in a wireless LAN that are below the level needed for robust radio performance. This feature can alert you to the need for an additional (or relocated) lightweight access point.

If clients on a lightweight access point are detected at threshold levels (RSSI, failed client count, percentage of failed packets, and number of failed packets) lower than those specified in the RRM configuration, the access point sends a “coverage hole” alert to the device. The alert indicates the existence of an area where clients are continually experiencing poor signal coverage, without having a viable access point to which to roam. The device discriminates between coverage holes that can and cannot be corrected. For coverage holes that can be corrected, the device mitigates the coverage hole by increasing the transmit power level for that specific access point. The device does not mitigate coverage holes caused by clients that are unable to increase their transmit power or are statically set to a power level because increasing their downstream transmit power might increase interference in the network.

## Configuring Coverage Hole Detection (GUI)

Follow the procedure given below to configure client accounting.

### Procedure

---

- Step 1** Click **Configuration > Radio Configurations > RRM**.
- On this page, you can configure Radio Resource Management parameters for 802.11a/n/ac (5 GHz) and 802.11b/g/n (2.4 GHz) radios, and flexible radio assignment parameters.
- Step 2** Check the **Enable Coverage Hole Detection** check box.
- Enables coverage hole detection.
-

## Configuring Coverage Hole Detection (CLI)

Coverage Hole Detection (CHD) is based on upstream RSSI metrics observed by the AP.

Follow the procedure given below to configure CHD:

### Before you begin

Disable the 802.11 network before applying the configuration.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>ap dot11 {24ghz   5ghz} rrm coverage data {fail-percentage   packet-count   rssi-threshold}</b></p> <p><b>Example:</b></p> <pre>Device(config)# ap dot11 24ghz rrm coverage data fail-percentage 60</pre>	<p>Configures the 802.11 coverage level for data packets.</p> <ul style="list-style-type: none"> <li>• <b>fail-percentage:</b> Configures the 802.11 coverage failure-rate threshold for uplink data packets as a percentage that ranges from 1 to 100%.</li> <li>• <b>packet-count:</b> Configures the 802.11 coverage minimum failure count threshold for uplink data packets that ranges from 1 to 255.</li> <li>• <b>rssi-threshold:</b> Configures the 802.11 minimum receive coverage level for data packets that range from -90 to -60 dBm.</li> </ul>
<b>Step 2</b>	<p><b>ap dot11 {24ghz   5ghz} rrm coverage exception global <i>exception level</i></b></p> <p><b>Example:</b></p> <pre>Device(config)# ap dot11 24ghz rrm coverage exception global 50</pre>	<p>Configures the 802.11 Cisco AP coverage exception level as a percentage that ranges from 0 to 100%.</p>
<b>Step 3</b>	<p><b>ap dot11{24ghz   5ghz}rrm coverage level global <i>cli_min exception level</i></b></p> <p><b>Example:</b></p> <pre>Device(config)# ap dot11 24ghz rrm coverage level global 10</pre>	<p>Configures the 802.11 Cisco AP client minimum exception level that ranges from 1 to 75 clients.</p>
<b>Step 4</b>	<p><b>ap dot11 {24ghz   5ghz} rrm coverage voice {fail-percentage   packet-count   rssi-threshold}</b></p> <p><b>Example:</b></p> <pre>Device(config)# ap dot11 24ghz rrm coverage voice packet-count 10</pre>	<p>Configures the 802.11 coverage hole detection for voice packets.</p> <ul style="list-style-type: none"> <li>• <b>fail-percentage:</b> Configures the 802.11 coverage failure-rate threshold for uplink voice packets as a percentage that ranges from 1 to 100%.</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• <b>packet-count</b>: Configures the 802.11 coverage minimum failure count threshold for uplink voice packets that ranges from 1 to 255.</li> <li>• <b>rsi-threshold</b>: Configures the 802.11 minimum receive coverage level for voice packets that range from -90 to -60 dBm.</li> </ul>
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.
<b>Step 6</b>	<b>show ap dot11 {24ghz   5ghz} coverage</b> <b>Example:</b> Device# <b>show ap dot11 5ghz coverage</b>	Displays the CHD details.



**Note** If both the number and percentage of failed packets exceed the values entered in the **packet-count** and **fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes. False positives are generally due to the poor roaming logic implemented on most clients. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **coverage level global** and **coverage exception global** commands over a 90-second period. The controller determines if the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

## Configuring CHD for RF Tag Profile (GUI)

### Procedure

- Step 1** Choose **Configuration > Radio Configurations > RRM**.
- Step 2** On the **Coverage** tab, select the **Enable Coverage Hole Detection** check box.
- Step 3** In the **Data Packet Count** field, enter the number of data packets.
- Step 4** In the **Data Packet Percentage** field, enter the percentage of data packets.
- Step 5** In the **Data RSSI Threshold** field, enter the actual value in dBm. Value ranges from -60 dBm to -90 dBm; the default value is -80 dBm.
- Step 6** In the **Voice Packet Count** field, enter the number of voice data packets.
- Step 7** In the **Voice Packet Percentage** field, enter the percentage of voice data packets.
- Step 8** In the **Voice RSSI Threshold** field, enter the actual value in dBm. Value ranges from -60 dBm to -90 dBm; the default value is -80 dBm.

- Step 9** In the **Minimum Failed Client per AP** field, enter the minimum number of clients on an AP with a signal-to-noise ratio (SNR) below the coverage threshold. Value ranges from 1 to 75 and the default value is 3.
- Step 10** In the **Percent Coverage Exception Level per AP** field, enter the maximum desired percentage of clients on an access point's radio operating below the desired coverage threshold and click Apply. Value ranges from 0 to 100% and the default value is 25%.
- Step 11** Click **Apply**.

## Configuring CHD for RF Profile (CLI)

Follow the procedure given below to configure Coverage Hole Detection (CHD) for RF profile.

### Before you begin

Ensure that the RF profile is already created.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ap dot11 {24ghz   5ghz } rf-profile</b> <i>rf-profile-tag</i>  <b>Example:</b> Device(config)# <code>ap dot11 24ghz rf-profile</code> <code>alpha-rfprofile-24ghz</code>	Configures the 802.11 coverage hole detection for data packets.
<b>Step 3</b>	<b>coverage data rssi threshold</b> <i>threshold-value</i>  <b>Example:</b> Device(config-rf-profile)# <code>coverage data</code> <code>rssi threshold -80</code>	Configures the minimum RSSI value for data packets received by the access point. Valid values range from -90 to -60 in dBm.
<b>Step 4</b>	<b>end</b>  <b>Example:</b> Device(config-rf-profile)# <code>end</code>	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show ap dot11 24ghz rf-profile summary</b>  <b>Example:</b> Device# <code>show ap dot11 24ghz rf-profile</code> <code>summary</code>	Displays summary of the available RF profiles.



## CHAPTER 14

# Cisco Flexible Radio Assignment

- [Information About Flexible Radio Assignment, on page 115](#)
- [Configuring an FRA Radio \(CLI\), on page 116](#)
- [Configuring an FRA Radio \(GUI\), on page 118](#)

## Information About Flexible Radio Assignment

Flexible Radio Assignment (FRA) takes advantage of the dual-band radios included in APs. The FRA is a new feature added to the RRM to analyze the Neighbor Discovery Protocol (NDP) measurements, which manages the hardware used to determine the role of the new flexible radio (2.4 GHz, 5 GHz, or monitor) in your network.

Traditional legacy dual-band APs always had 2 radio slots, (1 slot per band) and were organized by the band they were serving, that is slot 0= 802.11b,g,n and slot 1=802.11a,n,ac.

### XOR Support in 2.4-GHz or 5-GHz Bands

The flexible radio (XOR) offers the ability to serve the 2.4-GHz or the 5-GHz bands, or passively monitor both bands on the same AP. The AP models that are offered are designed to support dual 5-GHz band operations, with the Cisco APs *i* model supporting a dedicated Macro/Micro architecture, and the *e* and *p* models supporting Macro/Macro architecture.

When using FRA with the internal antenna (*i* series models), two 5-GHz radios can be used in a Micro/Macro cell mode. When using FRA with external antenna (*e* and *p* models) the antennas may be placed to enable the creation of two completely separate macro (wide-area cells) or two micro cells (small cells) for HDX or any combination.

FRA calculates and maintains a measurement of redundancy for 2.4-GHz radios and represents this as a new measurement metric called COF (Coverage Overlap Factor).

This feature is integrated into existing RRM and runs in mixed environments with legacy APs. The **AP MODE** selection sets the entire AP (slot 0 and slot1) into one of several operating modes, including:

- Local Mode
- Monitor Mode
- FlexConnect Mode
- Sniffer Mode
- Spectrum Connect Mode

Before XOR was introduced, changing the mode of an AP propagated the change to the entire AP, that is both radio slot 0 and slot 1. The addition of the XOR radio in the slot 0 position provides the ability to operate a single radio interface in many of the previous modes, eliminating the need to place the whole AP into a mode. When this concept is applied to a single radio level, it is called *role*. Three such roles can be assigned now:

- Client Serving
- Either 2.4 GHz(1) or 5 GHz(2)
- Monitor-Monitor mode (3)

**Note**

- MODE: Assigned to a whole AP (slot 0 and slot 1)
- ROLE: Assigned to a single radio interface (slot 0)

## Benefits of the FRA

- Solves the problem of 2.4-GHz over coverage.
- Creating two diverse 5-GHz cells doubles the airtime that is available.
- Permits one AP with one Ethernet drop to function like two 5-GHz APs.
- Introduces the concept of Macro/Micro cells for airtime efficiency.
- Allows more bandwidth to be applied to an area within a larger coverage cell.
- Can be used to address nonlinear traffic.
- Enhances the High-Density Experience (HDX) with one AP.
- XOR radio can be selected by the corresponding user in either band-servicing client mode or monitor mode.

## Configuring an FRA Radio (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device# <b>enable</b>	Enters privileged EXEC mode.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.





	Command or Action	Purpose
	<pre> : 1 Hour(s)  AP Name          MAC Address Slot ID  Current-Band      COF % Suggested Mode AP00A6.CA36.295A    006b.f09c.8290 0          2.4GHz          None 2.4GHz  COF : Coverage Overlap Factor  test_machine# </pre>	
<b>Step 10</b>	<p><b>show ap name <i>ap-name</i> config dot11 dual-band</b></p> <p><b>Example:</b></p> <pre> Device# show ap name config dot11 dual-band </pre>	Shows the current 802.11 dual-band parameters in a given AP.

## Configuring an FRA Radio (GUI)

### Procedure

- Step 1** Choose **Configuration > Radio Configurations > RRM > FRA**.
- Step 2** In the **Flexible Radio Assignment** window, enable FRA status and determine the overlapping 2.4 GHz or 5 GHz coverage for each AP, choose **Enabled** in the **FRA Status** field. By default, the FRA status is disabled.
- Step 3** Under the From the **FRA Interval** drop-down list, choose the FRA run interval. The interval values range from 1 hour to 24 hours. You can choose the FRA run interval value only after you enable the FRA status.
- Step 4** From the **FRA Sensitivity** drop-down list, choose the percentage of Coverage Overlap Factor (COF) required to consider a radio as redundant. You can select the supported value only after you enable the FRA status.

The supported values are as follows:

- Low: 100 percent
- Medium (default): 95 percent
- High: 90 percent

The **Last Run** and **Last Run Time** fields will show the time FRA was run last and the time it was run.

- Step 5** Check the **Client Aware** check box to take decisions on redundancy.

When enabled, the **Client Aware** feature monitors the dedicated 5-GHz radio and when the client load passes a pre-set threshold, automatically changes the Flexible Radio assignment from a monitor role into a 5-GHz role, effectively doubling the capacity of the cell on demand. Once the capacity crisis is over and Wi-Fi load returns to normal, the radios resume their previous roles.

- Step 6** In the **Client Select** field, enter a value for client selection. The valid values range between 0 and 100 percent. The default value is 50 percent.
- This means that if the dedicated 5-GHz interface reaches 50% channel utilization, this will trigger the monitor role dual-band interface to transition to a 5-GHz client-serving role.
- Step 7** In the **Client Reset** field, enter a reset value for the client. The valid values range between 0 and 100 percent. The default value is 5 percent.
- Once the AP is operating as a dual 5-GHz AP, this setting indicates the reduction in the combined radios' overall channel utilization required to reset the dual-band radio to monitor role.
- Step 8** Click **Apply** to save the configuration.
-





# CHAPTER 15

## XOR Radio Support

---

- [Information About Dual-Band Radio Support](#) , on page 121
- [Configuring Default XOR Radio Support](#), on page 122
- [Configuring XOR Radio Support for the Specified Slot Number \(GUI\)](#), on page 124
- [Configuring XOR Radio Support for the Specified Slot Number](#), on page 124

## Information About Dual-Band Radio Support

The Dual-Band (XOR) radio in Cisco 2800, 3800, 4800, and the 9120 series AP models offer the ability to serve 2.4-GHz or 5-GHz bands or passively monitor both the bands on the same AP. These APs can be configured to serve clients in 2.4-GHz and 5-GHz bands, or serially scan both 2.4-GHz and 5-GHz bands on the flexible radio while the main 5-GHz radio serves clients.

Cisco APs models up and through the Cisco 9120 APs are designed to support dual 5-GHz band operations with the *i* model supporting a dedicated Macro/Micro architecture and the *e* and *p* models supporting Macro/Macro. The Cisco 9130AXI APs and the Cisco 9136 APs support dual 5-GHz operations as Micro/Messo cell.

When a radio moves between bands (from 2.4-GHz to 5-GHz and vice versa), clients need to be steered to get an optimal distribution across radios. When an AP has two radios in the 5-GHz band, client steering algorithms contained in the Flexible Radio Assignment (FRA) algorithm are used to steer a client between the same band co-resident radios.

The XOR radio support can be steered manually or automatically:

- Manual steering of a band on a radio—The band on the XOR radio can only be changed manually.
- Automatic client and band steering on the radios is managed by the FRA feature that monitors and changes the band configurations as per site requirements.



---

**Note** RF measurement will not run when a static channel is configured on slot 1. Due to this, the dual band radio slot 0 will move only with 5-GHz radio and not to the monitor mode.

When slot 1 radio is disabled, RF measurement will not run, and the dual band radio slot 0 will be only on 2.4-GHz radio.

---

# Configuring Default XOR Radio Support

## Before you begin



**Note** The default radio points to the XOR radio hosted on slot 0.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# <b>enable</b>	Enters privileged EXEC mode.
<b>Step 2</b>	<b>ap name <i>ap-name</i> dot11 dual-band antenna ext-ant-gain <i>antenna_gain_value</i></b> <b>Example:</b> Device# ap name <i>ap-name</i> dot11 dual-band antenna ext-ant-gain 2	Configures the 802.11 dual-band antenna on a specific Cisco access point.  <i>antenna_gain_value</i> : The valid range is from 0 to 40.
<b>Step 3</b>	<b>ap name <i>ap-name</i> [no] dot11 dual-band shutdown</b> <b>Example:</b> Device# ap name <i>ap-name</i> dot11 dual-band shutdown	Shuts down the default dual-band radio on a specific Cisco access point.  Use the <b>no</b> form of the command to enable the radio.
<b>Step 4</b>	<b>ap name <i>ap-name</i> dot11 dual-band role manual client-serving</b> <b>Example:</b> Device# ap name <i>ap-name</i> dot11 dual-band role manual client-serving	Switchs to client-serving mode on the Cisco access point.
<b>Step 5</b>	<b>ap name <i>ap-name</i> dot11 dual-band band 24ghz</b> <b>Example:</b> Device# ap name <i>ap-name</i> dot11 dual-band band 24ghz	Switchs to 2.4-GHz radio band.
<b>Step 6</b>	<b>ap name <i>ap-name</i> dot11 dual-band txpower {<i>transmit_power_level</i>   auto}</b> <b>Example:</b>	Configures the transmit power for the radio on a specific Cisco access point.

	Command or Action	Purpose
	<pre>Device# ap name <i>ap-name</i> dot11 dual-band txpower 2</pre>	<p><b>Note</b> When an FRA-capable radio (slot 0 on 9120 AP[for instance]) is set to Auto, you cannot configure static channel and Txpower on this radio.</p> <p>If you want to configure static channel and Txpower on this radio, you will need to change the radio role to Manual Client-Serving mode.</p>
<b>Step 7</b>	<p><b>ap name <i>ap-name</i> dot11 dual-band channel <i>channel-number</i></b></p> <p><b>Example:</b></p> <pre>Device# ap name <i>ap-name</i> dot11 dual-band channel 2</pre>	<p>Enters the channel for the dual band.</p> <p><i>channel-number</i>—The valid range is from 1 to 173.</p>
<b>Step 8</b>	<p><b>ap name <i>ap-name</i> dot11 dual-band channel auto</b></p> <p><b>Example:</b></p> <pre>Device# ap name <i>ap-name</i> dot11 dual-band channel auto</pre>	<p>Enables the auto channel assignment for the dual-band.</p>
<b>Step 9</b>	<p><b>ap name <i>ap-name</i> dot11 dual-band channel width {20 MHz   40 MHz   80 MHz   160 MHz}</b></p> <p><b>Example:</b></p> <pre>Device# ap name <i>ap-name</i> dot11 dual-band channel width 20 MHz</pre>	<p>Chooses the channel width for the dual band.</p>
<b>Step 10</b>	<p><b>ap name <i>ap-name</i> dot11 dual-band cleanair</b></p> <p><b>Example:</b></p> <pre>Device# ap name <i>ap-name</i> dot11 dual-band cleanair</pre>	<p>Enables the Cisco CleanAir feature on the dual-band radio.</p>
<b>Step 11</b>	<p><b>ap name <i>ap-name</i> dot11 dual-band cleanair band {24 GHz   5 GMHz}</b></p> <p><b>Example:</b></p> <pre>Device# ap name <i>ap-name</i> dot11 dual-band cleanair band 5 GHz  Device# ap name <i>ap-name</i> [no] dot11 dual-band cleanair band 5 GHz</pre>	<p>Selects a band for the Cisco CleanAir feature.</p> <p>Use the <b>no</b> form of this command to disable the Cisco CleanAir feature.</p>
<b>Step 12</b>	<p><b>ap name <i>ap-name</i> dot11 dual-band dot11n antenna {A   B   C   D}</b></p> <p><b>Example:</b></p> <pre>Device# ap name <i>ap-name</i> dot11 dual-band dot11n antenna A</pre>	<p>Configures the 802.11n dual-band parameters for a specific access point.</p>

	Command or Action	Purpose
<b>Step 13</b>	<b>show ap name <i>ap-name</i> auto-rf dot11 dual-band</b>  <b>Example:</b> <pre>Device# show ap name <i>ap-name</i> auto-rf dot11 dual-band</pre>	Displays the auto-RF information for the Cisco access point.
<b>Step 14</b>	<b>show ap name <i>ap-name</i> wlan dot11 dual-band</b>  <b>Example:</b> <pre>Device# show ap name <i>ap-name</i> wlan dot11 dual-band</pre>	Displays the list of BSSIDs for the Cisco access point.

## Configuring XOR Radio Support for the Specified Slot Number (GUI)

### Procedure

- 
- Step 1** Click **Configuration > Wireless > Access Points**.
- Step 2** In the **Dual-Band Radios** section, select the AP for which you want to configure dual-band radios.
- The AP name, MAC address, CleanAir capability and slot information for the AP are displayed. If the Hyperlocation method is HALO, the antenna PID and antenna design information are also displayed.
- Step 3** Click **Configure**.
- Step 4** In the **General** tab, set the **Admin Status** as required.
- Step 5** Set the **CleanAir Admin Status** field to Enable or Disable.
- Step 6** Click **Update & Apply to Device**.
- 

## Configuring XOR Radio Support for the Specified Slot Number

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> <pre>Device# enable</pre>	Enters privileged EXEC mode.



	Command or Action	Purpose
Step 2	<b>ap name <i>ap-name</i> dot11 dual-band slot 0 antenna ext-ant-gain <i>external_antenna_gain_value</i></b> <b>Example:</b> <pre>Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 antenna ext-ant-gain 2</pre>	Configures dual-band antenna for the XOR radio hosted on slot 0 for a specific access point.  <i>external_antenna_gain_value</i> - Is the external antenna gain value in multiples of .5 dBi unit. The valid range is from 0 to 40.
Step 3	<b>ap name <i>ap-name</i> dot11 dual-band slot 0 band {24ghz   5ghz}</b> <b>Example:</b> <pre>Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 band 24ghz</pre>	Configures current band for the XOR radio hosted on slot 0 for a specific access point.
Step 4	<b>ap name <i>ap-name</i> dot11 dual-band slot 0 channel {<i>channel_number</i>   auto   width [160   20   40   80]}</b> <b>Example:</b> <pre>Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 channel 3</pre>	Configures dual-band channel for the XOR radio hosted on slot 0 for a specific access point.  <i>channel_number</i> - The valid range is from 1 to 165.
Step 5	<b>ap name <i>ap-name</i> dot11 dual-band slot 0 cleanair band {24Ghz   5Ghz}</b> <b>Example:</b> <pre>Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 cleanair band 24Ghz</pre>	Enables CleanAir features for dual-band radios hosted on slot 0 for a specific access point.
Step 6	<b>ap name <i>ap-name</i> dot11 dual-band slot 0 dot11n antenna {A   B   C   D}</b> <b>Example:</b> <pre>Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 dot11n antenna A</pre>	Configures 802.11n dual-band parameters hosted on slot 0 for a specific access point.  Here, <b>A</b> - Enables antenna port A. <b>B</b> - Enables antenna port B. <b>C</b> - Enables antenna port C. <b>D</b> - Enables antenna port D.
Step 7	<b>ap name <i>ap-name</i> dot11 dual-band slot 0 role {auto   manual [<i>client-serving</i>   monitor]}</b> <b>Example:</b> <pre>Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 role auto</pre>	Configures dual-band role for the XOR radio hosted on slot 0 for a specific access point.  The following are the dual-band roles: <ul style="list-style-type: none"> <li>• <b>auto</b>- Refers to the automatic radio role selection.</li> <li>• <b>manual</b>- Refers to the manual radio role selection.</li> </ul>
Step 8	<b>ap name <i>ap-name</i> dot11 dual-band slot 0 shutdown</b>	Disables dual-band radio hosted on slot 0 for a specific access point.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 shutdown</pre> <pre>Device# ap name AP-SIDD-A06 [no] dot11 dual-band slot 0 shutdown</pre>	Use the <b>no</b> form of this command to enable the dual-band radio.
<b>Step 9</b>	<p><b>ap name</b> <i>ap-name</i> <b>dot11 dual-band slot 0 txpower</b> {<i>tx_power_level</i>   <b>auto</b>}</p> <p><b>Example:</b></p> <pre>Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 txpower 2</pre>	<p>Configures dual-band transmit power for XOR radio hosted on slot 0 for a specific access point.</p> <ul style="list-style-type: none"> <li>• <i>tx_power_level</i>- Is the transmit power level in dBm. The valid range is from 1 to 8.</li> <li>• <b>auto</b>- Enables auto-RF.</li> </ul>



## CHAPTER 16

# Cisco Receiver Start of Packet

- [Information About Receiver Start of Packet Detection Threshold](#), on page 127
- [Restrictions for Rx SOP](#), on page 127
- [Configuring Rx SOP \(CLI\)](#), on page 128
- [Customizing RF Profile \(CLI\)](#), on page 128

## Information About Receiver Start of Packet Detection Threshold

The Receiver Start of Packet (Rx SOP) Detection Threshold feature determines the Wi-Fi signal level in dBm at which an access point's radio demodulates and decodes a packet. As the Wi-Fi level increases, the radio sensitivity decreases and the receiver cell size becomes smaller. Reduction of the cell size affects the distribution of clients in the network.

Rx SOP is used to address clients with weak RF links, sticky clients, and client load balancing across access points. Rx SOP helps to optimize the network performance in high-density deployments, such as stadiums and auditoriums where access points need to optimize the nearest and strongest clients.

## Restrictions for Rx SOP

- Rx SOP configuration is not applicable to the third radio module pluggable on Cisco Aironet Series APs.
- Rx SOP configurations are supported only in Local, FlexConnect, Bridge, and Flex+Bridge modes.
- Rx SOP configurations are not supported in the FlexConnect+PPPoE, FlexConnect+PPPoE-wIPS, and FlexConnect+OEAP submodes.

The following table shows the permitted range for the Rx SOP threshold.

**Table 3: Rx SOP Threshold**

Radio Band	Threshold High	Threshold Medium	Threshold Low
2.4 GHz	-79 dBm	-82 dBm	-85 dBm
5 GHz	-76 dBm	-78 dBm	-80 dBm

## Configuring Rx SOP (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ap dot11 {24ghz   5ghz} rx-sop threshold {auto   custom   high   low   medium}</b> <b>Example:</b> Device(config)# <code>ap dot11 5ghz rx-sop threshold high</code>	Configures the 802.11bg/802.11a radio Rx SOP threshold.
<b>Step 3</b>	<code>end</code>	Returns to privileged EXEC mode.
<b>Step 4</b>	<b>show ap dot11 {24ghz   5ghz} high-density</b> <b>Example:</b> Device# <code>show ap dot11 5ghz high-density</code>	Displays the 802.11bg/802.11a high-density parameters.
<b>Step 5</b>	<b>show ap summary</b> <b>Example:</b> Device# <code>show ap summary</code>	Displays a summary of all the connected Cisco APs.

## Customizing RF Profile (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ap dot11 {24ghz   5ghz } rf-profile <i>profile-name</i></b> <b>Example:</b> Device(config)# <code>ap dot11 24ghz rf-profile AHS_2.4ghz</code>	Configures the 802.11a and 11b parameters.

	Command or Action	Purpose
<b>Step 3</b>	<b>high-density rx-sop threshold {auto   custom   high   low   medium}</b> <b>Example:</b> Device(config-rf-profile)# <b>high-density rx-sop threshold high</b>	Configures the 802.11bg, 802.11a high-density parameters.
<b>Step 4</b>	<b>show ap summary</b> <b>Example:</b> Device# <b>show ap summary</b>	Displays a summary of all the connected Cisco APs.
<b>Step 5</b>	end	Returns to privileged EXEC mode. <b>Note</b> <ul style="list-style-type: none"> <li>• Irrespective of radio mode, the controller configures the radio with configured RX-SOP value. The AP determines whether to use the configured RX-SOP value.</li> <li>• For the XOR radio (Slot 0), when the AP is in monitor mode the RX-SOP value that gets pushed to AP depends on the band it was operating before moving to monitor mode (basically if radio operating band is 24g then RX-SOP params picked from 24GHz RF profile (or default rf-profile). If it was in 5g then RX-SOP params picked from 5GHz RF profile (or default rf-profile) configured for the AP).</li> </ul>





# CHAPTER 17

## Client Limit

- [Information About Client Limit](#), on page 131
- [Configuring Client Limit Per WLAN \(GUI\)](#), on page 131
- [Configuring Client Limit Per WLAN \(CLI\)](#), on page 131

### Information About Client Limit

This feature enforces a limit on the number of clients that can be associated with an AP. Further, you can configure the number of clients that can be associated with each AP radio.

### Configuring Client Limit Per WLAN (GUI)

#### Procedure

- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** Click a WLAN from the list of WLANs.
- Step 3** Click the **Advanced** tab.
- Step 4** Under the **Max Client Connections** settings, enter the client limit for **Per WLAN**, **Per AP Per WLAN**, and **Per AP Radio Per WLAN**.
- Step 5** Click **Update & Apply to Device**.

### Configuring Client Limit Per WLAN (CLI)

#### Procedure

	Command or Action	Purpose
Step 1	enable Example:	Enters privileged EXEC mode.

	Command or Action	Purpose
	Device# <b>enable</b>	
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>wlan wlan-name</b> <b>Example:</b> Device(config)# <b>wlan ramban</b>	Specifies the WLAN name.
<b>Step 4</b>	<b>client association limit</b> <i>maximum-clients-per-WLAN</i> <b>Example:</b> Device(config-wlan)# <b>client association limit 110</b>	Configures the maximum number of clients that can be associated to the given WLAN.  <b>Note</b> Depending on the primary AP in the Cisco Embedded Wireless Controller network, the maximum number of clients supported varies. For more information about the client count limit per WLAN in a Cisco Embedded Wireless Controller network, see <a href="#">Table 4: Scale Supported in a Cisco Embedded Wireless Controller Network</a> , on page 132  <b>Table 4: Scale Supported in a Cisco Embedded Wireless Controller Network</b>
<b>Step 5</b>	<b>client association limit ap</b> <i>max-clients-per-AP-per-WLAN</i> <b>Example:</b> Device(config-wlan)# <b>client association limit ap 120</b>	Configures the maximum number of clients that can be associated to an AP in the WLAN.
<b>Step 6</b>	<b>client association limit radio</b> <i>max-clients-per-AP-radio-per-WLAN</i> <b>Example:</b> Device(config-wlan)# <b>client association limit radio 100</b>	Configures the maximum number of clients that can be associated to an AP radio in the WLAN.
<b>Step 7</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.
<b>Step 8</b>	<b>show wlan id wlan-id</b> <b>Example:</b> Device# <b>show wlan id 2</b>	Displays the current configuration of the WLAN and the corresponding client association limits.





## CHAPTER 18

# IP Theft

---

- [Introduction to IP Theft, on page 133](#)
- [Configuring IP Theft \(GUI\), on page 134](#)
- [Configuring IP Theft, on page 134](#)
- [Configuring the IP Theft Exclusion Timer, on page 134](#)
- [Verifying IP Theft Configuration, on page 135](#)

## Introduction to IP Theft

The IP Theft feature prevents the usage of an IP address that is already assigned to another device. If the controller finds that two wireless clients are using the same IP address, it declares the client with lesser precedence binding as the IP thief and allows the other client to continue. If blocked list is enabled, the client is put on the exclusion list and thrown out.

The IP Theft feature is enabled by default on the controller. The preference level of the clients (new and existing clients in the database) are also used to report IP theft. The preference level is a learning type or source of learning, such as Dynamic Host Configuration Protocol (DHCP), Address Resolution Protocol (ARP), data glean (looking at the IP data packet that shows what IP address the client is using), and so on. The wired clients always get a higher preference level. If a wireless client tries to steal the wired IP, that client is declared as a thief.

The order of preference for IPv4 clients are:

1. DHCPv4
2. ARP
3. Data packets

The order of preference for IPv6 clients are:

1. DHCPv6
2. NDP
3. Data packets



---

**Note** The static wired clients have a higher preference over DHCP.

---

## Configuring IP Theft (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Security > Wireless Protection Policies > Client Exclusion Policies**.
  - Step 2** Check the **IP Theft or IP Reuse** check box.
  - Step 3** Click **Apply**.
- 

## Configuring IP Theft

Follow the procedure given below to configure the IP Theft feature:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless wps client-exclusion ip-theft</b>  <b>Example:</b> Device(config)# wireless wps client-exclusion ip-theft	Configures the client exclusion policy.

## Configuring the IP Theft Exclusion Timer

Follow the procedure given below to configure the IP theft exclusion timer:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile policy <i>profile-policy</i></b>  <b>Example:</b> Device(config)# wireless profile policy default-policy-profile	Configures a WLAN policy profile and enters wireless policy configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>exclusionlist timeout</b> <i>time-in-seconds</i> <b>Example:</b> Device(config-wireless-policy)# exclusionlist timeout 5	Specifies the timeout, in seconds. The valid range is from 0-2147483647. Enter zero (0) for no timeout.

## Verifying IP Theft Configuration

Use the following command to check if the IP Theft feature is enabled or not:

```
Device# show wireless wps summary

Client Exclusion Policy
  Excessive 802.11-association failures : Enabled
  Excessive 802.11-authentication failures: Enabled
  Excessive 802.1x-authentication      : Enabled
  IP-theft                             : Enabled
  Excessive Web authentication failure : Enabled
  Cids Shun failure                    : Enabled
  Misconfiguration failure             : Enabled
  Failed Qos Policy                    : Enabled
  Failed Epm                           : Enabled
```

Use the following commands to view additional details about the IP Theft feature:

```
Device# show wireless client summary

Number of Local Clients: 1

MAC Address      AP Name          WLAN State      Protocol Method  Role
-----
000b.bbb1.0001  SimAP-1         2 Run           11a      None      Local

Number of Excluded Clients: 1

MAC Address      AP Name          WLAN State      Protocol Method
-----
10da.4320.cce9  charlie2        2 Excluded      11ac     None

Device# show wireless device-tracking database ip

IP              VLAN  STATE      DISCOVERY  MAC
-----
20.20.20.2     20   Reachable  Local      001e.14cc.cbff
20.20.20.6     20   Reachable  IPv4 DHCP  000b.bbb1.0001

Device# show wireless exclusionlist

Excluded Clients

MAC Address      Description          Exclusion Reason      Time Remaining
-----
10da.4320.cce9          IP address theft      59
```

```
Device# show wireless exclusionlist client mac 12da.4820.cce9 detail
```

```
Client State : Excluded  
Client MAC Address : 12da.4820.cce9  
Client IPv4 Address: 20.20.20.6  
Client IPv6 Address: N/A  
Client Username: N/A  
Exclusion Reason : IP address theft  
Authentication Method : None  
Protocol: 802.11ac  
AP MAC Address : 58ac.780e.08f0  
AP Name: charlie2  
AP slot : 1  
Wireless LAN Id : 2  
Wireless LAN Name: mhe-ewlc  
VLAN Id : 20
```



## CHAPTER 19

# Unscheduled Automatic Power Save Delivery

- [Information About Unscheduled Automatic Power Save Delivery, on page 137](#)
- [Viewing Unscheduled Automatic Power Save Delivery \(CLI\), on page 137](#)

## Information About Unscheduled Automatic Power Save Delivery

Unscheduled automatic power save delivery (U-APSD) is a QoS facility that is defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending the battery life, this feature reduces the latency of traffic flow that is delivered over the wireless media. Because U-APSD does not require the client to poll each individual packet that is buffered at the access point, it allows delivery of multiple downlink packets by sending a single uplink trigger packet.

U-APSD is enabled automatically when WMM is enabled.

## Viewing Unscheduled Automatic Power Save Delivery (CLI)

### Procedure

```
show wireless client mac-address client_mac detail
```

### Example:

```
Device# show wireless client mac-address 2B:5B:B3:18:56:E9 detail
Output Policy State : Unknown
Output Policy Source : Unknown
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 15
  APSD ACs    : BK(T/D), BE, VI(T/D), VO(T/D)
Power Save : OFF
Current Rate :

-----
BK : Background
BE : Best Effort
VI : Video
VO : Voice.

T: UAPSD Trigger Enabled
```

```
D: UAPSD Delivery Enabled  
T/D : UAPSD Trigger and Delivery Enabled
```

Show detailed information of a client by MAC address.

---



## CHAPTER 20

# Enabling USB Port on Access Points

- [USB Port as Power Source for Access Points](#), on page 139
- [Configuring an AP Profile \(CLI\)](#), on page 140
- [Configuring USB Settings for an Access Point \(CLI\)](#), on page 140
- [Monitoring USB Configurations for Access Points \(CLI\)](#), on page 141

## USB Port as Power Source for Access Points

Some Cisco APs have a USB port that can act as a source of power for some USB devices. The power can be up to 2.5W; if a USB device draws more than 2.5W of power, the USB port shuts down automatically. The port is enabled when the power draw is 2.5W and lower. Refer to the datasheet of your AP to check if the AP has a USB port that can act as a source of power.



---

**Note** The controller records the last five power-overdrawn incidents in its logs.

---



---

**Caution** When unsupported USB device is connected to the Cisco AP, the following message is displayed:

```
The inserted USB module is not a supported device. The behavior of
this USB device and the impact to the Access Point is not guaranteed.
If Cisco determines that a fault or defect can be isolated due to the
use of third-party USB modules installed by a customer or reseller,
Cisco may withhold support under warranty or support program under
contract. In the course of providing support for Cisco networking
products, the end user may be required to install Cisco-supported USB
modules in the event Cisco determines that removing third-party parts
will assist Cisco in diagnosing root cause for troubleshooting
purposes. Cisco also reserves the right to charge the customer per
then-current time and material rates for services provided to the
customer when Cisco determines, after having provided such services,
that an unsupported device caused the root cause of the defective
product
```

---

## Configuring an AP Profile (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ap profile <i>ap-profile</i></b>  <b>Example:</b> Device(config)# <code>ap profile xyz-ap-profile</code>	Configures an AP profile and enters the AP profile configuration mode.  <b>Note</b> When you delete a named profile, the APs associated with that profile will not revert to the default profile.
<b>Step 3</b>	<b>usb-enable</b>  <b>Example:</b> Device(config-ap-profile)# <code>usb-enable</code>	Enables USB for each AP profile.  <b>Note</b> By default, the USB for each AP profile is enabled.  Use the <b>no usb-enable</b> command to disable USB for each AP profile.
<b>Step 4</b>	<b>end</b>  <b>Example:</b> Device(config-ap-profile)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring USB Settings for an Access Point (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device# <code>enable</code>	Enters privileged EXEC mode.
<b>Step 2</b>	<b>ap name <i>ap-name</i> usb-module</b>  <b>Example:</b> Device# <code>ap name AP44d3.xy45.69a1 usb-module</code>	Enables the USB port on the AP.  Use the <b>ap name <i>ap-name</i> no usb-module</b> command to disable the USB port on the AP.
<b>Step 3</b>	<b>ap name <i>ap-name</i> usb-module override</b>  <b>Example:</b>	Overrides USB status of the AP profile and considers the local AP configuration.



	Command or Action	Purpose
	Device# <b>ap name AP44d3.xy45.69a1 usb-module override</b>	Use the <b>ap name <i>ap-name</i> no usb-module override</b> command to override USB status of the AP and consider the AP profile configuration.  <b>Note</b> You can configure the USB status for an AP only if you enable USB override for it.

## Monitoring USB Configurations for Access Points (CLI)

- To view the inventory details of APs, use the following command:

**show ap name *ap-name* inventory**

The following is a sample output:

```
Device# show ap name AP500F.8059.1620 inventory
NAME: AP2800 , DESCR: Cisco Aironet 2800 Series (IEEE 802.11ac) Access Point
PID: AIR-AP2802I-D-K9 , VID: 01, SN: XXX1111Y2ZZZZ2800
NAME: SanDisk , DESCR: Cruzer Blade
PID: SanDisk , SN: XXXX1110010, MaxPower: 224
```

- To view the summary of an AP module, use the following command:

**show ap module summary**

The following is a sample output:

```
Device# show ap module summary
AP Name           External Module      External Module PID  External Module
Description
-----
AP500F.1111.2222  Enable              SanDisk              Cruzer Blade
```

- To view the USB configuration details for each AP, use the following command:

**show ap name *ap-name* config general**

The following is a sample output:

```
Device# show ap name AP500F.111.2222 config general
.
.
.
USB Module Type..... USB Module
USB Module Status..... Disabled
USB Module Operational State..... Enabled
USB Override ..... Enabled
```

- To view status of the USB module, use the following command:

**show ap profile name *xyz* detailed**

The following is a sample output:

```
Device# show ap profile name xyz detailed
USB Module           : ENABLED
```





## PART **IV**

# Network Management

- [DHCP Option82, on page 145](#)
- [RADIUS Realm, on page 155](#)
- [Persistent SSID Broadcast, on page 161](#)
- [Network Monitoring, on page 163](#)





## CHAPTER 21

# DHCP Option82

- [Information About DHCP Option 82, on page 145](#)
- [Configuring DHCP Option 82 Global Interface, on page 146](#)
- [Configuring DHCP Option 82 Format, on page 148](#)
- [Configuring DHCP Option82 Through a VLAN Interface, on page 149](#)

## Information About DHCP Option 82

The embedded wireless controller can be configured to add Option 82 information to DHCP requests from clients before forwarding the requests to a DHCP server. The DHCP server can then be configured to allocate IP addresses to the wireless client based on the information present in DHCP Option 82.

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that are stored in the Options field of the DHCP message. The data items themselves are also called options. Option 82 contains information known by the relay agent.

The Relay Agent Information option is organized as a single DHCP option that contains one or more suboptions that convey information known by the relay agent. Option 82 was designed to allow a DHCP Relay Agent to insert circuit-specific information into a request that is being forwarded to a DHCP server. This option works by setting two suboptions:

- Circuit ID
- Remote ID

The Circuit ID suboption includes information that is specific to the circuit the request came in on. This suboption is an identifier that is specific to the relay agent. Thus, the circuit that is described will vary depending on the relay agent.

The Remote ID suboption includes information on the remote host-end of the circuit. This suboption usually contains information that identifies the relay agent. In a wireless network, this would likely be a unique identifier of the wireless access point.

You can configure the following DHCP Option 82 options in a embedded wireless controller:

- DHCP Enable
- DHCP Opt82 Enable
- DHCP Opt82 Ascii

- DHCP Opt82 RID
- DHCP Opt Format
- DHCP AP MAC
- DHCP SSID
- DHCP AP ETH MAC
- DHCP AP NAME
- DHCP Site Tag
- DHCP AP Location
- DHCP VLAN ID



**Note** For Cisco Catalyst 9800 Series Configuration Best Practices, see the following link:  
<https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/guide-c07-743627.html>

## Configuring DHCP Option 82 Global Interface

### Configuring DHCP Option 82 Globally Through Server Override (CLI)

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b>  Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ip dhcp-relay information option server-override</b>  <b>Example:</b>  Device(config)# <code>ip dhcp-relay information option server-override</code>	Inserts global server override and link selection suboptions.

## Configuring DHCP Option 82 Globally Through Different SVIs (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > VLAN**.
- Step 2** Choose a VLAN from the drop-down list.  
The **Edit SVI** window appears.
- Step 3** Click the **Advanced** tab.
- Step 4** Choose an option from the **IPv4 Inbound ACL** drop-down list.
- Step 5** Choose an option from the **IPv4 Outbound ACL** drop-down list.
- Step 6** Choose an option from the **IPv6 Inbound ACL** drop-down list.
- Step 7** Choose an option from the **IPv6 Outbound ACL** drop-down list.
- Step 8** Enter an IP address in the **IPv4 Helper Address** field.
- Step 9** Set the status to **Enabled** if you want to enable the **Relay Information Option** setting.
- Step 10** Enter the **Subscriber ID**.
- Step 11** Set the status to **Enabled** if you want to enable the **Server ID Override** setting.
- Step 12** Set the status to **Enabled** if you want to enable the **Option Insert** setting.
- Step 13** Choose an option from the **Source-Interface Vlan** drop-down list.
- Step 14** Click **Update & Apply to Device**.
- 

## Configuring DHCP Option 82 Globally Through Different SVIs (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b>  Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ip dhcp-relay source-interface vlan <i>vlan-id</i></b>  <b>Example:</b>  Device(config)# <code>ip dhcp-relay source-interface vlan 74</code>	Sets global source interface for relayed messages.

# Configuring DHCP Option 82 Format

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile policy</b> <i>policy-name</i> <b>Example:</b> Device (config) # <b>wireless profile policy</b> <i>pp3</i>	Enables configuration for the specified profile policy.
<b>Step 3</b>	<b>shutdown</b> <b>Example:</b> Device (config-wireless-policy) # <b>shutdown</b>	Shuts down the profile policy.
<b>Step 4</b>	<b>vlan</b> <i>vlan-name</i> <b>Example:</b> Device (config-wireless-policy) # <b>vlan 72</b>	Assigns the profile policy to a VLAN.
<b>Step 5</b>	<b>session-timeout</b> <i>value-btwn-20-86400</i> <b>Example:</b> Device (config-wireless-policy) # <b>session-timeout 300</b>	(Optional) Sets the session timeout value in seconds. The range is between 20-86400.
<b>Step 6</b>	<b>idle-timeout</b> <i>value-btwn-15-100000</i> <b>Example:</b> Device (config-wireless-policy) # <b>idle-timeout 15</b>	(Optional) Sets the idle timeout value in seconds. The range is between 15-100000.
<b>Step 7</b>	<b>central switching</b> <b>Example:</b> Device (config-wireless-policy) # <b>central</b> <b>switching</b>	Enables central switching.
<b>Step 8</b>	<b>ipv4 dhcp opt82</b> <b>Example:</b> Device (config-wireless-policy) # <b>ipv4</b> <b>dhcp opt82</b>	Enables DHCP Option 82 for the wireless clients.
<b>Step 9</b>	<b>ipv4 dhcp opt82 ascii</b> <b>Example:</b>	(Optional) Enables ASCII on the DHCP Option 82 feature.



	Command or Action	Purpose
	Device(config-wireless-policy) # <b>ipv4 dhcp opt82 ascii</b>	
<b>Step 10</b>	<b>ipv4 dhcp opt82 rid</b> <b>Example:</b> Device(config-wireless-policy) # <b>ipv4 dhcp opt82 rid</b>	(Optional) Supports the addition of Cisco 2 byte Remote ID (RID) for the DHCP Option 82 feature.
<b>Step 11</b>	<b>ipv4 dhcp opt82 format</b> <b>{ap_mac ap_hostname apmac aname policy sid vlan_id}</b> <b>Example:</b> Device(config-wireless-policy) # <b>ipv4 dhcp opt82 format apmac</b>	Enables DHCP Option 82 on the corresponding AP.  For information on the various options available with the command, see <a href="#">Cisco Catalyst 9800 Series Wireless Controller Command Reference</a> .
<b>Step 12</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wireless-policy) # <b>no shutdown</b>	Enables the profile policy.

## Configuring DHCP Option82 Through a VLAN Interface

### Configuring DHCP Option 82 Through Option-Insert Command (CLI)

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>interface vlan <i>vlan-id</i></b> <b>Example:</b> Device(config) # <b>interface vlan 72</b>	Configures a VLAN ID.
<b>Step 3</b>	<b>ip dhcp relay information option-insert</b> <b>Example:</b> Device(config-if) # <b>ip dhcp relay information option-insert</b>	Inserts relay information in BOOTREQUEST.
<b>Step 4</b>	<b>ip address <i>ip-address</i></b> <b>Example:</b>	Configures the IP address for the interface.

	Command or Action	Purpose
	Device(config-if)# <b>ip address</b> 9.3.72.38 255.255.255.0	
<b>Step 5</b>	<b>ip helper-address</b> <i>ip-address</i>  <b>Example:</b> Device(config-if)# <b>ip helper-address</b> 9.3.72.1	Configures the destination address for UDP broadcasts.
<b>Step 6</b>	<b>[no] mop enabled</b>  <b>Example:</b> Device(config-if)# <b>no mop enabled</b>	Disables the MOP for an interface.
<b>Step 7</b>	<b>[no] mop sysid</b>  <b>Example:</b> Device(config-apgroup)# <b>[no] mop sysid</b>	Disables the task of sending MOP periodic system ID messages.

## Configuring DHCP Option 82 Through the server-ID-override Command (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>ip dhcp compatibility suboption server-override cisco</b>  <b>Example:</b> Device(config)# <b>ip dhcp compatibility suboption server-override cisco</b>	Configures the server-id override suboption to an RFC or Cisco specific value.
<b>Step 3</b>	<b>ip dhcp compatibility suboption link-selection cisco</b>  <b>Example:</b> Device(config)# <b>ip dhcp compatibility suboption link-selection cisco</b>	Configures the link-selection suboption to an RFC or Cisco specific value.
<b>Step 4</b>	<b>interface vlan</b> <i>vlan-id</i>  <b>Example:</b> Device(config)# <b>interface vlan</b> 72	Configures a VLAN ID.
<b>Step 5</b>	<b>ip dhcp relay information option server-id-override</b>  <b>Example:</b>	Inserts the server id override and link selection suboptions.

	Command or Action	Purpose
	<code>Device(config-if)# ip dhcp relay information option server-id-override</code>	
<b>Step 6</b>	<b>ip address</b> <i>ip-address</i> <b>Example:</b> <code>Device(config-if)# ip address 9.3.72.38 255.255.255.0</code>	Configures the IP address for the interface.
<b>Step 7</b>	<b>ip helper-address</b> <i>ip-address</i> <b>Example:</b> <code>Device(config-if)# ip helper-address 9.3.72.1</code>	Configures the destination address for UDP broadcasts.
<b>Step 8</b>	<b>[no] mop enabled</b> <b>Example:</b> <code>Device(config-if)# no mop enabled</code>	Disables MOP for an interface.
<b>Step 9</b>	<b>[no] mop sysid</b> <b>Example:</b> <code>Device(config-if)# [no] mop sysid</code>	Disables the task of sending MOP periodic system ID messages.

## Configuring DHCP Option 82 Through a Subscriber-ID (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <code>Device# configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>interface vlan</b> <i>vlan-id</i> <b>Example:</b> <code>Device(config)# interface vlan 72</code>	Configures a VLAN ID.
<b>Step 3</b>	<b>ip dhcp relay information option subscriber-id</b> <i>subscriber-id</i> <b>Example:</b> <code>Device(config-if)# ip dhcp relay information option subscriber-id test10</code>	Inserts the subscriber identifier suboption.
<b>Step 4</b>	<b>ip address</b> <i>ip-address</i> <b>Example:</b>	Configures the IP address for the interface.

	Command or Action	Purpose
	Device(config-if)# <b>ip address</b> 9.3.72.38 255.255.255.0	
<b>Step 5</b>	<b>ip helper-address</b> <i>ip-address</i>  <b>Example:</b> Device(config-if)# <b>ip helper-address</b> 9.3.72.1	Configures the destination address for UDP broadcasts.
<b>Step 6</b>	<b>[no] mop enabled</b>  <b>Example:</b> Device(config-if)# <b>no mop enabled</b>	Disables MOP for an interface.
<b>Step 7</b>	<b>[no] mop sysid</b>  <b>Example:</b> Device(config-apgroup)# <b>[no] mop sysid</b>	Disables the task of sending MOP periodic system ID messages.

## Configuring DHCP Option 82 Through server-ID-override and subscriber-ID Commands (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>interface vlan</b> <i>vlan-id</i>  <b>Example:</b> Device(config)# <b>interface vlan</b> 72	Configures a VLAN ID.
<b>Step 3</b>	<b>ip dhcp relay information option server-id-override</b>  <b>Example:</b> Device(config-if)# <b>ip dhcp relay information option server-id-override</b>	Inserts server ID override and link selection suboptions.
<b>Step 4</b>	<b>ip dhcp relay information option subscriber-id</b> <i>subscriber-id</i>  <b>Example:</b> Device(config-if)# <b>ip dhcp relay information option subscriber-id test10</b>	Inserts the subscriber identifier suboption.

	Command or Action	Purpose
<b>Step 5</b>	<b>ip address</b> <i>ip-address</i> <b>Example:</b> Device(config-if)# <b>ip address 9.3.72.38</b> 255.255.255.0	Configures the IP address for the interface.
<b>Step 6</b>	<b>ip helper-address</b> <i>ip-address</i> <b>Example:</b> Device(config-if)# <b>ip helper-address</b> 9.3.72.1	Configures the destination address for UDP broadcasts.
<b>Step 7</b>	<b>[no] mop enabled</b> <b>Example:</b> Device(config-if)# <b>no mop enabled</b>	Disables the MOP for an interface.
<b>Step 8</b>	<b>[no] mop sysid</b> <b>Example:</b> Device(config-apgroup)# <b>[no] mop sysid</b>	Disables the task of sending MOP periodic system ID messages.

## Configuring DHCP Option 82 Through Different SVIs (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>interface vlan</b> <i>vlan-id</i> <b>Example:</b> Device(config)# <b>interface vlan 72</b>	Configures a VLAN ID.
<b>Step 3</b>	<b>ip dhcp relay source-interface</b> <i>vlan vlan-id</i> <b>Example:</b> Device(config-if)# <b>ip dhcp relay</b> <b>source-interface vlan 74</b>	Configures a source interface for relayed messages on a VLAN ID.
<b>Step 4</b>	<b>ip address</b> <i>ip-address</i> <b>Example:</b> Device(config-if)# <b>ip address 9.3.72.38</b> 255.255.255.0	Configures the IP address for the interface.

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 5</b>	<b>ip helper-address</b> <i>ip-address</i> <b>Example:</b> Device(config-if) # <b>ip helper-address</b> <b>9.3.72.1</b>	Configure the destination address for UDP broadcasts.
<b>Step 6</b>	<b>[no] mop enabled</b> <b>Example:</b> Device(config-if) # <b>no mop enabled</b>	Disables the MOP for an interface.
<b>Step 7</b>	<b>[no] mop sysid</b> <b>Example:</b> Device(config-apgroup) # <b>[no] mop sysid</b>	Disables the task of sending MOP periodic system ID messages.



## CHAPTER 22

# RADIUS Realm

- [Information About RADIUS Realm, on page 155](#)
- [Enabling RADIUS Realm, on page 156](#)
- [Configuring Realm to Match the RADIUS Server for Authentication and Accounting, on page 156](#)
- [Configuring the AAA Policy for a WLAN, on page 157](#)
- [Verifying the RADIUS-Realm Configuration, on page 159](#)

## Information About RADIUS Realm

The RADIUS Realm feature is associated with the domain of the user. Using this feature, a client can choose the RADIUS server through which authentication and accounting is to be processed.

When mobile clients are associated with a WLAN, RADIUS realm is received as a part of Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA) identity response request in the authentication request packet. The Network Access Identifier (NAI) format (EAP-AKA) for WLAN can be specified as *username@domain.com*. The realm in the NAI format is represented after the @ symbol, which is specified as domain.com. If vendor-specific attributes are added as *test*, the NAI format is represented as *test@domain.com*.

The RADIUS Realm feature can be enabled and disabled on a WLAN. If Realm is enabled on a WLAN, the corresponding user should send the username in the NAI format. The embedded wireless controller sends the authentication request to the AAA server only when the realm, which is in the NAI format and is received from the client, is compiled as per the given standards. Apart from authentication, accounting requests are also required to be sent to the AAA server based on realm filtering.

### Realm Support on a WLAN

Each WLAN is configured to support NAI realms. After the realm is enabled on a particular SSID, the lookup is done to match the realms received in the EAP identity response against the configured realms on the RADIUS server. If the client does not send a username with the realm, the default RADIUS server that is configured on the WLAN is used for authentication. If the realm that is received from the client does not match the configured realms on the WLAN, the client is deauthenticated and dropped.

If the RADIUS Realm feature is not enabled on a WLAN, the username that is received as part of the EAP identity request is directly used as the username and the configured RADIUS server is used for authentication and accounting. By default, the RADIUS Realm feature is disabled on WLANs.

- **Realm Match for Authentication:** In dot1x with EAP methods (similar to EAP AKA), the username is received as part of an EAP identity response. A realm is derived from the username and are matched

with the realms that are already configured in the corresponding RADIUS authentication server. If there is a match, the authentication requests are forwarded to the RADIUS server. If there is a mismatch, the client is deauthenticated.

- **Realm Match for Accounting:** A client's username is received through an access-accept message. When accounting messages are triggered, the realm is derived from the corresponding client's username and compared with the accounting realms configured on the RADIUS accounting server. If there is a match, accounting requests are forwarded to the RADIUS server. If there is a mismatch, accounting requests are dropped.

## Enabling RADIUS Realm

Follow the procedure given below to enable RADIUS realm:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless aaa policy <i>aaa-policy</i></b>  <b>Example:</b> Device(config)# wireless aaa policy policy-1	Creates a new AAA policy.
<b>Step 3</b>	<b>aaa-realm enable</b>  <b>Example:</b> Device(config-aaa-policy)# aaa-realm enable	Enables AAA RADIUS realm selection.  <b>Note</b> Use the <b>no aaa-realm enable</b> or the <b>default aaa-realm enable</b> command to disable the RADIUS realm.

## Configuring Realm to Match the RADIUS Server for Authentication and Accounting

Follow the procedure given below to configure the realm to match the RADIUS server for authentication and accounting:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.



	Command or Action	Purpose
<b>Step 2</b>	<b>aaa new-model</b> <b>Example:</b> Device(config)# aaa new-model	Creates a AAA authentication model.
<b>Step 3</b>	<b>aaa authorization network default group radius-server-group</b> <b>Example:</b> Device(config)# aaa authorization network default group aaa_group_name	Sets the authorization method.
<b>Step 4</b>	<b>aaa authentication dot1x realm group radius-server-group</b> <b>Example:</b> Device(config)# aaa authentication dot1x cisco.com group cisco1	Indicates that dot1x must use the realm group RADIUS server.
<b>Step 5</b>	<b>aaa authentication login realm group radius-server-group</b> <b>Example:</b> Device(config)# aaa authentication login cisco.com group cisco1	Defines the authentication method at login.
<b>Step 6</b>	<b>aaa accounting identity realm start-stop group radius-server-group</b> <b>Example:</b> Device(config)# aaa accounting identity cisco.com start-stop group cisco1	Enables accounting to send a start-record accounting notice when a client is authorized, and a stop-record at the end.

## Configuring the AAA Policy for a WLAN

Follow the procedure given below to configure the AAA policy for a WLAN:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless aaa policy aaa-policy-name</b> <b>Example:</b> Device(config)# wireless aaa policy aaa-policy-1	Creates a new AAA policy for wireless.

	Command or Action	Purpose
<b>Step 3</b>	<b>aaa-realm enable</b> <b>Example:</b> Device(config-aaa-policy)# aaa-realm enable	Enables AAA RADIUS server selection by realm.
<b>Step 4</b>	<b>exit</b> <b>Example:</b> Device(config-aaa-policy)# exit	Returns to global configuration mode.
<b>Step 5</b>	<b>wireless profile policy wlan-policy-profile</b> <b>Example:</b> Device(config)# wireless profile policy wlan-policy-a	Configures a WLAN policy profile.
<b>Step 6</b>	<b>aaa-policy aaa-policy</b> <b>Example:</b> Device(config-wireless-policy)# aaa-policy aaa-policy-1	Maps the AAA policy.
<b>Step 7</b>	<b>accounting-list acct-config-realm</b> <b>Example:</b> Device(config-wireless-policy)# accounting-list cisco.com	Sets the accounting list.
<b>Step 8</b>	<b>exit</b> <b>Example:</b> Device(config-wireless-policy)# exit	Returns to global configuration mode.
<b>Step 9</b>	<b>wlan wlan-name wlan-id ssid</b> <b>Example:</b> Device(config)# wlan wlan2 14 wlan-aaa	Configures a WLAN.
<b>Step 10</b>	<b>security dot1x authentication-list auth-list-realm</b> <b>Example:</b> Device(config-wlan)# security dot1x authentication-list cisco.com	Enables the security authentication list for IEEE 802.1x.
<b>Step 11</b>	<b>exit</b> <b>Example:</b> Device(config-wireless-policy)# exit	Returns to global configuration mode.
<b>Step 12</b>	<b>wireless tag policy policy</b> <b>Example:</b> Device(config)# wireless tag policy tag-policy-1	Configures a policy tag.

	Command or Action	Purpose
<b>Step 13</b>	<b>wlan wlan-name policy policy-profile</b>  <b>Example:</b> Device(config-policy-tag)# wlan Abc-wlan policy wlan-policy-a	Maps a policy profile to the WLAN.
<b>Step 14</b>	<b>exit</b>  <b>Example:</b> Device(config-policy-tag)# exit	Returns to global configuration mode.

## Verifying the RADIUS-Realm Configuration

Use the following command to verify the RADIUS-realm configuration:

```
Device# show wireless client mac-address 14bd.61f3.6a24 detail
```

```
Client MAC Address : 14bd.61f3.6a24
Client IPv4 Address : 9.4.113.103
Client IPv6 Addresses : fe80::286e:9fe0:7fa6:8f4
Client Username : sacthoma@cisco.com
AP MAC Address : 4c77.6d79.5a00
AP Name: AP4c77.6d53.20ec
AP slot : 1
Client State : Associated
Policy Profile : name-policy-profile
Flex Profile : N/A
Wireless LAN Id : 3
Wireless LAN Name: ha_realm_WLAN_WPA2_AES_DOT1X
BSSID : 4c77.6d79.5a0f
Connected For : 26 seconds
Protocol : 802.11ac
Channel : 44
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Re-Authentication Timeout : 1800 sec (Remaining time: 1775 sec)
Input Policy Name : None
Input Policy State : None
Input Policy Source : None
Output Policy Name : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs : BK, BE, VI, VO
Fastlane Support : Disabled
Power Save : OFF
Supported Rates : 9.0,18.0,36.0,48.0,54.0
Mobility:
  Move Count : 0
  Mobility Role : Local
  Mobility Roam Type : None
  Mobility Complete Timestamp : 06/12/2018 19:52:35 IST
Policy Manager State: Run
```

```

NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 25 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : No
EAP Type : PEAP
VLAN : 113
Multicast VLAN : 0
Access VLAN : 113
Anchor VLAN : 0
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Interface       : capwap_9040000f
  IIF ID          : 0x9040000f
  Authorized      : TRUE
  Session timeout : 1800
  Common Session ID: 097704090000000DF4607B3B
  Acct Session ID : 0x00000fa2
  Aaa Server Details
  Server IP       : 9.4.23.50
  Auth Method Status List
    Method : Dot1x
      SM State      : AUTHENTICATED
      SM Bend State : IDLE
  Local Policies:
    Service Template : wlan_svc_name-policy-profile_local (priority 254)
      Absolute-Timer : 1800
      VLAN           : 113
  Server Policies:
  Resultant Policies:
    VLAN           : 113
    Absolute-Timer : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Central
FlexConnect Dhcp Status : Central
FlexConnect Authentication : Central
FlexConnect Central Association : No
.
.
.
Fabric status : Disabled
Client Scan Reports
Assisted Roaming Neighbor List

```



## CHAPTER 23

# Persistent SSID Broadcast

- [Persistent SSID Broadcast, on page 161](#)
- [Configuring Persistent SSID Broadcast, on page 161](#)
- [Verifying Persistent SSID Broadcast, on page 162](#)

## Persistent SSID Broadcast

Access Points within a mesh network work as Root Access Points (RAP) or Mesh Access Points (MAP). RAPs have wired connection to the embedded wireless controller and MAPs have wireless connection to the embedded wireless controller. This feature is applicable only to the Cisco Aironet 1542 Access Points in the Flex+Bridge mode.

This feature is about the Root Access Points (RAPs) and Mesh Access Points (MAPs) broadcasting the SSID even when the WAN connectivity is down. This is required in order to isolate the responsibility; whether the fault is with backhaul or with the access wireless network, since there can be different operators owning each part of the network.

RAPs and MAPs broadcast SSID while in standalone mode, as long as the default gateway is reachable.

Also refer [Mesh Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers](#).

## Configuring Persistent SSID Broadcast

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ap profile</b> <i>ap-profile-name</i> <b>Example:</b> Device(config)# ap profile ap-profile-name	Configures the AP profile.

	Command or Action	Purpose
<b>Step 3</b>	<p><b>[no]ssid broadcast persistent</b></p> <p><b>Example:</b></p> <pre>Device(config-ap-profile)# [no] ssid broadcast persistent</pre>	<p>The <b>ssid broadcast</b> command configures the SSID broadcast mode. The <b>persistent</b> keyword enables a persistent SSID broadcast, where the associated APs will re-join. Use the <b>[no]</b> form of the command to disable the feature.</p> <p><b>Note</b> Enabling or disabling this feature causes the AP to re-join.</p>

## Verifying Persistent SSID Broadcast

To view the configuration of all Cisco APs, use the following **show** command:

```
Device#show ap config general
Cisco AP Name   : AP4C77.6DF2.D598
=====
Office Extend Mode           : Disabled
Persistent SSID Broadcast    : Enabled
Remote AP Debug              : Disabled
```



## CHAPTER 24

# Network Monitoring

---

- [Network Monitoring](#) , on page 163
- [Status Information Received Synchronously - Configuration Examples](#), on page 163
- [Alarm and Event Information Received Asynchronously - Configuration Examples](#), on page 165

## Network Monitoring

Using this feature, the embedded wireless controller exposes the APIs or pushes data to a third-party system, which is utilized to develop an application for monitoring certain parameters such as, Name of the Village, Access Points in Each Village, and so on.

The mechanism that is used to transfer data to the third-party system is NETCONF/YANG. YANG can be used with the Network Configuration Protocol (NETCONF) to provide the desired solution of automated and programmable network operations.

You can contact the API or Developer Support for NETCONF/YANG features using the following link:

<https://developer.cisco.com/site/support/#>

The two types of information provided are:

- Status information received synchronously - NETCONF is the management interface used for status information, which allows to publish the operational state of the device, including the embedded wireless controller.
- Alarm and event information sent asynchronously - NETCONF/YANG push is the solution used for alarm and event information, which provides the mechanism to send NETCONF notifications subscribed for.

## Status Information Received Synchronously - Configuration Examples

NETCONF/YANG interface is used to accomplish customer requests.

The prerequisite configuration for Status Information and Alarm and Event Information is to enable NETCONF server on the embedded wireless controller by using the following command:

```
netconf-yang
```

The above command not only enables notifications, but also allows for configuration and operation access (OAM) via Netconf/Yang. For more information on Netconf/Yang, see the *NETCONF Protocol* chapter of the Programmability Configuration Guide at: <https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/products-installation-and-configuration-guides-list.html>

In the Status Information Received Synchronously type, the following information is exported through NETCONF:

- Name of the village
- APs in each village
- Status of each AP
- Number of clients currently connected and logged on in each village and each AP

All the data for the items listed above is already available as the embedded wireless controller operational data exported through NETCONF. The examples below explain where the data items listed are available.

The following command is used in the embedded wireless controller:

```
wireless tag site village_name_1
```

The site tags can be retrieved by NETCONF using the **get-config** operation.

Example output for **Name of the Village**:

```
<site-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-site-cfg">
[...]
```

```
<site-tag-configs>
  <site-tag-config>
    <site-tag-name>village_name_1</site-tag-name>
    <description>custom user site tag for a village</description>
  </site-tag-config>
[...]
```

```
</site-tag-configs>
```

The embedded wireless controller's operational data contains all the connected (joined) APs and lists their site tags. The example output displays the detailed information about the APs and the site tags. The following example displays the relevant fields and the corresponding embedded wireless controller show commands:

Example output of **Access Point per Village**:

```
<data>
  <access-point-oper-data
xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-access-point-oper">
  [...]
    <radio-oper-data>
      <wtp-mac>00:1b:0c:00:02:00</wtp-mac> #show ap dot11 {24ghz|5ghz} summary "MAC
Address"
      <radio-slot-id>0</radio-slot-id> #show ap dot11 {24ghz|5ghz} summary "Slot"
      <ap-mac>00:1b:0c:00:02:00</ap-mac>
      <slot-id>0</slot-id>
      <radio-type>1</radio-type> # 1 - 2.4GHz, 2 - 5GHz
      <admin-state>enabled</admin-state> #show ap dot11 {24ghz|5ghz} summary "Admin
State"
      <oper-state>radio-up</oper-state> #show ap dot11 {24ghz|5ghz} summary "Oper
State"
    [...]
  [...]
  <capwap-data>
```



```

        <wtp-mac>00:1b:0c:00:02:00</wtp-mac> #show ap summary "Radio MAC"
        <ap-operation-state>registered</ap-operation-state> #show ap summary "State"
        <ip-addr>10.102.140.10</ip-addr> #show ap summary "IP Address"
        [...]
        <admin-state>1</admin-state> #show ap status "Status", 1 - Enabled,
2 - Disabled
        <location>default-location </location> #show ap summary "Location"
        <country-code>CH </country-code>
        <name>AP_A-1</name> #show ap summary "AP Name"
    [...]
    <tag-info>
        [...]
        <site-tag>
            <site-tag-name>village_name_1</site-tag-name> #show ap name AP_A-1 config general
"Site Tag Name"
            [...]
        </site-tag>
    [...]

```

The operational data of the embedded wireless controller contains all the connected wireless clients information, which includes detailed client device information, such as the MAC address, IP address, State and the AP name.

Example output of the **Number of clients currently online and logged in each village and each AP:**

```

<data>
  <client-oper-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-client-oper">
    <common-oper-data>
      <client-mac>00:00:1a:04:00:02</client-mac> #show wireless client summary "MAC
Address"
      <ap-name>AP_A-1</ap-name> #show wireless client summary "AP
Name"
      [...]
    </co-state>client-status-run</co-state> #show wireless client summary "State"
  </client-oper-data>
</data>

```

## Alarm and Event Information Received Asynchronously - Configuration Examples

The push functionality for the alarm and event information is fulfilled with on-change notifications through NETCONF dynamic subscriptions, with XML encoding.

Example output of **AP Up/Down Events - Subscription**

Request:

```

<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="urn:uuid:b0c581c9-ff5a-4352-9e64-7f2ce1ec603a"
xmlns="urn:iETF:params:xml:ns:netconf:base:1.0">
  <establish-subscription xmlns="urn:iETF:params:xml:ns:yang:iETF-event-notifications"
xmlns:yp="urn:iETF:params:xml:ns:yang:iETF-yang-push">
    <stream>yp:yang-push</stream>
    <yp:xpath-filter>/access-point-oper-data/capwap-data/ap-operation-state</yp:xpath-filter>

    <yp:dampening-period>0</yp:dampening-period>
  </establish-subscription>
</rpc>

```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="urn:uuid:673b42b2-e988-4e20-a6c3-0679c08e6114"><subscription-result
xmlns='urn:ietf:params:xml:ns:yang:ietf-event-notifications'
xmlns:notif-bis="urn:ietf:params:xml:ns:yang:ietf-event-notifications">notif-bis:ok</subscription-result>
<subscription-id
xmlns='urn:ietf:params:xml:ns:yang:ietf-event-notifications'>2147483652</subscription-id>
</rpc-reply>
-->
(Default Callback)
Event time      : 2018-03-09 15:08:21.880000+00:00
Subscription Id : 2147483651
Type           : 2
Data           :
<datastore-changes-xml xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-push">
  <yang-patch xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-patch">
    <patch-id>null</patch-id>
    <edit>
      <edit-id>edit1</edit-id>
      <operation>merge</operation>
      <target>/access-point-oper-data/capwap-data</target>
      <value>
        <capwap-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-access-point-oper">
          <ap-operation-state>registered</ap-operation-state>
          <wtp-mac>00ab11006600</wtp-mac>
        </capwap-data>
      </value>
    </edit>
  </yang-patch>
</datastore-changes-xml>
<<--
```



## PART **V**

# System Management

- [Network Mobility Services Protocol, on page 169](#)
- [Application Visibility and Control, on page 181](#)
- [Cisco Connected Mobile Experiences Cloud, on page 197](#)
- [EDCA Parameters, on page 201](#)
- [802.11 parameters and Band Selection, on page 205](#)
- [Image Download, on page 223](#)
- [Conditional Debug and Radioactive Tracing, on page 239](#)
- [Aggressive Client Load Balancing, on page 247](#)
- [Accounting Identity List, on page 251](#)
- [Volume Metering, on page 255](#)
- [Enabling Syslog Messages in Access Points and Controller for Syslog Server, on page 257](#)
- [Introduction to Software Maintenance Upgrade, on page 267](#)





## CHAPTER 25

# Network Mobility Services Protocol

- [Information About Network Mobility Services Protocol, on page 169](#)
- [Enabling NMSP On-Premises Services, on page 170](#)
- [Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues , on page 170](#)
- [Modifying the NMSP Notification Threshold for Clients, and Tags, on page 171](#)
- [Configuring NMSP Strong Cipher, on page 171](#)
- [Verifying NMSP Settings, on page 172](#)
- [Examples: NMSP Settings Configuration, on page 174](#)
- [Probe RSSI Location, on page 174](#)
- [Configuring Probe RSSI , on page 175](#)
- [Verifying Probe RSSI, on page 176](#)
- [RFID Tag Support, on page 176](#)
- [Configuring RFID Tag Support, on page 177](#)
- [Verifying RFID Tag Support, on page 177](#)

## Information About Network Mobility Services Protocol

Cisco Network Mobility Services Protocol (NMSP) is a secure two-way protocol that can be run over a connection-oriented (TLS) or connection-less (DTLS) transport. The wireless infrastructure runs the NMSP server and Cisco Connected Mobile Experiences (Cisco CMX) acts as an NMSP client. The embedded wireless controller supports multiple services and multiple Cisco CMXs can connect to the NMSP server to get the data for the services (location of wireless devices, probe RSSI, hyperlocation, wIPS, and so on.) over the NMSP session.

NMSP defines the intercommunication between Cisco CMX and the embedded wireless controller. Cisco CMX communicates to the embedded wireless controller over a routed IP network. Both publish-subscribe and request-reply communication models are supported. Typically, Cisco CMX establishes a subscription to receive services data from the embedded wireless controller in the form of periodic updates. The embedded wireless controller acts as a data publisher, broadcasting services data to multiple CMXs. Besides subscription, Cisco CMX can also send requests to the embedded wireless controller, causing the embedded wireless controller to send a response back.

NMSP essentially provides a way to the applications in the embedded wireless controller to talk to the outside world. The NMSP in the embedded wireless controller also provides the flexibility to change the protocol to talk to the outside world.

The following is a list of the Network Mobility Services Protocol features:

- NMSP is disabled by default.
- NMSP communicates with Cisco CMX using TCP, and uses TLS for encryption.



**Note** HTTPS is not supported for data transport between embedded wireless controller and Cisco CMX.

## Enabling NMSP On-Premises Services

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>nmsp enable</b> <b>Example:</b> Device(config)# <code>nmsp enable</code>	Enables NMSP on premises services. <b>Note</b> By default, the NMSP is disabled on the embedded wireless controller.
<b>Step 3</b>	<b>end</b> <b>Example:</b> Device(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues

NMSP manages communication between the Cisco Connected Mobile Experiences (Cisco CMX) and the embedded wireless controller for incoming and outgoing traffic. If your application requires more frequent location updates, you can modify the NMSP notification interval (to a value between 1 and 180 seconds) for clients, active RFID tags, and rogue access points and clients.



**Note** The TCP port (16113) that the embedded wireless controller and Cisco CMX communicate over must be open (not blocked) on any firewall that exists between the embedded wireless controller and the Cisco CMX for NMSP to function.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>end</b> <b>Example:</b> Device(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Modifying the NMSP Notification Threshold for Clients, and Tags

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>location notify-threshold {clients   tags } threshold</b> <b>Example:</b> Device(config)# <code>location notify-threshold clients 5</code>	Configures the NMSP notification threshold for clients, and tags.  <i>threshold</i> - RSSI threshold value in db. Valid range is from 0 to 10.
<b>Step 3</b>	<b>end</b> <b>Example:</b> Device(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring NMSP Strong Cipher

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	<b>nmosp strong-cipher</b> <b>Example:</b> Device(config)# <b>nmosp strong-cipher</b>	Enable strong ciphers for NMSP server, which contains "ECDHE-RSA-AES128-GCM-SHA256;, ECDHE-ECDSA-AES128-GCM-SHA256;, AES256-SHA256:AES256-SHA; and AES128-SHA256:AES128-SHA".  Normal cipher suite contains, "ECDHE-RSA-AES128-GCM-SHA256;, ECDHE-ECDSA-AES128-GCM-SHA256;, and AES128-SHA".
<b>Step 3</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Verifying NMSP Settings

To view the NMSP capabilities of the embedded wireless controller, use the following command:

```
Device# show nmosp capability
Service          Subservice
-----
RSSI              Rogue, Tags, Mobile Station,
Spectrum          Aggregate Interferer, Air Quality, Interferer,
Info              Rogue, Mobile Station,
Statistics         Rogue, Tags, Mobile Station,
AP Monitor        Subscription
On Demand Services Device Info
AP Info           Subscription
```

To view the NMSP notification intervals, use the following command:

```
Device# show nmosp notification interval
NMSP Notification Intervals
-----

RSSI Interval:
  Client          : 2 sec
  RFID            : 50 sec
  Rogue AP        : 2 sec
  Rogue Client    : 2 sec
  Spectrum        : 2 sec
```

To view the connection-specific statistics counters for all CMX connections, use the following command:

```
Device# show nmosp statistics connection
NMSP Connection Counters
-----
CMX IP Address: 10.22.244.31, Status: Active
State:
  Connections : 1
  Disconnections : 0
  Rx Data Frames : 13
  Tx Data Frames : 99244
  Unsupported messages : 0
```



```

Rx Message Counters:
  ID  Name                               Count
-----
   1  Echo Request                         6076
   7  Capability Notification                2
  13  Measurement Request                   5
  16  Information Request                   3
  20  Statistics Request                    2
  30  Service Subscribe Request            1

Tx Message Counters:
  ID  Name                               Count
-----
   2  Echo Response                         6076
   7  Capability Notification                1
  14  Measurement Response                  13
  15  Measurement Notification              91120
  17  Information Response                   6
  18  Information Notification              7492
  21  Statistics Response                   2
  22  Statistics Notification               305
  31  Service Subscribe Response            1
  67  AP Info Notification                  304

```

To view the common statistic counter of the embedded wireless controller's NMSP service, use the following command:

```

Device# show nmsp statistics summary
NMSP Global Counters
-----
Number of restarts          :

SSL Statistics
-----
Total amount of verifications      : 6
Verification failures            : 6
Verification success              : 0
Amount of connections created      : 8
Amount of connections closed       : 7
Total amount of accept attempts    : 8
Failures in accept                : 0
Amount of successful accepts       : 8
Amount of failed registrations     : 0

AAA Statistics
-----
Total amount of AAA requests       : 7
Failed to send requests            : 0
Requests sent to AAA               : 7
Responses from AAA                 : 7
Responses from AAA to validate     : 7
Responses validate error           : 6
Responses validate success         : 1

```

To view the overall NMSP connections, use the following command:

```

Device# show nmsp status
NMSP Status
-----
CMX IP Address  Active  Tx Echo Resp  Rx Echo Req  Tx Data  Rx Data  Transport
-----
127.0.0.1      Active  6              6              1         2         TLS

```

To view all mobility services subscribed by all CMXs, use the following command:

```
Device# show nmosp subscription detail
CMX IP address 127.0.0.1:
Service          Subservice
-----
RSSI             Rogue, Tags, Mobile Station,
Spectrum
Info            Rogue, Mobile Station,
Statistics      Tags, Mobile Station,
AP Info         Subscription
```

To view all mobility services subscribed by a specific CMX, use the following command:

```
Device# show nmosp subscription detail <ip_addr>
CMX IP address 127.0.0.1:
Service          Subservice
-----
RSSI             Rogue, Tags, Mobile Station,
Spectrum
Info            Rogue, Mobile Station,
Statistics      Tags, Mobile Station,
AP Info         Subscription
```

To view the overall mobility services subscribed by all CMXs, use the following command:

```
Device# show nmosp subscription summary
Service          Subservice
-----
RSSI             Rogue, Tags, Mobile Station,
Spectrum
Info            Rogue, Mobile Station,
Statistics      Tags, Mobile Station,
AP Info         Subscription
```

## Examples: NMSP Settings Configuration

This example shows how to configure the NMSP notification interval for RFID tags:

```
Device# configure terminal
Device(config)# nmosp notification interval rssi rfid 50
Device(config)# end
Device# show nmosp notification interval
```

This example shows how to configure the NMSP notification interval for clients:

```
Device# configure terminal
Device(config)# nmosp notification interval rssi clients 180
Device(config)# end
Device# show nmosp notification interval
```

## Probe RSSI Location

The Probe RSSI Location feature allows the wireless embedded wireless controller and Cisco CMX to support the following:

- Load balancing
- Coverage Hole detection

- Location updates to CMX

When a wireless client is enabled, it sends probe requests to identify the wireless networks in the vicinity and also to find the received signal strength indication (RSSI) associated with the identified Service Set Identifiers (SSIDs).

The wireless client periodically performs active scanning in background even after being connected to an access point. This helps them to have an updated list of access points with best signal strength to connect. When the wireless client can no longer connect to an access point, it uses the access point list stored to connect to another access point that gives it the best signal strength. The access points in the WLAN gather these probe requests, RSSI and MAC address of the wireless clients and forwards them to the wireless embedded wireless controllers. The Cisco CMX gathers this data from the wireless embedded wireless controller and uses it to compute the updated location of the wireless client when it roams across the network.

## Configuring Probe RSSI

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless probe filter</b> <b>Example:</b> Device(config)# wireless probe filter	Enables filtering of unacknowledged probe requests from AP to improve the location accuracy.  Use the <b>no</b> form of the command to disable the feature. This will forward both acknowledged and unacknowledged probe requests to the embedded wireless controller.
<b>Step 3</b>	<b>wireless probe limit <i>limit-value interval</i></b> <b>Example:</b> Device(config)# wireless probe limit 10 100	Configures the number of probe request reported to the wireless embedded wireless controller from the AP for the same client on a given interval.  Use the <b>no</b> form of the command to revert to the default limit, which is 2 probes at an interval of 500 ms.
<b>Step 4</b>	<b>wireless probe locally-administered-mac</b> <b>Example:</b> Device(config)# wireless probe locally-administered-mac	Enables the reporting of probes from clients having locally administered MAC address.
<b>Step 5</b>	<b>location algorithm rssi-average</b> <b>Example:</b> Device(config)# location algorithm rssi-average	Sets the probe RSSI measurement updates to a more accurate algorithm but with more CPU overhead.

	Command or Action	Purpose
<b>Step 6</b>	<b>location algorithm simple</b> <b>Example:</b> Device(config)# location algorithm simple	(Optional) Sets the probe RSSI measurement updates to a faster algorithm with smaller CPU overhead, but less accuracy.  Use the <b>no</b> form of the command to revert the algorithm type to the default one, which is <i>rssi-average</i> .
<b>Step 7</b>	<b>location expiry client interval</b> <b>Example:</b> Device(config)# location expiry client 300	Configures the timeout for RSSI values.  The <b>no</b> form of the command sets it to a default value of 15.
<b>Step 8</b>	<b>location notify-threshold client threshold-db</b> <b>Example:</b> Device(config)# location notify-threshold client 5	Configures the notification threshold for clients.  The <b>no</b> form of the command sets it to a default value of 0.
<b>Step 9</b>	<b>location rssi-half-life client time-in-seconds</b> <b>Example:</b> Device(config)# location rssi-half-life client 20	Configures half life when averaging two RSSI readings.  To disable this option, set the value to 0.

### What to do next

Use the **show wireless client probing** command to view each probing client (associated and probing only) by batch of 10 mac addresses.

## Verifying Probe RSSI

To view the details of the AP the associated client was detected with, and with which RSSI:

```
Device# show wireless client mac-address 4.4.4 detail
****snippet of the output****
Nearby AP Statistics:
TEST_AP-1 (slot 0)
antenna 0: 0 s ago ..... -77 dBm
antenna 1: 0 s ago ..... -88 dBm
TEST_AP-5 (slot 0)
antenna 0: 0 s ago ..... -64 dBm
antenna 1: 0 s ago ..... -36 dBm
TEST_AP-6 (slot 0)
antenna 0: 0 s ago ..... -69 dBm
antenna 1: 0 s ago ..... -79 dBm
```

## RFID Tag Support

The embedded wireless controller enables you to configure radio frequency identification (RFID) tag tracking. RFID tags are small wireless battery-powered tags that continuously broadcast their own signal and are affixed

to assets for real-time location tracking. They operate by advertising their location using special 802.11 packets, which are processed by access points, the embedded wireless controller, and the Cisco CMX. Only active RFIDs are supported. A combination of active RFID tags and wireless embedded wireless controller allows you to track the current location of equipment. *Active* tags are typically used in real-time tracking of high-value assets in *closed-loop* systems (that is,) systems in which the tags are not intended to physically leave the control premises of the tag owner or originator.

For more information on RFID tags, see the [Active RFID Tags](#) section of the *Wi-Fi Location-Based Services 4.1 Design Guide*.

### General Guidelines

- Only Cisco-compliant [active RFID tags](#) are supported.
- You can verify the RFID tags on the embedded wireless controller.
- High Availability for RFID tags are supported.

## Configuring RFID Tag Support

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless rfid</b> <b>Example:</b> Device(config)# <code>wireless rfid</code>	Enables RFID tag tracking. The default value is enabled. Use the <b>no</b> form of this command to disable RFID tag tracking.
<b>Step 3</b>	<b>wireless rfid timeout <i>timeout-value</i></b> <b>Example:</b> Device(config)# <code>wireless rfid timeout 90</code>	Configures the RFID tag data timeout value to cleanup the table. The timeout value is the amount of time that the embedded wireless controller maintains tags before expiring them. For example, if a tag is configured to beacon every 30 seconds, we recommend that you set the timeout value to 90 seconds (approximately three times the beacon value). The default value is 1200 seconds.

## Verifying RFID Tag Support

To view the summary of RFID tags that are clients, use the following command:

```
Device# show wireless rfid client
```

To view the detailed information for an RFID tag, use the following command:

```
Device# show wireless rfid detail <rfid-mac-address>

RFID address 000c.cc96.0001
Vendor Cisco
Last Heard 6 seconds ago
Packets Received 187
Bytes Received 226

Content Header
=====
  CCX Tag Version 0
  Tx power: 12
  Channel: 11
  Reg Class: 4
CCX Payload
=====
  Last Sequence Control 2735
  Payload length 221
  Payload Data Hex Dump:
00000000 00 02 00 00 01 09 00 00 00 00 0c b8 ff ff ff 02 |.....|
00000010 07 42 03 20 00 00 0b b8 03 4b 00 00 00 00 00 00 |.B. ....K.....|
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
```

To view the summary information for all known RFID tags, use the following command:

```
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 3 minutes 30 seconds ago
0012.b80a.c953 Cisco 7069.5a63.0460 -33 4 minutes 5 seconds ago
0012.b80b.806c Cisco 7069.5a63.0520 -46 15 seconds ago
0012.b80d.e9f9 Cisco 7069.5a63.0460 -38 4 minutes 28 seconds ago
0012.b80d.ea03 Cisco 7069.5a63.0520 -43 4 minutes 29 seconds ago
0012.b80d.ea6b Cisco 7069.5a63.0460 -39 4 minutes 26 seconds ago
0012.b80d.ebe8 Cisco 7069.5a63.0520 -43 3 minutes 21 seconds ago
0012.b80d.ebeb Cisco 7069.5a63.0520 -43 4 minutes 28 seconds ago
0012.b80d.ec48 Cisco 7069.5a63.0460 -42 4 minutes 7 seconds ago
0012.b80d.ec55 Cisco 7069.5a63.0520 -41 1 minute 52 seconds ago
```

To view the location-based system RFID statistics, use the following command:

```
Device# show wireless rfid stats

RFID stats :
=====
RFID error db full : 0
RFID error invalid payload : 0
RFID error invalid tag : 0
RFID error dot11 hdr : 0
RFID error pkt len : 0
RFID error state drop : 0
RFID total pkt received : 369
RFID populated error value : 0
RFID error insert records : 0
RFID error update records : 0
RFID total insert record : 16
RFID ccx payload error : 0
```

```
RFID total delete record : 0
RFID error exceeded ap count : 0
RFID error record remove : 0
RFID old rssi expired count: 0
RFID smallest rssi expired count : 0
RFID total query insert : 0
RFID error invalid rssi count : 0
```

To view the NMSP notification interval, use the following command:

```
Device# show nmsp notification interval
```

```
NMSP Notification Intervals
```

```
-----
RSSI Interval:
  Client           : 2 sec
  RFID             : 50 sec
  Rogue AP         : 2 sec
  Rogue Client     : 2 sec
  Spectrum         : 2 sec
```







## CHAPTER 26

# Application Visibility and Control

- [Information About Application Visibility and Control, on page 181](#)
- [Create a Flow Monitor, on page 183](#)
- [Configuring a Flow Monitor \(GUI\), on page 184](#)
- [Create a Flow Exporter , on page 184](#)
- [Configure a WLAN for AVC, on page 185](#)
- [Configuring a Policy Tag, on page 186](#)
- [Attaching a Policy Profile to a WLAN Interface \(GUI\), on page 186](#)
- [Attaching a Policy Profile to a WLAN Interface \(CLI\), on page 186](#)
- [Attaching a Policy Profile to an AP, on page 188](#)
- [Verify the AVC Configuration, on page 188](#)
- [AVC-Based Selective Reanchoring, on page 189](#)
- [Restrictions for AVC-Based Selective Reanchoring, on page 189](#)
- [Configuring the Flow Exporter, on page 189](#)
- [Configuring the Flow Monitor, on page 190](#)
- [Configuring the AVC Reanchoring Profile, on page 191](#)
- [Configuring the Wireless WLAN Profile Policy , on page 191](#)
- [Verifying AVC Reanchoring, on page 192](#)

## Information About Application Visibility and Control

Application Visibility and Control (AVC) is a subset of the entire Flexible NetFlow (FNF) package that can provide traffic information. The AVC feature employs a distributed approach that benefits from NBAR running on the access point (AP) or embedded wireless controller whose goal is to run deep packet inspection (DPI) and reports the results using FNF messages.

AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades. Traffic flows are analyzed and recognized using the NBAR2 engine. The specific flow is marked with the recognized protocol or application. This per-flow information can be used for application visibility using FNF. After the application visibility is established, a user can define control rules with policing mechanisms for a client.

Using AVC rules, you can limit the bandwidth of a particular application for all the clients joined on the WLAN. These bandwidth contracts coexist with per-client downstream rate limiting that takes precedence over the per-application rate limits.

FNF feature is supported in wireless, and relies on the NetFlow enablement on the embedded wireless controller for flex mode.

The behavior of the AVC solution changes based on the wireless deployments. The following sections describe the commonalities and differences in all scenarios:

### Flex Mode

- NBAR is enabled on an AP
- AVC pushes the FNF configuration to the APs.
- Supports context transfer for roaming in AVC-FNF.
- Supports NetFlow exporter.

## Prerequisites for Application Visibility and Control

- The access points should be AVC capable.
- For the control part of AVC (QoS) to work, the application visibility feature with FNF has to be configured.

## Restrictions for Application Visibility and Control

- Layer 2 roaming is not supported across embedded wireless controllercontrollers.
- Multicast traffic is not supported.
- AVC is supported only on the following access points:
  - Cisco Aironet 1800 Series Access Points
  - Cisco Aironet 2700 Series Access Point
  - Cisco Aironet 2800 Series Access Point
  - Cisco Aironet 3700 Series Access Points
  - Cisco Aironet 3800 Series Access Points
  - Cisco Aironet 4800 Series Access Points
- AVC is not supported on Cisco Aironet 702W, 702I (128 M memory), and 1530 Series access points.
- Only the applications that are recognized with App visibility can be used for applying QoS control.
- Data link is not supported for NetFlow fields in AVC.
- You cannot map the same WLAN profile to both the AVC-not-enabled policy profile and the AVC-enabled policy profile.
- NBAR-based QoS policy configuration is allowed at client level and BSSID level, configured on policy profile.

When AVC is enabled, the AVC profile supports only up to 23 rules, which includes the default DSCP rule. The AVC policy will not be pushed down to the AP, if rules are more than 23.

## AVC Configuration Overview

To configure AVC, follow these steps:

1. Create a flow monitor using the **record wireless avc basic** command.
2. Create a wireless policy profile.
3. Apply the flow monitor to the wireless policy profile.
4. Create a wireless policy tag.
5. Map the WLAN to the policy profile
6. Attach the policy tag to the APs.

## Create a Flow Monitor

The NetFlow configuration requires a flow record, a flow monitor, and a flow exporter. This configuration should be the first step in the overall AVC configuration.



**Note** In Flex mode, the default values for **cache timeout active** and **cache timeout inactive** commands are not optimal for AVC. We recommend that you set both the values to 60 in the flow monitor.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>flow monitor</b> <i>monitor-name</i> <b>Example:</b> Device(config)# flow monitor fm_avc	Creates a flow monitor.
<b>Step 3</b>	<b>record wireless avc basic</b> <b>Example:</b> Device(config-flow-monitor)# record wireless avc basic	Specifies the basic wireless AVC flow template. <b>Note</b> The <b>record wireless avc basic</b> command is same as <b>record wireless avc ipv4 basic</b> command. However, <b>record wireless avc ipv4 basic</b> command is not supported in Flex or Fabric modes. In such scenarios, use the <b>record wireless avc basic</b> command.

# Configuring a Flow Monitor (GUI)

## Before you begin

You must have created a flow exporter to export data from the flow monitor.

## Procedure

- Step 1** Choose **Configuration > Services > Application Visibility** and go to the **Flow Monitor** tab .
- Step 2** In the **Monitor** area, click **Add** to add a flow monitor.
- Step 3** In the **Flow Monitor** window, add a flow monitor and a description.
- Step 4** Select the Flow exporter from the drop-down list to export the data from the flow monitor to a collector.

**Note** To export wireless netflow data, use the templates below:

- ETA (Encrypted Traffic Analysis)
- wireless avc basic
- wireless avc basic IPv6

- Step 5** Click **Apply to Device** to save the configuration.

# Create a Flow Exporter

You can create a flow exporter to define the export parameters for a flow. This is an optional procedure for configuring flow exporter parameters.



**Note** For the AVC statistics to be visible at the embedded wireless controller, you should configure a local flow exporter using the following commands:

- **flow exporter** *my\_local*
- **destination local wlc**

Also, your flow monitor must use this local exporter for the statistics to be visible at the embedded wireless controller.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>flow exporter</b> <i>flow-export-name</i> <b>Example:</b>	Creates a flow monitor.

	Command or Action	Purpose
	Device(config)# flow exporter export-test	
<b>Step 2</b>	<b>description</b> <i>string</i> <b>Example:</b> Device(config-flow-exporter)# <b>description</b> <b>IPv4flow</b>	Describes the flow record as a maximum 63-character string.
<b>Step 3</b>	<b>Example:</b> Device(config-flow-exporter) # <b>destination</b> local wlc	Specifies the local WLC to which the exporter sends data.
<b>Step 4</b>	<b>show flow exporter</b> <b>Example:</b> Device # <b>show flow exporter</b>	(Optional) Verifies your configuration.

## Configure a WLAN for AVC

Follow the procedure given below to configure a WLAN for AVC:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>wlan</b> <i>wlan-avc 1 ssid-avc</i> <b>Example:</b> Device(config)# wlan wlan1 1 ssid1	Configures WLAN.
<b>Step 2</b>	<b>shutdown</b> <b>Example:</b> Device(config-wlan)# shutdown	Shuts down the WLAN.
<b>Step 3</b>	<b>no security wpa akm dot1x</b> <b>Example:</b> Device(config-wlan)# no security wpa akm dot1x	Disables security AKM for dot1x.
<b>Step 4</b>	<b>no security wpa wpa2 ciphers aes</b> <b>Example:</b> Device(config-wlan)# no security wpa wpa2 ciphers aes	Disables WPA2 ciphers for AES.

## Configuring a Policy Tag

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless tag policy <i>policy-tag-name</i></b>  <b>Example:</b> Device(config-policy-tag)# wireless tag policy rr-xyz-policy-tag	Configures policy tag and enters policy tag configuration mode.
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Device(config-policy-tag)# end	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.

## Attaching a Policy Profile to a WLAN Interface (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Tags**.
  - Step 2** On the **Manage Tags** page, click **Policy** tab.
  - Step 3** Click **Add** to view the **Add Policy Tag** window.
  - Step 4** Enter a name and description for the policy tag.
  - Step 5** Click **Add** to map WLAN and policy.
  - Step 6** Choose the WLAN profile to map with the appropriate policy profile, and click the tick icon.
  - Step 7** Click **Save & Apply to Device**.
- 

## Attaching a Policy Profile to a WLAN Interface (CLI)

### Before you begin

- Do not attach different AVC policy profiles on the same WLAN across different policy tags.

The following is an example of incorrect configuration:

```
wireless profile policy avc_poll
  ipv4 flow monitor fm-avc1 input
```

```

ipv4 flow monitor fm-avc1 output
no shutdown
wireless profile policy avc_pol2
ipv4 flow monitor fm-avc2 input
ipv4 flow monitor fm-avc2 output
no shutdown
wireless tag policy avc-tag1
wlan wlan1 policy avc_pol1
wireless tag policy avc-tag2
wlan wlan1 policy avc_pol2

```

This example violates the restriction stated earlier, that is, the WLAN *wlan1* is mapped to 2 policy profiles, *avc\_pol1* and *avc\_pol2*. This configuration is, therefore, incorrect because the WLAN *wlan1* should be mapped to either *avc\_pol1* or *avc\_pol2* everywhere.

- Conflicting policy profiles on the same WLAN are not supported. For example, policy profile (with and without AVC) applied to the same WLAN in different policy tags.

The following is an example of an incorrect configuration:

```

wireless profile policy avc_pol1
no shutdown
wireless profile policy avc_pol2
ipv4 flow monitor fm-avc2 input
ipv4 flow monitor fm-avc2 output
no shutdown
wireless tag policy avc-tag1
wlan wlan1 policy avc_pol1
wireless tag policy avc-tag2
wlan wlan1 policy avc_pol2

```

In this example, a policy profile with and without AVC is applied to the same WLAN in different tags.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>wireless tag policy <i>avc-tag</i></b> <b>Example:</b> Device(config)# wireless tag policy avc-tag	Creates a policy tag.
<b>Step 2</b>	<b>wlan <i>wlan-avc</i> policy <i>avc-policy</i></b> <b>Example:</b> Device(config-policy-tag)# wlan wlan_avc policy avc_pol	Attaches a policy profile to a WLAN profile.

## What to do next

- Run the **no shutdown** command on the WLAN after completing the configuration.
- If the WLAN is already in **no shutdown** mode, run the **shutdown** command, followed by **no shutdown** command.

## Attaching a Policy Profile to an AP

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>ap</b> <i>ap-ether-mac</i>  <b>Example:</b> Device(config)# ap 34a8.2ec7.4cf0	Enters AP configuration mode.
<b>Step 2</b>	<b>policy-tag</b> <i>policy-tag</i>  <b>Example:</b> Device(config)# policy-tag avc-tag	Specifies the policy tag that is to be attached to the access point.

## Verify the AVC Configuration

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>show avc wlan</b> <i>wlan-name</i> <b>top</b> <i>num-of-applications</i> <b>applications</b> { <b>aggregate</b>   <b>downstream</b>   <b>upstream</b> }  <b>Example:</b> Device# show avc wlan wlan_avc top 2 applications aggregate	Displays information about top applications and users using these applications.  <b>Note</b> Ensure that wireless clients are associated to the WLAN and generating traffic, and then wait for 90 seconds (to ensure the availability of statistics) before running the command.
<b>Step 2</b>	<b>show avc client</b> <i>mac</i> <b>top</b> <i>num-of-applications</i> <b>applications</b> { <b>aggregate</b>   <b>downstream</b>   <b>upstream</b> }  <b>Example:</b> Device# show avc client 9.3.4 top 3 applications aggregate	Displays information about the top number of applications.  <b>Note</b> Ensure that wireless clients are associated to the WLAN and generating traffic, and then wait for 90 seconds (to ensure the availability of statistics) before running the command.
<b>Step 3</b>	<b>show avc wlan</b> <i>wlan-name</i> <b>application</b> <i>app-name</i> <b>top</b> <i>num-of-clients</i> <b>aggregate</b>  <b>Example:</b> Device# show avc wlan wlan_avc application app top 4 aggregate	Displays information about top applications and users using these applications.



	Command or Action	Purpose
<b>Step 4</b>	<b>show ap summary</b> <b>Example:</b> Device# show ap summary	Displays a summary of all the access points attached to the embedded wireless controller.
<b>Step 5</b>	<b>show ap tag summary</b> <b>Example:</b> Device# show ap tag summary	Displays a summary of all the access points with policy tags.

## AVC-Based Selective Reanchoring

The AVC-Based Selective Reanchoring feature is designed to reanchor clients when they roam from one embedded wireless controller to another. Reanchoring of clients prevents the depletion of IP addresses available for new clients in Cisco WLC. The AVC profile-based statistics are used to decide whether a client must be reanchored or deferred. This is useful when a client is actively running a voice or video application defined in the AVC rules.

The reanchoring process also involves deauthentication of anchored clients. The clients get deauthenticated when they do not transmit traffic for the applications listed in the AVC rules while roaming between WLCs.

## Restrictions for AVC-Based Selective Reanchoring

- This feature is supported only in local mode. FlexConnect and fabric modes are not supported.
- This feature is not supported in guest tunneling and export anchor scenarios.
- The old IP address is not released after reanchoring, until IP address' lease period ends.

## Configuring the Flow Exporter

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>flow exporter <i>name</i></b> <b>Example:</b> Device(config)# flow exporter avc-reanchor	Creates a flow exporter and enters flow exporter configuration mode.  <b>Note</b> You can use this command to modify an existing flow exporter too.

	Command or Action	Purpose
<b>Step 3</b>	<b>destination local wlc</b>  <b>Example:</b> Device(config-flow-exporter)# destination local wlc	Sets the exporter as local.

## Configuring the Flow Monitor

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>flow monitor <i>monitor-name</i></b>  <b>Example:</b> Device(config)# flow monitor fm_avc	Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode.  <b>Note</b> You can use this command to modify an existing flow monitor too.
<b>Step 3</b>	<b>exporter <i>exporter-name</i></b>  <b>Example:</b> Device(config-flow-monitor)# exporter avc-reanchor	Specifies the name of an exporter.
<b>Step 4</b>	<b>record wireless avc basic</b>  <b>Example:</b> Device(config-flow-monitor)# record wireless avc basic	Specifies the flow record to use to define the cache.
<b>Step 5</b>	<b>cache timeout active <i>value</i></b>  <b>Example:</b> Device(config-flow-monitor)# cache timeout active 60	Sets the active flow timeout, in seconds.
<b>Step 6</b>	<b>cache timeout inactive <i>value</i></b>  <b>Example:</b> Device(config-flow-monitor)# cache timeout inactive 60	Sets the inactive flow timeout, in seconds.

# Configuring the AVC Reanchoring Profile

## Before you begin

- Ensure that you use the AVC-Reanchor-Class class map. All other class-map names are ignored by Selective Reanchoring.
- During boot up, the system checks for the existence of the AVC-Reanchor-Class class map. If it is not found, default protocols, for example, jabber-video, wifi-calling, and so on, are created. If AVC-Reanchor-Class class map is found, configuration changes are not made and updates to the protocols that are saved to the startup configuration persist across reboots.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>class-map <i>cmap-name</i></b> <b>Example:</b> Device(config)# class-map AVC-Reanchor-Class	Configures the class map.
<b>Step 3</b>	<b>match any</b> <b>Example:</b> Device(config-cmap)# match any	Instructs the device to match with any of the protocols that pass through it.
<b>Step 4</b>	<b>match protocol jabber-audio</b> <b>Example:</b> Device(config-cmap)# match protocol jabber-audio	Specifies a match to the application name.  You can edit the class-map configuration later, in order to add or remove protocols, for example, jabber-video, wifi-calling, and so on, if required.

# Configuring the Wireless WLAN Profile Policy

Follow the procedure given below to configure the WLAN profile policy:

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 2</b>	<b>wireless profile policy</b> <i>policy-name</i> <b>Example:</b> Device(config)# wireless profile policy default-policy-profile	Configures the WLAN policy profile and enters wireless policy configuration mode.
<b>Step 3</b>	<b>shutdown</b> <b>Example:</b> Device(config-wireless-policy)# shutdown	Disables the policy profile.
<b>Step 4</b>	<b>central switching</b> <b>Example:</b> Device(config-wireless-policy)# central switching	Enables central switching.
<b>Step 5</b>	<b>ipv4 flow monitor</b> <i>monitor-name</i> <b>input</b> <b>Example:</b> Device(config-wireless-policy)# ipv4 flow monitor fm_avc input	Specifies the name of the IPv4 ingress flow monitor.
<b>Step 6</b>	<b>ipv4 flow monitor</b> <i>monitor-name</i> <b>output</b> <b>Example:</b> Device(config-wireless-policy)# ipv4 flow monitor fm_avc output	Specifies the name of the IPv4 egress flow monitor.
<b>Step 7</b>	<b>reanchor class</b> <i>class-name</i> <b>Example:</b> Device(config-wireless-policy)# reanchor class AVC-Reanchor-Class	Configure a class map with protocols for the Selective Reanchoring feature.
<b>Step 8</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wireless-policy)# no shutdown	Enables the policy profile.

## Verifying AVC Reanchoring

Use the following commands to verify the AVC reanchoring configuration:

```
Device# show wireless profile policy detailed avc_reanchor_policy
```

```
Policy Profile Name      : avc_reanchor_policy
Description              :
Status                   : ENABLED
VLAN                     : 1
Wireless management interface VLAN : 34
!
.
.
```

```

.
AVC VISIBILITY : Enabled
Flow Monitor IPv4
  Flow Monitor Ingress Name : fm_avc
  Flow Monitor Egress Name : fm_avc
Flow Monitor IPv6
  Flow Monitor Ingress Name : Not Configured
  Flow Monitor Egress Name : Not Configured
NBAR Protocol Discovery : Disabled
Reanchoring : Enabled
Classmap name for Reanchoring
  Reanchoring Classmap Name : AVC-Reanchor-Class
!
.
.
.
-----

```

Device# **show platform software trace counter tag wstatsd chassis active R0 avc-stats debug**

```

Counter Name Thread ID Counter Value
-----
Reanch_deassociated_clients 28340 1
Reanch_tracked_clients 28340 4
Reanch_deleted_clients 28340 3

```

Device# **show platform software trace counter tag wncd chassis active R0 avc-afc debug**

```

Counter Name Thread ID Counter Value
-----
Reanch_co_ignored_clients 30063 1
Reanch_co_anchored_clients 30063 5
Reanch_co_deauthed_clients 30063 4

```

Device# **show platform software wlavc status wncd**

Event history of WNCDB:

```

AVC key: [1,wlan_avc,N/A,Reanc,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Reanchoring
Flow-mon-name : N/A
Policy-tag : default-policy-tag
Switching Mode : CENTRAL

```

Timestamp FSM State Event RC Ctx

```

-----
06/12/2018 16:45:30.630342 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:28.822780 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:28.822672 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:15.172073 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:12.738367 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:12.738261 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:01.162689 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:55.757643 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:55.757542 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:04.468749 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:02.18857 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:02.18717 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:38:20.164304 2 :READY 3 :FSM_AFM_SWEEP 0 2
06/12/2018 16:35:20.163877 2 :READY 1 :FSM_AFM_BIND 0 2

```

```
06/12/2018 16:35:18.593257 1 :INIT 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:18.593152 1 :INIT 24:CREATE_FSM 0 0
```

```
AVC key: [1,wlan_avc,fm_avc,v4-In,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Ingress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
```

```
Timestamp FSM State Event RC Ctx
```

```
-----
06/12/2018 16:45:30.664772 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:28.822499 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:28.822222 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:15.207605 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:12.738105 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:12.737997 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:01.164225 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:55.757266 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:55.757181 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:04.472778 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:02.15413 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:02.15263 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:38:20.164254 2 :READY 3 :FSM_AFM_SWEEP 0 2
06/12/2018 16:35:20.163209 1 :INIT 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:20.163189 1 :INIT 24:CREATE_FSM 0 0
```

```
AVC key: [1,wlan_avc,fm_avc,v4-Ou,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Egress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
```

```
Timestamp FSM State Event RC Ctx
```

```
-----
06/12/2018 16:45:30.630764 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:28.822621 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:28.822574 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:15.172357 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:12.738212 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:12.738167 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:01.164048 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:55.757403 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:55.757361 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:04.472561 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:02.18660 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:02.18588 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:38:20.164293 2 :READY 3 :FSM_AFM_SWEEP 0 2
06/12/2018 16:35:20.163799 1 :INIT 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:20.163773 1 :INIT 24:CREATE_FSM 0 0
```

```
Device# show platform software wlavc status wncmgrd
```

```
Event history of WNCMgr DB:
```

```
AVC key: [1,wlan_avc,N/A,Reanc,default-policy-tag]
Current state : READY
Wlan-id : 1
```

```

Wlan-name : wlan_avc
Feature type : Reanchoring
Flow-mon-name : N/A
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
Policy-profile : AVC_POL_PYATS

```

```
Timestamp FSM State Event RC Ctx
```

```

-----
06/12/2018 16:45:30.629278 3 :WLAN_READY 24:BIND_WNCD 0 0
06/12/2018 16:45:30.629223 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.629179 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.510867 2 :PLUMB_READY 22:BIND_IOSD 0 0
06/12/2018 16:45:30.510411 2 :PLUMB_READY 2 :FSM_WLAN_UP 0 0
06/12/2018 16:45:30.510371 2 :PLUMB_READY 1 :FSM_WLAN_FM_PLUMB 0 0
06/12/2018 16:45:28.886377 2 :PLUMB_READY 20:UNBIND_ACK_IOSD 0 0
!
```

```

AVC key: [1,wlan_avc,fm_avc,v4-In,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Ingress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
Policy-profile : AVC_POL_PYATS

```

```
Timestamp FSM State Event RC Ctx
```

```

-----
06/12/2018 16:45:30.664032 3 :WLAN_READY 24:BIND_WNCD 0 0
06/12/2018 16:45:30.663958 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.663921 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.511151 2 :PLUMB_READY 22:BIND_IOSD 0 0
06/12/2018 16:45:30.510624 2 :PLUMB_READY 2 :FSM_WLAN_UP 0 0
06/12/2018 16:45:30.510608 2 :PLUMB_READY 1 :FSM_WLAN_FM_PLUMB 0 0
06/12/2018 16:45:28.810867 2 :PLUMB_READY 20:UNBIND_ACK_IOSD 0 0
06/12/2018 16:45:28.807239 4 :READY 25:UNBIND_WNCD 0 0
06/12/2018 16:45:28.807205 4 :READY 23:UNBIND_IOSD 0 0
06/12/2018 16:45:28.806734 4 :READY 3 :FSM_WLAN_DOWN 0 0
!
```

```

AVC key: [1,wlan_avc,fm_avc,v4-Ou,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Egress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
Policy-profile : AVC_POL_PYATS

```

```
Timestamp FSM State Event RC Ctx
```

```

-----
06/12/2018 16:45:30.629414 3 :WLAN_READY 24:BIND_WNCD 0 0
06/12/2018 16:45:30.629392 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.629380 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.510954 2 :PLUMB_READY 22:BIND_IOSD 0 0
06/12/2018 16:45:30.510572 2 :PLUMB_READY 2 :FSM_WLAN_UP 0 0
06/12/2018 16:45:30.510532 2 :PLUMB_READY 1 :FSM_WLAN_FM_PLUMB 0 0
06/12/2018 16:45:28.886293 2 :PLUMB_READY 20:UNBIND_ACK_IOSD 0 0
06/12/2018 16:45:28.807844 4 :READY 25:UNBIND_WNCD 0 0
06/12/2018 16:45:28.807795 4 :READY 23:UNBIND_IOSD 0 0

```

```
06/12/2018 16:45:28.806990 4 :READY 3 :FSM_WLAN_DOWN 0 0  
!
```





## CHAPTER 27

# Cisco Connected Mobile Experiences Cloud

Cisco Connected Mobile Experiences (CMX) communicates with the Cisco wireless embedded wireless controller using the Network Mobility Services Protocol (NMSP), which runs over a connection-oriented (TLS) transport. This transport provides a secure 2-way connectivity and is convenient when both the embedded wireless controller and CMX are on-premise and there is direct IP connectivity between them.

Cisco CMX Cloud is a cloud-delivered version of the on-premise CMX. To access Cisco CMX Cloud services, HTTPS is used as a transport protocol.

- [Configuring Cisco CMX Cloud](#) , on page 197
- [Verifying Cisco CMX Cloud Configuration](#), on page 198

## Configuring Cisco CMX Cloud

Follow the procedure given below to configure CMX Cloud:

### Before you begin

- **Configure DNS**—To resolve fully qualified domain names used by NMSP cloud-services, configure a DNS using the **ip name-server** *server\_address* configuration command as shown in Step 2.
- **Import 3rd party root CAs**—The controller verifies the peer and the host based on the certificate that is sent by the CMX when a connection is established. However, root CAs are not preinstalled on the controller. You have to import a set of root CAs trusted by Cisco to the trustpool of the crypto PKI by using the **crypto pki trustpool import url** <url> configuration command as shown in Step 3.
- A successful registration to Cisco DNA Spaces is required to enable **server url** and **server token** parameters configuration which is needed to complete this setup.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	<b>ip name-server</b> <i>namesvr-ip-addr</i>  <b>Example:</b> Device(config)#ip name-server 10.10.10.205	Configures the DNS on the controller to resolve the FQDN names used by the NMSP cloud-services.
<b>Step 3</b>	<b>crypto pki trustpool import url</b> <i>url</i>  <b>Example:</b> Device(config)#crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b	Imports the 3rd party root CA. The controller verifies the peer using the imported certificate.
<b>Step 4</b>	<b>[no] nmsp cloud-services server url</b> <i>url</i>  <b>Example:</b> Device(config)# nmsp cloud-services server url https://cisco.com	Configures the URL used for cloud services. Use the <b>no</b> form of the command to delete the server url from the configuration.
<b>Step 5</b>	<b>[no] nmsp cloud-services server token</b> <i>token</i>  <b>Example:</b> Device(config)# nmsp cloud-services server token test	Configures the authentication token for the NMSP cloud service. Use the <b>no</b> form of the command to delete the server token from the configuration.
<b>Step 6</b>	<b>[no] nmsp cloud-services http-proxy</b> <i>proxy-server port</i>  <b>Example:</b> Device(config)# nmsp cloud-services http-proxy 10.0.0.1 10	(Optional) Configures HTTP proxy details for the NMSP cloud service. Use the <b>no</b> form of the command to disable the use of a HTTP proxy.
<b>Step 7</b>	<b>[no] nmsp cloud-services enable</b>  <b>Example:</b> Device(config)# nmsp cloud-services enable	Enables NMSP cloud services. Use the <b>no</b> form of the command to disable the feature.

## Verifying Cisco CMX Cloud Configuration

Use the following commands to verify the CMX Cloud configuration.

To view the status of active NMSP connections, use the following command:

```
Device# show nmsp status
```

```

MSE IP Address   Tx Echo Resp  Rx Echo Req   Tx Data      Rx Data      Transport
-----
9.9.71.78       0             0             1             1            TLS
64.103.36.133  0             0             1230          2391         HTTPs

```

To view the NMSP cloud service status, use the following command:

```
Device# show nmsp cloud-services summary
```

```
CMX Cloud-Services Status
```

```
-----  
Server:                https://yenth8.cmxcisco.com  
IP Address:            64.103.36.133  
Cmx Service:          Enabled  
Connectivity:         https: UP  
Service Status:       Active  
Last Request Status:  HTTP/1.1 200 OK  
Heartbeat Status:     OK
```

To view the NMSP cloud service statistics, use the following command:

```
Device# show nmsp cloud-services statistics
```

```
CMX Cloud-Services Statistics  
-----
```

```
Tx DataFrames:          3213  
Rx DataFrames:          1606  
Tx HeartBeat Req:      31785  
Heartbeat Timeout:     0  
Rx Subscr Req:         2868  
Tx DataBytes:          10069  
Rx DataBytes:          37752  
Tx HeartBeat Fail:     2  
Tx Data Fail:          0  
Tx Conn Fail:          0
```

To view the mobility services summary, use the following command:

```
Device# show nmsp subscription summary
```

```
Mobility Services Subscribed:
```

```
Index Server IP Services  
-----
```

```
1 209.165.200.225 RSSI, Info, Statistics, AP Monitor, AP Info  
2 209.165.200.225 RSSI, Statistics, AP Info
```





## CHAPTER 28

# EDCA Parameters

---

- [Enhanced Distributed Channel Access Parameters, on page 201](#)
- [Configuring EDCA Parameters \(GUI\), on page 201](#)
- [Configuring EDCA Parameters \(CLI\), on page 202](#)

## Enhanced Distributed Channel Access Parameters

Enhanced Distributed Channel Access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality of service (QoS) traffic.

This section contains the following subsections:

## Configuring EDCA Parameters (GUI)

### Procedure

---

- Step 1** Choose **Configuration > Radio Configurations > Parameters**. Using this page, you can configure global parameters for 802.11a/n/ac (5 GHz) and 802.11b/g/n (2.4 GHz) radios.
- Note** You cannot configure or modify parameters, if the radio network is enabled. Disable the network status on the Configuration > Radio Configurations > Network page before you proceed.
- Step 2** In the **EDCA Parameters** section, choose an EDCA profile from the **EDCA Profile** drop-down list. Enhanced Distributed Channel Access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality-of-service (QoS) traffic.
- Step 3** Click **Apply**.
-

## Configuring EDCA Parameters (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ap dot11 {5ghz   24ghz } shutdown</b> <b>Example:</b> Device(config)# <code>ap dot11 5ghz shutdown</code>	Disables the radio network.
<b>Step 3</b>	<b>ap dot11 {5ghz   24ghz} edca-parameters {custom-voice   fastlane   optimized-video-voice   optimized-voice   svp-voice   wmm-default}</b> <b>Example:</b> Device(config)# <code>ap dot11 5ghz edca-parameters optimized-voice</code>	Enables specific EDCA parameters for the 802.11a or 802.11b/g network. <ul style="list-style-type: none"> <li>• <b>custom-voice:</b> Enables custom voice parameters for the 802.11a or 802.11b/g network.</li> <li>• <b>fastlane:</b> Enables the fastlane parameters for the 802.11a or 802.11b/g network.</li> <li>• <b>optimized-video-voice:</b> Enables EDCA voice-optimized and video-optimized parameters for the 802.11a or 802.11b/g network. Choose this option when both voice and video services are deployed on your network.</li> <li>• <b>optimized-voice:</b> Enables non-SpectraLink voice-optimized profile parameters for the 802.11a or 802.11b/g network. Choose this option when voice services other than SpectraLink are deployed on your network.</li> <li>• <b>svp-voice:</b> Enables SpectraLink voice-priority parameters for the 802.11a or 802.11b/g network. Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls.</li> <li>• <b>wmm-default:</b> Enables the Wi-Fi Multimedia (WMM) default parameters for the 802.11a or 802.11b/g network. This is the default option. Choose this option when voice or video services are not deployed on your network.</li> </ul>

	Command or Action	Purpose
<b>Step 4</b>	<b>no ap dot11 {5ghz   24ghz} shutdown</b> <b>Example:</b> Device(config)# <b>no ap dot11 5ghz shutdown</b>	Re-enables the radio network.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 6</b>	<b>show ap dot11 {5ghz   24ghz} network</b> <b>Example:</b> Device# <b>show ap dot11 5ghz network</b>	Displays the current status of MAC optimization for voice.







## CHAPTER 29

# 802.11 parameters and Band Selection

- [Information About Configuring Band Selection, 802.11 Bands, and Parameters, on page 205](#)
- [Restrictions for Band Selection, 802.11 Bands, and Parameters, on page 206](#)
- [How to Configure 802.11 Bands and Parameters, on page 207](#)
- [Monitoring Configuration Settings for Band Selection, 802.11 Bands, and Parameters, on page 216](#)
- [Configuration Examples for Band Selection, 802.11 Bands, and Parameters, on page 220](#)

## Information About Configuring Band Selection, 802.11 Bands, and Parameters

### Band Select

Band select enables client radios that are capable of dual-band (2.4 and 5-GHz) operations to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of 3 nonoverlapping channels. To prevent these sources of interference and improve overall network performance, configure band selection on the device.

Band select works by regulating probe responses to clients and it can be enabled on a per-WLAN basis. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels. In an access point, the band select table can be viewed by running the **show dot11 band-select** command. It can also be viewed by running the **show cont d0/d1 | begin Lru** command.

### Band Select Algorithm

The band select algorithm affects clients that use 2.4-GHz band. Initially, when a client sends a probe request to an access point, the corresponding client probe's Active and Count values (as seen from the band select table) become 1. The algorithm functions based on the following scenarios:

- Scenario 1: Client RSSI (as seen from the **show cont d0/d1 | begin RSSI** command output) is greater than both Mid RSSI and Acceptable Client RSSI.
  - Dual-band clients: No 2.4-GHz probe responses are seen at any time; 5-GHz probe responses are seen for all 5-GHz probe requests.
  - Single-band (2.4-GHz) clients: 2.4-GHz probe responses are seen only after the probe suppression cycle.

- After the client's probe count reaches the configured probe cycle count, the algorithm waits for the Age Out Suppression time and then marks the client probe's Active value as 0. Then, the algorithm is restarted.
- Scenario2: Client RSSI (as seen from **show cont d0/d1 | begin RSSI**) lies between Mid-RSSI and Acceptable Client RSSI.
  - All 2.4-GHz and 5-GHz probe requests are responded to without any restrictions.
  - This scenario is similar to the band select disabled.




---

**Note** The client RSSI value (as seen in the **sh cont d0 | begin RSSI** command output) is the average of the client packets received, and the Mid RSSI feature is the instantaneous RSSI value of the probe packets. As a result, the client RSSI is seen as weaker than the configured Mid RSSI value (7-dB delta). The 802.11b probes from the client are suppressed to push the client to associate with the 802.11a band.

---

## 802.11 Bands

You can configure the 802.11b/g/n (2.4 GHz) and 802.11a/n (5 GHz) bands for the controller to comply with the regulatory requirements in your country. By default, both 802.11b/g/n and 802.11a/n are enabled.

This section contains the following subsections:

## 802.11n Parameters

This section provides instructions for managing 802.11n access points on your network. The 802.11n devices support the 2.4 and 5-GHz bands and offer high throughput data rates.

The 802.11n high throughput rates are available on all the 802.11n access points for the WLANs using WMM with no Layer 2 encryption or with WPA2/AES encryption enabled.




---

**Note** Some Cisco 802.11n APs may intermittently emit incorrect beacon frames, which can trigger false wIPS alarms. We recommend that you ignore these alarms.

---

## 802.11h Parameters

802.11h informs client devices about channel changes and can limit the transmit power of those client devices.

## Restrictions for Band Selection, 802.11 Bands, and Parameters

- Band selection-enabled WLANs do not support time-sensitive applications such as voice and video because of roaming delays.
- Band selection is supported only on Cisco Wave 2 and 802.11ax APs.

For more information about support on specific APs, see

[https://www.cisco.com/c/en/us/td/docs/wireless/access\\_point/feature-matrix/ap-feature-matrix.html](https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html).

- Band selection operates only on APs that are connected to a controller. A FlexConnect AP without a controller connection does not perform band selection after a reboot.
- The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same AP, and it only runs on an AP when both the 2.4-GHz and 5-GHz radios are up and running.
- It is not possible to enable or disable band selection and client load balancing globally through the controller GUI or CLI. You can, however, enable or disable band selection and client load balancing for a particular WLAN. Band selection and client load balancing are enabled globally by default.

# How to Configure 802.11 Bands and Parameters

## Configuring Band Selection (GUI)

### Before you begin

Ensure that you have configured an AP Join Profile prior to configuring the primary and backup controllers.

### Procedure

- 
- Step 1** Choose **Configuration** > **Wireless Advanced** > **Band Select**.
  - Step 2** In the **Cycle Count** field, enter a value between 1 and 10. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.
  - Step 3** In the **Cycle Threshold (milliseconds)** field, enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle. The default cycle threshold is 200 milliseconds.
  - Step 4** In the **Age Out Suppression (seconds)** field, enter a value between 10 and 200 seconds. Age-out suppression sets the expiration time for pruning previously known 802.11b/g/n clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.
  - Step 5** In the **Age Out Dual Band (seconds)** field, enter a value between 10 and 300 seconds. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 50 seconds. After this time elapses, clients become new and are subject to probe response suppression.
  - Step 6** In the **Client RSSI (dbm)** field, enter a value between -90 to -20. This is the average of the client packets received.
  - Step 7** In the **Client Mid RSSI (dbm)** field, enter a value between -90 to -20. This is the instantaneous RSSI value of the probe packets.
  - Step 8** On the **AP Join Profile** page, click the AP Join Profile name.
  - Step 9** Click **Apply**.
-

## Configuring Band Selection (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless client band-select cycle-count</b> <i>cycle_count</i>  <b>Example:</b> Device(config)# <code>wireless client band-select cycle-count 3</code>	Sets the probe cycle count for band select. Valid range is between 1 and 10.
<b>Step 3</b>	<b>wireless client band-select cycle-threshold</b> <i>milliseconds</i>  <b>Example:</b> Device(config)# <code>wireless client band-select cycle-threshold 5000</code>	Sets the time threshold for a new scanning cycle period. Valid range is between 1 and 1000.
<b>Step 4</b>	<b>wireless client band-select expire suppression</b> <i>seconds</i>  <b>Example:</b> Device(config)# <code>wireless client band-select expire suppression 100</code>	Sets the suppression expire to the band select. Valid range is between 10 and 200.
<b>Step 5</b>	<b>wireless client band-select expire dual-band</b> <i>seconds</i>  <b>Example:</b> Device(config)# <code>wireless client band-select expire dual-band 100</code>	Sets the dual band expire. Valid range is between 10 and 300.
<b>Step 6</b>	<b>wireless client band-select client-rssi</b> <i>client_rssi</i>  <b>Example:</b> Device(config)# <code>wireless client band-select client-rssi 40</code>	Sets the client RSSI threshold. Valid range is between 20 and 90.
<b>Step 7</b>	<b>wlan wlan_profile_name wlan_ID SSID_network_name band-select</b>  <b>Example:</b> Device(config)# <code>wlan wlan1 25 ssid12</code>  Device(config-wlan)# <code>band-select</code>	Configures band selection on specific WLANs. Valid range is between 1 and 512. You can enter up to 32 alphanumeric characters for <i>SSID_network_name</i> parameter.

## Configuring the 802.11 Bands (GUI)

### Procedure

---

- Step 1** Choose **Configuration > Radio Configurations > Network**.
- Step 2** Click either **5 GHz Band** or **2.4 GHz Band**.
- Step 3** Uncheck the **Network Status** check box to disable the network in order to be able to configure the network parameters.
- Step 4** In the **Beacon Interval** field, enter the rate at which the SSID is broadcast by the APs, from 100 to 600 milliseconds. The default is 100 milliseconds.
- Step 5** For 802.11b/g/n (2.4-GHz) radios, to enable short preamble on the radio, check the **Short Preamble** check box. A short preamble improves throughput performance.
- Step 6** In the **Fragmentation Threshold (in bytes)** field, enter a value between 256 to 2346 bytes. Packets larger than the size you specify here will be fragmented.
- Step 7** Check the **DTPC Support** check box to advertise the transmit power level of the radio in the beacons and the probe responses. Client devices using dynamic transmit power control (DTPC) receive the channel and power level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan could rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there. You cannot configure a power constraint value on your 802.11a/n/ac (5-GHz) radio network if the **DTPC Support** check box is checked.
- Step 8** Click **Apply**.
- Step 9** In the **CCX Location Measurement** section, check the **Mode** check box to globally enable CCX radio management for the network. This parameter causes the APs connected to this device to issue broadcast radio measurement requests to clients running CCX v2 or later releases.
- Step 10** In the **Interval** field, enter a value to specify how often the APs must issue broadcast radio measurement requests.
- Step 11** Click **Apply**.
- Step 12** In the **Data Rates** section, choose a value to specify the rates at which data can be transmitted between the access point and the client:
- **Mandatory:** Clients must support this data rate in order to associate to an access point on the controller embedded wireless controller.
  - **Supported:** Any associated clients that support this data rate may communicate with the access point using that rate.
  - **Disabled:** The clients specify the data rates used for communication.
- Step 13** Click **Apply**.
- Step 14** Save the configuration.
- 

## Configuring the 802.11 Bands (CLI)

Follow the procedure given below to configure 802.11 bands and parameters:

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ap dot11 5ghz shutdown</b> <b>Example:</b> Device(config)# <code>ap dot11 5ghz shutdown</code>	Disables the 802.11a band. <b>Note</b> You must disable the 802.11a band before configuring the 802.11a network parameters.
<b>Step 3</b>	<b>ap dot11 24ghz shutdown</b> <b>Example:</b> Device(config)# <code>ap dot11 24ghz shutdown</code>	Disables the 802.11b band. <b>Note</b> You must disable the 802.11b band before configuring the 802.11b network parameters.
<b>Step 4</b>	<b>ap dot11 {5ghz   24ghz } beaconperiod</b> <i>time_unit</i> <b>Example:</b> Device(config)# <code>ap dot11 5ghz beaconperiod 500</code>	Specifies the rate at which the SSID is broadcast by the corresponding access point.  The beacon interval is measured in time units (TUs). One TU is 1024 microseconds. You can configure the access point to send a beacon every 20 to 1000 milliseconds.
<b>Step 5</b>	<b>ap dot11 {5ghz   24ghz } fragmentation</b> <i>threshold</i> <b>Example:</b> Device(config)# <code>ap dot11 5ghz fragmentation 300</code>	Specifies the size at which packets are fragmented.  The threshold is a value between 256 and 2346 bytes (inclusive). Specify a low number for areas where communication is poor or where there is a great deal of radio interference.
<b>Step 6</b>	<b>[no] ap dot11 {5ghz   24ghz } dtpc</b> <b>Example:</b> Device(config)# <code>ap dot11 5ghz dtpc</code> Device(config)# <code>no ap dot11 24ghz dtpc</code>	Enables access points to advertise their channels and transmit the power levels in beacons and probe responses.  The default value is enabled. Client devices using dynamic transmit power control (DTPC) receive the channel-level and power-level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan can rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there.  The <b>no</b> form of the command disables the DTPC setting.
<b>Step 7</b>	<b>wireless client association limit</b> <i>number</i> <i>interval milliseconds</i>	Specifies the maximum allowed clients that can be configured.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device(config)# wireless client association limit 50 interval 1000</pre>	<p>You can configure the maximum number of association requests on a single access point slot at a given interval. The range of association limit that you can configure is from 1 to 100.</p> <p>The association request limit interval is measured between 100 to 10000 milliseconds.</p>
<b>Step 8</b>	<p><b>ap dot11 {5ghz   24ghz} rate rate {disable   mandatory   supported}</b></p> <p><b>Example:</b></p> <pre>Device(config)# ap dot11 5ghz rate 36 mandatory</pre>	<p>Specifies the rate at which data can be transmitted between the controller embedded wireless controller and the client.</p> <ul style="list-style-type: none"> <li>• <b>disable:</b> Defines that the clients specify the data rates used for communication.</li> <li>• <b>mandatory:</b> Defines that the clients support this data rate in order to associate to an access point on the controller embedded wireless controller.</li> <li>• <b>supported:</b> Any associated clients that support this data rate can communicate with the access point using that rate. However, the clients are not required to use this rate in order to associate.</li> <li>• <b>rate:</b> Specifies the rate at which data is transmitted. For the 802.11a and 802.11b bands, the data is transmitted at the rate of 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps.</li> </ul>
<b>Step 9</b>	<p><b>no ap dot11 5ghz shutdown</b></p> <p><b>Example:</b></p> <pre>Device(config)# no ap dot11 5ghz shutdown</pre>	<p>Enables the 802.11a band.</p> <p><b>Note</b> The default value is enabled.</p>
<b>Step 10</b>	<p><b>no ap dot11 24ghz shutdown</b></p> <p><b>Example:</b></p> <pre>Device(config)# no ap dot11 24ghz shutdown</pre>	<p>Enables the 802.11b band.</p> <p><b>Note</b> The default value is enabled.</p>
<b>Step 11</b>	<p><b>ap dot11 24ghz dot11g</b></p> <p><b>Example:</b></p> <pre>Device(config)# ap dot11 24ghz dot11g</pre>	<p>Enables or disables 802.11g network support.</p> <p>The default value is enabled. You can use this command only if the 802.11b band is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support.</p>

	Command or Action	Purpose
<b>Step 12</b>	<b>end</b>  <b>Example:</b> Device (config) # <b>end</b>	Returns to privileged EXEC mode.

## Configuring a Band-Select RF Profile (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Wireless > Advanced**.
- Step 2** In the **Band Select** tab, enter a value between 1 and 10 in the **Cycle Count** field. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.
- Step 3** In the **Cycle Threshold** field, enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle. The default cycle threshold is 200 milliseconds.
- Step 4** In the **Age Out Suppression** field, enter a value between 10 and 200 seconds. Age-out suppression sets the expiration time for pruning previously known 802.11b/g/n clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.
- Step 5** In the **Age Out Dual Band** field, enter a value between 10 and 300 seconds. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 50 seconds. After this time elapses, clients become new and are subject to probe response suppression.
- Step 6** In the **Client RSSI** field, enter a value between -90 dBm and -20 dBm. This is the minimum RSSI for a client to respond to a probe.
- Step 7** In the **Client Mid RSSI** field, enter a value between -20 dBm and -90 dBm. This parameter sets the mid-RSSI, whose value can be used for toggling 2.4 GHz probe suppression based on the RSSI value.
- Step 8** Click **Apply**.
- 

## Configuring 802.11n Parameters (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > RF**.
- Step 2** Click **Add** to view the **Add RF Profile** window.
- Step 3** In the **802.11** tab, proceed as follows:
- Choose the required operational rates.
  - Select the required **802.11n MCS Rates** by checking the corresponding check boxes.
- Step 4** Click **Save & Apply to Device**.
-



## Configuring 802.11n Parameters (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ap dot11 {5ghz   24ghz} dot11n</b> <b>Example:</b> Device(config)# <code>ap dot11 5ghz dot11n</code>	Enables 802.11n support on the network.  The <b>no</b> form of this command disables the 802.11n support on the network.
<b>Step 3</b>	<b>ap dot11 {5ghz   24ghz} dot11n mcs tx rtu</b> <b>Example:</b> Device(config)# <code>ap dot11 5ghz dot11n mcs tx 20</code>	Specifies the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client.  <i>rtu</i> -The valid range is between 0 and 23.  The <b>no</b> form of this command disables the MCS rates that are configured.
<b>Step 4</b>	<b>wlan wlan_profile_name wlan_ID SSID_network_name wmm require</b> <b>Example:</b> Device(config)# <code>wlan wlan1 25 ssid12</code> Device(config-wlan)# <code>wmm require</code>	Enables WMM on the WLAN and uses the 802.11n data rates that you configured.  The <b>require</b> keyword requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.
<b>Step 5</b>	<b>ap dot11 {5ghz   24ghz} shutdown</b> <b>Example:</b> Device(config)# <code>ap dot11 5ghz shutdown</code>	Disables the network.
<b>Step 6</b>	<b>{ap   no ap} dot11 {5ghz   24 ghz} dot11n a-mpdu tx priority {all   0-7}</b> <b>Example:</b> Device(config)# <code>ap dot11 5ghz dot11n a-mpdu tx priority all</code>	Specifies the aggregation method used for 802.11n packets.  Aggregation is the process of grouping packet data frames together, rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU). Both A-MPDU and A-MSDU are performed in the software.  You can specify the aggregation method for various types of traffic from the access point to the clients.  The list defines the priority levels (0-7) assigned per traffic type.  • 0—Best effort

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• 1—Background</li> <li>• 2—Spare</li> <li>• 3—Excellent effort</li> <li>• 4—Controlled load</li> <li>• 5—Video, less than 100-ms latency and jitter</li> <li>• 6—Voice, less than 100-ms latency and jitter</li> <li>• 7—Network control</li> </ul> <p>You can configure each priority level independently, or you can use the all the parameters to configure all the priority levels at once. You can configure priority levels so that the traffic uses either A-MPDU transmission or A-MSDU transmission.</p> <ul style="list-style-type: none"> <li>• When you use the <b>ap</b> command along with the other options, the traffic associated with that priority level uses A-MPDU transmission.</li> <li>• When you use the <b>no ap</b> command along with the other options, the traffic associated with that priority level uses A-MSDU transmission.</li> </ul> <p>Configure the priority levels to match the aggregation method used by the clients. By default, A-MPDU is enabled for priority level 0, 4, and 5, and the rest are disabled. By default, A-MPDU is enabled for all priorities except 6 and 7.</p>
<b>Step 7</b>	<b>no ap dot11 {5ghz   24ghz} shutdown</b>  <b>Example:</b> Device(config)# <b>no ap dot11 5ghz shutdown</b>	Re-enables the network.
<b>Step 8</b>	<b>ap dot11 {5ghz   24ghz} dot11n guard-interval {any   long}</b>  <b>Example:</b> Device(config)# <b>ap dot11 5ghz dot11n guard-interval long</b>	Configures the guard interval for the network.

	Command or Action	Purpose
<b>Step 9</b>	<b>ap dot11 {5ghz   24ghz} dot11n rifs rx</b> <b>Example:</b> Device(config)# <b>ap dot11 5ghz dot11n rifs rx</b>	Configures the Reduced Interframe Space (RIFS) for the network.
<b>Step 10</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring 802.11h Parameters (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>ap dot11 5ghz shutdown</b> <b>Example:</b> Device(config)# <b>ap dot11 5ghz shutdown</b>	Disables the 802.11 network.
<b>Step 2</b>	<b>{ap   no ap} dot11 5ghz channelswitch mode switch_mode</b> <b>Example:</b> Device(config)# <b>ap dot11 5ghz channelswitch mode 0</b>	Enables or disables the access point to announce when it is switching to a new channel.  <i>switch_mode</i> --Enter 0 or 1 to specify whether transmissions are restricted until the actual channel switch ( <b>0</b> ) or are not restricted ( <b>1</b> ). The default value is disabled.
<b>Step 3</b>	<b>ap dot11 5ghz power-constraint value</b> <b>Example:</b> Device(config)# <b>ap dot11 5ghz power-constraint 200</b>	Configures the 802.11h power constraint value in dB. The valid range is from 0 to 255.  The default value is 3.
<b>Step 4</b>	<b>no ap dot11 5ghz shutdown</b> <b>Example:</b> Device(config)# <b>no ap dot11 5ghz shutdown</b>	Re-enables the 802.11a network.

# Monitoring Configuration Settings for Band Selection, 802.11 Bands, and Parameters

## Verifying Configuration Settings Using Band Selection and 802.11 Bands Commands

The following commands can be used to verify band selection, 802.11 bands, and parameters on the embedded wireless controller.

*Table 5: Monitoring Configuration Settings Using Band Selection and 802.11 Band Commands*

Command	Purpose
<b>show ap dot11 5ghz network</b>	Displays 802.11a band network parameters, 802.11a operational rates, 802.11n MCS settings, and 802.11n status information.
<b>show ap dot11 24ghz network</b>	Displays 802.11b band network parameters, 802.11b/g operational rates, 802.11n MCS settings, and 802.11n status information.
<b>show wireless dot11h</b>	Displays 802.11h configuration parameters.
<b>show wireless band-select</b>	Displays band-select configuration settings.

## Example: Viewing the Configuration Settings for the 5-GHz Band

```

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
```

**Example: Viewing the Configuration Settings for the 2.4-GHz Band**

```

SIP Codec Type : CODEC_TYPE_G711
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

```

**Example: Viewing the Configuration Settings for the 2.4-GHz Band**

```

Device# 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
802.11g 6M : Supported
802.11g 9M : Supported
802.11b 11M : Mandatory
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
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 : 11
Default Tx Power Level : 1
DTPC Status : true
Call Admission Limit : 105
G711 CU Quantum : 15
ED Threshold : -50
Fragmentation Threshold : 2346
PBCC Mandatory : Disabled
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
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 : 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 Codec Type : CODEC_TYPE_G711
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
```

## Example: Viewing the status of 802.11h Parameters

```
Device# show wireless dot11h
Power Constraint: 0
Channel Switch: 0
Channel Switch Mode: 0
```

## Example: Verifying the Band-Selection Settings

The following example displays a band-select configuration:

```
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
Client Mid RSSI (dBm)     : -80
```

# Configuration Examples for Band Selection, 802.11 Bands, and Parameters

## Examples: Band Selection Configuration

This example shows how to set the probe cycle count and time threshold for a new scanning cycle period for band select:

```
Device# configure terminal
Device(config)# wireless client band-select cycle-count 3
Device(config)# wireless client band-select cycle-threshold 5000
Device(config)# end
```

This example shows how to set the suppression expiry time to the band select:

```
Device# configure terminal
Device(config)# wireless client band-select expire suppression 100
Device(config)# end
```

This example shows how to set the dual-band expiry time for the band select:

```
Device# configure terminal
Device(config)# wireless client band-select expire dual-band 100
Device(config)# end
```

This example shows how to set the client RSSI threshold for the band select:

```
Device# configure terminal
Device(config)# wireless client band-select client-rssi 40
Device(config)# end
```

This example shows how to configure band selection on specific WLANs:

```
Device# configure terminal
Device(config)# wlan wlan1 25 ssid12
Device(config-wlan)# band-select
Device(config)# end
```



## Examples: 802.11 Bands Configuration

This example shows how to configure 802.11 bands using beacon interval, fragmentation, and dynamic transmit power control:

```
Device# configure terminal
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 24ghz shutdown
Device(config)# ap dot11 5ghz beaconperiod 500
Device(config)# ap dot11 5ghz fragmentation 300
Device(config)# ap dot11 5ghz dtpc
Device(config)# wireless client association limit 50 interval 1000
Device(config)# ap dot11 5ghz rate 36 mandatory
Device(config)# no ap dot11 5ghz shutdown
Device(config)# no ap dot11 24ghz shutdown
Device(config)# ap dot11 24ghz dot11g
Device(config)#end
```

## Examples: 802.11n Configuration

This example shows how to configure 802.11n parameters for 5-GHz band using aggregation method:

```
Device# configure terminal
Device(config)# ap dot11 5ghz dot11n
Device(config)# ap dot11 5ghz dot11n mcs tx 20
Device(config)# wlan wlan1 25 ssid12
Device(config-wlan)# wmm require\
Device(config-wlan)# exit
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz dot11n a-mpdu tx priority all
Device(config)# no ap dot11 5ghz shutdown
Device(config)#exit
```

This example shows how to configure the guard interval for 5-GHz band:

```
Device# configure terminal
Device(config)# ap dot11 5ghz dot11n
Device(config)# ap dot11 5ghz dot11n mcs tx 20
Device(config)# wlan wlan1 25 ssid12
Device(config-wlan)# wmm require\
Device(config-wlan)# exit
Device(config)# no ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz dot11n guard-interval long
Device(config)#end
```

This example shows how to configure the RIFS for 5-GHz band:

```
Device# configure terminal
Device(config)# ap dot11 5ghz dot11n
Device(config)# ap dot11 5ghz dot11n mcs tx 20
Device(config)# wlan wlan1 25 ssid12
Device(config-wlan)# wmm require\
Device(config-wlan)# exit
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz dot11n rifs rx
Device(config)#end
```

## Examples: 802.11h Configuration

This example shows how to configure the access point to announce when it is switching to a new channel using restriction transmission:

```
Device# configure terminal
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz channelswitch mode 0
Device(config)# no ap dot11 5ghz shutdown
Device(config)#end
```

This example shows how to configure the 802.11h power constraint for 5-GHz band:

```
Device# configure terminal
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz power-constraint 200
Device(config)# no ap dot11 5ghz shutdown
Device(config)#end
```



## CHAPTER 30

# Image Download

---

- [Information About Image Download, on page 223](#)
- [Prerequisites for Image Download, on page 226](#)
- [Configuring Image Download Profile, on page 227](#)
- [Initiating Pre-Download \(CLI\), on page 235](#)
- [Verifying Image Download, on page 236](#)

## Information About Image Download

Software updates ensure that all the access points in the Cisco Embedded Wireless Controller network are running the latest software. The software update or image download can be performed using both the GUI and the CLI.

A typical Cisco Embedded Wireless Controller network contains the following components:

- Cisco Catalyst APs acting as controller (embedded wireless controller)
- Cisco Embedded Wireless Controller-capable APs (Other Cisco Catalyst series APs that participate in the Virtual Router Redundancy Protocol (VRRP)-based election process)
- Subordinate APs (Cisco Catalyst Series or Cisco Aironet Series Wave 2 APs)
- External TFTP and SFTP server.



---

**Note** For best user experience when using the GUI, view the browser at 100% resolution. The lines may break if the resolution is greater than 100%.

---

## Updates to the AP Image Predownload Status (GUI)

From Cisco IOS XE Amsterdam, Release 17.3.1 onwards, during an access point (AP) image download, the Cisco Embedded Wireless Controller on Catalyst Access Points calculates the current percentage of the download and the estimated completion time of the download. (You can view these values in the CLI output by running the **show wireless ewc-ap ap image predownload status** command.)

To access the **Software Upgrade** window, from the Cisco Embedded Wireless Controller on Catalyst Access Points home page, choose **Administration > Software Management > Software Upgrade**.

The **Software Update Status** section in the GUI displays the update status bar that shows the progress of a software update, such as, **Initiate, Controller Image Download, AP Image Download, Network Upgrade, Activate, and Reload.**

To view the logs, click the **Show Install Logs** link.

The **Status** field displays the current status of the upgrade and indicates further action, if any, that you should perform.

The other details displayed in the window are - **Total Number of APs, Initiated, Predownloading AP Image, Predownloading Controller Image, Completed Predownloading AP Image, Completed Predownloading Controller Image, Failed to Predownload AP Image, Failed to Predownload Controller Image.**

The currently active AP, the AP on standby, and the preferred active AP are also displayed.

## Image Download Scenarios

In a Cisco Embedded Wireless Controller network, image download from the embedded wireless controller to the subordinate AP takes place in the following scenarios:

- During AP join
- During network software upgrade (pre-download)

### Image Download During AP Join

APs with older software trying to join the Cisco Embedded Wireless Controller network are automatically upgraded to match the latest software version on the embedded wireless controller. The embedded wireless controller compares the software version on the new AP with that on itself. If there is a mismatch, the AP requests the controller for a software upgrade and image download is triggered. The embedded wireless controller facilitates the transfer of the latest software from an external TFTP server or SFTP server, to the new AP.

Depending on the new AP joining the network, there are two image downloads that take place:

- **AP software image download:** This applies to all new APs joining the Cisco Embedded Wireless Controller.
- **Controller software image download:** This applies only to Cisco Catalyst series APs, capable of becoming a controller, trying to join the Cisco Embedded Wireless Controller network.

### AP Software Image Download

Any Cisco Catalyst Series AP or Cisco Aironet Series Wave 2 AP can only join an embedded wireless controller if its AP software image version matches that of the controller.

During the AP join process, the embedded wireless controller first checks the AP software image version on the new AP and if it does not match what is on the controller, the latest AP software is downloaded from the controller to the new AP. Once the AP software image on the new AP is upgraded to match the version that is on the embedded wireless controller in the network, the new AP reloads. Once the new AP is back up with the upgraded AP software image, it joins the embedded wireless controller.

### Controller Software Image Download

If the new AP joining the network is a Cisco Catalyst Series AP capable of becoming an embedded wireless controller, first the controller checks the AP software image on the new AP and if outdated, it is upgraded to

match the AP software version on the controller. The AP then reloads with the new AP software image and joins the embedded wireless controller in the network.

Next, the embedded wireless controller does a similar check to compare the controller software version on the embedded wireless controller-capable AP. Similar to the AP software upgrade, if there is a mismatch, the controller software on this Cisco Catalyst Series AP is also upgraded to the latest version on the embedded wireless controller. The AP reloads again, this time with the upgraded controller software image.

### Efficient AP Join

If the Cisco Embedded Wireless Controller network contains an AP of the same image type as the newly joining AP, then the new AP downloads the AP software image from this AP. For example, if a Cisco Catalyst 9130AX Series AP is newly joining the Cisco Embedded Wireless Controller network and another Cisco Catalyst 9130AX Series AP already exists in the network, then the new AP gets its AP software image from the already joined AP.

This method, known as efficient AP join, enables homogenous APs to get the software locally (within the Cisco Embedded Wireless Controller network) rather than downloading it from an external server. This improves software download efficiency.

The first AP of a series that joins the network and downloads the software from the embedded wireless controller is called a primary image. The other APs of the same series are known as image subordinates.

## Network Software Upgrade (Pre-Download)

In the pre-download scenario, image download in the Cisco Embedded Wireless Controller network occurs to upgrade the software on all the APs from one software version to another. However, these APs continue to serve existing as well as new clients and there is no network disruption.

For pre-download, all the APs should be connected to the embedded wireless controller in a stable join state. Once image download is initiated during pre-download, new APs are not allowed to join the embedded wireless controller.

### Efficient AP Upgrade

In this method, the first AP of an AP series to get the image from the embedded wireless controller becomes the primary image. The remaining APs of the same AP series, the image subordinates, then download the software image locally from this primary image. This method is also known as efficient AP upgrade.

## Methods Supported for Image Download

In a Cisco Embedded Wireless Controller network, there are four ways in which the software image can be downloaded from the embedded wireless controller. These methods are based on the location from where the controller transfers the software image to the subordinate AP:

- From an external TFTP server
- From an external SFTP server
- From the desktop (via HTTP)

## TFTP Image Download Method

In the TFTP method, the AP and controller software images are stored on a TFTP server. To download the software images from the TFTP server, you need to specify the IP address of the TFTP server and the path to the software image bundle on the TFTP server.

The TFTP image download method can be triggered using both the GUI and CLI.

## SFTP Image Download Method

In the SFTP method, the AP and controller software images are stored on an SFTP server. To download the software images from the SFTP server, in addition to the IP address of the SFTP server and the software image bundle path, you need to specify the SFTP server credentials.

The SFTP image download method also can be triggered using both the GUI and CLI.

## Desktop (HTTP) Image Download Method

Image download through desktop (HTTP) is applicable only in the network software upgrade (pre-download) scenario.

For the desktop (HTTP) method, download the software image bundle for the Cisco Embedded Wireless Controller to your computer or laptop desktop. This downloaded bundle contains the AP and controller software images which need to be extracted to the computer or laptop desktop before they can be uploaded to the embedded wireless controller.

Note that the desktop (HTTP) method works only for a homogenous network. A homogenous Cisco Embedded Wireless Controller network is one which contains APs that have the same AP software image type. For example, the Cisco Catalyst 9115AX series AP and the Cisco Catalyst 9120AX series AP use the ap1g7 AP software image file. So, the Cisco Embedded Wireless Controller network in this example containing Cisco Catalyst 9115AX series and 9120AX series APs is a homogenous network.

The embedded wireless controller CLI can only be used to set the mode for image download as desktop (HTTP). The Cisco Embedded Wireless Controller GUI has to be used to configure and trigger network software upgrade (pre-download) using the desktop (HTTP) image download method.

## Prerequisites for Image Download

- Connectivity to an external (TFTP or SFTP) server is required for image download during AP join in a Cisco Embedded Wireless Controller network.
- Connectivity to a PC or laptop is required for image download during network software upgrade in a Cisco Embedded Wireless Controller network.
- All APs should be connected to the embedded wireless controller for image download in the network software upgrade (pre-download) scenario.
- For image upgrade, you must not configure a preferred-master. If you configure a preferred-master, ensure that it points to the currently active AP, which is displayed in the **show wireless ewc-ap redundancy summary** command.

If a different AP is configured as the preferred-master, the upgrade process will not take place in the **install activate** step. If the upgrade does not take place, you should either remove the preferred-master

configuration, or re-configure the preferred-master to match the AP that is currently active, and then run the **install activate** command, again.

.

## Configuring Image Download Profile

You need to configure the image download profile for both the AP join image download and pre-download scenarios. The only profile supported is *default*. In a Cisco Embedded Wireless Controller network, only one site tag is supported, the *default-site-tag*. The *default* image download profile is attached to the *default-site-tag*.

## Configuring TFTP Image Download (GUI)

### Procedure

- 
- Step 1** Choose **Administration > Software Management**.
- Step 2** On the **Software Management** page, under the **Software Upgrade** tab, select the **Mode** as TFTP.
- Step 3** In the **Image Server** field, enter the TFTP server IP address.
- Step 4** In the **Image Path** field, enter the absolute or relative path to the software image bundle.
- Step 5** Choose one of the following:
- **Save:** Choose this option to save the image download profile and enable image download for new APs joining the Cisco Embedded Wireless Controller network.
  - **Save & Download:** Choose this option to save the configuration and enable network software upgrade (pre-download). The image download profile is saved (even if no change is made to the configuration) and the latest image is downloaded in the background. This allows the APs to continue serving the clients.
  - **Activate:** Choose this option to enable the APs in the network to swap to the latest image and reboot. The Cisco Embedded Wireless Controller network is activated once the APs come up with the new image file.
  - **Cancel:** Choose this option to cancel any changes made to the image download profile.

Option	Description
Save	Choose this option to save the image download profile and enable image download for new APs joining the Cisco Embedded Wireless Controller network.
Save & Download	Choose this option to save the configuration and enable network software upgrade (pre-download). The image download profile is saved (even if no change is made to the configuration) and the latest image is downloaded in the background. This allows the APs to continue serving the clients.
Activate	Choose this option to enable the APs in the network to swap to the latest image and reboot. The Cisco Embedded Wireless Controller network is activated once the APs come up with the new image file.

Option	Description
Cancel	Choose this option to cancel any changes made to the image download profile.

## Configuring TFTP Image Download (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile image-download default</b> <b>Example:</b> Device (config)# <b>wireless profile image-download default</b>	Configures the default AP profile.
<b>Step 3</b>	<b>image-download-mode tftp</b> <b>Example:</b> Device (config-wireless-image-download-profile)# <b>image-download-mode tftp</b>	Configure image download using TFTP.
<b>Step 4</b>	<b>tftp-image-server server-ip</b> <b>Example:</b> Device (config-wireless-image-download-profile-tftp)# <b>tftp-image-server 10.1.1.1</b>	Configure the TFTP server for image download by specifying the IPv4 or IPv6 <i>server-ip</i> address.
<b>Step 5</b>	<b>tftp-image-path server-path</b> <b>Example:</b> Device (config-wireless-image-download-profile-tftp)# <b>tftp-image-path</b> <i>/download/object/stream/images/ap-images</i>	Configure the absolute or relative path to the software image on the TFTP server.
<b>Step 6</b>	<b>end</b> <b>Example:</b> Device (config-wireless-image-download-profile-tftp)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.



## Configuring SFTP Image Download (GUI)

### Procedure

- Step 1** Choose **Administration > Software Management**.
- Step 2** On the **Software Management** page, under the **Software Upgrade** tab, select the **Mode** as SFTP.  
The SFTP port is not configurable and is fixed at 22.
- Step 3** In the **Image Server** field, enter the SFTP server IP address.
- Step 4** In the **Image Path** field, enter the path to the software image bundle.
- Step 5** In the **User Name** field, enter the SFTP server username.
- Step 6** Choose the appropriate **Password Type** from Unencrypted or AES Encrypted.
- Step 7** In the **Password** field, enter the SFTP server password.
- Step 8** Choose one of the following:

Option	Description
Save	Choose this option to save the image download profile and enable image download for new APs joining the Cisco Embedded Wireless Controller network.
Save & Download	Choose this option to save the configuration and enable network software upgrade (pre-download). The image download profile is saved (even if no change is made to the configuration) and the latest image is downloaded in the background. This allows the APs to continue serving the clients.
Activate	Choose this option to enable the APs in the network to swap to the latest image and reboot. The Cisco Embedded Wireless Controller network is activated once the APs come up with the new image file.
Cancel	Choose this option to cancel any changes made to the image download profile.

## Configuring SFTP Image Download (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile image-download default</b> <b>Example:</b> Device (config)# <b>wireless profile image-download default</b>	Configures the default AP profile.

	Command or Action	Purpose
<b>Step 3</b>	<b>image-download-mode sftp</b> <b>Example:</b> Device (config-wireless-image-download-profile) # <b>image-download-mode sftp</b>	Configure image download using SFTP.
<b>Step 4</b>	<b>sftp-image-server server-ip</b> <b>Example:</b> Device (config-wireless-image-download-profile-sftp) # <b>sftp-image-server 10.1.1.1</b>	Configure the SFTP server for image download by specifying the IPv4 or IPv6 <i>server-ip</i> address.
<b>Step 5</b>	<b>sftp-image-path server-path</b> <b>Example:</b> Device (config-wireless-image-download-profile-sftp) # <b>sftp-image-path</b> <i>/download/object/stream/images/ap-images</i>	Configure the path to the software image on the SFTP server.
<b>Step 6</b>	<b>sftp-username username</b> <b>Example:</b> Device (config-wireless-image-download-profile-sftp) # <b>sftp-username test</b>	Specify the username to log in to the SFTP server for image download.
<b>Step 7</b>	<b>sftp-password {0 8} password</b> <b>Example:</b> Device (config-wireless-image-download-profile-sftp) # <b>sftp-password 0 password1</b>	Specify the password associated with the above username to download the image from the SFTP server. You need to re-enter the password to confirm the entry.  To configure an AES encrypted password, specify 8, else specify 0 to configure an unencrypted password.
<b>Step 8</b>	<b>end</b> <b>Example:</b> Device (config-wireless-image-download-profile-tftp) # <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring CCO Mode for Software Upgrade (GUI)

### Before you begin

The CCO account must have a physical address entered at the CCO Profile Manager. The account must have EULA and K9 acknowledged. For more information about creating a CCO account, refer to <https://www.cisco.com/c/en/us/about/help/registration-benefits-help.html>.

## Procedure

- Step 1** Choose **Administration > Software Management**.
- Step 2** On the **Software Management** page, under the **Software Upgrade** tab, select the **Mode** as CCO.
- Step 3** In the **User Name** field, enter the CCO username.
- Step 4** In the **Password** field, enter the password to access the CCO server.
- Step 5** Choose the appropriate **Password Type** from Unencrypted or AES Encrypted.
- Step 6** Choose either Enabled or Disabled from the **Automatically Check for Updates** field. If you enable this option, the system automatically checks for software updates.
- The interval is for 30 days. After the interval expires, the controller automatically checks and updates for the latest or recommend software version information in the controller configuration.
- Step 7** In the **Software Check** field, click the **Check now** button and retrieve up-to-date information about the **Latest software release** (the latest version available on the CCO website) and the **Recommended software release** (the recommended software version for the currently running software) version numbers.
- Step 8** The **Last CCO Response** field displays the error messages encountered when configuring the CCO image download method. For example, if you have entered a wrong username and password, the following error message is displayed: HTTP 400 Error: 400 Client Error: Bad Request for url: <https://cloudsso.cisco.com/as/token.oauth2> Please check your username/password and try again. For more information about the **Last CCO Response** error messages, refer to [Troubleshooting - CCO Image Download Error Messages](#), on page 234.
- Step 9** From the **Version** drop-down list, choose either **Recommended** or **Latest**. After fetching the latest and the recommended software versions, you can choose the version to upgrade.

- Step 10** Choose one of the following:

Option	Description
Save	Choose this option to save the image download profile and enable image download for new APs joining the Cisco Embedded Wireless Controller network.
Save & Download	Choose this option to save the configuration and enable network software upgrade (pre-download). The image download profile is saved (even if no change is made to the configuration) and the latest image is downloaded in the background. This allows the APs to continue serving the clients.
Activate	Choose this option to enable the APs in the network to swap to the latest image and reboot. The Cisco Embedded Wireless Controller network is activated once the APs come up with the new image file.
Cancel	Choose this option to cancel any changes made to the image download profile.

## Configuring CCO Image Download (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile image-download default</b> <b>Example:</b> Device (config)# <b>wireless profile image-download default</b>	Configures the default AP profile.
<b>Step 3</b>	<b>image-download-mode cco</b> <b>Example:</b> Device (config-wireless-image-download-profile)# <b>image-download-mode cco</b>	Configure image download using CCO.
<b>Step 4</b>	<b>cco-username username</b> <b>Example:</b> Device (config-wireless-image-download-profile-cco)# <b>cco-username username</b>	Specify the username to log in to the CCO server for image download.
<b>Step 5</b>	<b>cco-password {0   8} password</b> <b>Example:</b> Device (config-wireless-image-download-profile-cco)# <b>cco-password 0 password1</b>	Specify the password associated with the above username to download the image from the CCO server. You need to re-enter the password to confirm the entry.  To configure an AES encrypted password, specify 8, else specify 0 to configure an unencrypted password.
<b>Step 6</b>	<b>cco-version {latest   suggested}</b> <b>Example:</b> Device (config-wireless-image-download-profile-cco)# <b>cco-version latest</b>	Specify the <b>latest</b> or the <b>suggested</b> version to be downloaded from the CCO server. By default the <b>suggested</b> version is downloaded.
<b>Step 7</b>	<b>cco-auto-check</b> <b>Example:</b> Device (config-wireless-image-download-profile-cco)# <b>cco-auto-check</b>	Enables or disables automatic check of new software versions at CCO every 30 days. This is applicable to Image Upgrade or Predownload only. By default, <b>cco-auto-check</b> is enabled. To disable the command use the <b>no</b> form of the command.

	Command or Action	Purpose
<b>Step 8</b>	<b>end</b> <b>Example:</b> Device (config-wireless-image-download-profile-cco) # <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.
<b>Step 9</b>	<b>wireless ewc-ap predownload poll-cco</b> <b>Example:</b> Device# <b>wireless ewc-ap predownload poll-cco</b>	Polls the CCO server to check for the latest software version.
<b>Step 10</b>	<b>clear ap predownload statistics</b> <b>Example:</b> Device# <b>clear ap predownload statistics</b>	Clears the AP predownload statistics.
<b>Step 11</b>	<b>install remove profile default</b> <b>Example:</b> Device# <b>install remove profile default</b>	Removes the image download profile. Choose <b>Y</b> to remove the profile or choose <b>N</b> to cancel.
<b>Step 12</b>	<b>install add profile default</b> <b>Example:</b> Device# <b>clear ap predownload statistics</b>	Downloads the controller and AP software image from the embedded wireless controller.  The controller image is sent to all Cisco Embedded Wireless Controller-capable APs. The AP image is downloaded to all APs sharing the same image type
<b>Step 13</b>	<b>install activate</b> <b>Example:</b> Device# <b>install activate</b>	Activates the network after upgrade.  All the subordinate APs get the new AP image and reboot. Once all APs are rebooted, the embedded wireless controller also reboots.  <b>Note</b> The network can also be activated if the controller image is downloaded but all APs have not received the AP image via predownload.  <b>Important</b> If the network is activated during partial predownload success, and a Cisco Embedded Wireless Controller-capable AP with old controller software becomes the controller, then the network will not get upgraded to the new image.

	Command or Action	Purpose
<b>Step 14</b>	<b>install commit</b> <b>Example:</b> Device# <b>install commit</b>	Commits the current software image once the embedded wireless controller comes up after rebooting.

## Troubleshooting - CCO Image Download Error Messages

Following are the expected error messages and the causes, which will be displayed at the **Last CCO Response** field:

### DNS resolution or connectivity issue

Connection Error: HTTPSConnectionPool(host='cloudsso.cisco.com', port=443): Max retries exceeded with url: /as/token.oauth2 (Caused by NewConnectionError('<urllib3.connection.VerifiedHTTPSConnection object at 0xf6170250>: Failed to establish a new connection: [Errno -3] Temporary failure in name resolution',))

### CCO username/password error

HTTP 400 Error: 400 Client Error: Bad Request for url: <https://cloudsso.cisco.com/as/token.oauth2> Please check your username/password and try again

### Address missing exception

Thank you for registering with Cisco.com. In order to consume software or services we require your full address. Please follow [this link](https://rpfa.cloudapps.cisco.com/rpfa/profile/profile_management.do) to return to profile manager to complete your profile.

### EULA form missing exception

Eula form have not been accepted or rejected to continue download. Please go to <https://software.cisco.com/download/eula>.

### K9 form missing exception

K9 form have not been accepted or rejected to continue download. Please go to <https://software.cisco.com/download/k9>

## Configuring Desktop (HTTP) Image Download (GUI)

- Image download using desktop (HTTP) is only enabled in a homogeneous network, that is a network containing APs that have the same image type.
- Image download using desktop (HTTP) can only be configured from the GUI.
- The CLI can only be used to set the image download mode to desktop (HTTP).

## Procedure

- Step 1** Choose **Administration > Software Management**.
- Step 2** On the **Software Management** page, under the **Software Upgrade** tab, select the **Mode** as Desktop (HTTP).
- Step 3** In the **Controller Image** field, navigate to the embedded wireless controller software image on your computer or laptop desktop.
- Step 4** In the **AP Image** field, navigate to the AP software image on your computer or laptop desktop.

The GUI displays the name of the AP image to be used. Depending on the AP model, the name of the AP image varies.

- Step 5** Choose one of the following:

Option	Description
Save	Choose this option to save the image download profile and enable image download for new APs joining the Cisco Embedded Wireless Controller network.
Save & Download	Choose this option to save the configuration and enable network software upgrade (pre-download). The image download profile is saved (even if no change is made to the configuration) and the latest image is downloaded in the background. This allows the APs to continue serving the clients.
Activate	Choose this option to enable the APs in the network to swap to the latest image and reboot. The Cisco Embedded Wireless Controller network is activated once the APs come up with the new image file.
Cancel	Choose this option to cancel any changes made to the image download profile.

## Initiating Pre-Download (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>clear ap predownload statistics</b>	Clear AP predownload statistics.
<b>Step 2</b>	<b>install remove profile default</b>	Remove the image download profile. Choose <b>Y</b> to remove the profile or choose <b>N</b> to cancel.
<b>Step 3</b>	<b>install add profile default</b>	Download the controller and AP software image from the embedded wireless controller.  The controller image is sent to all Cisco Embedded Wireless Controller-capable APs. The AP image is downloaded to all APs sharing the same image type.

	Command or Action	Purpose
<b>Step 4</b>	<b>show wireless ewc-ap predownload status</b>	Monitor the overall software download status.  The download is successful when the status message is <code>Controller Image Predownload to EWC Capable APs Complete</code> .
<b>Step 5</b>	<b>install activate</b>	Activate the network after upgrade.  All the subordinate APs get the new AP image and reboot. Once all APs are rebooted, the embedded wireless controller also reboots.  <b>Note</b> The network can also be activated if the controller image is downloaded but all APs have not received the AP image via predownload.  <b>Important</b> If the network is activated during partial predownload success, and a Cisco Embedded Wireless Controller-capable AP with old controller software becomes the controller, then the network will not get upgraded to the new image.
<b>Step 6</b>	<b>show install summary</b>	Verify the current image status after rebooting.  If the status is <code>Activated</code> and <code>Uncommitted</code> , proceed to Step 7, else wait.
<b>Step 7</b>	<b>install commit</b>	Commits the current software image once the embedded wireless controller comes up after rebooting.

## Verifying Image Download

To monitor the overall progress of the software download process during predownload, run the following command.

```
Device# show wireless ewc-ap predownload status
```

The following are the various status messages indicating the status of the predownload operation. These are displayed when you run the **show wireless ewc-ap predownload status** command:

- None
- Controller Image Download Initiated
- Controller Image Download In Progress
- Controller Image Download Complete



- Controller Image Download Failed
- AP Image Predownload Initiated
- AP Image Predownload In Progress
- AP Image Predownload Complete
- AP Image Predownload Unsupported
- AP Image Predownload Failed
- Controller Image Predownload to EWC Capable APs In Progress
- Controller Image Predownload to EWC Capable APs Complete
- Controller Image Predownload to EWC Capable APs Failed
- Image Activation Succeeded
- Image Activation Failed
- Invalid State

To view the AP image predownload statistics, run the following command:

```
Device# show wireless ewc-ap ap image predownload status
Total number of APs                : 5
Total number of EWC capable APs    : 4
Number of APs
  Initiated                        : 0
  Predownloading AP image          : 0
  Predownloading Controller image   : 1
  Completed predownloading AP       : 5
  Completed predownloading Controller : 0
  Failed to Predownload AP          : 0
  Failed to Predownload Controller  : 0
AP Name      Primary Image (AP/Controller)      Backup Image (AP/Controller)
Role      Retries  AP image      Controller image      AP Image
ETA/Percent  ETA/Percent
-----
APXXXX.9XXX.8FXX  17.3.0.85  /17.3.01.0.XXXX  17.2.2.2  /17.2.02.0.XXXX
  Complete 17.2.2.2 /17.2.02.0.2XXX  aplg7  Slave
  0 00:00:00/100% 00:00:00/ 0%
APXXXX.5XXX.71XX  17.3.0.85  / 17.2.2.2 / 17.2.2.2  /
  Complete 17.2.2.2 / aplg5
Master 0 00:00:00/100% 00:00:00/ 0%
APXXXX.8XXX.59XX  17.3.0.85  /17.3.01.0.XXXX  17.2.2.2  /17.2.02.0.XXXX
  Complete 17.2.2.2 / aplg7  Slave
  0 00:00:00/100% 00:00:00/ 0%
APXXXX.8XXX.5AXX  17.3.0.85  /17.3.01.0.XXXX  17.2.2.2  /17.3.01.0.XXX
  Controller Predownloading 17.2.2.2 / aplg7
Master 0 00:00:00/100% 00:00:00/ 0%
APXXXX.8XXX.5BXX  17.3.0.85  /17.3.01.0.XXXX  17.2.2.2  /
  Complete 17.2.2.2 / aplg7
Slave 0 00:00:00/100% 00:00:00/ 0%
```

To view details of the AP acting as the primary image , use the following command:

```
Device# show wireless ewc-ap image-master
Image Master List
Image Name: aplg7
```

```
-----
Master AP MAC          AP          AP          Controller
      Controller
      Predownload In Progress  Predownload Complete  Predownload In Progress
      Predownload Complete
-----
c0XX.eXXX.90XX      No          No          No
      Yes
Image Name: aplg5
```

```
-----
Master AP MAC          AP          AP          Controller
      Controller
      Predownload In Progress  Predownload Complete  Predownload In Progress
      Predownload Complete
-----
70XX.1XXX.4bXX      No          No          No
      Yes
```

To check the image download status on all the APs, run the following command:

```
Device# show ap image
```

To check AP status during image download, run the following command:

```
Device# show ap summary
```

To monitor efficient AP join status, run the following command:

```
Device# show ap master list
```

To view the details of the last AP image download attempt, run the following command:

```
Device# show wireless stats ap image-download
```

To check the current status of the upgraded image, run the following command:

```
Device# show install summary
```

To check the download status from external servers (TFTP or SFTP), run the following command:

```
Device# show install log
```



## CHAPTER 31

# Conditional Debug and Radioactive Tracing

- [Introduction to Conditional Debugging, on page 239](#)
- [Introduction to Radioactive Tracing, on page 239](#)
- [Conditional Debugging and Radioactive Tracing, on page 240](#)
- [Location of Tracefiles, on page 240](#)
- [Configuring Conditional Debugging \(GUI\), on page 241](#)
- [Configuring Conditional Debugging, on page 241](#)
- [Recommended Workflow for Trace files, on page 242](#)
- [Copying Tracefiles Off the Box, on page 243](#)
- [Configuration Examples for Conditional Debugging, on page 244](#)
- [Verifying Conditional Debugging, on page 244](#)
- [Example: Verifying Radioactive Tracing Log for SISF, on page 244](#)

## Introduction to Conditional Debugging

The Conditional Debugging feature allows you to selectively enable debugging and logging for specific features based on the set of conditions you define. This feature is useful in systems where a large number of features are supported.

The Conditional debug allows granular debugging in a network that is operating at a large scale with a large number of features. It allows you to observe detailed debugs for granular instances within the system. This is very useful when we need to debug only a particular session among thousands of sessions. It is also possible to specify multiple conditions.

A condition refers to a feature or identity, where identity could be an interface, IP Address, or a MAC address and so on.

This is in contrast to the general debug command, that produces its output without discriminating on the feature objects that are being processed. General debug command consumes a lot of system resources and impacts the system performance.

## Introduction to Radioactive Tracing

Radioactive tracing (RA) provides the ability to stitch together a chain of execution for operations of interest across the system, at an increased verbosity level. This provides a way to conditionally print debug information (up to DEBUG Level or a specified level) across threads, processes and function calls.



- 
- Note**
- The radioactive tracing supports First-Hop Security (FHS).
  - The radioactive tracing filter does not work, if the certificate is not valid.
  - For effective debugging of issues on mesh features, ensure that you add both Ethernet and Radio MAC address as conditional MAC for RA tracing, while collecting logs.
  - To enable debug for wireless IPs, use the **debug platform condition feature wireless ip ip-address** command.
- 

## Conditional Debugging and Radioactive Tracing

Radioactive Tracing when coupled with Conditional Debugging, enable us to have a single debug CLI to debug all execution contexts related to the condition. This can be done without being aware of the various control flow processes of the feature within the box and without having to issue debugs at these processes individually.



- 
- Note** Use the **clear platform condition all** command to remove the debug conditions applied to the platform.
- 

## Location of Tracefiles

By default the tracefile logs will be generated for each process and saved into either the **/tmp/rp/trace** or **/tmp/fp/trace** directory. In this temp directory, the trace logs are written to files, which are of 1 MB size each. You can verify these logs (per-process) using the **show platform software trace message process\_name chassis active R0** command. The directory can hold up to a maximum of 25 such files for a given process. When a tracefile in the **/tmp** directory reaches its 1MB limit or whatever size was configured for it during the boot time, it is rotated out to an archive location in the **/crashinfo** partition under **tracelogs** directory.

The **/tmp** directory holds only a single tracefile for a given process. Once the file reaches its file size limit it is rotated out to **/crashinfo/tracelogs**. In the archive directory, up to 25 files are accumulated, after which the oldest one is replaced by the newly rotated file from **/tmp**. File size is process dependent and some processes uses larger file sizes (upto 10MB). Similarly, the number of files in the **tracelogs** directory is also decided by the process. For example, WNCN process uses a limit of 400 files per instance, depending on the platform.

The tracefiles in the crashinfo directory are located in the following formats:

1. Process-name\_Process-ID\_running-counter.timestamp.gz  
Example: IOSRP\_R0-0.bin\_0.14239.20151101234827.gz
2. Process-name\_pmanlog\_Process-ID\_running-counter.timestamp.bin.gz  
Example: wncmgrd\_R0-0.27958\_1.20180902081532.bin.gz

# Configuring Conditional Debugging (GUI)

## Procedure

- 
- Step 1** Choose **Troubleshooting > Radioactive Trace**.
  - Step 2** Click **Add**.
  - Step 3** Enter the **MAC/IP Address**.
  - Step 4** Click **Apply to Device**.
  - Step 5** Click **Start** to start or **Stop** to stop the conditional debug.
  - Step 6** Click **Generate** to create a radioactive trace log.
  - Step 7** Click the radio button to set the time interval.
  - Step 8** Click the **Download Logs** icon that is displayed next to the trace file name, to download the logs to your local folder.
  - Step 9** Click the **View Logs** icon that is displayed next to the trace file name, to view the log files on the GUI page. Click **Load More** to view more lines of the log file.
  - Step 10** Click **Apply to Device**.
- 

# Configuring Conditional Debugging

Follow the procedure given below to configure conditional debugging:

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>debug platform condition feature wireless mac {mac-address}</b>  <b>Example:</b> Device# <code>debug platform condition feature wireless mac b838.61a1.5433</code>	Configures conditional debugging for a feature using the specified MAC address.  <b>Note</b> This is supported with AP or client MAC/IP and also on CMX IP address and mobility peer IP.
<b>Step 2</b>	<b>debug platform condition start</b>  <b>Example:</b> Device# <code>debug platform condition start</code>	Starts conditional debugging (this will start radioactive tracing if there is a match on one of the conditions above).  <b>Note</b> This is supported with AP or client MAC/IP and also on CMX IP address and mobility peer IP.
<b>Step 3</b>	<b>show platform condition OR show debug</b>  <b>Example:</b>	Displays the current conditions set.

	Command or Action	Purpose
	Device# <code>show platform condition</code> Device# <code>show debug</code>	
<b>Step 4</b>	<b>debug platform condition stop</b>  <b>Example:</b> Device# <code>debug platform condition stop</code>	Stops conditional debugging (this will stop radioactive tracing).  <b>Note</b> This is supported with AP or client MAC/IP and also on CMX IP address and mobility peer IP.
<b>Step 5</b>	<b>show logging profile wireless</b> [ <code>counter</code>   [ <code>last</code> ]{ <i>x days/hours</i> }   <code>filter mac</code> {< <i>mac address</i> >} [ <code>to-file</code> ]{< <i>destination</i> >}  <b>Example:</b> Device# <code>show logging profile wireless start last 20 minutes to-file bootflash:logs.txt</code>	Displays the logs from the latest wireless profile.  <b>Note</b> You can use either the <i>show logging profile wireless</i> command or <i>show logging process</i> command to collect the logs.
<b>Step 6</b>	<b>show logging process</b> < <i>process name</i> >  <b>Example:</b> Device# <code>show logging process wncd to-file flash:wncd.txt</code>	Displays the logs collection specific to the process.
<b>Step 7</b>	<b>clear platform condition all</b>  <b>Example:</b> Device# <code>clear platform condition all</code>	Clears all conditions.

### What to do next



**Note** The command `request platform software trace filter-binary wireless {mac-address}` generates 3 flash files:

- `collated_log_<.date..>`
- `mac_log <..date..>`
- `mac_database ..file`

Of these, `mac_log <..date..>` is the most important file, as it gives the messages for the MAC address we are debugging. The command `show platform software trace filter-binary` also generates the same flash files, and also prints the `mac_log` on the screen.

## Recommended Workflow for Trace files

1. To request the tracelogs for a specific time period.

EXAMPLE 1 day.

Use the command:

```
Device#show logging process wncd to-file flash:wncd.txt
```

2. The system generates a text file of the tracelogs in the location /flash:
3. Copy the file off the device. By copying the file, the tracelogs can be used to work offline. For more details on copying files, see section below.
4. Delete the tracelog file (.txt) file from /flash: location. This will ensure enough space on the device for other operations.

## Copying Tracefiles Off the Box

An example of the tracefile is shown below:

```
Device# dir flash:/tracelogs
Directory of crashinfo:/tracelogs/

50664 -rwx 760 Sep 22 2015 11:12:21 +00:00 plogd_F0-0.bin_0.gz
50603 -rwx 991 Sep 22 2015 11:12:08 +00:00 fed_pmanlog_F0-0.bin_0.9558.20150922111208.gz
50610 -rw- 11 Nov 2 2015 00:15:59 +00:00 timestamp
50611 -rwx 1443 Sep 22 2015 11:11:31 +00:00
auto_upgrade_client_sh_pmanlog_R0-.bin_0.3817.20150922111130.gz
50669 -rwx 589 Sep 30 2015 03:59:04 +00:00 cfgwr-8021_R0-0.bin_0.gz
50612 -rwx 1136 Sep 22 2015 11:11:46 +00:00 reflector_803_R0-0.bin_0.1312.20150922111116.gz
50794 -rwx 4239 Nov 2 2015 00:04:32 +00:00 IOSRP_R0-0.bin_0.14239.20151101234827.gz
50615 -rwx 131072 Nov 2 2015 00:19:59 +00:00 linux_iosd_image_pmanlog_R0-0.bin_0
```

The trace files can be copied using one of the various options shown below:

```
Device# copy flash:/tracelogs ?
crashinfo: Copy to crashinfo: file system
flash: Copy to flash: file system
ftp: Copy to ftp: file system
http: Copy to http: file system
https: Copy to https: file system
null: Copy to null: file system
nvram: Copy to nvram: file system
rcp: Copy to rcp: file system
running-config Update (merge with) current system configuration
scp: Copy to scp: file system
startup-config Copy to startup configuration
syslog: Copy to syslog: file system
system: Copy to system: file system
tftp: Copy to tftp: file system
tmpsys: Copy to tmpsys: file system
```

The general syntax for copying onto a TFTP server is as follows:

```
Device# copy source: tftp:
Device# copy crashinfo:/tracelogs/IOSRP_R0-0.bin_0.14239.20151101234827.gz tftp:
Address or name of remote host []? 2.2.2.2
Destination filename [IOSRP_R0-0.bin_0.14239.20151101234827.gz]?
```



**Note** It is important to clear the generated report or archive files off the switch in order to have flash space available for tracelog and other purposes.

## Configuration Examples for Conditional Debugging

The following is an output example of the *show platform condition* command.

```
Device# show platform condition
Conditional Debug Global State: Stop
Conditions Direction
-----|-----
MAC Address 0024.D7C7.0054 N/A
Feature Condition Type Value
-----|-----
Device#
```

The following is an output example of the *show debug* command.

```
Device# show debug
IOSXE Conditional Debug Configs:
Conditional Debug Global State: Start
Conditions Direction
-----|-----
MAC Address 0024.D7C7.0054 N/A
Feature Condition Type Value
-----|-----
Packet Infra debugs:
Ip Address Port
-----|-----
Device#
```

## Verifying Conditional Debugging

The table shown below lists the various commands that can be used to verify conditional debugging:

Command	Purpose
<b>show platform condition</b>	Displays the current conditions set.
<b>show debug</b>	Displays the current debug conditions set.
<b>show platform software trace filter-binary</b>	Displays logs merged from the latest tracefile.
<b>request platform software trace filter-binary</b>	Displays historical logs of merged tracefiles on the system.

## Example: Verifying Radioactive Tracing Log for SISF

The following is an output example of the *show platform software trace message ios chassis active R0 | inc sif* command.



```
Device# show platform software trace message ios chassis active R0 | inc sisf

2017/10/26 13:46:22.104 {IOSRP_R0-0}{1}: [parser]: [5437]: UUID: 0, ra: 0 (note): CMD:
'show platform software trace message ios switch active R0 | inc sisf' 13:46:22 UTC Thu Oct
 26 2017
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]: UUID: 4800000000060, ra: 7 (debug):
  FF8E802918 semaphore system unlocked
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]: UUID: 4800000000060, ra: 7 (debug):
  Unlocking, count is now 0
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]: UUID: 4800000000060, ra: 7 (debug):
  FF8E802918 semaphore system unlocked
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]: UUID: 4800000000060, ra: 7 (debug):
  Unlocking, count is now 1
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]: UUID: 4800000000060, ra: 7 (debug):
  Gil/0/5 vlan 10 aaaa.bbbb.cccc Setting State to 2
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]: UUID: 4800000000060, ra: 7 (debug):
  Gil/0/5 vlan 10 aaaa.bbbb.cccc Start timer 0
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]: UUID: 4800000000060, ra: 7 (debug):
  Gil/0/5 vlan 10 aaaa.bbbb.cccc Timer value/granularity for 0 :299998/1000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]: UUID: 4800000000060, ra: 7 (debug):
  Gil/0/5 vlan 10 aaaa.bbbb.cccc Updated Mac Timer : 299998
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]: UUID: 4800000000060, ra: 7 (debug):
  Gil/0/5 vlan 10 aaaa.bbbb.cccc Before Timer : 350000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]: UUID: 4800000000060, ra: 7 (debug):
  Gil/0/5 vlan 10 aaaa.bbbb.cccc Timer 0, default value is 350000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]: UUID: 4800000000060, ra: 7 (debug):
  Allocating timer wheel for 0
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]: UUID: 4800000000060, ra: 7 (debug):
  Gil/0/5 vlan 10 aaaa.bbbb.cccc No timer running
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]: UUID: 4800000000060, ra: 7 (debug):
  Granularity for timer MAC_T1 is 1000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]: UUID: 4800000000060, ra: 7 (debug):
  Gil/0/5 vlan 10 aaaa.bbbb.cccc Current State :MAC-STALE, Req Timer : MAC_T1 Current Timer
  MAC_T1
```





## CHAPTER 32

# Aggressive Client Load Balancing

- [Information About Aggressive Client Load Balancing](#), on page 247
- [Enabling Aggressive Client Load Balancing \(GUI\)](#), on page 248
- [Configuring Aggressive Client Load Balancing \(GUI\)](#), on page 248
- [Configuring Aggressive Client Load Balancing \(CLI\)](#), on page 249

## Information About Aggressive Client Load Balancing

The Aggressive Client Load Balancing feature allows lightweight access points to load balance wireless clients across access points.

When a wireless client attempts to associate to a lightweight access point, the associated response packets are sent to a client with an 802.11 response packet including status code 17. This code 17 indicates that the corresponding AP is busy. The AP does not respond with the response 'success' if the AP threshold is not met, and with code 17 (AP busy) if the AP utilization threshold is exceeded, and another less busy AP hears the client request.

For example, if the number of clients on AP1 is more than the number of clients on AP2 and the load-balancing window, then AP1 is considered to be busier than AP2. When a client attempts to associate to AP1, the client receives an 802.11 response packet with status code 17, indicating that the access point is busy, and the client attempts to associate to a different access point.

You can configure the embedded wireless controller to deny client associations up to 10 times (if a client attempts to associate 11 times, it will be allowed to associate on the 11th try). You can also enable or disable load balancing on a particular WLAN, which is useful if you want to disable load balancing for a select group of clients, such as time-sensitive voice clients.



---

**Note** A voice client does not authenticate when delay is configured to more than 300 ms. To avoid this, configure a central-authentication, local-switching WLAN with Cisco Centralized Key Management (CCKM), configure a pagent router between an AP and WLC with a delay of 600 ms (300 ms UP and 300 ms DOWN), and try associating the voice client.

---



---

**Note** For a FlexConnect AP, the association is locally handled. The load-balancing decisions are taken at the controller. A FlexConnect AP sends an initial response to the client before knowing the result of the calculations in the controller. Load-balancing does not take effect when the FlexConnect AP is in standalone mode.

A FlexConnect AP does not send (re)association response with status 17 for load balancing the way local-mode APs do; instead, it first sends (re)association with status 0 (success) and then death with reason 5.

---

## Enabling Aggressive Client Load Balancing (GUI)

### Procedure

---

- Step 1** Choose **Configuration > Wireless > WLANs > Wireless Networks**.
  - Step 2** Select a **WLAN** to view the **Edit WLAN** window.
  - Step 3** Click **Advanced** tab.
  - Step 4** Select the **Load Balance** check box to enable the feature.
  - Step 5** Click **Update & Apply to Device**.
- 

## Configuring Aggressive Client Load Balancing (GUI)

### Procedure

---

- Step 1** Choose **Configuration > Wireless > Advanced**.  
The **Load Balancing** window is displayed.
  - Step 2** In the **Aggressive Load Balancing Window (clients)** field, enter the number of clients for the aggressive load balancing client window.
  - Step 3** In the **Aggressive Load Balancing Denial Count** field, enter the load balancing denial count.
  - Step 4** Click **Apply**.
-

# Configuring Aggressive Client Load Balancing (CLI)

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# <b>enable</b>	Enters privileged EXEC mode.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>wlan wlan-name</b> <b>Example:</b> Device(config)# <b>wlan test-wlan</b>	Specifies the WLAN name.
<b>Step 4</b>	<b>shutdown</b> <b>Example:</b> Device(config-wlan)# <b>shutdown</b>	Disables the WLAN.
<b>Step 5</b>	<b>load-balance</b> <b>Example:</b> Device(config-wlan)# <b>load-balance</b>	Configures a guest embedded wireless controller as mobility controller, in order to enable client load balance to a particular WLAN.  Configure the WLAN security settings as the WLAN requirements.
<b>Step 6</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wlan)# <b>no shutdown</b>	Enables WLAN.
<b>Step 7</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.
<b>Step 8</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 9</b>	<b>ap dot11</b> <b>{24ghz   5ghz} load-balancingdenial count</b> <b>Example:</b> Device(config)# <b>ap dot11 5ghz</b> <b>load-balancing denial 10</b>	Configures the load balancing denial count.

	Command or Action	Purpose
<b>Step 10</b>	<b>ap dot11</b> <b>{ 24ghz   5ghz } load-balancingwindow</b> <i>clients</i>  <b>Example:</b> Device(config)# <b>ap dot11 5ghz</b> <b>load-balancing denial 10</b>	Configures the number of clients for the aggressive load balancing client window.
<b>Step 11</b>	<b>end</b>  <b>Example:</b> Device(config-wlan)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 12</b>	<b>show running-config   section wlan-name</b>  <b>Example:</b> Device# <b>show running-config   section</b> <b>test-wlan</b>	Displays a filtered section of the current configuration.



## CHAPTER 33

# Accounting Identity List

---

- [Configuring Accounting Identity List \(GUI\), on page 251](#)
- [Configuring Accounting Identity List \(CLI\), on page 251](#)
- [Configuring Client Accounting \(GUI\), on page 252](#)
- [Configuring Client Accounting \(CLI\), on page 252](#)

## Configuring Accounting Identity List (GUI)

### Procedure

---

- Step 1** Choose **Configuration** > **Security** > **AAA**.
  - Step 2** In the **AAA Method List** tab, go to the **Accounting** section, and click **Add**.
  - Step 3** In the **Quick Setup: AAA Accounting** window that is displayed, enter a name for your method list.
  - Step 4** Choose the type of authentication as identity, in the **Type** drop-down list.
  - Step 5** Choose the server groups you want to use to authenticate access to your network, from the **Available Server Groups** list and click > icon to move them to the **Assigned Server Groups** list.
  - Step 6** Click **Save & Apply to Device**.
- 

## Configuring Accounting Identity List (CLI)

Accounting is the process of logging the user actions and keeping track of their network usage. Whenever a user successfully executes an action, the RADIUS accounting server logs the changed attributes, the user ID of the person who made the change, the remote host where the user is logged in, the date and time when the command was executed, the authorization level of the user, and a description of the action performed and the values provided.

Follow the procedure given below to configure accounting identity list.

### Before you begin

Configure the RADIUS server and AAA group server.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>aaa accounting identity <i>named-list</i> start-stop group <i>server-group-name</i></b>  <b>Example:</b> <pre>Device(config)# aaa accounting identity user1 start-stop group aaa-test</pre>	Enables accounting to send a start-record accounting notice when a client is authorized and a stop-record at the end.  <b>Note</b> You can also use the default list, instead of a named list.

Whenever there is a change in the client attribute, for example, change in IP address, client roaming, and so on, an accounting interim update is sent to the RADIUS server.

## Configuring Client Accounting (GUI)

**Procedure**

- 
- Step 1** Choose **Configuration > Tags & Profiles > Policy**.
  - Step 2** Click the **Policy Profile Name** and in the **Edit Policy Profile** window, go to the **Advanced** tab.
  - Step 3** From the **Accounting List** drop-down, select the appropriate accounting list for this policy profile. This will ensure that the policy profile undergoes that type of accounting you want to perform, before allowing it access to the network.
  - Step 4** Click **Save & Apply to Device**.
- 

## Configuring Client Accounting (CLI)

Follow the procedure given below to configure client accounting.

**Before you begin**

Ensure that RADIUS accounting is configured.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>wireless profile policy <i>profile-policy</i></b>  <b>Example:</b> <pre>Device(config)# wireless profile policy default-policy-profile</pre>	Configures WLAN policy profile and enters wireless policy configuration mode.
<b>Step 2</b>	<b>shutdown</b>  <b>Example:</b>	Disables the policy profile.



	<b>Command or Action</b>	<b>Purpose</b>
	Device(config-wireless-policy)# shutdown	
<b>Step 3</b>	<b>accounting-list</b> <i>list-name</i> <b>Example:</b> Device(config-wireless-policy)# accounting-list user1	Sets the accounting list.
<b>Step 4</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wireless-policy)# no shutdown	Enables the policy profile.





# CHAPTER 34

## Volume Metering

The Volume Metering feature allows you to configure the interval at which an access point (AP) updates client accounting statistics to the embedded wireless controller and in turn to the RADIUS server. Currently, the report is sent from an AP to the controller every 90 seconds. With this feature, you can configure the time from 5 to 90 seconds. This helps reduce the delay in accounting data usage by a device.

- [Configuring Volume Metering, on page 255](#)

## Configuring Volume Metering

Follow the procedure given below to configure volume metering:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ap profile profile-name</b> <b>Example:</b> Device(config)# ap profile yy-ap-profile	Configures an AP profile and enters ap profile configuration mode.
<b>Step 3</b>	<b>dot11 24ghz reporting-interval reporting-interval</b> <b>Example:</b> Device(config-ap-profile)# dot11 24ghz reporting-interval 60	Configures the dot11 parameters.
<b>Step 4</b>	<b>dot11 5ghz reporting-interval reporting-interval</b> <b>Example:</b> Device(config-ap-profile)# dot11 5ghz reporting-interval 60	Configures the dot11 parameters.

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 5</b>	<b>exit</b> <b>Example:</b> Device(config-ap-profile)# exit	Returns to global configuration mode.
<b>Step 6</b>	<b>aaa accounting update periodic</b> <i>interval-in-minutes</i> <b>Example:</b> Device(config)# aaa accounting update periodic 75	Sets the time interval (in minutes) at which the embedded wireless controller sends interim accounting updates of the client to the RADIUS server.
<b>Step 7</b>	<b>exit</b> <b>Example:</b> Device(config)# exit	Exits configuration mode and returns to privileged EXEC mode.



## CHAPTER 35

# Enabling Syslog Messages in Access Points and Controller for Syslog Server

---

- [Information About Enabling Syslog Messages in Access Points and Embedded Wireless Controller for Syslog Server, on page 257](#)
- [Configuring Syslog Server for an AP Profile, on page 258](#)
- [Configuring Syslog Server for the Controller \(GUI\), on page 260](#)
- [Configuring Syslog Server for the Embedded Wireless Controller, on page 261](#)
- [Verifying Syslog Server Configurations, on page 262](#)

## Information About Enabling Syslog Messages in Access Points and Embedded Wireless Controller for Syslog Server



---

**Note** You will be able to view the Syslog server messages only after an AP join.

---

The Syslog server on access points and embedded wireless controller has many levels and facilities.

The following are the Syslog levels:

- Emergencies
- Alerts
- Critical
- Errors
- Warnings
- Notifications
- Informational
- Debugging

The following options are available for the Syslog facility:

- auth—Authorization system.
- cron—Cron/ at facility.
- daemon—System daemons.
- kern—Kernel.
- local0—Local use.
- local1—Local use.
- local2—Local use.
- local3—Local use.
- local4—Local use.
- local5—Local use.
- local6—Local use.
- local7—Local use.
- lpr—Line printer system.
- mail—Mail system.
- news—USENET news.
- sys10—System use.
- sys11—System use.
- sys12—System use.
- sys13—System use.
- sys14—System use.
- sys9—System use.
- syslog—Syslog itself.
- user—User process.
- uucp—Unix-to-Unix copy system.

## Configuring Syslog Server for an AP Profile

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	<b>ap profile</b> <i>ap-profile</i> <b>Example:</b> Device(config)# <b>ap profile xyz-ap-profile</b>	Configures an AP profile and enters the AP profile configuration mode.
<b>Step 3</b>	<b>syslog facility</b> <b>Example:</b> Device(config-ap-profile)# <b>syslog facility</b>	Configures the facility parameter for Syslog messages.
<b>Step 4</b>	<b>syslog host</b> <i>ip-address</i> <b>Example:</b> Device(config-ap-profile)# <b>syslog host 9.3.72.1</b>	Configures the Syslog server IP address and parameters.
<b>Step 5</b>	<b>syslog level</b> { <b>alerts</b>   <b>critical</b>   <b>debugging</b>   <b>emergencies</b>   <b>errors</b>   <b>informational</b>   <b>notifications</b>   <b>warnings</b> } <b>Example:</b> Device(config-ap-profile)# <b>syslog level</b>	Configures the Syslog server logging level. The following are the Syslog server logging levels: <ul style="list-style-type: none"> <li>• <b>emergencies</b>—Signifies severity 0. Implies that the system is not usable.</li> <li>• <b>alerts</b>—Signifies severity 1. Implies that an immediate action is required.</li> <li>• <b>critical</b>—Signifies severity 2. Implies critical conditions.</li> <li>• <b>errors</b>—Signifies severity 3. Implies error conditions.</li> <li>• <b>warnings</b>—Signifies severity 4. Implies warning conditions.</li> <li>• <b>notifications</b>—Signifies severity 5. Implies normal but significant conditions.</li> <li>• <b>informational</b>—Signifies severity 6. Implies informational messages.</li> <li>• <b>debugging</b>—Signifies severity 7. Implies debugging messages.</li> </ul>

	Command or Action	Purpose
		<p><b>Note</b> To know the number of Syslog levels supported, you need to select a Syslog level. Once a Syslog level is selected, all the levels below it are also enabled.</p> <p>If you enable <i>critical</i> Syslog level then all levels below it are also enabled. So, all three of them, namely, <i>critical</i>, <i>alerts</i>, and <i>emergencies</i> are enabled.</p>
<b>Step 6</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-ap-profile)# end</pre>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring Syslog Server for the Controller (GUI)

### Procedure

- 
- Step 1** Choose **Troubleshooting > Logs**.
- Step 2** Click **Manage Syslog Servers** button.
- Step 3** In **Log Level Settings**, from the **Syslog** drop-down list, choose a security level.
- Step 4** From the **Message Console** drop-down list, choose a logging level.
- Step 5** In **Message Buffer Configuration**, from the **Level** drop-down list, choose a server logging level.
- Step 6** In **IP Configuration** settings, click **Add**.
- Step 7** Choose the **Server Type**, from the **IPv4 / IPv6** or **FQDN** option.
- Step 8** For Server Type **IPv4 / IPv6**, enter the **IPv4 / IPv6 Server Address**. For Server Type **FQDN**, enter the **Host Name**, choose the IP type and the appropriate **VRF Name** from the drop-down lists.
- To delete a syslog server, click 'x' next to the appropriate server entry, under the **Remove** column.
- Note** When creating a host name, spaces are not allowed.
- Step 9** Click **Apply to Device**.
- Note** When you click on **Apply to Device**, the changes are configured. If you click on **Cancel**, the configurations are discarded.
-



# Configuring Syslog Server for the Embedded Wireless Controller

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>logging host {hostname   ipv6}</b> <b>Example:</b> Device(config)# <code>logging host 124.3.52.62</code>	Enables Syslog server IP address and parameters.
<b>Step 3</b>	<b>logging facility {auth   cron   daemon   kern   local0   local1   local2   local3   local4   local5   local6   local7   lpr   mail   news   sys10   sys11   sys12   sys13   sys14   sys9   syslog   user   uucp}</b> <b>Example:</b> Device(config)# <code>logging facility syslog</code>	Enables facility parameter for the Syslog messages.  You can enable the following facility parameter for the Syslog messages: <ul style="list-style-type: none"> <li>• <b>auth</b>—Authorization system.</li> <li>• <b>cron</b>—Cron facility.</li> <li>• <b>daemon</b>—System daemons.</li> <li>• <b>kern</b>—Kernel.</li> <li>• <b>local0</b> to <b>local7</b>—Local use.</li> <li>• <b>lpr</b>—Line printer system.</li> <li>• <b>mail</b>—Mail system.</li> <li>• <b>news</b>—USENET news.</li> <li>• <b>sys10</b> to <b>sys14</b> and <b>sys9</b>—System use.</li> <li>• <b>syslog</b>—Syslog itself.</li> <li>• <b>user</b>—User process.</li> <li>• <b>uucp</b>—Unix-to-Unix copy system.</li> </ul>
<b>Step 4</b>	<b>logging trap {severity-level   alerts   critical   debugging   emergencies   errors   informational   notifications   warnings}</b> <b>Example:</b> Device(config)# <code>logging trap 2</code>	Enables Syslog server logging level.  <i>severity-level</i> - Refers to the logging severity level. The valid range is from 0 to 7.  The following are the Syslog server logging levels: <ul style="list-style-type: none"> <li>• <b>emergencies</b>—Signifies severity 0. Implies that the system is not usable.</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• <b>alerts</b>—Signifies severity 1. Implies that an immediate action is required.</li> <li>• <b>critical</b>—Signifies severity 2. Implies critical conditions.</li> <li>• <b>errors</b>—Signifies severity 3. Implies error conditions.</li> <li>• <b>warnings</b>—Signifies severity 4. Implies warning conditions.</li> <li>• <b>notifications</b>—Signifies severity 5. Implies normal but significant conditions.</li> <li>• <b>informational</b>—Signifies severity 6. Implies informational messages.</li> <li>• <b>debugging</b>—Signifies severity 7. Implies debugging messages.</li> </ul> <p><b>Note</b> To know the number of Syslog levels supported, you need to select a Syslog level. Once a Syslog level is selected, all the levels below it are also enabled.</p> <p>If you enable <i>critical</i> Syslog level then all levels below it are also enabled. So, all three of them, namely, <i>critical</i>, <i>alerts</i>, and <i>emergencies</i> are enabled.</p>
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Verifying Syslog Server Configurations

### Verifying Global Syslog Server Settings for all Access Points

To view the global Syslog server settings for all access points that joins the controller, use the following command:

```
Device# show ap config general
Cisco AP Name : APA0F8.4984.5E48
=====

Cisco AP Identifier : a0f8.4985.d360
Country Code : IN
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-DN
```

```
AP Country Code : IN - India
AP Regulatory Domain
Slot 0 : -A
Slot 1 : -D
MAC Address : a0f8.4984.5e48
IP Address Configuration : DHCP
IP Address : 9.4.172.111
IP Netmask : 255.255.255.0
Gateway IP Address : 9.4.172.1
Fallback IP Address Being Used :
Domain :
Name Server :
CAPWAP Path MTU : 1485
Telnet State : Disabled
SSH State : Disabled
Jumbo MTU Status : Disabled
Cisco AP Location : default location
Site Tag Name : ST1
RF Tag Name : default-rf-tag
Policy Tag Name : PT3
AP join Profile : default-ap-profile
Primary Cisco Controller Name : WLC2
Primary Cisco Controller IP Address : 9.4.172.31
Secondary Cisco Controller Name : Not Configured
Secondary Cisco Controller IP Address : 0.0.0.0
Tertiary Cisco Controller Name : Not Configured
Tertiary Cisco Controller IP Address : 0.0.0.0
Administrative State : Enabled
Operation State : Registered
AP Certificate type : Manufacturer Installed Certificate
AP Mode : Local
AP VLAN tagging state : Disabled
AP VLAN tag : 0
CAPWAP Preferred mode : Not Configured
AP Submode : Not Configured
Office Extend Mode : Disabled
Remote AP Debug : Disabled
Logging Trap Severity Level : notification
Software Version : 16.10.1.24
Boot Version : 1.1.2.4
Mini IOS Version : 0.0.0.0
Stats Reporting Period : 180
LED State : Enabled
PoE Pre-Standard Switch : Disabled
PoE Power Injector MAC Address : Disabled
Power Type/Mode : PoE/Full Power (normal mode)
Number of Slots : 3
AP Model : AIR-AP1852I-D-K9
IOS Version : 16.10.1.24
Reset Button : Disabled
AP Serial Number : KWC212904UB
Management Frame Protection Validation : Disabled
AP User Mode : Automatic
AP User Name : Not Configured
AP 802.1X User Mode : Global
AP 802.1X User Name : Not Configured
Cisco AP System Logging Host : 9.4.172.116
AP Up Time : 11 days 1 hour 15 minutes 52 seconds
AP CAPWAP Up Time : 6 days 3 hours 11 minutes 6 seconds
Join Date and Time : 09/05/2018 04:18:52
Join Taken Time : 3 minutes 1 second
Join Priority : 1
Ethernet Port Duplex : Auto
Ethernet Port Speed : Auto
```

```

AP Link Latency : Disable
AP Lag Configuration Status : Disabled
AP Lag Operational Status : Disabled
Lag Support for AP : Yes
Rogue Detection : Enabled
Rogue Containment auto-rate : Disabled
Rogue Containment of standalone flexconnect APs : Disabled
Rogue Detection Report Interval : 10
Rogue AP minimum RSSI : -90
Rogue AP minimum transient time : 0
AP TCP MSS Adjust : Enabled
AP TCP MSS Size : 1250
AP IPv6 TCP MSS Adjust : Enabled
AP IPv6 TCP MSS Size : 1250
Hyperlocation Admin Status : Disabled
Retransmit count : 5
Retransmit interval : 3
Fabric status : Disabled
FIPS status : Disabled
WLANCC status : Disabled
USB Module Type : USB Module
USB Module State : Enabled
USB Operational State : Disabled
USB Override : Disabled
Lawful-Interception Admin status : Disabled
Lawful-Interception Oper status : Disabled

```

### Verifying Syslog Server Settings for a Specific Access Point

To view the Syslog server settings for a specific access point, use the following command:

```

Device# show ap name <ap-name> config general
show ap name APA0F8.4984.5E48 config general
Cisco AP Name : APA0F8.4984.5E48
=====

Cisco AP Identifier : a0f8.4985.d360
Country Code : IN
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-DN
AP Country Code : IN - India
AP Regulatory Domain
Slot 0 : -A
Slot 1 : -D
MAC Address : a0f8.4984.5e48
IP Address Configuration : DHCP
IP Address : 9.4.172.111
IP Netmask : 255.255.255.0
Gateway IP Address : 9.4.172.1
Fallback IP Address Being Used :
Domain :
Name Server :
CAPWAP Path MTU : 1485
Telnet State : Disabled
SSH State : Disabled
Jumbo MTU Status : Disabled
Cisco AP Location : default location
Site Tag Name : ST1
RF Tag Name : default-rf-tag
Policy Tag Name : PT3
AP join Profile : default-ap-profile
Primary Cisco Controller Name : WLC2
Primary Cisco Controller IP Address : 9.4.172.31
Secondary Cisco Controller Name : Not Configured
Secondary Cisco Controller IP Address : 0.0.0.0

```

```
Tertiary Cisco Controller Name : Not Configured
Tertiary Cisco Controller IP Address : 0.0.0.0
Administrative State : Enabled
Operation State : Registered
AP Certificate type : Manufacturer Installed Certificate
AP Mode : Local
AP VLAN tagging state : Disabled
AP VLAN tag : 0
CAPWAP Preferred mode : Not Configured
AP Submode : Not Configured
Office Extend Mode : Disabled
Remote AP Debug : Disabled
Logging Trap Severity Level : notification
Software Version : 16.10.1.24
Boot Version : 1.1.2.4
Mini IOS Version : 0.0.0.0
Stats Reporting Period : 180
LED State : Enabled
PoE Pre-Standard Switch : Disabled
PoE Power Injector MAC Address : Disabled
Power Type/Mode : PoE/Full Power (normal mode)
Number of Slots : 3
AP Model : AIR-AP1852I-D-K9
IOS Version : 16.10.1.24
Reset Button : Disabled
AP Serial Number : KWC212904UB
Management Frame Protection Validation : Disabled
AP User Mode : Automatic
AP User Name : Not Configured
AP 802.1X User Mode : Global
AP 802.1X User Name : Not Configured
Cisco AP System Logging Host : 9.4.172.116
AP Up Time : 11 days 1 hour 15 minutes 52 seconds
AP CAPWAP Up Time : 6 days 3 hours 11 minutes 6 seconds
Join Date and Time : 09/05/2018 04:18:52
Join Taken Time : 3 minutes 1 second
Join Priority : 1
Ethernet Port Duplex : Auto
Ethernet Port Speed : Auto
AP Link Latency : Disable
AP Lag Configuration Status : Disabled
AP Lag Operational Status : Disabled
Lag Support for AP : Yes
Rogue Detection : Enabled
Rogue Containment auto-rate : Disabled
Rogue Containment of standalone flexconnect APs : Disabled
Rogue Detection Report Interval : 10
Rogue AP minimum RSSI : -90
Rogue AP minimum transient time : 0
AP TCP MSS Adjust : Enabled
AP TCP MSS Size : 1250
AP IPv6 TCP MSS Adjust : Enabled
AP IPv6 TCP MSS Size : 1250
Hyperlocation Admin Status : Disabled
Retransmit count : 5
Retransmit interval : 3
Fabric status : Disabled
FIPS status : Disabled
WLANCC status : Disabled
USB Module Type : USB Module
USB Module State : Enabled
USB Operational State : Disabled
USB Override : Disabled
```

```
Lawful-Interception Admin status : Disabled  
Lawful-Interception Oper status : Disabled
```



## CHAPTER 36

# Introduction to Software Maintenance Upgrade

The Software Maintenance Upgrade (SMU) is a package that can be installed on a system to provide a patch fix or a security resolution to a released image. A SMU package is provided for each release and is specific to the corresponding platform.

A SMU provides a significant benefit over classic Cisco IOS software because it allows you to address the network issue quickly while reducing the time and scope of the testing required. The Cisco IOS XE platform internally validates the SMU compatibility and does not allow you to install noncompatible SMUs.

All the SMUs are integrated into the subsequent Cisco IOS XE software maintenance releases. A SMU is an independent and self-sufficient package and does not have any prerequisites or dependencies. You can choose which SMUs to install or uninstall in any order.



---

**Note** SMUs are supported only on Extended Maintenance releases and for the full lifecycle of the underlying software release.

---

SMU infrastructure can be used to meet the following requirements in the wireless context:

- Controller SMU: Embedded Wireless Controller bug fixes or Cisco Product Security Incident Response information (PSIRT).
- AP bug fixes, PSIRTs, or minor features which do not require any embedded wireless controller changes.
- APDP: Support for new AP models without introduction of new hardware or software capabilities.



---

**Note** The **show ap image** command displays cumulative statistics regarding the AP images in the controller. We recommend that you clear the statistics using the **clear ap predownload statistics** command, before using the **show ap image** command, to ensure that correct data is displayed.

---

### SMU Workflow

The SMU process should be initiated with a request to the SMU committee. Contact your customer support to raise an SMU request. During the release, the SMU package is posted on the Cisco Software Download page and can be downloaded and installed.

### SMU Package

An SMU package contains the metadata and fix for the reported issue the SMU is requested for.

### SMU Reload

The SMU type describes the effect to a system after installing the SMU. SMUs can be non-traffic affecting or can result in device restart, reload, or switchover.

Controller hot patching support allows SMU to be effective immediately after activation without reloading the system. Other controller SMUs require a cold reload of the system during activation. A cold reload is the complete reload of the operating system. This action affects the traffic flow for the duration of the reload (~5 min currently). This reload ensures that all processes are started with the correct libraries and files that are installed as part of the SMU.

After the SMU is committed, the activation changes are persistent across reloads.

- [Overview of Controller SMUs](#) , on page 268
- [Managing Controller Hot or Cold SMU Package](#), on page 269
- [Creating SMU Files \(GUI\)](#), on page 270
- [Configuration Examples for SMU](#), on page 271
- [Rolling AP Upgrade](#), on page 273
- [AP Device Pack \(APDP\) and AP Service Pack \(APSP\)](#), on page 275

## Overview of Controller SMUs

The following table describes the SMU types supported in the Cisco Embedded Wireless Controller:

**Table 6: Supported SMU Types in the Embedded Wireless Controller**

Package Type	Use Case	SMU Type	Supported on EWC
Controller SMU - Cold Patch	Replace impacted binaries, libraries, or subpackages.	Reload	Limited support (Patch size < 20 MB). No support for IOSD.
Controller SMU - Hot Patch	Replace impacted functions.	Nonreload	Yes
APSP	AP fix by replacing the AP image (does not impact the AP running the active controller).	Nonreload	Yes
APSP	AP fix by replacing the AP image (impacts the AP that is running the active controller).	Reload	Yes (EWC specific variation)
APDP	New AP model support without upgrading the controller.	Nonreload	Yes



# Managing Controller Hot or Cold SMU Package

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>install add file</b> <code>tftp://&lt;server-ip&gt;/&lt;path&gt;/&lt;smu-filename&gt;</code> <b>Example:</b> <pre>Device# install add file tftp://&lt;server-ip&gt;/&lt;path&gt;/&lt;smu-filename&gt;</pre>	The <code>install add</code> command copies the file from the external server to the <code>backup_image</code> directory on the embedded wireless controller.
<b>Step 2</b>	<b>install activate file backup_image:</b> <code>smu-filename</code> <b>Example:</b> <pre>Device# install activate file backup_image:&lt;smu-filename&gt;</pre>	This command is used to activate the patch. The <code>install activate</code> causes the controller reload only for a cold patch. There is no reload for a hot patch.
<b>Step 3</b>	<b>install auto-abort-timer stop</b> <b>Example:</b> <pre>Device# install auto-abort-timer stop</pre>	(Optional) Stops the auto cancel timer in case of activated or deactivated SMUs.
<b>Step 4</b>	<b>install commit</b> <b>Example:</b> <pre>Device# install commit</pre>	Commits the activation changes to be persistent across reloads.  The commit can be done after activation while the system is up, or after the first reload. If a patch is activated and not committed, the auto cancel timer automatically cancels the activation of the patch in six hours .
<b>Step 5</b>	<b>show install rollback</b> <b>Example:</b> <pre>Device# show install rollback</pre>	Displays the list of rollback IDs that are available.
<b>Step 6</b>	<b>install rollback to {base   committed   id   label } specific-rollback-point</b> <b>Example:</b> <pre>Device# install rollback to base</pre>	Rolls back a committed patch. The committed patch can be deactivated and the commit for deactivation can be done using the single <code>install rollback</code> command.
<b>Step 7</b>	<b>install deactivate file backup_image:</b> <code>smu-filename</code> <b>Example:</b> <pre>Device# install deactivate file backup_image:&lt;Smu-Filename&gt;</pre>	Deactivates a committed patch. The <code>install deactivate</code> command causes the reload of the controller in case of a cold patch. There is no reload of the controller in case of a hot patch.
<b>Step 8</b>	<b>install auto-abort-timer stop</b> <b>Example:</b>	(Optional) Stops the auto cancel timer in case of activated or deactivated SMUs.

	Command or Action	Purpose
	<code>Device# install auto-abort-timer stop</code>	
<b>Step 9</b>	<b>install commit</b> <b>Example:</b> <code>Device# install commit</code>	Commits the deactivation changes to be persistent across reloads.
<b>Step 10</b>	<b>install remove file backup_image:</b> <i>smu-filename</i> <b>Example:</b> <code>Device# install remove file backup_image:&lt;smu-filename&gt;</code>	Removes a patch that is in the inactive state. This command also removes the file physically from backup-image:
<b>Step 11</b>	<b>install abort</b> <b>Example:</b> <code>Device# install abort</code>	Cancels the upgrade by resetting the APs in rolling fashion.
<b>Step 12</b>	<b>show install summary</b> <b>Example:</b> <code>Device# show install summary</code>	Displays information about the active package. The output of this command varies based on the packages, and the package states that are installed.
<b>Step 13</b>	<b>show install package backup_image:</b> <i>smu-filename</i> <b>Example:</b> <code>Device# show install package backup-image: &lt;smu_filename&gt;</code>	Displays information about the SMU package.

## Creating SMU Files (GUI)

Follow the steps given below to create SMU files:

### Procedure

- 
- Step 1** Choose **Administration > Software Management > Software Maintenance Upgrade (SMU)**.
- Step 2** Click **Add**.  
A dialog box is displayed.
- Step 3** From the **Transport Type** drop-down list,
- **TFTP**: Specify the **Server IP Address (IPv4/IPv6)**, **File Path**, **File Name**, and **File System**.
  - **SFTP**: Specify the **Server IP Address (IPv4/IPv6)**, **Port Number** (Default port number is 22), **SFTP username and password**, **File Path**, **File Name**, and **File System**.
  - **FTP**: Specify the **Server IP Address (IPv4/IPv6)**, **Port Number** (Default port number is 22), **FTP username and password**, **File Path**, **File Name**, and **File System**.
  - **Device**: Specify the **File System** and **File path**.
  - **My Desktop**: Specify the **File System** and **Source File Path**.

**Step 4** Click Add File.

## Configuration Examples for SMU

The following is sample of the SMU configuration:

```
Device# install add file
tftp://10.1.1.2/auto/tftpboot/user1/ewc/ewc-apspl.bin
install_add: START Tue Jun 4 15:08:26 UTC 2019
Downloading file tftp://10.1.1.2/auto/tftpboot/user1/ewc/ewc-smu.bin
Finished downloading file tftp://10.1.1.2/auto/tftpboot/user1/ewc/ewc-smu.bin to
backup_image:ewc-smu.bin
install_add: Adding SMU
install_add: Checking whether new add is allowed ....
install_add: ap image predownload is allowed.

--- Starting initial file syncing ---
Info: Finished copying backup_image: ewc-smu.bin to the selected chassis
Finished initial file syncing

--- Starting SMU Add operation ---
Performing SMU_ADD on all members
[1] SMU_ADD package(s) on chassis 1
MEWLC response success sync_successCumulative SMU Size: 24 KB
Cumulative size of all SMU's will not exceed 20000 KB
Available Memory in /backup_image is 251480 KB
Available memory 251480 KB is greater than available memory required 2000 KB
[1] Finished SMU_ADD on chassis 1
Checking status of SMU_ADD on [1]
SMU_ADD: Passed on [1]
Finished SMU Add operation

SUCCESS: install_add

Device# install activate file backup_image:ewc-apspl.bin
install_activate: START Tue Jun 4 15:18:58 UTC 2019
install_activate: Activating SMU
Cumulative SMU Size: 24 KB
Cumulative size of all SMU's will not exceed 20000 KB
Available Memory in /backup_image is 250984 KB
Available memory 250984 KB is greater than available memory required 2000 KB
MEWLC response success sync_successExecuting pre scripts....
Executing pre sripts done.

--- Starting SMU Activate operation ---
Performing SMU_ACTIVATE on all members
ls: cannot access '/tmp/sw/fp/*/*/*mount/.pkginfo': No such file or directory
ls: cannot access '/tmp/sw/fp/*/*/*mount/.pkginfo': No such file or directory
[1] SMU_ACTIVATE package(s) on chassis 1
valid
install_activate: FP fp error skipping. Platform to fix this in Fru List
[1] Finished SMU_ACTIVATE on chassis 1
Checking status of SMU_ACTIVATE on [1]
SMU_ACTIVATE: Passed on [1]
Finished SMU Activate operation

Executing post scripts....
Executing post scripts done.
Executing post scripts....
```

```
Executing post scripts done.
SUCCESS: install_activate /backup_image/ewc-apspl.bin
```

#### Device#install commit

```
install_commit: START Tue Jun 4 16:15:25 UTC 2019
install_commit: Committing SMU
Executing pre scripts....
install_commit:
Executing pre sripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on all members
ls: cannot access '/tmp/sw/fp/***/mount/.pkginfo': No such file or directory
ls: cannot access '/tmp/sw/fp/***/mount/.pkginfo': No such file or directory
[1] SMU_COMMIT package(s) on chassis 1
valid
[1] Finished SMU_COMMIT on chassis 1
Checking status of SMU_COMMIT on [1]
SMU_COMMIT: Passed on [1]
Finished SMU Commit operation
```

```
Waiting for the platform to set the SMU sync timerSMU sync status is sync_successSMU sync
to AP's success
/tmp/rp/chasfs/wireless/wlc_notify
SUCCESS: install_commit /backup_image/ewc-apspl.bin
```

#### Device#install rollback to base

```
install_rollback: START Tue Jun 4 16:42:24 UTC 2019
install_rollback: Rolling back SMU
Executing pre scripts....
install_rollback:
Executing pre sripts done.
```

```
--- Starting SMU Rollback operation ---
Performing SMU_ROLLBACK on all members
ls: cannot access '/tmp/sw/fp/***/mount/.pkginfo': No such file or directory
ls: cannot access '/tmp/sw/fp/***/mount/.pkginfo': No such file or directory
[1] SMU_ROLLBACK package(s) on chassis 1
[1] Finished SMU_ROLLBACK on chassis 1
Checking status of SMU_ROLLBACK on [1]
SMU_ROLLBACK: Passed on [1]
Finished SMU Rollback operation
```

```
Executing post scripts....
Executing post scripts done.
Waiting for the platform to set the SMU sync timerSMU sync status is sync_successSMU sync
to AP's success
/tmp/rp/chasfs/wireless/wlc_notifyExecuting post scripts....
Executing post scripts done.
SUCCESS: install_rollback /backup_image/ewc-apspl.bin Tue Jun 4 16:43:01 UTC 2019
```

#### Device# install deactivate file backup\_image: ewc-apspl.bin

```
install remove file backup_image:ewc-apspl.bin
```

#### Device#show install sum

```
[ Chassis 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
```

```
-----
Type St Filename/Version
-----
```

```
APSP C backup_image:ewc-apspl.bin
IMG C 17.1.1.0.69043
-----
```

Auto abort timer: inactive  
-----

## Rolling AP Upgrade

Rolling AP upgrade is a method of upgrading the APs in a staggered manner such that some APs are always up in the network and provide seamless coverage to clients, while the other APs are selected to be upgraded.



---

**Note** The AP images should be downloaded before the rolling upgrade is triggered, so that all the APs that are to be upgraded have the new image version.

---

## Rolling AP Upgrade Process

Rolling AP upgrade is done on a per controller basis. The number of APs to be upgraded at a given time, is the percentage of the total number of APs that are connected to the controller. The percentage is capped at a user configured value. The default percentage is 15. The non-client APs will be upgraded before the actual upgrade of APs begin.

The upgrade process is as follows:

### 1. Candidate AP Set Selection

In this stage, a set of AP candidates are selected based on neighbouring AP information. For example, if you identify an AP for upgrade, a certain number (N) of its neighbours are excluded from candidate selection. The N values are generated in the following manner:

If the user configurable capped percentage is 25%, then N=6 (Expected number of iterations =5)

If the user configurable capped percentage is 15%, then N=12 (Expected number of iterations=12)

If the user configurable capped percentage is 5%, then N=24 (Expected number of iterations =22)

If the candidates cannot be selected using the neighbouring AP information, select candidates from indirect neighbours. If you still are not able to select candidates, the AP will be upgraded successfully without any failure.



---

**Note** After the candidates are selected, if the number of candidates are more than the configured percentage value, the extra candidates are removed to maintain the percentage cap.

---

### 2. Client Steering

Clients that are connected to the candidate APs are steered to APs that are not there in the candidate AP list, prior to rebooting the candidate APs. The AP sends out a request to each of its associated clients with a list of APs that are best suited for them. This does not include the candidate APs. The candidate APs are marked as unavailable for neighbour lists. Later, the markings are reset in the AP rejoin and reload process.

### 3. AP Rejoin and Reload Process

After the client steering process, if the clients are still connected to the candidate AP, the clients are sent a de-authorization and the AP is reloaded and comes up with a new image. A three-minute timer is set for the APs to rejoin. When this timer expires, all the candidates are checked and marked if they have either joined the controller or the mobility peer. If 90% of the candidate APs have joined, the iteration is concluded; if not, the timer is extended to three more minutes. The same check is repeated after three minutes. After checking thrice, the iteration ends and the next iteration begins. Each iteration may last for about 10 minutes.

For rolling AP upgrade, there is only one configuration that is required. It is the number of APs to be upgraded at a time, as a percentage of the total number of APs in the network.

Default value will be 15.

```
Device (config)#ap upgrade staggered <25 | 15 | 5>
```

## Verifying AP Upgrade on the Controller

Use the following **show** command to verify the AP upgrade on the controller:

```
Device# show ap upgrade
AP upgrade is in progress

From version: 17.1.0.6
To version: 17.1.0.99

Started at: 06/04/2019 15:19:32 UTC
Configured percentage: 15
Percentage complete: 0
Expected time of completion: 06/04/2019 16:39:32 UTC

Progress Report
-----
Iterations
-----
Iteration Start time End time AP count
-----
0 06/04/2019 15:19:33 UTC 06/04/2019 15:19:33 UTC 1
1 06/04/2019 15:19:33 UTC ONGOING 1

Upgraded
-----
Number of APs: 1
AP Name Ethernet MAC Iteration Status Site
-----
AP7069.5A74.7604 7069.5a78.5580 0 Not Impacted default-site-tag

In Progress
-----
Number of APs: 1
AP Name Ethernet MAC
-----
APB4DE.3169.7842 4c77.6dc4.a220

Remaining
-----
Number of APs: 0

AP Name Ethernet MAC
-----

APs not handled by Rolling AP Upgrade
```

-----  
AP Name Ethernet MAC Status Reason for not handling by Rolling AP Upgrade

# AP Device Pack (APDP) and AP Service Pack (APSP)

## APSP and APDP

**AP Service Pack (APSP)** - APSP rolls out fixes to AP images for one or more AP models. Pre-download the AP images and activate (through rolling upgrade) these images to a subset of AP models.

- Patched APs run a different CAPWAP version than the rest of the APs. For e.g. 17.1.0.100 and 17.1.0.0.
- Per site APSP rollout is not supported. In embedded wireless controller APSP all APs must be in a single default site.

### **AP Device Pack (APDP)** -

Currently, when a new AP hardware model is introduced, those get shipped along with the corresponding embedded wireless controller related major software version. Then you need to wait for the release of a corresponding embedded wireless controller version relative to the new AP model and upgrade the entire network.

APDP allows you introduce the new AP model into your wireless network using the SMU infrastructure without the need to upgrade to the new embedded wireless controller version.

### **AP Image Changes** -

When new AP models are introduced, there may or may not be corresponding new AP images. This means that AP images are mapped to the AP model families. If a new AP model belongs to an existing AP model family then you will have existing AP image entries (Example: ap3g3, ap1g5, and so on). For instance, if an AP model belongs to either ap3g3 or ap1g5, the respective image file is bundled with APDP SMU zip file. The corresponding metadata file is updated with the new AP model capability information including the AP image that it requires.

If a new AP model belongs to a new AP model family, a new image file would be bundled in the APDP SMU zip file. The corresponding metadata file is updated with the new AP model capability information including the AP image that it requires.

### **Information about APSP and APDP**

SMU AP images are not part of the SMU binary, and the AP images are hosted outside the controller.

- Only SFTP and TFTP methods are supported for SMU AP image download.
- HTTP, HTTPS, and CCO methods are not supported for APSP or APDP.

A SMU package contains the metadata that carry AP model and its capability related details.



**Note** All the zipped files are required in order to successfully proceed with the upgrade. All the contained files in the zip folder are made accessible through the download method.

Following are the pre-requisites for TFTP/SFTP software upgrade:

- A TFTP/SFTP server is reachable from the management IP address of the embedded wireless controller.
- The upgrade bundle with the AP images (ap1g6, ap1g6a, ap1g7, ap3g3, and so on) and the controller image (C9800-AP-iosxe-wlc.bin) that is downloaded from the website is unzipped and copied onto the TFTP/SFTP server.

## Managing APSP and APDP

AP images are hosted outside the wireless controller. In the embedded wireless controller, only TFTP or SFTP is supported for SMU AP image download.

### Configuring the APSP and APDP Files (GUI)

Follow the steps given below to add APSP or APDP files:

#### Procedure

- Step 1** Choose **Administration > Software Management > AP Service Package (APSP)** or **AP Device Package (APDP)**.  
The **Add an AP Device Package** or **Add an AP Service Package** window is displayed.
- Step 2** From the **Transport Type** drop-down list,
  - **TFTP**: Specify the **Server IP Address (IPv4/IPv6)**, **File Path**, **File Name**, and **File System**.
  - **SFTP**: Specify the **Server IP Address (IPv4/IPv6)**, **Port Number** (Default port number is 22), SFTP username and password, **File Path**, **File Name**, and **File System**.
- Step 3** Click **Add File**.

### Configuring the TFTP Server Directory

To set up the TFTP server directory, complete the following steps:

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device#configure terminal	Enter the configuration mode.



	Command or Action	Purpose
<b>Step 2</b>	<b>wireless profile image-download default</b> <b>Example:</b> Device(config)#wireless profile image-download default	Configures EWC-AP image download parameters. Use only default as the image download profile name.
<b>Step 3</b>	<b>image-download-mode { tftp   sftp }</b> <b>Example:</b> Device(config-wireless-image-download-profile)#image-download-mode tftp	Configures image download using TFTP.
<b>Step 4</b>	<b>tftp-image-path tftp-image-path</b> <b>Example:</b> Device(config-wireless-image-download-profile-tftp)#tftp-image-path /tftpboot/cisco/ewc/	Configures the TFTP server root directory for the AP images.
<b>Step 5</b>	<b>tftp-image-server { A.B.C.D   X:X:X:X::X }</b> <b>Example:</b> Device(config-wireless-image-download-profile-tftp)#tftp-image-server 5.5.5.5	Configures the TFTP server address.

### What to do next

- Set up the remote server directory: When you receive the complete bundle in a zip file, copy the zip file to a root directory, for example, /tftpboot/user/ewc. Example of the complete bundle - /tftpboot/user/ewc/17.1.zip.
- Unzip the file. The following are the examples of the files that will be present in the root directory: ap3g3, ap1g4, C9800-AP-iosxe-wlc.bin, and so on.



**Note** When there is an issue and you want to patch an APSP SMU based on the 17.1 patch file C9800\_AP.17\_1.22.CSCvr11111.apsp.zip is pasted in the same root folder, that is, /tftpboot/user/ewc/C9800\_AP.17\_1.22.CSCvr11111.apsp.zip. When you unzip the file, a sub-directory, for example, /tftpboot/user/ewc/17\_1.22.CSCvr11111/ is created automatically. The AP images (for example, ap3g3) and SMU binary (apsp\_CSCvr11111.bin) are present in that sub-directory.

## Configuring the SFTP Server Directory

To set up the SFTP server directory, complete the following steps:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>	Enter the configuration mode.

	Command or Action	Purpose
	Device#configure terminal	
<b>Step 2</b>	<b>wireless profile image-download default</b> <b>Example:</b> Device(config)#wireless profile image-download default	Configures EWC-AP image download parameters. Use only default as the image download profile name.
<b>Step 3</b>	<b>image-download-mode { tftp   sftp }</b> <b>Example:</b> Device(config-wireless-image-download-profile)#image-download-mode sftp	Configures image download using SFTP.
<b>Step 4</b>	<b>sftp-image-path sftp-image-path</b> <b>Example:</b> Device(config-wireless-image-download-profile-sftp)#sftp-image-path/sftpboot/cisco/ewc/	Configures the SFTP server root directory for the AP images.
<b>Step 5</b>	<b>sftp-image-server { A.B.C.D   X:X:X:X::X }</b> <b>Example:</b> Device(config-wireless-image-download-profile-sftp)#sftp-image-server 5.5.5.5	Configures the SFTP server address.
<b>Step 6</b>	<b>sftp-password { 0   8 } password re-enter password</b> <b>Example:</b> Device(config-wireless-image-download-profile-sftp)#sftp-password 0 admin	Configures the SFTP password.
<b>Step 7</b>	<b>sftp-username username</b> <b>Example:</b> Device(config-wireless-image-download-profile-sftp)#sftp-username admin	Configures the SFTP username.

### What to do next

- Set up the remote server directory: When you receive the complete bundle in a zip file, copy the zip file to a root directory, for example, /sftpboot/user/ewc. Example of the complete bundle - /sftpboot/user/ewc/17.1.zip.
- Unzip the file. The following are the examples of the files that will be present in the root directory: ap3g3, ap1g4, C9800-AP-iosxe-wlc.bin, and so on.



**Note** When there is an issue and you want to patch an APSP SMU based on the 17.1 patch file C9800\_AP.17\_1.22.CSCvr11111.apsp.zip is pasted in the same root folder, that is, /sftpboot/user/ewc/C9800\_AP.17\_1.22.CSCvr11111.apsp.zip. When you unzip the file, a sub-directory, for example, /sftpboot/user/ewc/17\_1.22.CSCvr11111/ is created automatically, and the AP images (for example, ap3g3) and SMU binary (apsp\_CSCvr11111.bin) are present in that sub-directory.

## Positive Workflow - APSP and APDP

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>install add file {tftp:   sftp:   backup_image:} apsp.bin</b>  <b>Example:</b> TFTP and Backup Image - <pre>Device# install add file tftp://server_path/ftpboot/user/ewc/17_1.22.CSCvr11111/apsp_CSCvr11111.bin Device#install add file backup-image:apsp_CSCvr11111.bin</pre>	The <code>install add</code> command copies the file from the external server to the <code>backup_image</code> directory on the embedded wireless controller.
<b>Step 2</b>	<b>ap image predownload</b>  <b>Example:</b> <pre>Device# ap image predownload</pre>	This command is optional. The command predownloads the AP image. If the predownload has started, ensure that it completes before step 3 is initiated.
<b>Step 3</b>	<b>install activate file backup-image: apsp.bin</b>  <b>Example:</b> <pre>Device# install activate file backup-image:apsp.bin</pre>	This command starts the rolling AP upgrade.  <b>Note</b> For APDP, after activate, the EWC Controller allows APs of the new AP model to join, and get the newly installed SMU AP image.
<b>Step 4</b>	<b>install commit</b>  <b>Example:</b> <pre>Device# install commit</pre>	Commits the activation changes to be persistent across reloads.  The commit can be done after activation while the system is up, or after one reload. If a patch is activated and not committed, the auto abort timer automatically cancels the activation of the patch in six hours .

## Rollback and Cancel

### One-Shot Rollback

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>show install rollback</b> <b>Example:</b> Device# show install rollback	Displays the possible rollback points.
<b>Step 2</b>	<b>install rollback to {base   committed   id   label } specific-rollback-point</b> <b>Example:</b> Device# install rollback to base	<p>This command triggers the Rolling AP upgrade. Rolling upgrade works for all APs that have the required image. Rest of the APs are rebooted together.</p> <p>Rolls back a committed patch. The committed patch can be deactivated and the commit for deactivation can be done using the single install rollback command.</p>

### Multi-Step Rollback

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>show install profile</b> <b>Example:</b> Device# show install profile	The <code>show install profile</code> command displays the profiles corresponding to the rollback points.
<b>Step 2</b>	<b>install add profile profile-rollback-point</b> <b>Example:</b> Device# install add profile profile-rollback-point	This command prepares the wireless module for the predownload step corresponding to the rollback point.
<b>Step 3</b>	<b>install rollback to {base   committed   id   label } specific-rollback-point</b> <b>Example:</b> Device# install rollback to base	<p>This command triggers the Rolling AP upgrade. Rolling upgrade works for all APs that have the required image. Rest of the APs are rebooted together.</p> <p>Rolls back a committed patch. The committed patch can be deactivated and the commit for deactivation can be done using the single install rollback command.</p>

### One-Shot Cancel

The following command is used for the One-Shot manual cancel:

**Procedure**

- **install abort**

**Example:**

```
Device# install abort
```

This command triggers rolling AP upgrade. Cancel is allowed only if commit is not yet completed. With One-Shot Cancel there is no predownload step. Rolling AP upgrade works for all APs which have the required image. Rest are rebooted together.

## Automatic Timer-Based One-Shot Cancel

After activation, a default 6-hour cancel timer is started. The cancel timer can be set to a different value when the **activate** command is issued, through the **auto-abort-timer** parameter. When the cancel timer expires, cancellation is performed the same way as the manual cancellation.

**Configuring Rollback (GUI)**

Follow the steps given below to configure rollback for APSP and APDP:

**Procedure**

- 
- Step 1** Choose **Administration > Software Management** .
  - Step 2** Select either **AP Service Pack (APSP)** or **AP Device Pack (APDP)**.
  - Step 3** From the **Rollback to** drop-down list, choose the Rollback type as *Base* or *Committed*.
  - Step 4** Click **Submit**.
- 

**Verifying APDP on the Embedded Wireless Controller**

To verify the status of APDP packages on the embedded wireless controller, use the following command:

```
Device# show install summary
```

```
[ Chassis 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
             C - Activated & Committed, D - Deactivated & Uncommitted
```

```
-----
Type  St  Filename/Version
-----
APDP  I   bootflash:apdp_CSCvp12345.bin
IMG   C   17.1.0.0
-----
```

```
Auto abort timer: inactive
-----
```




---

**Note** The output of this command varies based on the packages, and the package states that are installed.

---





## PART VI

# Security

- [IPv4 ACLs](#) , on page 285
- [DNS-Based Access Control Lists](#), on page 313
- [Allowed List of Specific URLs](#), on page 323
- [Web-Based Authentication](#) , on page 327
- [Central Web Authentication](#), on page 349
- [ISE Simplification and Enhancements](#), on page 363
- [Authentication and Authorization Between Multiple RADIUS Servers](#), on page 377
- [Secure LDAP](#), on page 387
- [RADIUS DTLS](#), on page 395
- [MAC Authentication Bypass](#), on page 407
- [Dynamic Frequency Selection](#), on page 417
- [Managing Rogue Devices](#), on page 419
- [Classifying Rogue Access Points](#), on page 439
- [Configuring Secure Shell](#) , on page 449
- [Private Shared Key](#), on page 457
- [Multi-Preshared Key](#), on page 465
- [Multiple Authentications for a Client](#), on page 473
- [Information About Cisco Umbrella WLAN](#), on page 485
- [Locally Significant Certificates](#), on page 495







## CHAPTER 37

# IPv4 ACLs

- [Information about Network Security with ACLs, on page 285](#)
- [Restrictions for Configuring IPv4 Access Control Lists, on page 293](#)
- [How to Configure ACLs, on page 294](#)
- [Configuration Examples for ACLs, on page 307](#)
- [Monitoring IPv4 ACLs, on page 310](#)

## Information about Network Security with ACLs

This chapter describes how to configure network security on the switch by using access control lists (ACLs), which in commands and tables are also referred to as access lists.

### ACL Overview

Packet filtering can help limit network traffic and restrict network use by certain users or devices. ACLs filter traffic as it passes through a controller and permit or deny packets crossing specified interfaces. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. One by one, it tests packets against the conditions in an access list. The first match decides whether the controller accepts or rejects the packets. Because the controller stops testing after the first match, the order of conditions in the list is critical. If no conditions match, the controller rejects the packet. If there are no restrictions, the controller forwards the packet; otherwise, the controller drops the packet. The controller can use ACLs on all packets it forwards. There is implicit any host deny deny rule.

You configure access lists on a controller to provide basic security for your network. If you do not configure ACLs, all packets passing through the switch could be allowed onto all parts of the network. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at router interfaces. For example, you can allow e-mail traffic to be forwarded but not Telnet traffic.

### Access Control Entries

An ACL contains an ordered list of access control entries (ACEs). Each ACE specifies *permit* or *deny* and a set of conditions the packet must satisfy in order to match the ACE. The meaning of *permit* or *deny* depends on the context in which the ACL is used.



---

**Note** The maximum number of ACEs that can be applied under an access policy (ACL) for central switching is 256 ACEs. The maximum number of ACEs applicable for Flex Mode or Local Switching is 64 ACEs.

---

## ACL Supported Types

The switch supports IP ACLs and Ethernet (MAC) ACLs:

- IP ACLs filter IPv4 traffic, including TCP, User Datagram Protocol (UDP), Internet Group Management Protocol (IGMP), and Internet Control Message Protocol (ICMP).
- Ethernet ACLs filter non-IP traffic.

This switch also supports quality of service (QoS) classification ACLs.

## Supported ACLs

The controller supports three types of ACLs to filter traffic:

- Port ACLs access-control traffic entering a Layer 2 interface. You can apply port ACLs to a Layer 2 interface in each direction to each access list type — IPv4 and MAC.
- Router ACLs access-control routed traffic between VLANs and are applied to Layer 3 interfaces in a specific direction (inbound or outbound).
- FQDN ACL: FQDN ACL is encoded along with IPv6 ACL and sent to AP. FQDN ACL is always a custom ACL. AP does DNS snooping and sends the IPv4 and IPv6 addresses to the controller.

## ACL Precedence

When Port ACLs, and router ACLs are configured on the same switch, the filtering precedence, from greatest to least for ingress traffic is port ACL, and then router ACL. For egress traffic, the filtering precedence is router ACL, and then port ACL.

The following examples describe simple use cases:

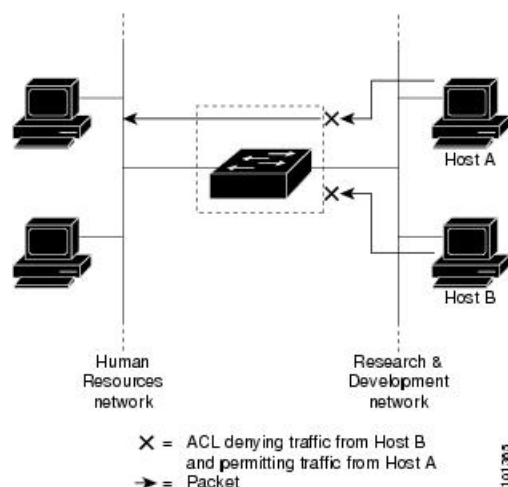
- When an input router ACL and input port ACL exist in a switch virtual interface (SVI), incoming packets received on ports to which a port ACL is applied are filtered by the port ACL. Incoming routed IP packets received on ports are filtered by the router ACL. Other packets are not filtered.
- When an output router ACL and input port ACL exist in an SVI, incoming packets received on the ports to which a port ACL is applied are filtered by the port ACL. Outgoing routed IP packets are filtered by the router ACL. Other packets are not filtered.

## Port ACLs

- Standard IP access lists using source addresses
- Extended IP access lists using source and destination addresses and optional protocol type information
- MAC extended access lists using source and destination MAC addresses and optional protocol type information

The switch examines ACLs on an interface and permits or denies packet forwarding based on how the packet matches the entries in the ACL. In this way, ACLs control access to a network or to part of a network.

**Figure 4: Using ACLs to Control Traffic in a Network**



This is an example of using port ACLs to control access to a network when all workstations are in the same VLAN. ACLs applied at the Layer 2 input would allow Host A to access the Human Resources network, but prevent Host B from accessing the same network. Port ACLs can only be applied to Layer 2 interfaces in the inbound direction.

When you apply a port ACL to a trunk port, the ACL filters traffic on all VLANs present on the trunk port. When you apply a port ACL to a port with voice VLAN, the ACL filters traffic on both data and voice VLANs.

With port ACLs, you can filter IP traffic by using IP access lists and non-IP traffic by using MAC addresses. You can filter both IP and non-IP traffic on the same Layer 2 interface by applying both an IP access list and a MAC access list to the interface.



**Note** You can't apply more than one IP access list and one MAC access list to a Layer 2 interface. If an IP access list or MAC access list is already configured on a Layer 2 interface and you apply a new IP access list or MAC access list to the interface, the new ACL replaces the previously configured one.

## Router ACLs

You can apply router ACLs on switch virtual interfaces (SVIs), which are Layer 3 interfaces to VLANs; on physical Layer 3 interfaces; and on Layer 3 EtherChannel interfaces. You apply router ACLs on interfaces for specific directions (inbound or outbound). You can apply one router ACL in each direction on an interface.

The switch supports these access lists for IPv4 traffic:

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses and optional protocol type information for matching operations.

As with port ACLs, the switch examines ACLs associated with features configured on a given interface. As packets enter the switch on an interface, ACLs associated with all inbound features configured on that interface are examined. After packets are routed and before they are forwarded to the next hop, all ACLs associated with outbound features configured on the egress interface are examined.

ACLs permit or deny packet forwarding based on how the packet matches the entries in the ACL, and can be used to control access to a network or to part of a network.

## ACEs and Fragmented and Unfragmented Traffic

IP packets can be fragmented as they cross the network. When this happens, only the fragment containing the beginning of the packet contains the Layer 4 information, such as TCP or UDP port numbers, ICMP type and code, and so on. All other fragments are missing this information.

Some access control entries (ACEs) do not check Layer 4 information and therefore can be applied to all packet fragments. ACEs that do test Layer 4 information cannot be applied in the standard manner to most of the fragments in a fragmented IP packet. When the fragment contains no Layer 4 information and the ACE tests some Layer 4 information, the matching rules are modified:

- Permit ACEs that check the Layer 3 information in the fragment (including protocol type, such as TCP, UDP, and so on) are considered to match the fragment regardless of what the missing Layer 4 information might have been.




---

**Note** For TCP ACEs with L4 Ops, the fragmented packets will be dropped per RFC 1858.

---

- Deny ACEs that check Layer 4 information never match a fragment unless the fragment contains Layer 4 information.

## ACEs and Fragmented and Unfragmented Traffic Examples

Consider access list 102, configured with these commands, applied to three fragmented packets:

```
Device(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Device(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Device(config)# access-list 102 permit tcp any host 10.1.1.2
Device(config)# access-list 102 deny tcp any any
```




---

**Note** In the first and second ACEs in the examples, the *eq* keyword after the destination address means to test for the TCP-destination-port well-known numbers equaling Simple Mail Transfer Protocol (SMTP) and Telnet, respectively.

---

- Packet A is a TCP packet from host 10.2.2.2., port 65000, going to host 10.1.1.1 on the SMTP port. If this packet is fragmented, the first fragment matches the first ACE (a permit) as if it were a complete packet because all Layer 4 information is present. The remaining fragments also match the first ACE, even though they do not contain the SMTP port information, because the first ACE only checks Layer 3 information when applied to fragments. The information in this example is that the packet is TCP and that the destination is 10.1.1.1.

- Packet B is from host 10.2.2.2, port 65001, going to host 10.1.1.2 on the Telnet port. If this packet is fragmented, the first fragment matches the second ACE (a deny) because all Layer 3 and Layer 4 information is present. The remaining fragments in the packet do not match the second ACE because they are missing Layer 4 information. Instead, they match the third ACE (a permit).

Because the first fragment was denied, host 10.1.1.2 cannot reassemble a complete packet, so packet B is effectively denied. However, the later fragments that are permitted will consume bandwidth on the network and resources of host 10.1.1.2 as it tries to reassemble the packet.

- Fragmented packet C is from host 10.2.2.2, port 65001, going to host 10.1.1.3, port ftp. If this packet is fragmented, the first fragment matches the fourth ACE (a deny). All other fragments also match the fourth ACE because that ACE does not check any Layer 4 information and because Layer 3 information in all fragments shows that they are being sent to host 10.1.1.3, and the earlier permit ACEs were checking different hosts.

## Standard and Extended IPv4 ACLs

This section describes IP ACLs.

An ACL is a sequential collection of permit and deny conditions. One by one, the switch tests packets against the conditions in an access list. The first match determines whether the switch accepts or rejects the packet. Because the switch stops testing after the first match, the order of the conditions is critical. If no conditions match, the switch denies the packet.

The software supports these types of ACLs or access lists for IPv4:

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses for matching operations and optional protocol-type information for finer granularity of control.



---

**Note** Only extended ACLs are supported while the standard ACLs are not supported.

---

### IPv4 ACL Switch Unsupported Features

Configuring IPv4 ACLs on the switch is the same as configuring IPv4 ACLs on other Cisco switches and routers.

The following ACL-related features are not supported:

- Non-IP protocol ACLs
- IP accounting
- Reflexive ACLs and dynamic ACLs are not supported.
- 
- 

### Access List Numbers

The number you use to denote your ACL shows the type of access list that you are creating.

This lists the access-list number and corresponding access list type and shows whether or not they are supported in the switch. The switch supports IPv4 standard and extended access lists, numbers 1 to 199 and 1300 to 2699.

**Table 7: Access List Numbers**

Access List Number	Type	Supported
1–99	IP standard access list	Yes
100–199	IP extended access list	Yes
200–299	Protocol type-code access list	No
300–399	DECnet access list	No
400–499	XNS standard access list	No
500–599	XNS extended access list	No
600–699	AppleTalk access list	No
700–799	48-bit MAC address access list	No
800–899	IPX standard access list	No
900–999	IPX extended access list	No
1000–1099	IPX SAP access list	No
1100–1199	Extended 48-bit MAC address access list	No
1200–1299	IPX summary address access list	No
1300–1999	IP standard access list (expanded range)	Yes
2000–2699	IP extended access list (expanded range)	Yes

In addition to numbered standard and extended ACLs, you can also create standard and extended named IP ACLs by using the supported numbers. That is, the name of a standard IP ACL can be 1 to 99; the name of an extended IP ACL can be 100 to 199. The advantage of using named ACLs instead of numbered lists is that you can delete individual entries from a named list.

## Numbered Standard IPv4 ACLs

When creating an ACL, remember that, by default, the end of the ACL contains an implicit deny statement for all packets that it did not find a match for before reaching the end. With standard access lists, if you omit the mask from an associated IP host address ACL specification, 0.0.0.0 is assumed to be the mask.

The switch always rewrites the order of standard access lists so that entries with **host** matches and entries with matches having a *don't care* mask of 0.0.0.0 are moved to the top of the list, above any entries with

non-zero *don't care* masks. Therefore, in **show** command output and in the configuration file, the ACEs do not necessarily appear in the order in which they were entered.

After creating a numbered standard IPv4 ACL, you can apply it to terminal lines (virtual teletype (VTY) lines), or to interfaces.

## Numbered Extended IPv4 ACLs

Although standard ACLs use only source addresses for matching, you can use extended ACL source and destination addresses for matching operations and optional protocol type information for finer granularity of control. When you are creating ACEs in numbered extended access lists, remember that after you create the ACL, any additions are placed at the end of the list. You cannot reorder the list or selectively add or remove ACEs from a numbered list.

The switch does not support dynamic or reflexive access lists. It also does not support filtering based on the type of service (ToS) minimize-monetary-cost bit.

Some protocols also have specific parameters and keywords that apply to that protocol.

You can define an extended TCP, UDP, ICMP, IGMP, or other IP ACL. The switch also supports these IP protocols:

These IP protocols are supported:

- Authentication Header Protocol (**ahp**)
- Encapsulation Security Payload (**esp**)
- Enhanced Interior Gateway Routing Protocol (**eigrp**)
- generic routing encapsulation (**gre**)
- Internet Control Message Protocol (**icmp**)
- Internet Group Management Protocol (**igmp**)
- any Interior Protocol (**ip**)
- IP in IP tunneling (**ipinip**)
- KA9Q NOS-compatible IP over IP tunneling (**nos**)
- Open Shortest Path First routing (**ospf**)
- Payload Compression Protocol (**pcp**)
- Protocol-Independent Multicast (**pim**)
- Transmission Control Protocol (**tcp**)
- User Datagram Protocol (**udp**)

## Named IPv4 ACLs

You can identify IPv4 ACLs with an alphanumeric string (a name) rather than a number. You can use named ACLs to configure more IPv4 access lists in a router than if you were to use numbered access lists. If you identify your access list with a name rather than a number, the mode and command syntax are slightly different. However, at times, not all commands that use IP access lists accept a named access list.




---

**Note** The name you give to a standard or extended ACL can also be a number in the supported range of access list numbers. That is, the name of a standard IP ACL can be 1 to 99 and . The advantage of using named ACLs instead of numbered lists is that you can delete individual entries from a named list.

---

Consider these guidelines before configuring named ACLs:

- Numbered ACLs are also available.
- A standard ACL and an extended ACL cannot have the same name.

## ACL Logging

The controller software can provide logging messages about packets permitted or denied by a standard IP access list. That is, any packet that matches the ACL causes an informational logging message about the packet to be sent to the console. The level of messages logged to the console is controlled by the **logging console** commands controlling the syslog messages.




---

**Note** Because routing is done in hardware and logging is done in software, if a large number of packets match a *permit* or *deny* ACE containing a **log** keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

---

The first packet that triggers the ACL causes a logging message right away, and subsequent packets are collected over 5-minute intervals before they appear or logged. The logging message includes the access list number, whether the packet was permitted or denied, the source IP address of the packet, and the number of packets from that source permitted or denied in the prior 5-minute interval.




---

**Note** The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

---

## Hardware and Software Treatment of IP ACLs

ACL processing is performed in hardware. If the hardware reaches its capacity to store ACL configurations, all packets on that interface are dropped.

The ACL scale for controllers is as follows:

- Cisco Catalyst 9800-40 Wireless Controller, Cisco Catalyst 9800-L Wireless Controller, Cisco Catalyst 9800-CL Wireless Controller (small and medium) support 128 ACLs with 128 Access List Entries (ACEs).
- Cisco Catalyst 9800-80 Wireless Controller and Cisco Catalyst 9800-CL Wireless Controller (large) support 256 ACLs and 256 ACEs.
- FlexConnect and Fabric mode APs support 96 ACLs.





---

**Note** If an ACL configuration cannot be implemented in the hardware due to an out-of-resource condition on the controller, then only the traffic in that VLAN arriving on that controller is affected.

---

When you enter the **show ip access-lists** privileged EXEC command, the match count displayed does not account for packets that are access controlled in hardware. Use the `show ip access-lists hardware` privileged EXEC command to obtain some basic hardware ACL statistics for switched and routed packets.

## IPv4 ACL Interface Considerations

For inbound ACLs, after receiving a packet, the controller checks the packet against the ACL. If the ACL permits the packet, the controller continues to process the packet. If the ACL rejects the packet, the controller discards the packet.

For outbound ACLs, after receiving and routing a packet to a controlled interface, the controller checks the packet against the ACL. If the ACL permits the packet, the controller sends the packet. If the ACL rejects the packet, the controller discards the packet.

If an undefined ACL has nothing listed in it, it is an empty access list.

## Restrictions for Configuring IPv4 Access Control Lists

The following are restrictions for configuring network security with ACLs:

### General Network Security

The following are restrictions for configuring network security with ACLs:

- A standard ACL and an extended ACL cannot have the same name.
- Though visible in the command-line help strings, **AppleTalk** is not supported as a matching condition for the **deny** and **permit** MAC access-list configuration mode commands.
- DNS traffic is permitted by default with or without ACL entries for clients that are awaiting web authentication.

### IPv4 ACL Network Interfaces

The following restrictions apply to IPv4 ACLs to network interfaces:

- When controlling access to an interface, you can use a named or numbered ACL.
- You do not have to enable routing to apply ACLs to Layer 2 interfaces.

### MAC ACLs on a Layer 2 Interface

After you create a MAC ACL, you can apply it to a Layer 2 interface to filter non-IP traffic coming in that interface. When you apply the MAC ACL, consider these guidelines:

- You can apply no more than one IP access list and one MAC access list to the same Layer 2 interface. The IP access list filters only IP packets, and the MAC access list filters non-IP packets.

- A Layer 2 interface can have only one MAC access list. If you apply a MAC access list to a Layer 2 interface that has a MAC ACL configured, the new ACL replaces the previously configured one.



---

**Note** The **mac access-group** interface configuration command is only valid when applied to a physical Layer 2 interface. You cannot use the command on EtherChannel port channels.

---

#### IP Access List Entry Sequence Numbering

- This feature does not support dynamic, reflexive, or firewall access lists.

## How to Configure ACLs

### Configuring IPv4 ACLs (GUI)

#### Procedure

---

- Step 1** Choose **Configuration > Security > ACL**.
- Step 2** Click **Add**.
- Step 3** In the **Add ACL Setup** dialog box, enter the following parameters.
- **ACL Name:** Enter the name for the ACL.
  - **ACL Type:** IPv4 Standard.
  - **Sequence:** Enter the sequence number.
  - **Action:** Choose **Permit** or **Deny** the packet flow from the drop-down list.
  - **Source Type:** Choose **any**, **Host** or **Network** from which the packet is sent.
  - **Log:** Enable or disable logging.
- Step 4** Click **Add**.
- Step 5** Add the rest of the rules and click **Apply to Device**.
- 

### Configuring IPv4 ACLs

Follow the procedure given below to use IP ACLs on the switch:

#### Procedure

---

- Step 1** Create an ACL by specifying an access list number or name and the access conditions.

**Step 2** Apply the ACL to interfaces or terminal lines..

## Creating a Numbered Standard ACL (GUI)

### Procedure

- Step 1** Choose **Configuration > Security > ACL**.
- Step 2** On the **ACL** page, click **Add**.
- Step 3** In the **Add ACL Setup** window, enter the following parameters.
- **ACL Name:** Enter the name for the ACL.
  - **ACL Type:** IPv4 Standard.
  - **Sequence:** Enter the sequence number.
  - **Action:** Choose **Permit** or **Deny** access from the drop-down list.
  - **Source Type:** Choose **any**, **Host** or **Network**
  - **Log:** Enable or disable logging, this is limited to ACLs associated to Layer 3 interface only.
- Step 4** Click **Add**.
- Step 5** Click **Save & Apply to Device**.

## Creating a Numbered Standard ACL (CLI)

Follow the procedure given below to create a numbered standard ACL:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b>  Device> <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>  Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>access-list</b> <i>access-list-number</i> { <b>deny</b>   <b>permit</b> } <i>source source-wildcard</i> ]	Defines a standard IPv4 access list by using a source address and wildcard.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device(config)# access-list 2 deny your_host</pre>	<p>The <i>access-list-number</i> is a decimal number from 1 to 99 or 1300 to 1999.</p> <p>Enter <b>deny</b> or <b>permit</b> to specify whether to deny or permit access if conditions are matched.</p> <p>The <i>source</i> is the source address of the network or host from which the packet is being sent specified as:</p> <ul style="list-style-type: none"> <li>• The 32-bit quantity in dotted-decimal format.</li> <li>• The keyword <b>any</b> as an abbreviation for <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard.</li> <li>• The keyword <b>host</b> as an abbreviation for source and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.</li> </ul> <p>(Optional) The <i>source-wildcard</i> applies wildcard bits to the source.</p> <p><b>Note</b> Logging is supported only on ACLs attached to Layer 3 interfaces.</p>
<b>Step 4</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 5</b>	<p><b>show running-config</b></p> <p><b>Example:</b></p> <pre>Device# show running-config</pre>	Verifies your entries.
<b>Step 6</b>	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## Creating a Numbered Extended ACL (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Security > ACL**.
- Step 2** On the **ACL** page, click **Add**.
- Step 3** In the **Add ACL Setup** window, enter the following parameters.
- **ACL Name:** Enter the name for the ACL.
  - **ACL Type:** IPv4 Extended.
  - **Sequence:** Enter the sequence number.
  - **Action:** Choose **Permit** or **Deny** the packet flow from the drop-down list.
  - **Source Type:** Choose **any**, **Host** or **Network** from which the packet is sent.
  - **Destination Type:** Choose **any**, **Host** or **Network** to which the packet is sent.
  - **Protocol:** Choose a protocol from the drop-down list.
  - **Log:** Enable or disable logging.
  - **DSCP:** Enter to match packets with the DSCP value
- Step 4** Click **Add**.
- Step 5** Click **Save & Apply to Device**.
- 

## Creating a Numbered Extended ACL (CLI)

Follow the procedure given below to create a numbered extended ACL:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>access-list access-list-number {deny   permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp]</b>	Defines an extended IPv4 access list and the access conditions. The <i>access-list-number</i> is a decimal number from 100 to 199 or 2000 to 2699.

Command or Action	Purpose
<p><b>Example:</b></p> <pre>Device(config)# access-list 101 permit ip host 10.1.1.2 any precedence 0 tos 0 log</pre>	<p>Enter <b>deny</b> or <b>permit</b> to specify whether to deny or permit the packet if conditions are matched.</p> <p>For <i>protocol</i>, enter the name or number of an IP protocol: <b>ahp</b>, <b>eigrp</b>, <b>esp</b>, <b>gre</b>, <b>icmp</b>, <b>igmp</b>, <b>igrp</b>, <b>ip</b>, <b>ipinip</b>, <b>nos</b>, <b>ospf</b>, <b>pcp</b>, <b>pim</b>, <b>tcp</b>, or <b>udp</b>, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the keyword <b>ip</b>.</p> <p><b>Note</b> This step includes options for most IP protocols. For additional specific parameters for TCP, UDP, ICMP, and IGMP, see the following steps.</p> <p>The <i>source</i> is the number of the network or host from which the packet is sent.</p> <p>The <i>source-wildcard</i> applies wildcard bits to the source.</p> <p>The <i>destination</i> is the network or host number to which the packet is sent.</p> <p>The <i>destination-wildcard</i> applies wildcard bits to the destination.</p> <p>Source, source-wildcard, destination, and destination-wildcard can be specified as:</p> <ul style="list-style-type: none"> <li>• The 32-bit quantity in dotted-decimal format.</li> <li>• The keyword <b>any</b> for 0.0.0.0 255.255.255.255 (any host).</li> <li>• The keyword <b>host</b> for a single host 0.0.0.0.</li> </ul> <p>The other keywords are optional and have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>precedence</b>—Enter to match packets with a precedence level specified as a number from 0 to 7 or by name: <b>routine</b> (0), <b>priority</b> (1), <b>immediate</b> (2), <b>flash</b> (3), <b>flash-override</b> (4), <b>critical</b> (5), <b>internet</b> (6), <b>network</b> (7).</li> <li>• <b>fragments</b>—Enter to check non-initial fragments.</li> <li>• <b>tos</b>—Enter to match by type of service level, specified by a number from 0 to 15</li> </ul>

	Command or Action	Purpose
		<p>or a name: <b>normal</b> (0), <b>max-reliability</b> (2), <b>max-throughput</b> (4), <b>min-delay</b> (8).</p> <ul style="list-style-type: none"> <li>• <b>time-range</b>—Specify the time-range name.</li> <li>• <b>dscp</b>—Enter to match packets with the DSCP value specified by a number from 0 to 63, or use the question mark (?) to see a list of available values.</li> </ul> <p><b>Note</b> Your embedded controller must support the ability to:</p> <ul style="list-style-type: none"> <li>• Mark DCSP</li> <li>• Mark UP</li> <li>• Map DSCP and UP</li> </ul> <p>For more information on <b>DSCP-to-UP Mapping</b>, see:</p> <p><a href="https://tools.ietf.org/html/draft-ietf-tsvwg-ieee-802-11-01">https://tools.ietf.org/html/draft-ietf-tsvwg-ieee-802-11-01</a></p> <p><b>Note</b> If you enter a <b>dscp</b> value, you cannot enter <b>tos</b> or <b>precedence</b>. You can enter both a <b>tos</b> and a <b>precedence</b> value with no <b>dscp</b>.</p>
<b>Step 3</b>	<p><b>access-list</b> <i>access-list-number</i> {<b>deny</b>   <b>permit</b>}  <b>tcp</b> <i>source source-wildcard</i> [<i>operator port</i>]  <i>destination destination-wildcard</i> [<i>operator port</i>]  [<b>precedence</b> <i>precedence</i>] [<b>tos</b> <i>tos</i>] [<b>fragments</b>]  [<b>time-range</b> <i>time-range-name</i>] [<b>dscp</b> <i>dscp</i>]  [<i>flag</i>]</p> <p><b>Example:</b></p> <pre>Device(config)# access-list 101 permit tcp any any eq 500</pre>	<p>Defines an extended TCP access list and the access conditions.</p> <p>The parameters are the same as those described for an extended IPv4 ACL, with these exceptions:</p> <p>(Optional) Enter an <i>operator</i> and <i>port</i> to compare source (if positioned after <i>source source-wildcard</i>) or destination (if positioned after <i>destination destination-wildcard</i>) port. Possible operators include <b>eq</b> (equal), <b>gt</b> (greater than), <b>lt</b> (less than), <b>neq</b> (not equal), and <b>range</b> (inclusive range). Operators require a port number (range requires two port numbers separated by a space).</p> <p>Enter the <i>port</i> number as a decimal number (from 0 to 65535) or the name of a TCP port. Use only TCP port numbers or names when filtering TCP.</p>

	Command or Action	Purpose
		<p>The other optional keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <i>flag</i>—Enter one of these flags to match by the specified TCP header bits: <b>ack</b> (acknowledge), <b>fin</b> (finish), <b>psh</b> (push), <b>rst</b> (reset), <b>syn</b> (synchronize), or <b>urg</b> (urgent).</li> </ul>
<b>Step 4</b>	<p><b>access-list</b> <i>access-list-number</i> {<b>deny</b>   <b>permit</b>}  <b>udp</b> <i>source source-wildcard</i> [<i>operator port</i>]  <i>destination destination-wildcard</i> [<i>operator port</i>]  [<b>precedence</b> <i>precedence</i>] [<b>tos</b> <i>tos</i>] [<b>fragments</b>]  [<b>time-range</b> <i>time-range-name</i>] [<b>dscp</b> <i>dscp</i>]</p> <p><b>Example:</b></p> <pre>Device(config)# access-list 101 permit udp any any eq 100</pre>	<p>(Optional) Defines an extended UDP access list and the access conditions.</p> <p>The UDP parameters are the same as those described for TCP except that the [<i>operator port</i>] port number or name must be a UDP port number or name, and the <b>flag</b> not valid for UDP.</p>
<b>Step 5</b>	<p><b>access-list</b> <i>access-list-number</i> {<b>deny</b>   <b>permit</b>}  <b>icmp</b> <i>source source-wildcard destination</i>  <i>destination-wildcard</i> [<i>icmp-type</i>   [<i>icmp-type</i>  <i>icmp-code</i>]   [<i>icmp-message</i>]] [<b>precedence</b>  <i>precedence</i>] [<b>tos</b> <i>tos</i>] [<b>fragments</b>] [<b>time-range</b>  <i>time-range-name</i>] [<b>dscp</b> <i>dscp</i>]</p> <p><b>Example:</b></p> <pre>Device(config)# access-list 101 permit icmp any any 200</pre>	<p>Defines an extended ICMP access list and the access conditions.</p> <p>The ICMP parameters are the same as those described for most IP protocols in an extended IPv4 ACL, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <i>icmp-type</i>—Enter to filter by ICMP message type, a number from 0 to 255.</li> <li>• <i>icmp-code</i>—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255.</li> <li>• <i>icmp-message</i>—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name.</li> </ul>
<b>Step 6</b>	<p><b>access-list</b> <i>access-list-number</i> {<b>deny</b>   <b>permit</b>}  <b>igmp</b> <i>source source-wildcard destination</i>  <i>destination-wildcard</i> [<i>igmp-type</i>] [<b>precedence</b>  <i>precedence</i>] [<b>tos</b> <i>tos</i>] [<b>fragments</b>] [<b>time-range</b>  <i>time-range-name</i>] [<b>dscp</b> <i>dscp</i>]</p> <p><b>Example:</b></p> <pre>Device(config)# access-list 101 permit igmp any any 14</pre>	<p>(Optional) Defines an extended IGMP access list and the access conditions.</p> <p>The IGMP parameters are the same as those described for most IP protocols in an extended IPv4 ACL, with this optional parameter.</p> <p><i>igmp-type</i>—To match IGMP message type, enter a number from 0 to 15, or enter the message name: <b>dvmrp</b>, <b>host-query</b>, <b>host-report</b>, <b>pim</b>, or <b>trace</b>.</p>



	Command or Action	Purpose
<b>Step 7</b>	<b>end</b> <b>Example:</b> Device (config) # <b>end</b>	Returns to privileged EXEC mode.

## Creating Named Standard ACLs (GUI)

### Procedure

- 
- Step 1** Click **Configuration > Security > ACL**.
- Step 2** Click **Add** to create a new ACL setup.
- Step 3** In the **Add ACL Setup** window, enter the following parameters.
- **ACL Name:** Enter the name for the ACL
  - **ACL Type:** IPv4 Standard
  - **Sequence:** The valid range is between 1 and 99 or 1300 and 1999
  - **Action:** Choose **Permit** or **Deny** access from the drop-down list.
  - **Source Type:** Choose **any**, **Host** or **Network**
  - **Log:** Enable or disable logging, this is limited to ACLs associated to Layer 3 interface only.
- Step 4** Click **Add** to add the rule.
- Step 5** Click **Save & Apply to Device**.
- 

## Creating Named Standard ACLs

Follow the procedure given below to create a standard ACL using names:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>	Enters global configuration mode.

	Command or Action	Purpose
	Device# <code>configure terminal</code>	
<b>Step 3</b>	<p><b>ip access-list standard</b> <i>name</i></p> <p><b>Example:</b></p> <pre>Device(config)# ip access-list standard 20</pre>	<p>Defines a standard IPv4 access list using a name, and enter access-list configuration mode.</p> <p>The name can be a number from 1 to 99.</p>
<b>Step 4</b>	<p>Use one of the following:</p> <ul style="list-style-type: none"> <li>• <b>deny</b> {<i>source</i> [<i>source-wildcard</i>]   <b>host</b> <i>source</i>   <b>any</b>} [<b>log</b>]</li> <li>• <b>permit</b> {<i>source</i> [<i>source-wildcard</i>]   <b>host</b> <i>source</i>   <b>any</b>} [<b>log</b>]</li> </ul> <p><b>Example:</b></p> <pre>Device(config-std-nacl)# deny 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255</pre> <p>or</p> <pre>Device(config-std-nacl)# permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0</pre>	<p>In access-list configuration mode, specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.</p> <ul style="list-style-type: none"> <li>• <b>host</b> <i>source</i>—A source and source wildcard of <i>source</i> 0.0.0.0.</li> <li>• <b>any</b>—A source and source wildcard of 0.0.0.0 255.255.255.255.</li> </ul>
<b>Step 5</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-std-nacl)# end</pre>	Returns to privileged EXEC mode.
<b>Step 6</b>	<p><b>show running-config</b></p> <p><b>Example:</b></p> <pre>Device# show running-config</pre>	Verifies your entries.
<b>Step 7</b>	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## Creating Extended Named ACLs (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Security > ACL**.
- Step 2** Click **Add**.
- Step 3** In the **Add ACL Setup** window, enter the following parameters.
- **ACL Name:** Enter the name for the ACL.
  - **ACL Type:** IPv4 Extended.
  - **Sequence:** Enter the sequence number.
  - **Action:** Choose **Permit** or **Deny** the packet flow from the drop-down list.
  - **Source Type:** Choose **any**, **Host** or **Network** from which the packet is sent.
  - **Destination Type:** Choose **any**, **Host** or **Network** to which the packet is sent.
  - **Protocol:** Choose a protocol from the drop-down list.
  - **Log:** Enable or disable logging.
  - **DSCP:** Enter to match packets with the DSCP value
- Step 4** Click **Add**.
- Step 5** Add the rest of the rules and click **Apply to Device**.
- 

## Creating Extended Named ACLs

Follow the procedure given below to create an extended ACL using names:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>ip access-list extended</b> <i>name</i> <b>Example:</b> <pre>Device(config)# ip access-list extended 150</pre>	Defines an extended IPv4 access list using a name, and enter access-list configuration mode.  The name can be a number from 100 to 199.
<b>Step 4</b>	{ <b>deny</b>   <b>permit</b> } <i>protocol</i> { <i>source</i> [ <i>source-wildcard</i> ]   <b>host</b> <i>source</i>   <b>any</b> } { <i>destination</i> [ <i>destination-wildcard</i> ]   <b>host</b> <i>destination</i>   <b>any</b> } [ <b>precedence</b> <i>precedence</i> ] [ <b>tos</b> <i>tos</i> ] [ <b>log</b> ] [ <b>time-range</b> <i>time-range-name</i> ] <b>Example:</b> <pre>Device(config-ext-nacl)# permit 0 any any</pre>	In access-list configuration mode, specify the conditions allowed or denied. Use the <b>log</b> keyword to get access list logging messages, including violations. <ul style="list-style-type: none"> <li>• <b>host source</b>—A source and source wildcard of <i>source</i> 0.0.0.0.</li> <li>• <b>host destination</b>—A destination and destination wildcard of <i>destination</i> 0.0.0.0.</li> <li>• <b>any</b>—A source and source wildcard or destination and destination wildcard of 0.0.0.0 255.255.255.255.</li> </ul>
<b>Step 5</b>	<b>end</b> <b>Example:</b> <pre>Device(config-ext-nacl)# end</pre>	Returns to privileged EXEC mode.
<b>Step 6</b>	<b>show running-config</b> <b>Example:</b> <pre>Device# show running-config</pre>	Verifies your entries.
<b>Step 7</b>	<b>copy running-config startup-config</b> <b>Example:</b> <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

When you are creating extended ACLs, remember that, by default, the end of the ACL contains an implicit deny statement for everything if it did not find a match before reaching the end. For standard ACLs, if you omit the mask from an associated IP host address access list specification, 0.0.0.0 is assumed to be the mask.

After you create an ACL, any additions are placed at the end of the list. You cannot selectively add ACL entries to a specific ACL. However, you can use **no permit** and **no deny** access-list configuration mode commands to remove entries from a named ACL.

Being able to selectively remove lines from a named ACL is one reason you might use named ACLs instead of numbered ACLs.

**What to do next**

After creating a named ACL, you can apply it to interfaces or to VLANs.

## Applying an IPv4 ACL to an Interface (GUI)

**Procedure**

- 
- Step 1** Choose **Configuration > Security > ACL**.
  - Step 2** Click **Associating Interfaces**.
  - Step 3** Choose the interface from the **Available Interfaces** list to view its ACL details on the right-hand side. You can change the ACL details, if required.
  - Step 4** Click **Save & Apply to Device**.
- 

## Applying an IPv4 ACL to an Interface (CLI)

This section describes how to apply IPv4 ACLs to network interfaces.

Beginning in privileged EXEC mode, follow the procedure given below to control access to an interface:

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>  Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>interface <i>interface-id</i></b> <b>Example:</b>  Device(config)#	Identifies a specific interface for configuration, and enter interface configuration mode.  The interface can be a Layer 2 interface (port ACL), or a Layer 3 interface (router ACL).
<b>Step 3</b>	<b>ip access-group {<i>access-list-number</i>   <i>name</i>} {in   out}</b> <b>Example:</b>  Device(config-if)# <code>ip access-group 2 in</code>	Controls access to the specified interface.
<b>Step 4</b>	<b>end</b> <b>Example:</b>	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Device(config-if)# <b>end</b>	
<b>Step 5</b>	<b>show running-config</b>  <b>Example:</b>  Device# <b>show running-config</b>	Displays the access list configuration.
<b>Step 6</b>	<b>copy running-config startup-config</b>  <b>Example:</b>  Device# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## Applying ACL to Policy Profile (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Policy**.
  - Step 2** On the **Policy Profile** page, click **Add**.
  - Step 3** In the **Add Policy Profile** window, click **Access Policies** tab.
  - Step 4** In the **WLAN ACL** area, choose the IPv4 ACL from the **IPv4 ACL** drop-down list.
  - Step 5** Click **Apply to Device**.
- 

## Applying ACL to Policy Profile

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b>  Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile policy <i>profile-policy</i></b>  <b>Example:</b>  Device(config)# <b>wireless profile policy profile-policy</b>	Configures a WLAN policy profile and enters wireless policy configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>ipv4 acl</b> <i>acl-name</i> <b>Example:</b> Device(config-wireless-policy)# ipv4 acl test-acl	Configures an IPv4 ACL.
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config-wireless-policy)# end	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuration Examples for ACLs

### Examples: Including Comments in ACLs

You can use the **remark** keyword to include comments (remarks) about entries in any IP standard or extended ACL. The remarks make the ACL easier for you to understand and scan. Each remark line is limited to 100 characters.

The remark can go before or after a permit or deny statement. You should be consistent about where you put the remark so that it is clear which remark describes which permit or deny statement. For example, it would be confusing to have some remarks before the associated permit or deny statements and some remarks after the associated statements.

To include a comment for IP numbered standard or extended ACLs, use the **access-list** *access-list number* **remark** *remark* global configuration command. To remove the remark, use the **no** form of this command.

In this example, the workstation that belongs to Jones is allowed access, and the workstation that belongs to Smith is not allowed access:

```
Device(config)# access-list 1 remark Permit only Jones workstation through
Device(config)# access-list 1 permit 171.69.2.88
Device(config)# access-list 1 remark Do not allow Smith through
Device(config)# access-list 1 deny 171.69.3.13
```

For an entry in a named IP ACL, use the **remark** access-list configuration command. To remove the remark, use the **no** form of this command.

In this example, the Jones subnet is not allowed to use outbound Telnet:

```
Device(config)# ip access-list extended telnetting
Device(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Device(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

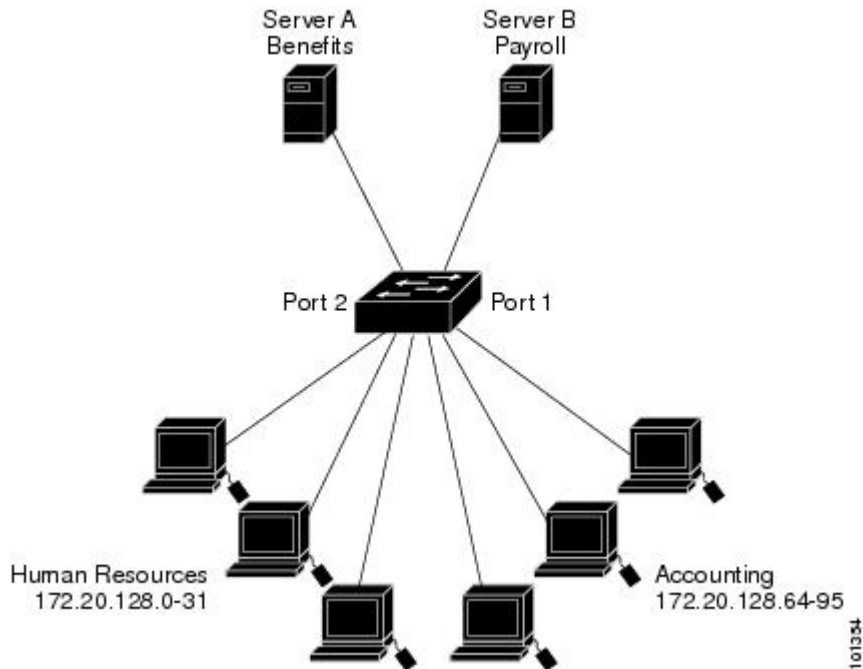
## IPv4 ACL Configuration Examples

This section provides examples of configuring and applying IPv4 ACLs. For detailed information about compiling ACLs, see the *Cisco IOS Security Configuration Guide, Release 12.4* and to the Configuring IP

Services” section in the “IP Addressing and Services” chapter of the *Cisco IOS IP Configuration Guide, Release 12.4*.

## ACLs in a Small Networked Office

Figure 5: Using Router ACLs to Control Traffic



This shows a small networked office environment with routed Port 2 connected to Server A, containing benefits and other information that all employees can access, and routed Port 1 connected to Server B, containing confidential payroll data. All users can access Server A, but Server B has restricted access.

Use router ACLs to do this in one of two ways:

- Create a standard ACL, and filter traffic coming to the server from Port 1.
- Create an extended ACL, and filter traffic coming from the server into Port 1.

### Examples: ACLs in a Small Networked Office

This example uses a standard ACL to filter traffic coming into Server B from a port, permitting traffic only from Accounting’s source addresses 172.20.128.64 to 172.20.128.95. The ACL is applied to traffic coming out of routed Port 1 from the specified source address.

```
Device(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Device(config)# end
Device# show access-lists
Standard IP access list 6
 10 permit 172.20.128.64, wildcard bits 0.0.0.31
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 6 out
```



This example uses an extended ACL to filter traffic coming from Server B into a port, permitting traffic from any source address (in this case Server B) to only the Accounting destination addresses 172.20.128.64 to 172.20.128.95. The ACL is applied to traffic going into routed Port 1, permitting it to go only to the specified destination addresses. Note that with extended ACLs, you must enter the protocol (IP) before the source and destination information.

```
Device(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Device(config)# end
Device# show access-lists
Extended IP access list 106
    10 permit ip any 172.20.128.64 0.0.0.31
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 106 in
```

## Example: Numbered ACLs

In this example, network 10.0.0.0 is a Class A network whose second octet specifies a subnet; that is, its subnet mask is 255.255.0.0. The third and fourth octets of a network 10.0.0.0 address specify a particular host. Using access list 2, the switch accepts one address on subnet 48 and reject all others on that subnet. The last line of the list shows that the switch accepts addresses on all other network 10.0.0.0 subnets. The ACL is applied to packets entering a port.

```
Device(config)# access-list 2 permit 10.48.0.3
Device(config)# access-list 2 deny 10.48.0.0 0.0.255.255
Device(config)# access-list 2 permit 10.0.0.0 0.255.255.255
Device(config)#
Device(config-if)# ip access-group 2 in
```

## Examples: Extended ACLs

In this example, the first line permits any incoming TCP connections with destination ports greater than 1023. The second line permits incoming TCP connections to the Simple Mail Transfer Protocol (SMTP) port of host 128.88.1.2. The third line permits incoming ICMP messages for error feedback.

```
Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
Device(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Device(config)# access-list 102 permit icmp any any
Device(config)#
Device(config-if)# ip access-group 102 in
```

In this example, suppose that you have a network connected to the Internet, and you want any host on the network to be able to form TCP connections to any host on the Internet. However, you do not want IP hosts to be able to form TCP connections to hosts on your network, except to the mail (SMTP) port of a dedicated mail host.

SMTP uses TCP port 25 on one end of the connection and a random port number on the other end. The same port numbers are used throughout the life of the connection. Mail packets coming in from the Internet have a destination port of 25. Because the secure system of the network always accepts mail connections on port 25, the incoming are separately controlled.

```
Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
Device(config)#
```

```
Device(config-if)# ip access-group 102 in
```

## Examples: Named ACLs

### Creating named standard and extended ACLs

This example creates a standard ACL named *internet\_filter* and an extended ACL named *marketing\_group*. The *internet\_filter* ACL allows all traffic from the source address 1.2.3.4.

```
Device(config)# ip access-list standard Internet_filter
Device(config-ext-nacl)# permit 1.2.3.4
Device(config-ext-nacl)# exit
```

The *marketing\_group* ACL allows any TCP Telnet traffic to the destination address and wildcard 171.69.0.0 0.0.255.255 and denies any other TCP traffic. It permits ICMP traffic, denies UDP traffic from any source to the destination address range 171.69.0.0 through 179.69.255.255 with a destination port less than 1024, denies any other IP traffic, and provides a log of the result.

```
Device(config)# ip access-list extended marketing_group
Device(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Device(config-ext-nacl)# deny tcp any any
Device(config-ext-nacl)# permit icmp any any
Device(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
Device(config-ext-nacl)# deny ip any any log
Device(config-ext-nacl)# exit
```

The *Internet\_filter* ACL is applied to outgoing traffic and the *marketing\_group* ACL is applied to incoming traffic on a Layer 3 port.

```
Device(config)# interface gigabitethernet3/0/1

Device(config-if)# ip address 2.0.5.1 255.255.255.0
Device(config-if)# ip access-group Internet_filter out
Device(config-if)# ip access-group marketing_group in
```

### Deleting individual ACEs from named ACLs

This example shows how you can delete individual ACEs from the named access list *border-list*:

```
Device(config)# ip access-list extended border-list
Device(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

## Monitoring IPv4 ACLs

You can monitor IPv4 ACLs by displaying the ACLs that are configured on the switch, and displaying the ACLs that have been applied to interfaces and VLANs.

When you use the **ip access-group** interface configuration command to apply ACLs to a Layer 2 or 3 interface, you can display the access groups on the interface. You can also display the MAC ACLs applied to a Layer 2 interface. You can use the privileged EXEC commands as described in this table to display this information.

**Table 8: Commands for Displaying Access Lists and Access Groups**

Command	Purpose
<b>show access-lists</b> [ <i>number</i>   <i>name</i> ]	Displays the contents of one or all current IP and MAC address access lists or a specific access list (numbered or named).
<b>show ip access-lists</b> [ <i>number</i>   <i>name</i> ]	Displays the contents of all current IP access lists or a specific IP access list (numbered or named).
<b>show ip interface</b> <i>interface-id</i>	Displays detailed configuration and status of an interface. If IP is enabled on the interface and ACLs have been applied by using the <b>ip access-group</b> interface configuration command, the access groups are included in the display.
<b>show running-config</b> [ <b>interface</b> <i>interface-id</i> ]	Displays the contents of the configuration file for the switch or the specified interface, including all configured MAC and IP access lists and which access groups are applied to an interface.





## CHAPTER 38

# DNS-Based Access Control Lists

- [Information About DNS-Based Access Control Lists, on page 313](#)
- [Restrictions on DNS-Based Access Control Lists, on page 315](#)
- [Flex Mode, on page 316](#)
- [Viewing DNS-Based Access Control Lists, on page 318](#)

## Information About DNS-Based Access Control Lists

The DNS-based ACLs are used for wireless client devices. When using these devices, you can set pre-authentication ACLs on the embedded wireless controller to determine the data requests that are allowed or blocked.

To enable DNS-based ACLs on the embedded wireless controller, you need to configure the allowed URLs or denied URLs for the ACLs. The URLs need to be pre-configured on the ACL.

With DNS-based ACLs, the client when in registration phase is allowed to connect to the configured URLs. The embedded wireless controller is configured with the ACL name that is returned by the AAA server. If the ACL name is returned by the AAA server, then the ACL is applied to the client for web-redirection.

At the client authentication phase, the AAA server returns the pre-authentication ACL (url-redirect-acl, which is the attribute name given to the AAA server). The DNS snooping is performed on the AP for each client until the registration is complete and the client is in SUPPLICANT PROVISIONING state. When the ACL configured with the URLs is received on the embedded wireless controller, the CAPWAP payload is sent to the AP enabling DNS snooping for the URLs to be snooped.

With URL snooping in place, the AP learns the IP address of the resolved domain name in the DNS response. If the domain name matches the configured URL, then the DNS response is parsed for the IP address. The AP adds the IP address to the allowed list of IP addresses and thus the client can access the URLs configured.

During pre-authentication or post-authentication, DNS ACL is applied to the client in the access point. If the client roams from one AP to another AP, the DNS learned IP addresses on the old AP is valid on the new AP as well.

This feature supports:

- A maximum of 32 URL lists.
- A maximum of 32 URLs per URL list.
- Up to 30 IP addresses per URL.

- A maximum of 16 URL lists with wild-cards.
- A maximum of 10 URLs per wild-card URL.




---

**Note** When configuring wild-card based URLs, generic wild-card URLs are not allowed; wild-cards cannot be present between the domain name; multiple wild-cards are not allowed in a URL. Wild-card specification in a URL can only be at a third-degree level or a higher level.

---




---

**Note** Conflicting or invalid configurations are not allowed. The same URL cannot have different actions. For example, Deny and Allow cannot be configured on [www.yahoo.com](http://www.yahoo.com).

---




---

**Note** URL filter needs to be attached to a policy profile in case of the local mode. In the flex mode, the URL filter is attached to the flex profile and it is not need to be attached to a policy profile.

---




---

**Note** DNS based URLs work with active DNS query from the client. Hence, for URL filtering, the DNS should be setup correctly.

---




---

**Note** URL filter takes precedence over punt or redirect ACL, and over custom or static pre-auth ACL.s

---

## FlexConnect in Embedded Wireless Controller

FlexConnect is a wireless solution for branch office and remote office deployments. It enables customers to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying an embedded wireless controller in each branch office.

The FlexConnect access points can switch client data traffic locally while carrying the authentication centrally. Also, FlexConnect APs perform client authentication locally when their connection to the controller is lost. When they are connected back to the controller, they can also send authentication/policy details back to the embedded wireless controller.

The embedded wireless controller network comprises of at least one 802.11ax Wave 2 Cisco Aironet Series access point (AP) with a software-based embedded wireless controller managing other APs in the network. The AP acting as the embedded wireless controller is referred to as the primary AP while the other APs in the network, which are managed by this primary AP, are referred to as subordinate APs. In addition to acting as an embedded wireless controller, the primary AP also operates as an AP to serve clients along with the subordinate APs.

Pre-Auth DNS ACL feature is also known as Walled Garden feature. The walled garden is a list of web sites or domains that you can visit without being authenticated. DNS snooping is performed on the AP for each client and configured rule is applied to client traffic after matching the Source or Destination IP.

## Roaming

During Roaming, the support clients roam from one AP to the other using the existing roaming support. DNS ACLs are retained at the target AP even after roaming. For Roaming with DNS Pre-Auth ACL and Post-Auth ACL, the target AP learns the client-resolved IP from the serving AP.

## Restrictions on DNS-Based Access Control Lists

The restriction for DNS-based ACLs is as follows:

- Only supported for FlexConnect local switching APs with Central Authorization.
- Post-Auth DNS based ACL is not supported for FlexConnect with local Authorization when AP is in FlexConnect local switching mode.
- Fully qualified domain name (FQDN) or DNS based ACLs are not supported on Cisco Wave 1 Access Points.
- The URL filter considers only the first 20 URLs, though you can add more.
- The URL filter employs regular regex patterns and permits wildcard characters only at the beginning or at the end of an URL.
- The URL ACLs are defined and added to the FlexConnect policy profile in which they associate with a WLAN. The URL ACL creation follows a similar mechanism as that of local mode URL ACLs.
- In FlexConnect mode, the URL domain ACL works only if they are connected to a FlexConnect policy profile.
- The ACL can be attached to a WLAN by associating a policy profile with a WLAN or local policies. However, you can override it using "url-redirect-acl".
- For the Cisco AV pair received from ISE, the policy that needs to be applied for a particular client is pushed as part of ADD MOBILE message.
- When an AP joins or when an existing URL ACL is modified and applied on FlexConnect profile, the ACL definition along with mapped URL filter list is pushed to the AP.
- The AP stores the URL ACL definition with mapped ACL name and snoops the DNS packets for learning the first IP address for each URL in the ACL. When the AP learns the IP addresses, it updates the controller of the URL and IP bindings. The controller records this information in the client database for future use.
- When a client roams to another AP during the pre-authentication state, the learned IP addresses are pushed to a new AP. Otherwise, these learned IP addresses are purged when a client moves to a post-authentication state or when the TTL for the learned IP address expires.

# Flex Mode

## Configuring the URL Filter List (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile flex <i>custom-flex-profile</i></b>  <b>Example:</b> Device(config)# <code>wireless profile flex custom-flex-profile</code>	Configures a wireless flex profile and enters wireless flex profile configuration mode.
<b>Step 3</b>	<b>acl-policy <i>acl-policy-name</i></b>  <b>Example:</b> Device(config-wireless-flex-profile)# <code>acl-policy acl-policy-name</code>	Configures the ACL policy description
<b>Step 4</b>	<b>urlfilter list <i>url-filterlist-name</i></b>  <b>Example:</b> Device(config-wireless-flex-profile-acl)# <code>urlfilter list url-filterlist-name</code>	Configures and applies the name of the URL filter list to the flex profile.  This is the Flex URL filter configuration command for ACL binding.

## Configuring the URL Filter List (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Security > URL Filters**. The **URL Filters** page is displayed.
  - Step 2** Click the **Add** button. The **Add URL Filters** window is displayed.
  - Step 3** From the **Type** drop-down list, choose either **PRE-AUTH** or **POST-AUTH**.
    - a) **POST-AUTH**: Specify the **Redirect Servers** for **IPv4** and **IPv6**.
  - Step 4** Use the slider to **Permit** or **Deny** the **Action**.
  - Step 5** Specify the URLs in the **URLs** field. Enter every URL on a new line.
  - Step 6** Click **Apply to Device**.
-



## Applying Custom Pre-Auth DNS ACL on WLAN

For pre-auth, this configuration should be on a web-auth WLAN.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wlan wlan-name wlan-id ssid-name</b> <b>Example:</b> Device(config)# <code>wlan wlan-name wlan-id ssid-name</code>	Enters the WLAN configuration sub-mode.  1. wlan-name — Enter the profile name. The range is from 1 to 32 alphanumeric characters.  2. wlan-id—Enter the WLANID. The range is from 1 to 512.  3. SSID-name—Enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID. If you have already configured WLAN, enter wlan wlan-name command.
<b>Step 3</b>	<b>ip access-group web access-list-name</b> <b>Example:</b> Device(config-wlan)# <code>ip access-group web preauth-acl-wlan</code>	Maps the ACL to the web auth WLAN. access-list-name is the IPv4 ACL name or ID.

## Applying Custom Post-Auth DNS ACL on Policy Profile

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>Wireless profile policy profile-name</b> <b>Example:</b> Device(config)# <code>wireless profile policy custom-policy-profile</code>	Creates policy profile for the WLAN.
<b>Step 3</b>	<b>{ ipv4   ipv6 } acl post-acl-name</b> <b>Example:</b> Device(config-wireless-policy)# <code>ipv4 acl post-acl</code>	Creates ACL configuration for wireless IPv4 or IPv6 configuration.

## Configuring ISE for Central Web Authentication (GUI)

Perform the following steps to configure ISE for Central Web Authentication.

### Procedure

- 
- Step 1** Login to the Cisco Identity Services Engine (ISE).
  - Step 2** Click **Policy** and then click **Policy Elements**.
  - Step 3** Click **Results**.
  - Step 4** Expand **Authorization** and click **Authorization Profiles**.
  - Step 5** Click **Add** to create a new authorization profile for URL filter.
  - Step 6** Enter a name for the profile in the **Name** field. For example, CentralWebauth.
  - Step 7** Choose **ACCESS\_ACCEPT** option from the **Access Type** drop-down list.
  - Step 8** Alternatively, in the **Common Tasks** section, check **Web Redirection**.
  - Step 9** Choose the **Centralized Web Auth** option from the drop-down list.
  - Step 10** Specify the ACL and choose the ACL value from the drop-down list.
  - Step 11** In the **Advanced Attributes Setting** section, choose **Cisco:cisco-av-pair** from the drop-down list.

**Note** Multiple ACL can be applied on the controller based on priority. In L2 Auth + webauth multi-auth scenario, if the ISE returns ACL during L2 Auth then ISE ACL takes precedence over the default webauth redirect ACL. This leads to traffic running in webauth pending state, if ISE ACL has permit rule. To avoid this scenario, you need to set the precedence for L2 Auth ISE returned ACL. The default webauth redirect ACL priority is 100. To avoid traffic issue, you need to configure the redirect ACL priority above 100 for ACL returned by ISE.

- Step 12** Enter the following one by one and click (+) icon after each of them:

- url-redirect-acl=<sample\_name>
- url-redirect=<sample\_redirect\_URL>

For example,

```
Cisco:cisco-av-pair = priv-lvl=15
Cisco:cisco-av-pair = url-redirect-acl=ACL-REDIRECT2
Cisco:cisco-av-pair = url-redirect=
https://9.10.8.247:port/portal/gateway?
sessionId=SessionIdValue&portal=0ce17ad0-6d90-11e5-978e-005056bf2f0a&daysToExpiry=value&action=cwa
```

- Step 13** Verify contents in the **Attributes Details** section and click **Save**.
- 

## Viewing DNS-Based Access Control Lists

To view the URL Lists, use the following command:

```
Device #show wireless urlacl-enhanced summary
URL-List
-----
```

```

urllist_ut
urllist_max1
urllist_max2
urllist_max3
urllist_max4
urllist_max5

```

To view the details of a particular URL List, use the following command:

```

Device#show wireless urlacl-enhanced details urllist_ut
List Name..... : urllist_ut
Configured List of URLs
URL              Preference Action Validity Invalidated URL
-----
url1.dns.com     1                PERMIT    VALID 0
url2.dns.com     2                DENY      VALID 0
url3.dns.com     3                PERMIT    VALID 0
url4.dns.com     4                DENY      VALID 0
url11.dns.com    6                DENY      VALID 0
url12.dns.com    7                PERMIT    VALID 0
url13.dns.com    8                DENY      VALID 0
www.example.com  14               PERMIT    VALID 0

```

To view the flex profile details, use the following command:

```

Device# sh wireless profile flex detailed custom-flex-profile
Flex Profile Name : custom-flex-profile
Description : custom flex profile
Local Auth :
  AP:
    Radius Enable      : ENABLED
    PEAP               : DISABLED
    LEAP               : DISABLED
    TLS                : DISABLED
    EAP fast profile   : Not Configured
    User List          : Not Configured
  RADIUS:
    RADIUS server group name : Not Configured
  Fallback Radio shut : DISABLED
  ARP caching         : ENABLED
  Efficient Image Upgrade : ENABLED
  OfficeExtend AP     : DISABLED
  Join min latency    : DISABLED
  Policy ACL :
    ACL Name          URL Filter List
    Name              Central Webauth
    -----
    post-acl          urllist_ut          DISABLED
    pre_v4             urllist_pre_cwa    DISABLED
    ACL-REDIRECTTTTTT2 urllist_ut          DISABLED
    VLAN Name - VLAN ID mapping : Not Configured

```

To view client details, use the following command:

```

Device#sh wireless client mac-address <Mac-address> detail

```

### Verifying the Access Point

To view the ACL configuration on the AP, use the following command:

```

Device# show ip access-lists
Extended IP access list pre_v4
  1 permit udp any range 0 65535 any eq 53
  2 permit tcp any range 0 65535 any eq 53
  3 permit udp any dhcp_server any range 0 65535

```

```

4 permit udp any range 0 65535 any eq 68
5 permit udp any dhcp_client any range 0 65535
6 deny ip any any

```

To view the URL List configuration, use the following command:

```

Device#show flexconnect url-acl
ACL-NAME      ACTION      URL-LIST
pre_v4
              allow      test.dns.com
              allow      url2.dns.com
              allow      url3.dns.com
              allow      url10.dns.com
              allow      url11.dns.com
              allow      www.cwapre.com
              allow      www.google.com
              allow      oldconfig.dns.com
              allow      *.cisco.com

```

To view pre-auth client configuration, use the following command:

```

Device# show client access-lists pre-auth all C0:C1:C0:70:58:2F
Pre-Auth URL ACLs for Client: C0:C1:C0:70:58:2F
IPv4 ACL: pre_v4
IPv6 ACL:
ACTION        URL-LIST
allow         url11.dns.com
deny          url12.dns.com
allow         url13.dns.com
deny          url14.dns.com
allow         www.example.com
deny          url111.dns.com
allow         url112.dns.com
deny          url113.dns.com

```

```

Resolved IPs for Client: C0:C1:C0:70:58:2F
HIT-COUNT     URL          ACTION      IP-LIST
post-acl
              rule 0:    allow true
No IPv6 ACL found

```

To view post-auth client configuration, use the following command:

```

Device# show client access-lists post-auth all C0:C1:C0:70:58:2F
Post-Auth URL ACLs for Client: C0:C1:C0:70:58:2F
IPv4 ACL: post-acl
IPv6 ACL:
ACTION        URL-LIST
allow         url11.dns.com
deny          url12.dns.com
allow         url13.dns.com
deny          url14.dns.com
allow         www.example.com
deny          url111.dns.com
allow         url112.dns.com
deny          url113.dns.com

```

```

Resolved IPs for Client: C0:C1:C0:70:58:2F
HIT-COUNT     URL          ACTION      IP-LIST
post-acl
              rule 0:    allow true
No IPv6 ACL found

```

To view the IPs learnt in pre-auth, use the following command:

```
Device#show client access-lists pre-auth all 60:14:B3:AA:C6:FB
Pre-Auth URL ACLs for Client: 60:14:B3:AA:C6:FB
IPv4 ACL: acl_1
IPv6 ACL:
ACTION          URL-LIST
allow           url1.dns.com
deny           url2.dns.com
```

```
Resolved IPs for Client: 60:14:B3:AA:C5:FB
HIT-COUNT      URL          ACTION      IP-LIST
10             url1.dns.com allow       9.10.8.1
```

To view the IPs learnt in post-auth, use the following command:

```
Device#show client access-lists post-auth all 60:14:B3:AA:C6:FB
Post-Auth URL ACLs for Client: 60:14:B3:AA:C5:FB
IPv4 ACL: post_acl
IPv6 ACL:
ACTION          URL-LIST
deny           url1.dns.com
allow          url2.dns.com
```

```
Resolved IPs for Client: 60:14:B3:AA:C5:FB
HIT-COUNT      URL          ACTION      IP-LIST
16             url2.dns.com allow       9.10.9.1
postauth_acl
                rule 0: allow true
```





## CHAPTER 39

# Allowed List of Specific URLs

- [Allowed List of Specific URLs, on page 323](#)
- [Adding URL to Allowed List, on page 323](#)
- [Verifying URLs on the Allowed List, on page 324](#)

## Allowed List of Specific URLs

This feature helps you to add specific URLs to allowed list on the embedded wireless controller or the AP so that those specific URLs are available for use, even when there is no connectivity to the internet. You can add URLs to allowed list for web authentication of captive portal and walled garden. Authentication is not required to access the allowed list of URLs. When you try to access sites that are not in allowed list, you are redirected to the Login page.

## Adding URL to Allowed List

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>urlfilter list &lt;urlfilter-name&gt;</b> <b>Example:</b> Device(config)# urlfilter list url-allowedlist-nbn	Configures the URL filter profile.
<b>Step 3</b>	<b>action [deny   permit]</b> <b>Example:</b> Device(config-urlfilter-params)# action permit	Configures the list as allowed list. The <b>permit</b> command configures the list as allowed list and the <b>deny</b> command configures the list as blocked list.

	Command or Action	Purpose
<b>Step 4</b>	<b>{ redirect-server-ipv4   redirect-server-ipv6 }</b> <b>Example:</b> Device(config-urlfilter-params)# redirect-server-ipv4 X.X.X.X	Configures the IP address of the redirect servers to which the user requests will be redirected in case of denied requests.
<b>Step 5</b>	<b>url url-to-be-allowed</b> <b>Example:</b> Device(config-urlfilter-params)# url www.cisco.com	Configures the URL to be allowed.



**Note** **redirect-server-ipv4** and **redirect-server-ipv6** is applicable only in the local mode, specifically in post-authentication. For any further tracking or displaying any warning messages, the denied user request is redirected to the configured server.

But the **redirect-server-ipv4** and **redirect-server-ipv6** configurations do not apply to pre-authentication scenario as you will be redirected to the controller for the redirect login URL for any denied access.

You can associate the allowed URL with the ACL policy in flex profile.

### Example

Associating the allowed URL with the ACL policy in flex profile:

```
Device(config)# wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# acl-policy user_v4_acl
Device(config-wireless-flex-profile-acl)# urlfilter list_url_allowedlist_nbn
Device(config-wireless-flex-profile-acl)# exit
Device(config-wireless-flex-profile)# description "default flex profile"

Device(config)# urlfilter enhanced-list urllist_pre_cwa
Device(config-urlfilter-enhanced-params)# url url1.dns.com preference 1 action permit
Device(config-urlfilter-enhanced-params)# url url2.dns.com preference 2 action deny
Device(config-urlfilter-enhanced-params)# url url3.dns.com preference 3 action permit

Device(config)# wlan wlan5 5 wlan5
Device(config-wlan)#ip access-group web user_v4_acl
Device(config-wlan)#no security wpa
Device(config-wlan)#no security wpa
Device(config-wlan)#no security wpa wpa2 ciphers aes
Device(config-wlan)#no security wpa akm dot1x
Device(config-wlan)#security web-auth
Device(config-wlan)#security web-auth authentication-list default
Device(config-wlan)#security web-auth parameter-map global
Device(config-wlan)#no shutdown
```

## Verifying URLs on the Allowed List

To verify the summary and the details of the URLs on the allowed list, use the following **show** commands:



```
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
url-whitelist	1	PRE-AUTH	PERMIT	1.1.1.1	

```
Device#
```

```
Device# show wireless urlfilter details url-whitelist
List Name..... : url-whitelist
Filter ID..... : : 1
Filter Type..... : PRE-AUTH
Action..... : PERMIT
Redirect server ipv4..... : 1.1.1.1
Redirect server ipv6..... :
Configured List of URLs
  URL..... : www.cisco.com
```





## CHAPTER 40

# Web-Based Authentication

This chapter describes how to configure web-based authentication on the device. It contains these sections:

- [Authentication Overview, on page 327](#)
- [How to Configure Local Web Authentication, on page 335](#)
- [Configuration Examples for Local Web Authentication, on page 340](#)
- [Authentication for Sleeping Clients, on page 345](#)

## Authentication Overview

Web authentication is a Layer 3 security solution designed for providing easy and secure guest access to hosts on WLAN with open authentication or appropriate layer 2 security methods. Web authentication allows users to get authenticated through a web browser on a wireless client, with minimal configuration on the client side. It allows users to associate with an open SSID without having to set up a user profile. The host receives an IP address and DNS information from the DHCP server, however cannot access any of the network resources until they authenticate successfully. When the host connects to the guest network, the WLC redirects the host to an authentication web page where the user needs to enter valid credentials. The credentials are authenticated by the WLC or an external authentication server and if authenticated successfully is given full access to the network. Hosts can also be given limited access to particular network resources before authentication for which the pre-authentication ACL functionality needs to be configured.

The following are the different types of web authentication methods:

- **Local Web Authentication (LWA):** Configured as Layer 3 security on the controller, the web authentication page and the pre-authentication ACL are locally configured on the controller. The controller intercepts http(s) traffic and redirects the client to the internal web page for authentication. The credentials entered by the client on the login page is authenticated by the controller locally or through a RADIUS or LDAP server.
- **External Web Authentication (EWA):** Configured as Layer 3 security on the controller, the controller intercepts http(s) traffic and redirects the client to the login page hosted on the external web server. The credentials entered by the client on the login page is authenticated by the controller locally or through a RADIUS or LDAP server. The pre-authentication ACL is configured statically on the controller.
- **Central Web Authentication (CWA):** Configured mostly as Layer 2 security on the controller, the redirection URL and the pre-authentication ACL reside on ISE and are pushed during layer 2 authentication to the controller. The controller redirects all web traffic from the client to the ISE login page. ISE validates the credentials entered by the client through HTTPS and authenticates the user.

Use the authentication feature, known as web authentication proxy, to authenticate end users on host systems that do not run the IEEE 802.1x supplicant.

When a client initiates an HTTP session, authentication intercepts ingress HTTP packets from the host and sends an HTML login page to the users. The users enter their credentials, which the authentication feature sends to the authentication, authorization, and accounting (AAA) server for authentication.

If authentication succeeds, authentication sends a Login-Successful HTML page to the host and applies the access policies returned by the AAA server.

If authentication fails, authentication forwards a Login-Fail HTML page to the user, prompting the user to retry the login. If the user exceeds the maximum number of attempts, authentication forwards a Login-Expired HTML page to the host, and the user is .




---

**Note** The traceback that you receive when webauth client tries to do authentication does not have any performance or behavioral impact. It happens rarely when the context for which FFM replied back to EPM for ACL application is already dequeued (possibly due to timer expiry) and the session becomes 'unauthorized'.

---




---

**Note** When command authorization is enabled as a part of AAA Authorization configuration through TACACS and the corresponding method list is not configured as a part of the HTTP configuration, WebUI pages will not load any data. However, some wireless feature pages may work as they are privilege based and not command based.

---

Based on where the web pages are hosted, the local web authentication can be categorized as follows:

- *Internal*—The internal default HTML pages (Login, Success, Fail, and Expire) in the embedded wireless controller are used during the local web authentication.
- *Customized*—The customized web pages (Login, Success, Fail, and Expire) are downloaded onto the embedded wireless controller and used during the local web authentication.
- *External*—The customized web pages are hosted on the external web server instead of using the in-built or custom web pages.

Based on the various web authentication pages, the types of web authentication are as follows:

- *Webauth*—This is a basic web authentication. Herein, the embedded wireless controller presents a policy page with the user name and password. You need to enter the correct credentials to access the network.
- *Consent or web-passthrough*—Herein, the controller presents a policy page with the Accept or Deny buttons. You need to click the Accept button to access the network.
- *Webconsent*—This is a combination of webauth and consent web authentication types. Herein, the embedded wireless controller presents a policy page with Accept or Deny buttons along with user name or password. You need to enter the correct credentials and click the Accept button to access the network.

**Note**

- You can view the webauth parameter-map information using the **show running-config** command output.
- The wireless Web-Authentication feature does not support the bypass type.
- Change in web authentication parameter map redirect login URL does not occur until a AP rejoin happens. You must enable and disable the WLAN to apply the new URL redirection.

**Note**

We recommend that you follow the Cisco guidelines to create a customized web authentication login page. If you have upgraded to the latest versions of Google Chrome or Mozilla Firefox browsers, ensure that your webauth bundle has the following line in the *login.html* file:

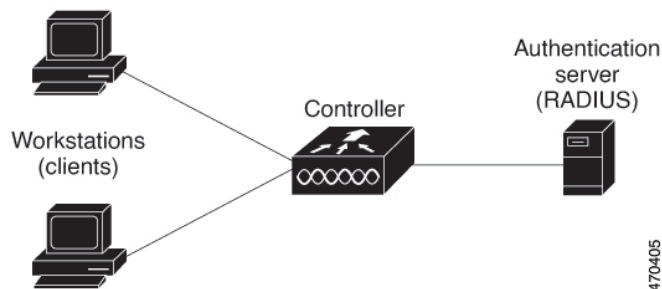
```
<body onload="loadAction();">
```

## Device Roles

With local web authentication, the devices in the network have these specific roles:

- *Client*—The device (workstation) that requests access to the network and the controller and responds to requests from the controller. The workstation must be running an HTML browser with Java Script enabled.
- *Authentication server*—Authenticates the client. The authentication server validates the identity of the client and notifies the controller that the client is authorized to access the network and the controller services or that the client is denied.
- *Controller*—Controls the physical access to the network based on the authentication status of the client. The controller acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client.

**Figure 6: Local Web Authentication Device Roles**



## Authentication Process

When the page is hosted on the controller, the controller uses its virtual IP (a non-routable IP like 192.0.2.1 typically) to serve the request. If the page is hosted externally, the web redirection sends the client first to the virtual IP, which then sends the user again to the external login page while it adds arguments to the URL,

such as the location of the virtual IP. Even when the page is hosted externally, the user submits its credentials to the virtual IP.

When you enable local web authentication, these events occur:

- The user initiates an HTTP session.
- The HTTP traffic is intercepted, and authorization is initiated. The controller sends the login page to the user. The user enters a username and password, and the controller sends the entries to the authentication server.
- If the authentication succeeds, the controller downloads and activates the user's access policy from the authentication server. The login success page is sent to the user.
- If the authentication fails, the controller sends the login fail page. The user retries the login. If the maximum number of attempts fails, the controller sends the login expired page, and the host is placed in a watch list. After the watch list times out, the user can retry the authentication process.
- If authentication server is not available, after the web authentication retries, the client moves to the excluded state and the client receives an Authentication Server is Unavailable page.
- The controller reauthenticates a client when the host does not respond to an ARP probe on a Layer 2 interface, or when the host does not send any traffic within the idle timeout on a Layer 3 interface.
- Web authentication sessions can not apply new VLAN as part of the authorization policy, as the client already has been assigned an IP address and you will not be able to change the IP address in the client, in case the VLAN changes.
- If the terminate action is default, the session is dismantled, and the applied policy is removed.

## Local Web Authentication Banner

With Web Authentication, you can create a default and customized web-browser banners that appears when you log in to the controller.

The banner appears on both the login page and the authentication-result pop-up pages. The default banner messages are as follows:

- *Authentication Successful*
- *Authentication Failed*
- *Authentication Expired*

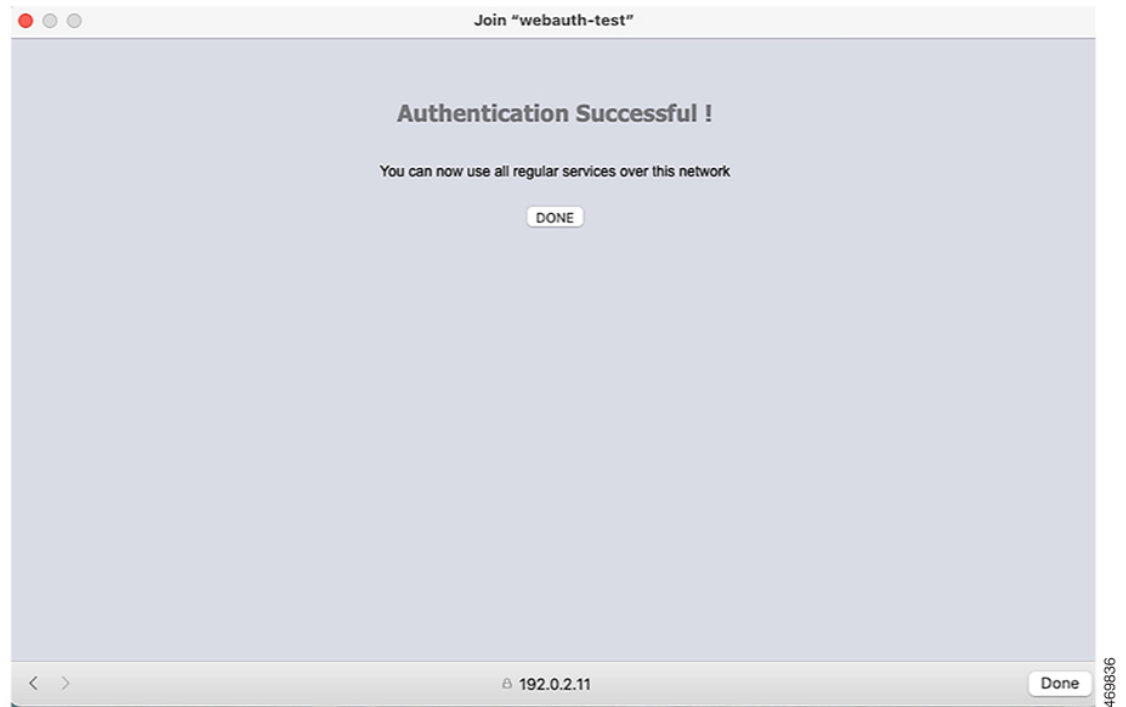
The Local Web Authentication Banner can be configured as follows:

- Use the following global configuration command:

```
Device(config)# parameter map type webauth global
Device(config-params-parameter-map)# banner ?
file <file-name>
text <Banner text>
title <Banner title>
```

The default banner *Cisco Systems* and *Switch host-name Authentication* appear on the Login Page. *Cisco Systems* appears on the authentication result pop-up page.

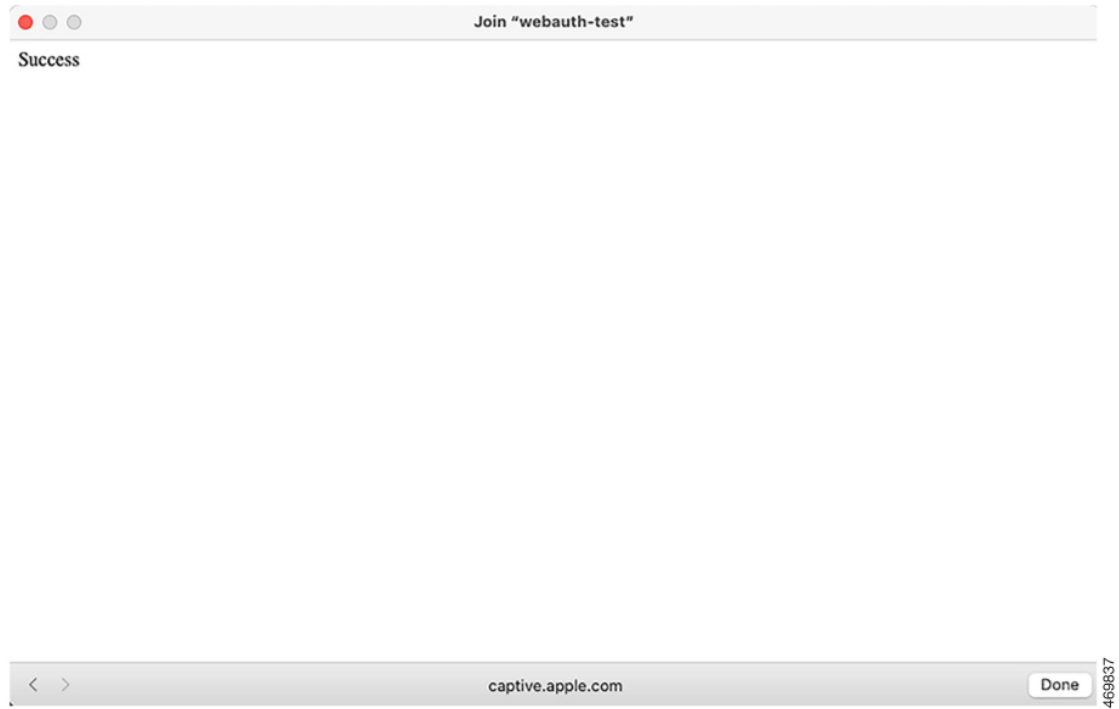
**Figure 7: Authentication Successful Banner**



The banner can be customized as follows:

- Add a message, such as switch, router, or company name to the banner:
  - New-style mode—Use the following global configuration command:  
**parameter-map type webauth global**  
**banner text <text>**
- Add a logo or text file to the banner:
  - New-style mode—Use the following global configuration command:  
**parameter-map type webauth global**  
**banner file <filepath>**

*Figure 8: Customized Web Banner*



If you do not enable a banner, only the username and password dialog boxes appear in the web authentication login screen, and no banner appears when you log into the switch.



Figure 9: Login Screen With No Banner

Join "webauth-test"

## Login

Welcome to the Cisco Web-Authentication network

Cisco is pleased to provide web-authentication infrastructure for your network. Please login.

User Name

Password

< > 192.0.2.11 Cancel 469838

## Customized Local Web Authentication

During the local web authentication process, the switch internal HTTP server hosts four HTML pages to deliver to an authenticating client. The server uses these pages to notify you of these four-authentication process states:

- Login—Your credentials are requested.
- Success—The login was successful.
- Fail—The login failed.
- Expire—The login session has expired because of excessive login failures.



---

**Note** Virtual IP address is mandatory to configure custom web authentication.

---

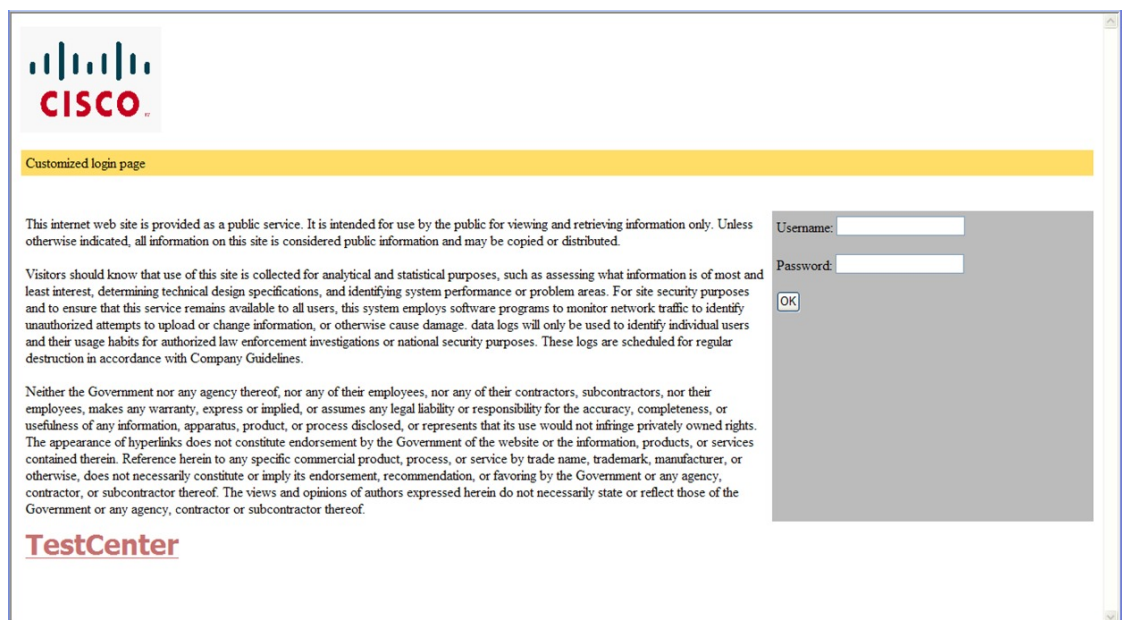
## Guidelines

- You can substitute your own HTML pages for the default internal HTML pages.
- You can use a logo or specify text in the *login*, *success*, *failure*, and *expire* web pages.
- On the banner page, you can specify text in the login page.
- The pages are in HTML.

- You must include an HTML redirect command in the success page to access a specific URL.
- The URL string must be a valid URL (for example, `http://www.cisco.com`). An incomplete URL might cause *page not found* or similar errors on a web browser.
- If you configure web pages for HTTP authentication, they must include the appropriate HTML commands (for example, to set the page time out, to set a hidden password, or to confirm that the same page is not submitted twice). The custom page samples in the webauth bundle are provided with the image and the details of what you can and cannot change.
- The CLI command to redirect users to a specific URL is not available when the configured login form is enabled. The administrator should ensure that the redirection is configured in the web page.
- If the CLI command redirecting users to specific URL after authentication occurs is entered and then the command configuring web pages is entered, the CLI command redirecting users to a specific URL does not take effect.
- Configured web pages can be copied to the switch boot flash or flash.
- The login page can be on one flash, and the success and failure pages can be another flash (for example, the flash on the active switch or a member switch).
- You must configure all four pages.
- All of the logo files (image, flash, audio, video, and so on) that are stored in the system directory (for example, flash, disk0, or disk) and that are displayed on the login page must use `web_auth_<filename>` as the file name.
- The configured authentication proxy feature supports both HTTP and SSL.

You can substitute your HTML pages for the default internal HTML pages. You can also specify a URL to which users are redirected after authentication occurs, which replaces the internal Success page.

**Figure 10: Customizable Authentication Page**



## Redirection URL for Successful Login Guidelines

When configuring a redirection URL for successful login, consider these guidelines:

- If the custom authentication proxy web pages feature is enabled, the redirection URL feature is disabled and is not available in the CLI. You can perform redirection in the custom-login success page.
- If the redirection URL feature is enabled, a configured auth-proxy-banner is not used
- To remove the specification of a redirection URL, use the **no** form of the command.
- If the redirection URL is required after the web-based authentication client is successfully authenticated, then the URL string must start with a valid URL (for example, http://) followed by the URL information. If only the URL is given without http://, then the redirection URL on successful authentication might cause page not found or similar errors on a web browser.

# How to Configure Local Web Authentication

## Configuring Default Local Web Authentication

The following table shows the default configurations required for local web authentication.

*Table 9: Default Local Web Authentication Configuration*

Feature	Default Setting
AAA	Disabled
RADIUS server <ul style="list-style-type: none"> <li>• IP address</li> <li>• UDP authentication port</li> <li>• Key</li> </ul>	<ul style="list-style-type: none"> <li>• None specified</li> </ul>
Default value of inactivity timeout	3600 seconds
Inactivity timeout	Disabled

## Configuring AAA Authentication (GUI)



**Note** The WebUI does not support the ipv6 radius source-interface under AAA radius server group configuration.

### Procedure

- 
- Step 1** Choose **Configuration > Security > AAA**.
- Step 2** In the **Authentication** section, click **Add**.
- Step 3** In the **Quick Setup: AAA Authentication** window that is displayed, enter a name for your method list.
- Step 4** Choose the type of authentication you want to perform before allowing access to the network, in the **Type** drop-down list.
- Step 5** Choose if you want to assign a group of servers as your access server, or if you want to use a local server to authenticate access, from the **Group Type** drop-down list.
- Step 6** To configure a local server to act as a fallback method when servers in the group are unavailable, check the **Fallback to local** check box.
- Step 7** Choose the server groups you want to use to authenticate access to your network, from the **Available Server Groups** list and click > icon to move them to the **Assigned Server Groups** list.
- Step 8** Click **Save & Apply to Device**.
- 

## Configuring AAA Authentication (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>aaa new-model</b> <b>Example:</b> <pre>Device(config)# aaa new-model</pre>	Enables AAA functionality.
<b>Step 2</b>	<b>aaa authentication login {default   named_authentication_list} group AAA_group_name</b> <b>Example:</b> <pre>Device(config)# aaa authentication login default group group1</pre>	Defines the list of authentication methods at login. <b>named_authentication_list</b> refers to any name that is not greater than 31 characters. <b>AAA_group_name</b> refers to the server group name. You need to define the server-group <b>server_name</b> at the beginning itself.
<b>Step 3</b>	<b>aaa authorization network {default   named} group AAA_group_name</b> <b>Example:</b> <pre>Device(config)# aaa authorization network default group group1</pre>	Creates an authorization method list for web-based authorization.
<b>Step 4</b>	<b>tacacs-server host {hostname   ip_address}</b> <b>Example:</b>	Specifies a AAA server.

	Command or Action	Purpose
	Device(config)# <code>tacacs-server host 10.1.1.1</code>	

## Configuring the HTTP/HTTPS Server (GUI)

### Procedure

- 
- Step 1** Choose **Administration > Management > HTTP/HTTPS/Netconf**.
  - Step 2** In the **HTTP/HTTPS Access Configuration** section, enable HTTP Access and enter the port that will listen for HTTP requests. The default port is 80. Valid values are 80, and ports between 1025 and 65535.
  - Step 3** Enable **HTTPS Access** on the device and enter the designated port to listen for HTTPS requests. The default port is 1025. Valid values are 443, and ports between 1025 and 65535. On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent over the Internet. HTTP with SSL encryption provides a secure connection to allow such functions as configuring a switch from a Web browser.
  - Step 4** Choose the **Personal Identity Verification** as enabled or disabled.
  - Step 5** In the **HTTP Trust Point Configuration** section, enable **Enable Trust Point** to use Certificate Authority servers as trustpoints.
  - Step 6** From the **Trust Points** drop-down list, choose a trust point.
  - Step 7** In the **Timeout Policy Configuration** section, enter the HTTP timeout policy in seconds. Valid values can range from 1 to 600 seconds.
  - Step 8** Enter the number of minutes of inactivity allowed before the session times out. Valid values can range from 180 to 1200 seconds.
  - Step 9** Enter the server life time in seconds. Valid values can range from 1 to 86400 seconds.
  - Step 10** Enter the maximum number of requests the device can accept. Valid values range from 1 to 86400 requests.
  - Step 11** Save the configuration.
- 

## Configuring the HTTP Server (CLI)

To use local web authentication, you must enable the HTTP server within the device. You can enable the server for either HTTP or HTTPS.




---

**Note** The Apple psuedo-browser will not open if you configure only the **ip http secure-server** command. You should also configure the **ip http server** command.

---

Follow the procedure given below to enable the server for either HTTP or HTTPS:

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>Device# configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ip http server</b> <b>Example:</b> Device(config)# <code>ip http server</code>	Enables the HTTP server. The local web authentication feature uses the HTTP server to communicate with the hosts for user authentication.
<b>Step 3</b>	<b>ip http secure-server</b> <b>Example:</b> Device(config)# <code>ip http secure-server</code>	Enables HTTPS.  You can configure custom authentication proxy web pages or specify a redirection URL for successful login.  <b>Note</b> To ensure secure authentication when you enter the <b>ip http secure-server</b> command, the login page is always in HTTPS (secure HTTP) even if the user sends an HTTP request.
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config)# <code>end</code>	Exits configuration mode.

## Creating a Parameter Map (GUI)

**Procedure**

- 
- Step 1** Choose **Configuration > Security > Web Auth**.
  - Step 2** Click **Add**.
  - Step 3** Click **Policy Map**.
  - Step 4** Enter **Parameter Name**, **Maximum HTTP connections**, **Init-State Timeout(secs)** and choose **webauth** in the **Type** drop-down list.
  - Step 5** Click **Apply to Device**.
- 

## Configuring the Maximum Web Authentication Request Retries

Follow these steps to configure the maximum web authentication request retries:

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>  Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>  Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<b>wireless security web-auth retries <i>number</i></b> <b>Example:</b>  Device(config)# <code>wireless security web-auth retries 2</code>	<i>number</i> is the maximum number of web auth request retries. The valid range is 0 to 20.
<b>Step 4</b>	<b>end</b> <b>Example:</b>  Device(config)# <code>end</code>	Returns to privileged EXEC mode.

## Configuring a Local Banner in Web Authentication Page (GUI)

**Procedure**

- 
- Step 1** Choose **Configuration > Security > Web Auth**.
- Step 2** In the **Webauth Parameter Map** tab, click the parameter map name. The **Edit WebAuth Parameter** window is displayed.
- Step 3** In the **General** tab and choose the required Banner Type:
- If you choose **Banner Text**, enter the required banner text to be displayed.
  - If you choose **File Name**, specify the path of the file from which the banner text has to be picked up.
- Step 4** Click **Update & Apply**.
- 

## Configuring a Local Banner in Web Authentication Page (CLI)

Follow the procedure given below to configure a local banner in web authentication pages.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>parameter-map type webauth <i>param-map</i></b> <b>Example:</b> Device(config)# parameter-map type webauth <i>param-map</i>	Configures the web authentication parameters. Enters the parameter map configuration mode.
<b>Step 3</b>	<b>banner [ <i>file</i>   <i>banner-text</i>   <i>title</i> ]</b> <b>Example:</b> Device(config-params-parameter-map)# banner http C My Switch C	Enables the local banner.  Create a custom banner by entering <i>C banner-text C</i> (where <i>C</i> is a delimiting character), or <i>file</i> that indicates a file (for example, a logo or text file) that appears in the banner, or <i>title</i> that indicates the title of the banner.
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config-params-parameter-map)# end	Returns to privileged EXEC mode.

## Configuration Examples for Local Web Authentication

### Example: Obtaining Web Authentication Certificate

This example shows how to obtain web authentication certificate.

```

Device# configure terminal
Device(config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapsrvr-cert.p12 cisco
Device(config)# end
Device# show crypto pki trustpoints cert
Trustpoint cert:
  Subject Name:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Serial Number (hex): 00
  Certificate configured.
Device# show crypto pki certificates cert
Certificate
  Status: Available
  Certificate Serial Number (hex): 04

```



```

Certificate Usage: General Purpose
Issuer:
  e=rkannajr@cisco.com
  cn=sthaliya-lnx
  ou=WNBU
  o=Cisco
  l=SanJose
  st=California
  c=US
Subject:
  Name: ldapserver
  e=rkannajr@cisco.com
  cn=ldapserver
  ou=WNBU
  o=Cisco
  st=California
  c=US
Validity Date:
  start date: 07:35:23 UTC Jan 31 2012
  end   date: 07:35:23 UTC Jan 28 2022
Associated Trustpoints: cert ldap12
Storage: nvram:rkannajrcisc#4.cer

```

```

CA Certificate
Status: Available
Certificate Serial Number (hex): 00
Certificate Usage: General Purpose
Issuer:
  e=rkannajr@cisco.com
  cn=sthaliya-lnx
  ou=WNBU
  o=Cisco
  l=SanJose
  st=California
  c=US
Subject:
  e=rkannajr@cisco.com
  cn=sthaliya-lnx
  ou=WNBU
  o=Cisco
  l=SanJose
  st=California
  c=US
Validity Date:
  start date: 07:27:56 UTC Jan 31 2012
  end   date: 07:27:56 UTC Jan 28 2022
Associated Trustpoints: cert ldap12 ldap
Storage: nvram:rkannajrcisc#0CA.cer

```

## Example: Displaying a Web Authentication Certificate

This example shows how to display a web authentication certificate.

```

Device# show crypto ca certificate verb
Certificate
Status: Available
Version: 3
Certificate Serial Number (hex): 2A9636AC00000000858B
Certificate Usage: General Purpose
Issuer:
cn=Cisco Manufacturing CA

```

```

o=Cisco Systems
Subject:
Name: WS-C3780-6DS-S-2037064C0E80
Serial Number: PID:WS-C3780-6DS-S SN:FOC1534X12Q
cn=WS-C3780-6DS-S-2037064C0E80
serialNumber=PID:WS-C3780-6DS-S SN:FOC1534X12Q
CRL Distribution Points:
http://www.cisco.com/security/pki/crl/cmca.crl
Validity Date:
start date: 15:43:22 UTC Aug 21 2011
end date: 15:53:22 UTC Aug 21 2021
Subject Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Signature Algorithm: SHA1 with RSA Encryption
Fingerprint MD5: A310B856 A41565F1 1D9410B5 7284CB21
Fingerprint SHA1: 04F180F6 CA1A67AF 9D7F561A 2BB397A1 0F5EB3C9
X509v3 extensions:
X509v3 Key Usage: F0000000
    Digital Signature
    Non Repudiation
    Key Encipherment
    Data Encipherment
X509v3 Subject Key ID: B9EEB123 5A3764B4 5E9C54A7 46E6EECA 02D283F7
X509v3 Authority Key ID: D0C52226 AB4F4660 ECAE0591 C7DC5AD1 B047F76C
Authority Info Access:
Associated Trustpoints: CISCO_IDEVID_SUDI
Key Label: CISCO_IDEVID_SUDI

```

## Example: Choosing the Default Web Authentication Login Page

This example shows how to choose a default web authentication login page.

```

Device# configure terminal
Device(config)# parameter-map type webauth test
This operation will permanently convert all relevant authentication commands to their CPL
control-policy equivalents. As this conversion is irreversible and will
disable the conversion CLI 'authentication display [legacy|new-style]', you are strongly
advised to back up your current configuration before proceeding.
Do you wish to continue? [yes]: yes
Device(config)# wlan wlan50
Device(config-wlan)# shutdown
Device(config-wlan)# security web-auth authentication-list test
Device(config-wlan)# security web-auth parameter-map test
Device(config-wlan)# no shutdown
Device(config-wlan)# end
Device# show running-config | section wlan50
wlan wlan50 50 wlan50
security wpa akm cckm
security wpa wpa1
security wpa wpa1 ciphers aes
security wpa wpa1 ciphers tkip
security web-auth authentication-list test
security web-auth parameter-map test
session-timeout 1800
no shutdown

Device# show running-config | section parameter-map type webauth test
parameter-map type webauth test
type webauth

```

## Example: Choosing a Customized Web Authentication Login Page from an IPv4 External Web Server

This example shows how to choose a customized web authentication login page from an IPv4 external web server.

```
Device# configure terminal
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# virtual-ip ipv4 1.1.1.1
Device(config-params-parameter-map)# parameter-map type webauth test
Device(config-params-parameter-map)# type webauth
Device(config-params-parameter-map)# redirect for-login http://9.1.0.100/login.html
Device(config-params-parameter-map)# redirect portal ipv4 9.1.0.100
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv4 1.1.1.1
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 9.1.0.100
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test
```

## Example: Choosing a Customized Web Authentication Login Page from an IPv6 External Web Server

This example shows how to choose a customized web authentication login page from an IPv6 external web server.

```
Device# configure terminal
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# virtual-ip ipv6 1:1:1::1
Device(config-params-parameter-map)# parameter-map type webauth test
Device(config-params-parameter-map)# type webauth
Device(config-params-parameter-map)# redirect for-login http://9:1:1::100/login.html
Device(config-params-parameter-map)# redirect portal ipv6 9:1:1::100
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv6 1:1:1::1
parameter-map type webauth test
type webauth
redirect for-login http://9:1:1::100/login.html
redirect portal ipv6 9:1:1::100
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test
```

## Example: Assigning Login, Login Failure, and Logout Pages per WLAN

This example shows how to assign login, login failure and logout pages per WLAN.

```

Device# configure terminal
Device(config)# parameter-map type webauth test
Device(config-params-parameter-map)# custom-page login device flash:loginsantosh.html
Device(config-params-parameter-map)# custom-page login expired device flash:loginexpire.html
Device(config-params-parameter-map)# custom-page failure device flash:loginfail.html
Device(config-params-parameter-map)# custom-page success device flash:loginsucess.html
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map type webauth test
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 9.1.0.100
custom-page login device flash:loginsantosh.html
custom-page success device flash:loginsucess.html
custom-page failure device flash:loginfail.html
custom-page login expired device flash:loginexpire.html

```

## Example: Configuring Preauthentication ACL

This example shows how to configure preauthentication ACL.

```

Device# configure terminal
Device(config)# wlan fff
Device(config-wlan)# shutdown
Device(config-wlan)# ip access-group web preauthrule
Device(config-wlan)# no shutdown
Device(config-wlan)# end
Device# show wlan name fff

```

## Example: Configuring Webpassthrough

This example shows how to configure webpassthrough.

```

Device# configure terminal
Device(config)# parameter-map type webauth webparalocal
Device(config-params-parameter-map)# type consent
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map type webauth test
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 9.1.0.100

```

## Verifying Web Authentication Type

To verify the web authentication type, run the following command:

```

Device# show parameter-map type webauth all
Type Name
-----
Global global
Named webauth
Named ext
Named redirect
Named abc

```

```
Named glbal
Named ewa-2

Device# show parameter-map type webauth global
Parameter Map Name : global
Banner:
Text : CisCo
Type : webauth
Auth-proxy Init State time : 120 sec
Webauth max-http connection : 100
Webauth logout-window : Enabled
Webauth success-window : Enabled
Consent Email : Disabled
Sleeping-Client : Enabled
Sleeping-Client timeout : 60 min
Virtual-ipv4 : 1.1.1.1
Virtual-ipv4 hostname :
Webauth intercept https : Disabled
Webauth Captive Bypass : Disabled
Webauth bypass intercept ACL :
Trustpoint name :
HTTP Port : 80
Watch-list:
Enabled : no
Webauth login-auth-bypass:

Device# show parameter-map type webauth name global
Parameter Map Name : global
Type : webauth
Auth-proxy Init State time : 120 sec
Webauth max-http connection : 100
Webauth logout-window : Enabled
Webauth success-window : Enabled
Consent Email : Disabled
Sleeping-Client : Disabled
Webauth login-auth-bypass:
```

# Authentication for Sleeping Clients

## Information About Authenticating Sleeping Clients

Clients with guest access that have had successful web authentication are allowed to sleep and wake up without having to go through another authentication process through the login page. You can configure the duration for which sleeping clients should be remembered for before reauthentication becomes necessary. The valid range is 10 minutes to 43200 minutes, with the default being 720 minutes. You can also configure this duration on WebAuth parameter map that is mapped to a WLAN. Note that the sleeping client timer comes into effect due to instances such as idle timeout, session timeout, disabling of the WLAN, and the AP being nonoperational.

This feature is supported in the following FlexConnect scenario: local switching and central authentication.

**Caution**

If the MAC address of a client that goes to sleep mode is spoofed, the fake device such as a laptop can be authenticated.

### Mobility Scenarios

Following are some guidelines in a mobility scenario:

- L2 roaming in the same subnet is supported.
- Anchor sleeping timer is applicable.
- The sleeping client information is shared between multiple autoanchors when a sleeping client moves from one anchor to another.

A sleeping client does not require reauthentication in the following scenarios:

- Suppose there are two embedded wireless controllers in a mobility group. A client that is associated with one embedded wireless controller goes to sleep and then wakes up and gets associated with the other embedded wireless controller.
- Suppose there are three embedded wireless controllers in a mobility group. A client that is associated with the second embedded wireless controller that is anchored to the first controller goes to sleep, wakes up, and gets associated with the third embedded wireless controller.
- A client sleeps, wakes up and gets associated with the same or different export foreign embedded wireless controller that is anchored to the export anchor.

## Restrictions on Authenticating Sleeping Clients

- The sleep client feature works only for WLAN configured with WebAuth security.
- You can configure the sleeping clients only on a per WebAuth parameter-map basis.
- The authentication of sleeping clients feature is supported only on WLANs that have Layer 3 security enabled.
- With Layer 3 security, the Authentication, Passthrough, and On MAC Filter failure web policies are supported. The Conditional Web Redirect and Splash Page Web Redirect web policies are not supported.
- The central web authentication of sleeping clients is not supported.
- The authentication of sleeping clients feature is not supported on guest LANs and remote LANs.
- A guest access sleeping client that has a local user policy is not supported. In this case, the WLAN-specific timer is applied.

## Configuring Authentication for Sleeping Clients (GUI)

### Procedure

---

- Step 1** Choose **Configuration > Security > Web Auth**.
- Step 2** In the **Webauth Parameter Map** tab, click the parameter map name. The **Edit WebAuth Parameter** window is displayed.
- Step 3** Select **Sleeping Client Status** check box.

**Step 4** Click Update & Apply to Device.

## Configuring Authentication for Sleeping Clients (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p>[no] <b>parameter-map type webauth</b> {<i>parameter-map-name</i>   <b>global</b>}</p> <p><b>Example:</b></p> <pre>Device(config)# parameter-map type webauth global</pre>	Creates a parameter map and enters parameter-map webauth configuration mode.
<b>Step 2</b>	<p><b>sleeping-client</b> [<b>timeout</b> <i>time</i>]</p> <p><b>Example:</b></p> <pre>Device(config-params-parameter-map)# sleeping-client timeout 100</pre>	<p>Configures the sleeping client timeout to 100 minutes. Valid range is between 10 minutes and 43200 minutes.</p> <p><b>Note</b> If you do not use the timeout keyword, the sleeping client is configured with the default timeout value of 720 minutes.</p>
<b>Step 3</b>	<b>end</b>	Exits parameter-map webauth configuration mode and returns to privileged EXEC mode.
<b>Step 4</b>	<p>(Optional) <b>show wireless client sleeping-client</b></p> <p><b>Example:</b></p> <pre>Device# show wireless client sleeping-client</pre>	Shows the MAC address of the clients and the time remaining in their respective sessions.
<b>Step 5</b>	<p>(Optional) <b>clear wireless client sleeping-client</b> [<b>mac-address</b> <i>mac-addr</i>]</p> <p><b>Example:</b></p> <pre>Device# clear wireless client sleeping-client mac-address 00e1.e1e1.0001</pre>	<ul style="list-style-type: none"> <li>• <b>clear wireless client sleeping-client</b>—Deletes all sleeping client entries from the sleeping client cache.</li> <li>• <b>clear wireless client sleeping-client mac-address</b> <i>mac-addr</i>—Deletes the specific MAC entry from the sleeping client cache.</li> </ul>







# CHAPTER 41

## Central Web Authentication

- [Information About Central Web Authentication, on page 349](#)
- [How to Configure ISE, on page 350](#)
- [How to Configure Central Web Authentication on the Controller, on page 352](#)
- [Authentication for Sleeping Clients, on page 359](#)

### Information About Central Web Authentication

Central web authentication offers the possibility to have a central device that acts as a web portal (in this example, the ISE). The major difference compared to the usual local web authentication is that it is shifted to Layer 2 along with MAC filtering or dot1x authentication. The concept also differs in that the radius server (ISE in this example) returns special attributes that indicate to the switch that a web redirection must occur. This solution eliminates any delay to start the web authentication.

The following are the different types of web authentication methods:

- **Local Web Authentication (LWA):** Configured as Layer 3 security on the controller, the web authentication page and the pre-authentication ACL are locally configured on the controller. The controller intercepts http(s) traffic and redirects the client to the internal web page for authentication. The credentials entered by the client on the login page is authenticated by the controller locally or through a RADIUS or LDAP server.
- **External Web Authentication (EWA):** Configured as Layer 3 security on the controller, the controller intercepts http(s) traffic and redirects the client to the login page hosted on the external web server. The credentials entered by the client on the login page is authenticated by the controller locally or through a RADIUS or LDAP server. The pre-authentication ACL is configured statically on the controller.
- **Central Web Authentication (CWA):** Configured mostly as Layer 2 security on the controller, the redirection URL and the pre-authentication ACL reside on ISE and are pushed during layer 2 authentication to the controller. The controller redirects all web traffic from the client to the ISE login page. ISE validates the credentials entered by the client through HTTPS and authenticates the user.

Globally, if the MAC address of the client station is not known by the radius server (but other criteria can also be used), the server returns the redirection attributes, and the embedded wireless controller authorizes the station (using the MAC filtering) but places an access list to redirect the web traffic to the portal.

Once the user logs into the guest portal, it is possible to re-authenticate the client so that a new Layer 2 MAC filtering occurs using the Change of Authorization (CoA). This way, the ISE remembers that it was a webauth

user and pushes the necessary authorization attributes to the embedded wireless controller for accessing the network.

## Prerequisites for Central Web Authentication

- Cisco Identity Services Engine (ISE)

## How to Configure ISE

To configure ISE, proceed as follows:

1. Create an authorization profile.
2. Create an authentication rule.
3. Create an authorization rule.

## Creating an Authorization Profile

### Procedure

---

- Step 1** Click **Policy**, and click **Policy Elements**.
- Step 2** Click **Results**.
- Step 3** Expand **Authorization**, and click **Authorization Profiles**.
- Step 4** Click **Add** to create a new authorization profile for central webauth.
- Step 5** In the **Name** field, enter a name for the profile. For example, CentralWebauth.
- Step 6** Choose **ACCESS\_ACCEPT** from the Access Type drop-down list.
- Step 7** Check the **Web Redirection (CWA, MDM, NSP, CPP)** check box, and choose **Centralized Web Auth** from the drop-down list.
- Step 8** In the **ACL** field, enter the name of the ACL that defines the traffic to be redirected. For example, redirect.
- Step 9** In the **Value** field, choose the default or customized values.  
The Value attribute defines whether the ISE sees the default or a custom web portal that the ISE admin created.
- Step 10** Click **Save**.
- 

## Creating an Authentication Rule

Follow the procedure given below to use the authentication profile and create the authentication rule:

### Procedure

---

- Step 1** In the **Policy > Authentication** page, click **Authentication**.
  - Step 2** Enter a name for your authentication rule. For example, MAB.
  - Step 3** In the If condition field, select the plus (+) icon.
  - Step 4** Choose **Compound condition**, and choose **Wireless\_MAB**.
  - Step 5** Click the arrow located next to **and ...** in order to expand the rule further.
  - Step 6** Click the + icon in the Identity Source field, and choose **Internal endpoints**.
  - Step 7** Choose **Continue** from the 'If user not found' drop-down list.  
This option allows a device to be authenticated even if its MAC address is not known.
  - Step 8** Click **Save**.
- 

## Creating an Authorization Rule

You can configure many rules in the authorization policy. The *MAC not known* rule is configured in this section:

### Procedure

---

- Step 1** Click **Policy > Authorization**.
- Step 2** In the Rule Name field, enter a name. For example: *Mac not known*.
- Step 3** In the Conditions field, click the plus (+) icon.
- Step 4** Choose **Compound Conditions**, and choose **Wireless\_MAB**.
- Step 5** From the settings icon, select **Add Attribute/Value** from the options.
- Step 6** In the Description field, choose **Network Access > AuthenticationStatus** as the attribute from the drop-down list.
- Step 7** Choose the **Equals** operator.
- Step 8** From the right-hand field, choose **UnknownUser**.
- Step 9** In the Permissions field, choose the authorization profile name that you had created earlier.  
The ISE continues even though the user (or MAC) is not known.  
Unknown users are now presented with the Login page. However, once they enter their credentials, they are presented again with an authentication request on the ISE; therefore, another rule must be configured with a condition that is met if the user is a guest user. For example, if `UseridentityGroup Equals Guest` is used then it is assumed that all guests belong to this group.
- Step 10** In the Conditions field, click the plus (+) icon.
- Step 11** Choose **Compound Conditions**, and choose to create a new condition.  
The new rule must come before the *MAC not known* rule.
- Step 12** From the settings icon, select **Add Attribute/Value** from the options.

**Step 13** In the Description field, choose **Network Access > UseCase** as the attribute from the drop-down list.

**Step 14** Choose the **Equals** operator.

**Step 15** From the right-hand field, choose **GuestFlow**.

**Step 16** In the Permissions field, click the plus (+) icon to select a result for your rule.

You can choose **Standard > PermitAccess** option or create a custom profile to return the attributes that you like.

When the user is authorized on the login page, the ISE triggers a COA that results in the restart of Layer 2 authentication. When the user is identified as a guest user, the user is authorized.

## How to Configure Central Web Authentication on the Controller

To configure central web authentication on the controller, proceed as follows:

1. Configure WLAN.
2. Configure policy profile.
3. Configure redirect ACL.
4. Configure AAA for central web authentication.
5. Configure redirect ACL in Flex profile.

### Configuring WLAN (GUI)

#### Before you begin

You need to enable MAC filtering for Layer 2 authentication to download the redirect URL and ACL.

#### Procedure

**Step 1** Choose **Configuration > Tags & Profiles > WLANs**.

**Step 2** In the **WLANs** window, click the name of the **WLAN** or click **Add** to create a new one.

**Step 3** In the **Add/Edit WLAN** window that is displayed, click the **General** tab to configure the following parameters.

- In the **Profile Name** field, enter or edit the name of the profile.
- In the **SSID** field, enter or edit the SSID name.  
The SSID name can be alphanumeric, and up to 32 characters in length.
- In the **WLAN ID** field, enter or edit the ID number. The valid range is between 1 and 512.
- From the **Radio Policy** drop-down list, choose the **802.11** radio band.
- Using the **Broadcast SSID** toggle button, change the status to either **Enabled** or **Disabled**.
- Using the **Status** toggle button, change the status to either **Enabled** or **Disabled**.

- Step 4** Click the **Security** tab, and then **Layer 2** tab to configure the following parameters:
- From the **Layer 2 Security Mode** drop-down list, choose **None**. This setting disables Layer 2 security.
  - Enter the **Reassociation Timeout** value, in seconds. This is the time after which a fast transition reassociation times out.
  - Check the **Over the DS** check box to enable Fast Transition over a distributed system.
  - Choose OWE, Opportunistic Wireless Encryption (OWE) provides data confidentiality with encryption over the air between an AP radio and a wireless client. OWE Transition Mode is meant to provide a sort of backwards compatibility.
  - Choose Fast Transition, 802.11r which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with a new AP is done even before the corresponding client roams to the target access point. This concept is called Fast Transition.
  - Check the check box to enable MAC filtering in the WLAN.
- Step 5** Click **Save & Apply to Device**.

## Configuring WLAN (CLI)



**Note** You need to enable MAC filtering for Layer 2 authentication to download the redirect URL and ACL. After completing the WLAN configuration, if the changes are not pushed to all the APs, the following syslog message appears:

```
2021/01/06 16:20:00.597927186 {wncd_x_R0-4}{1}: [wlanmgr-db] [20583]: UUID: 0, ra: 0, TID: 0
(note): Unable to push WLAN config changes to all APs, cleanup required for WlanId: 2, profile: wlan1
state: Delete pending
```

If the above mentioned syslog message appears for more than six minutes, reload the controller.

If the controller does not reload and still the syslog message appears, then collect the archive logs, wncd core file, and raise a case by clicking the following link: [Support Case Manager](#).

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>wlan wlan-name wlan-id SSID-name</b>  <b>Example:</b> <pre>Device(config)# wlan wlanProfileName 1 ngwcSSID</pre>	Enters the WLAN configuration sub-mode.  <b>wlan-name</b> is the name of the configured WLAN.  <b>wlan-id</b> is the wireless LAN identifier. The range is 1 to 512.  <b>SSID-name</b> is the SSID name which can contain 32 alphanumeric characters.

	Command or Action	Purpose
		<b>Note</b> If you have already configured this command, enter <b>wlan wlan-name</b> command.
<b>Step 2</b>	<b>mac-filtering</b> [name]  <b>Example:</b> Device(config-wlan)# mac-filtering name	Enables MAC filtering on a WLAN.  <b>Note</b> While configuring mac-filtering the default authentication list is considered, if the authentication list is not configured earlier.
<b>Step 3</b>	<b>no security wpa</b>  <b>Example:</b> Device(config-wlan)# no security wpa	Disable WPA security.
<b>Step 4</b>	<b>no shutdown</b>  <b>Example:</b> Device(config-wlan)# no shutdown	Enables the WLAN.
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Device(config-wlan)# end	Returns to privileged EXEC mode.

**Example**

```
Device# config terminal
Device(config)# wlan wlanProfileName 1 ngwcSSID
Device(config-wlan)# mac-filtering default
Device(config-wlan)# no security wpa
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

## Configuring Policy Profile (CLI)



**Note** You need a AAA override to apply policies coming from the AAA or ISE servers. When a redirect URL and redirect ACL is received from the ISE server, NAC is used to trigger the Central Web Authentication (CWA).

Both NAC and AAA override must be available in the policy profile to which the client is being associated.

The default policy profile is associated to an AP, if the AP is not associated to any other policy profiles.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>wireless profile policy default-policy-profile</b> <b>Example:</b> Device(config)# wireless profile policy default-policy-profile	Sets the policy profile.
<b>Step 2</b>	<b>vlan vlan-id</b> <b>Example:</b> Device(config-wireless-policy)# vlan 41	Maps the VLAN to a policy profile. If vlan-id is not specified, the default native vlan 1 is applied. The valid range for vlan-id is 1 to 4096. Management VLAN is applied if no VLAN is configured on the policy profile.
<b>Step 3</b>	<b>aaa-override</b> <b>Example:</b> Device(config-wireless-policy)# aaa-override	Configures AAA override to apply policies coming from the AAA or ISE servers.
<b>Step 4</b>	<b>nac</b> <b>Example:</b> Device(config-wireless-policy)# nac	Configures Network Access Control in the policy profile. NAC is used to trigger the Central Web Authentication (CWA).
<b>Step 5</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wireless-policy)# no shutdown	Enables the WLAN.
<b>Step 6</b>	<b>end</b> <b>Example:</b> Device(config-wireless-policy)# end	Returns to privileged EXEC mode.

**Example**

```

Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# vlan 41
Device(config-wireless-policy)# aaa-override
Device(config-wireless-policy)# nac
Device(config-wireless-policy)# no shutdown
Device(config-wireless-policy)# end

```

## Configuring a Policy Profile (GUI)

### Procedure

- 
- Step 1** Choose **Configuration** > **Tags & Profiles** > **Policy**.
- Step 2** On the **Policy Profile** page, click **Add**.
- Step 3** In the **Add Policy Profile** window, in General Tab, enter a name and description for the policy profile.
- Step 4** To enable the policy profile, set **Status** as Enabled.
- Step 5** Use the slider to enable or disable **Passive Client** and **Encrypted Traffic Analytics**.
- Step 6** (Optional) In the **CTS Policy** section, choose the appropriate status for the following:
- Inline Tagging—a transport mechanism using which an embedded wireless controller or access point understands the source SGT.
  - SGACL Enforcement
- Step 7** Specify a default **SGT**. The valid range is from 2 to 65519.
- Step 8** In the WLAN Switching Policy section, choose the following, as required:
- Central Switching
  - Central Authentication
  - Central DHCP
  - Central Association Enable
  - Flex NAT/PAT
- Step 9** Click **Save & Apply to Device**.
- 

## Creating Redirect ACL

The redirect ACL is a punt ACL that needs to be predefined on the controller (or the AP in case of FlexConnect local switching): the AAA server returns the name of the ACL and not its definition. The redirect ACL defines traffic (matching “deny” statements, as it denies redirection for it) that will be allowed through on the data plane and traffic (matching “permit” statements) that will be sent to the control plane towards the CPU for further processing (that is, the web interception and redirection in this case). The ACL has implicit (that is, the invisible) statements allowing DHCP and DNS traffic towards all IPs, just like it is the case with LWA. It also ends with a statement that a security ACL implicit deny.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>ip access-list extended redirect</b> <b>Example:</b>	The HTTP and HTTPS browsing does not work without authentication (per the other ACL) as



	Command or Action	Purpose
	Device(config)# ip access-list extended redirect	ISE is configured to use a redirect ACL (named <b>redirect</b> ).
<b>Step 2</b>	<b>deny ip any host ISE-IP-add</b> <b>Example:</b> Device(config)# deny ip any host 123.123.134.112	Allows traffic to ISE and all other traffic is blocked.
<b>Step 3</b>	<b>deny ip host ISE-IP-add any</b> <b>Example:</b> Device(config)# deny ip host 123.123.134.112 any	Allows traffic to ISE and all other traffic is blocked. <b>Note</b> This ACL is applicable for both local and flex mode.
<b>Step 4</b>	<b>permit TCP any any eq web address/port-number</b> <b>Example:</b> In case of HTTP: Device(config)# permit TCP any any eq www Device(config)# permit TCP any any eq 80 <b>Example:</b> In case of HTTPS: Device(config)# permit TCP any any eq 443	Redirects all HTTP or HTTPS access to the ISE login page. port-number 80 is used for HTTP and port-number 443 is used for HTTPS. For the ACE to allow traffic to ISE, ISE should be configured above the HTTP/HTTPS ACE.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config)# end	Returns to privileged EXEC mode.

## Configuring AAA for Central Web Authentication

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>aaa server radius dynamic-author</b> <b>Example:</b> Device(config)# aaa server radius dynamic-author	Configures the Change of Authorization (CoA) on the embedded wireless controller.
<b>Step 2</b>	<b>client ISE-IP-add server-key radius-shared-secret</b> <b>Example:</b>	Specifies a RADIUS client and the RADIUS key to be shared between a device and a RADIUS client.

	Command or Action	Purpose
	<pre>Device(config-locsvr-da-radius)# client 123.123.134.112 server-key 0 SECRET</pre>	<p><b>ISE-IP-add</b> is the IP address of the RADIUS client.</p> <p><b>server-key</b> is the radius client server-key.</p> <p><b>radius-shared-secret</b> covers the following:</p> <ul style="list-style-type: none"> <li>• <b>0</b>—Specifies unencrypted key.</li> <li>• <b>6</b>—Specifies encrypted key.</li> <li>• <b>7</b>—Specifies HIDDEN key.</li> <li>• <b>Word</b>—Unencrypted (cleartext) server key.</li> </ul> <p>The RADIUS shared secret should not exceed 240 characters while configuring WSMA data in GUI.</p> <p><b>Note</b> All these steps work only if the AAA configuration is in place. See the <i>Configuring AAA Authentication</i> for details.</p>

### Example

```
Device# config terminal
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 123.123.134.112 server-key 0 SECRET
Device(config-locsvr-da-radius)# end
```

## Configuring Redirect ACL in Flex Profile (GUI)

The redirect ACL definition must be sent to the access point in the FlexConnect profile. For this, the redirect ACL associated with an AP must be configured in the FlexConnect profile where the client is hosted. If an access point is not configured with any of the FlexConnect profiles, the default FlexConnect profile is associated with it.

### Procedure

- Step 1** Choose **Configuration > Tags & Profiles > Flex**.
- Step 2** On the **Flex Profile** page, click the name of the FlexConnect profile or click **Add** to create a new FlexConnect profile.
- Step 3** In the **Add/Edit Flex Profile** window that is displayed, click the **Policy ACL** tab.
- Step 4** Click **Add** to map an ACL to the FlexConnect profile.
- Step 5** Choose the ACL name, enable central web authentication, and specify the preauthentication URL filter.
- Step 6** Click **Save**.

**Step 7** Click **Update & Apply to Device**.

## Configuring Redirect ACL in Flex Profile (CLI)

The redirect ACL definition must be sent to the access point in the Flex profile. For this, the redirect ACL associated to an AP must be configured in the Flex profile where the client is being hosted. If an access point is not configured with any of the Flex profiles, the default Flex profile is associated with it.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>wireless profile flex default-flex-profile</b> <b>Example:</b> Device(config)# wireless profile flex default-flex-profile	Creates a new flex policy. The default flex profile name is <b>default-flex-profile</b> .
<b>Step 2</b>	<b>acl-policy <i>acl policy name</i></b> <b>Example:</b> Device(config-wireless-flex-profile)# acl-policy acl1	Configures ACL policy.
<b>Step 3</b>	<b>central-webauth</b> <b>Example:</b> Device(config-wireless-flex-profile-acl)# central-webauth	Configures central web authentication.
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config-wireless-flex-profile-acl)# end	Returns to privileged EXEC mode.

## Authentication for Sleeping Clients

### Information About Authenticating Sleeping Clients

Clients with guest access that have had successful web authentication are allowed to sleep and wake up without having to go through another authentication process through the login page. You can configure the duration for which sleeping clients should be remembered for before reauthentication becomes necessary. The valid range is 10 minutes to 43200 minutes, with the default being 720 minutes. You can also configure this duration on WebAuth parameter map that is mapped to a WLAN. Note that the sleeping client timer comes into effect due to instances such as idle timeout, session timeout, disabling of the WLAN, and the AP being nonoperational.

This feature is supported in the following FlexConnect scenario: local switching and central authentication.



---

**Caution** If the MAC address of a client that goes to sleep mode is spoofed, the fake device such as a laptop can be authenticated.

---

### Mobility Scenarios

Following are some guidelines in a mobility scenario:

- L2 roaming in the same subnet is supported.
- Anchor sleeping timer is applicable.
- The sleeping client information is shared between multiple autoanchors when a sleeping client moves from one anchor to another.

A sleeping client does not require reauthentication in the following scenarios:

- Suppose there are two embedded wireless controllers in a mobility group. A client that is associated with one embedded wireless controller goes to sleep and then wakes up and gets associated with the other embedded wireless controller.
- Suppose there are three embedded wireless controllers in a mobility group. A client that is associated with the second embedded wireless controller that is anchored to the first controller goes to sleep, wakes up, and gets associated with the third embedded wireless controller.
- A client sleeps, wakes up and gets associated with the same or different export foreign embedded wireless controller that is anchored to the export anchor.

## Restrictions on Authenticating Sleeping Clients

- The sleep client feature works only for WLAN configured with WebAuth security.
- You can configure the sleeping clients only on a per WebAuth parameter-map basis.
- The authentication of sleeping clients feature is supported only on WLANs that have Layer 3 security enabled.
- With Layer 3 security, the Authentication, Passthrough, and On MAC Filter failure web policies are supported. The Conditional Web Redirect and Splash Page Web Redirect web policies are not supported.
- The central web authentication of sleeping clients is not supported.
- The authentication of sleeping clients feature is not supported on guest LANs and remote LANs.
- A guest access sleeping client that has a local user policy is not supported. In this case, the WLAN-specific timer is applied.

## Configuring Authentication for Sleeping Clients (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Security > Web Auth**.
- Step 2** In the **Webauth Parameter Map** tab, click the parameter map name. The **Edit WebAuth Parameter** window is displayed.
- Step 3** Select **Sleeping Client Status** check box.
- Step 4** Click **Update & Apply to Device**.
- 

## Configuring Authentication for Sleeping Clients (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>[no] parameter-map type webauth</b>  <code>{parameter-map-name   global}</code></p> <p><b>Example:</b></p> <pre>Device(config)# parameter-map type webauth global</pre>	Creates a parameter map and enters parameter-map webauth configuration mode.
<b>Step 2</b>	<p><b>sleeping-client [timeout time]</b></p> <p><b>Example:</b></p> <pre>Device(config-params-parameter-map) # sleeping-client timeout 100</pre>	<p>Configures the sleeping client timeout to 100 minutes. Valid range is between 10 minutes and 43200 minutes.</p> <p><b>Note</b> If you do not use the timeout keyword, the sleeping client is configured with the default timeout value of 720 minutes.</p>
<b>Step 3</b>	<b>end</b>	Exits parameter-map webauth configuration mode and returns to privileged EXEC mode.
<b>Step 4</b>	<p>(Optional) <b>show wireless client sleeping-client</b></p> <p><b>Example:</b></p> <pre>Device# show wireless client sleeping-client</pre>	Shows the MAC address of the clients and the time remaining in their respective sessions.
<b>Step 5</b>	<p>(Optional) <b>clear wireless client sleeping-client</b>  <code>[mac-address mac-addr]</code></p> <p><b>Example:</b></p> <pre>Device# clear wireless client sleeping-client mac-address 00e1.e1e1.0001</pre>	<ul style="list-style-type: none"> <li>• <b>clear wireless client sleeping-client</b>—Deletes all sleeping client entries from the sleeping client cache.</li> <li>• <b>clear wireless client sleeping-client mac-address mac-addr</b>—Deletes the specific MAC entry from the sleeping client cache.</li> </ul>





## CHAPTER 42

# ISE Simplification and Enhancements

- [Utilities for Configuring Security, on page 363](#)
- [Configuring Captive Portal Bypassing for Local and Central Web Authentication, on page 365](#)
- [Sending DHCP Options 55 and 77 to ISE, on page 368](#)
- [Captive Portal, on page 371](#)

## Utilities for Configuring Security

This chapter describes how to configure all the RADIUS server side configuration using the following command:

**wireless-default radius server *ip key secret***

This simplified configuration option provides the following:

- Configures AAA authorization for network services, authentication for web auth and Dot1x.
- Enables local authentication with default authorization.
- Configures the default redirect ACL for CWA.
- Creates global parameter map with virtual IP and enables captive bypass portal.
- Configures all the AAA configuration for a default case while configuring the RADIUS server.
- The method-list configuration is assumed by default on the WLAN.
- Enables the radius accounting by default.
- Disables the radius aggressive failovers by default.
- Sets the radius request timeouts to 5 seconds by default.
- Enables captive bypass portal.

This command configures the following in the background:

```
aaa new-model
aaa authentication webauth default group radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting identity default start-stop group radius
!
aaa server radius dynamic-author
```

```

client <IP> server-key cisco123
!
radius server RAD_SRV_DEF_<IP>
description Configured by wireless-default
address ipv4 <IP> auth-port 1812 acct-port 1813
key <key>
!
aaa local authentication default authorization default
aaa session-id common
!
ip access-list extended CISCO-CWA-URL-REDIRECT-ACL-DEFAULT
remark " CWA ACL to be referenced from ISE "
deny udp any any eq domain
deny tcp any any eq domain
deny udp any any eq bootps any
deny udp any any eq bootpc
deny udp any eq bootpc any
deny ip any host <IP>
permit tcp any any eq www
!
parameter-map type webauth global
captive-bypass-portal
virtual-ip ipv4 192.0.2.1
virtual-ip ipv6 1001::1
!
wireless profile policy default-policy-profile
aaa-override
local-http-profiling
local-dhcp-profiling
accounting

```

Thus, you need not go through the entire Configuration Guide to configure wireless embedded wireless controller for a simple configuration requirement.

## Configuring Multiple Radius Servers

Use the following procedure to configure a RADIUS server.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless-default radius server ip key secret</b>  <b>Example:</b> Device(config)# wireless-default radius server 9.2.58.90 key cisco123	Configures a radius server.  <b>Note</b> You can configure up to ten RADIUS servers.
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Device(config)# end	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.



## Verifying AAA and Radius Server Configurations

To view details of AAA server, use the following command:

```
Device# show run aaa
!
aaa new-model
aaa authentication webauth default group radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting Identity default start-stop group radius
!
aaa server radius dynamic-author
  client 9.2.58.90 server-key cisco123
!
radius server RAD_SRV_DEF_9.2.58.90
  description Configured by wireless-default
  address ipv4 9.2.58.90 auth-port 1812 acct-port 1813
  key cisco123
!
aaa local authentication default authorization default
aaa session-id common
!
!
ip access-list extended CISCO-CWA-URL-REDIRECT-ACL-DEFAULT
remark " CWA ACL to be referenced from ISE "
deny udp any any eq domain
deny tcp any any eq domain
deny udp any eq bootps any
deny udp any any eq bootpc
deny udp any eq bootpc any
deny ip any host 9.2.58.90
permit tcp any any eq www
!
parameter-map type webauth global
  captive-bypass-portal
  virtual-ip ipv4 192.0.2.1
  virtual-ip ipv6 1001::1
!
wireless profile policy default-policy-profile
  aaa-override
  local-http-profiling
  local-dhcp-profiling
  accounting
```



---

**Note** The `show run aaa` output may change when new commands are added to this utility.

---

## Configuring Captive Portal Bypassing for Local and Central Web Authentication

### Information About Captive Bypassing

WISPr is a draft protocol that enables users to roam between different wireless service providers. Some devices (For example, Apple iOS devices) have a mechanism using which they can determine if the device is connected

to Internet, based on an HTTP WISPr request made to a designated URL. This mechanism is used for the device to automatically open a web browser when a direct connection to the internet is not possible. This enables the user to provide his credentials to access the internet. The actual authentication is done in the background every time the device connects to a new SSID.

The client device (Apple iOS device) sends a WISPr request to the embedded wireless controller, which checks for the user agent details and then triggers an HTTP request with a web authentication interception in the embedded wireless controller. After verification of the iOS version and the browser details provided by the user agent, the embedded wireless controller allows the client to bypass the captive portal settings and provides access to the Internet.

This HTTP request triggers a web authentication interception in the embedded wireless controller as any other page requests are performed by a wireless client. This interception leads to a web authentication process, which will be completed normally. If the web authentication is being used with any of the embedded wireless controller splash page features (URL provided by a configured RADIUS server), the splash page may never be displayed because the WISPr requests are made at very short intervals, and as soon as one of the queries is able to reach the designated server, any web redirection or splash page display process that is performed in the background is cancelled, and the device processes the page request, thus breaking the splash page functionality.

For example, Apple introduced an iOS feature to facilitate network access when captive portals are present. This feature detects the presence of a captive portal by sending a web request on connecting to a wireless network. This request is directed to <http://www.apple.com/library/test/success.html> for Apple iOS version 6 and older, and to several possible target URLs for Apple iOS version 7 and later. If a response is received, then the Internet access is assumed to be available and no further interaction is required. If no response is received, then the Internet access is assumed to be blocked by the captive portal and Apple's Captive Network Assistant (CNA) auto-launches the pseudo-browser to request portal login in a controlled window. The CNA may break when redirecting to an ISE captive portal. The embedded wireless controller prevents this pseudo-browser from popping up.

You can now configure the embedded wireless controller to bypass WISPr detection process, so the web authentication interception is only done when a user requests a web page leading to splash page load in user context, without the WISPr detection being performed in the background.

## Configuring Captive Bypassing for WLAN in LWA and CWA (GUI)

### Procedure

---

- Step 1** Choose **Configuration > Security > Web Auth**.
  - Step 2** In the **Webauth Parameter Map** tab, click the parameter map name. The **Edit WebAuth Parameter** window is displayed.
  - Step 3** Select **Captive Bypass Portal** check box.
  - Step 4** Click **Update & Apply to Device**.
-

## Configuring Captive Bypassing for WLAN in LWA and CWA (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>parameter-map type webauth</b> <i>parameter-map-name</i> <b>Example:</b> Device(config)# parameter-map type webauth WLAN1_MAP	Creates the parameter map.  The <i>parameter-map-name</i> must not exceed 99 characters.
<b>Step 3</b>	<b>captive-bypass-portal</b> <b>Example:</b> Device(config)# captive-bypass-portal	Configures captive bypassing.
<b>Step 4</b>	<b>wlan profile-name wlan-id ssid-name</b> <b>Example:</b> Device(config)# wlan WLAN1_NAME 4 WLAN1_NAME	Specifies the WLAN name and ID. <ul style="list-style-type: none"> <li>• <i>profile-name</i> is the WLAN name which can contain 32 alphanumeric characters.</li> <li>• <i>wlan-id</i> is the wireless LAN identifier. The valid range is from 1 to 512.</li> <li>• <i>ssid-name</i> is the SSID which can contain 32 alphanumeric characters.</li> </ul>
<b>Step 5</b>	<b>security web-auth</b> <b>Example:</b> Device(config-wlan)# security web-auth	Enables the web authentication for the WLAN.
<b>Step 6</b>	<b>security web-auth parameter-map</b> <i>parameter-map-name</i> <b>Example:</b> Device(config-wlan)# security web-auth parameter-map WLAN1_MAP	Maps the parameter map.  <b>Note</b> If parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
<b>Step 7</b>	<b>end</b> <b>Example:</b> Device(config-wlan)# end	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

# Sending DHCP Options 55 and 77 to ISE

## Information about DHCP Option 55 and 77

The DHCP sensors use the following DHCP options on the ISE for native and remote profiling:

- **Option 12:** Hostname
- **Option 6:** Class Identifier

Along with this, the following options needs to be sent to the ISE for profiling:

- **Option 55:** Parameter Request List
- **Option 77:** User Class

## Configuration to Send DHCP Options 55 and 77 to ISE (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Policy**.
  - Step 2** On the **Policy Profile** page, click **Add** to view the **Add Policy Profile** window.
  - Step 3** Click **Access Policies** tab, choose the **RADIUS Profiling** and **DHCP TLV Caching** check boxes to configure radius profiling and DHCP TLV Caching on a WLAN.
  - Step 4** Click **Save & Apply to Device**.
- 

## Configuration to Send DHCP Options 55 and 77 to ISE (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile policy <i>profile-policy</i></b>  <b>Example:</b> Device(config)# wireless profile policy rr-xyz-policy-1	Configures WLAN policy profile and enters the wireless policy configuration mode.
<b>Step 3</b>	<b>dhcp-tlv-caching</b>  <b>Example:</b>	Configures DHCP TLV caching on a WLAN.

	Command or Action	Purpose
	Device(config-wireless-policy) # dhcp-tlv-caching	
<b>Step 4</b>	<b>radius-profiling</b>  <b>Example:</b> Device(config-wireless-policy) # radius-profiling	Configures client radius profiling on a WLAN.
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Device(config-wireless-policy) # end	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring EAP Request Timeout (GUI)

Follow the steps given below to configure the EAP Request Timeout through the GUI:

### Procedure

- 
- Step 1** Choose **Configuration > Security > Advanced EAP**.
- Step 2** In the **EAP-Identity-Request Timeout** field, specify the amount of time (in seconds) in which the device attempts to send an EAP identity request to wireless clients using local EAP.
- Step 3** In the **EAP-Identity-Request Max Retries** field, specify the maximum number of times that the device attempts to retransmit the EAP identity request to wireless clients using local EAP.
- Step 4** Set **EAP Max-Login Ignore Identity Response** to **Enabled** state to limit the number of clients that can be connected to the device with the same username. You can log in up to eight times from different clients (PDA, laptop, IP phone, and so on) on the same device. The default state is **Disabled**.
- Step 5** In the **EAP-Request Timeout** field, specify the amount of time (in seconds) in which the device attempts to send an EAP request to wireless clients using local EAP.
- Step 6** In the **EAP-Request Max Retries** field, specify the maximum number of times that the device attempts to retransmit the EAP request to wireless clients using local EAP.
- Step 7** In the **EAPOL-Key Timeout** field, specify the amount of time (in seconds) in which the device attempts to send an EAP key over the LAN to wireless clients using local EAP.
- Step 8** In the **EAPOL-Key Max Retries** field, specify the maximum number of times that the device attempts to send an EAP key over the LAN to wireless clients using local EAP.
- Step 9** In the **EAP-Broadcast Key Interval** field, specify the time interval between rotations of the broadcast encryption key used for clients and click **Apply**.

**Note** After configuring the EAP-Broadcast key interval to a new time period, you must shut down or restart the WLAN for the changes to take effect. Once the WLAN is shut down or restarted, the M5 and M6 packets are exchanged when the configured timer value expires.

## Configuring EAP Request Timeout

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless wps client-exclusion dot1x-timeout</b> <b>Example:</b> Device(config)# wireless wps client-exclusion dot1x-timeout	Enables exclusion on timeout and no response.  By default, this feature is enabled.  To disable, append a <b>no</b> at the beginning of the command.
<b>Step 3</b>	<b>end</b> <b>Example:</b> Device(config)# end	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring EAP Request Timeout in Wireless Security (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless security dot1x request {retries 0 - 20   timeout 1 - 120}</b> <b>Example:</b> Device(config)# wireless security dot1x request timeout 60	Configures the EAP request retransmission timeout value in seconds.
<b>Step 3</b>	<b>end</b> <b>Example:</b> Device(config)# end	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

# Captive Portal

## Captive Portal Configuration

This feature enables you to configure multiple web authentication URLs (including external captive URLs) for the same SSID based on an AP. The default setting is to use the Global URL for authentication. The override option is available at WLAN and AP level.

The order of precedence is:

- AP
- WLAN
- Global configuration

### Restrictions for Captive Portal Configuration

- This configuration is supported in a standalone controller only.
- Export-Anchor configuration is not supported.

## Configuring Captive Portal (GUI)

### Procedure

---

- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** Click **Add**.
- Step 3** In the **General** tab, enter the **Profile Name**, the **SSID**, and the **WLAN ID**.
- Step 4** In the **Security > Layer2** tab, uncheck the **WPA Policy**, **AES** and **802.1x** check boxes.
- Step 5** In the **Security > Layer3** tab, choose the parameter map from the **Web Auth Parameter Map** drop-down list and authentication list from the **Authentication List** drop-down list.
- Step 6** In the **Security > AAA** tab, choose the Authentication list from the **Authentication List** drop-down list.
- Step 7** Click **Apply to Device**.
- Step 8** Choose **Configuration > Security > Web Auth**.
- Step 9** Choose a **Web Auth Parameter Map**.
- Step 10** In the **General** tab, enter the **Maximum HTTP connections**, **Init-State Timeout(secs)** and choose **webauth** from the **Type** drop-down list.
- Step 11** In the **Advanced** tab, under the **Redirect to external server** settings, enter the **Redirect for log-in** server.
- Step 12** Click **Update & Apply**.
-

## Configuring Captive Portal

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wlan</b> { <i>profile-name</i>   <b>shutdown</b> } <i>network-name</i> <b>Example:</b> Device(config)# wlan edc6 6 edc	Configures the WLAN profile. Enables or Disables all WLANs and creates the WLAN identifier. The profile-name and the SSID network name should be up to 32 alphanumeric characters.
<b>Step 3</b>	<b>ip</b> { <b>access-group</b>   <b>verify</b> } <b>web</b> <i>IPv4-ACL-Name</i> <b>Example:</b> Device(config-wlan)# ip access-group web CPWebauth	Configures the WLAN web ACL. <b>Note</b> WLAN needs to be disabled before performing this operation.
<b>Step 4</b>	<b>no security wpa</b> <b>Example:</b> Device(config-wlan)# no security wpa	Disables WPA security.
<b>Step 5</b>	<b>no security wpa akm dot1x</b> <b>Example:</b> Device(config-wlan)# no security wpa akm dot1x	Disables security AKM for dot1x.
<b>Step 6</b>	<b>no security wpa wpa2 ciphers aes</b> <b>Example:</b> Device(config-wlan)# no security wpa wpa2 ciphers aes	Disables WPA2 ciphers for AES.
<b>Step 7</b>	<b>security web-auth</b> { <b>authentication-list</b> <i>authentication-list-name</i>   <b>authorization-list</b> <i>authorization-list-name</i>   <b>on-macfilter-failure</b>   <b>parameter-map</b> <i>parameter-map-name</i> } <b>Example:</b> Device(config-wlan)# security web-auth authentication-list cp-webauth Device(config-wlan)# security web-auth parameter-map parMap6	Enables web authentication for WLAN. Here, <ul style="list-style-type: none"> <li>• <b>authentication-list</b> <i>authentication-list-name</i>: Sets the authentication list for IEEE 802.1x.</li> <li>• <b>authorization-list</b> <i>authorization-list-name</i>: Sets the override-authorization list for IEEE 802.1x.</li> <li>• <b>on-macfilter-failure</b>: Enables Web authentication on MAC filter failure.</li> </ul>



	Command or Action	Purpose
		<ul style="list-style-type: none"> <li><b>parameter-map</b> <i>parameter-map-name</i>: Configures the parameter map.</li> </ul> <p><b>Note</b> When <b>security web-auth</b> is enabled, you get to map the default <b>authentication-list</b> and global <b>parameter-map</b>. This is applicable for authentication-list and parameter-map that are not explicitly mentioned.</p>
<b>Step 8</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wlan)# no shutdown	Enables the WLAN.
<b>Step 9</b>	<b>exit</b> <b>Example:</b> Device(config-wlan)# exit	Exits from the WLAN configuration.
<b>Step 10</b>	<b>parameter-map type webauth</b> <i>parameter-map-name</i> <b>Example:</b> Device(config)# parameter-map type webauth parMap6	Creates a parameter map and enters parameter-map webauth configuration mode.
<b>Step 11</b>	<b>parameter-map type webauth</b> <i>parameter-map-name</i> <b>Example:</b> Device(config)# parameter-map type webauth parMap6	Creates a parameter map and enters parameter-map webauth configuration mode.
<b>Step 12</b>	<b>type webauth</b> <b>Example:</b> Device(config-params-parameter-map)# type webauth	Configures the webauth type parameter.
<b>Step 13</b>	<b>timeout init-state sec &lt;timeout-seconds&gt;</b> <b>Example:</b> Device(config-params-parameter-map)# timeout inti-state sec 3600	Configures the WEBAUTH timeout in seconds. Valid range for the time in sec parameter is 60 seconds to 3932100 seconds.
<b>Step 14</b>	<b>redirect for-login &lt;URL-String&gt;</b> <b>Example:</b> Device(config-params-parameter-map)# redirect for-login https://172.16.100.157/portal/login.html	Configures the URL string for redirect during login.

	Command or Action	Purpose
<b>Step 15</b>	<b>exit</b> <b>Example:</b> Device(config-params-parameter-map)# exit	Exits the parameters configuration.
<b>Step 16</b>	<b>wireless tag policy <i>policy-tag-name</i></b> <b>Example:</b> Device(config)# wireless tag policy policy_tag_edc6	Configures policy tag and enters policy tag configuration mode.
<b>Step 17</b>	<b>wlan <i>wlan-profile-name</i> policy <i>policy-profile-name</i></b> <b>Example:</b> Device(config-policy-tag)# wlan edc6 policy policy_profile_flex	Attaches a policy profile to a WLAN profile.
<b>Step 18</b>	<b>end</b> <b>Example:</b> Device(config-policy-tag)# end	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.

## Captive Portal Configuration - Example

The following example shows how you can have APs at different locations, broadcasting the same SSID but redirecting clients to different redirect portals:

Configuring multiple parameter maps pointing to different redirect portal:

```
parameter-map type webauth parMap1
type webauth
timeout init-state sec 21600
redirect for-login
https://172.16.12.3:8080/portal/PortalSetup.action?portal=cfdbce00-2ce2-11e8-b83c-005056a06b27
redirect portal ipv4 172.16.12.3
!
!
parameter-map type webauth parMap11
type webauth
timeout init-state sec 21600
redirect for-login
https://172.16.12.4:8443/portal/PortalSetup.action?portal=094e7270-3808-11e8-9797-02421e4cae0c
redirect portal ipv4 172.16.12.4
!
```

Associating these parameter maps to different WLANs:

```
wlan edc1 1 edc
ip access-group web CPWebauth
no security wpa
no security wpa akm dot1x
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list cp-webauth
security web-auth parameter-map parMap11
```

```
no shutdown
wlan edc2 2 edc
ip access-group web CPWebauth
no security wpa
no security wpa akm dot1x
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list cp-webauth
security web-auth parameter-map parMap1
no shutdown
```



---

**Note** All WLANs have identical SSIDs.

---

Associating WLANs to different policy tags:

```
wireless tag policy policy_tag_edc1
wlan edc1 policy policy_profile_flex
wireless tag policy policy_tag_edc2
wlan edc2 policy policy_profile_flex
```

Assigning these policy tags to the desired APs:

```
ap E4AA.5D13.14DC
policy-tag policy_tag_edc1
site-tag site_tag_flex
ap E4AA.5D2C.3CAC
policy-tag policy_tag_edc2
site-tag site_tag_flex
```





## CHAPTER 43

# Authentication and Authorization Between Multiple RADIUS Servers

---

- [Information About Authentication and Authorization Between Multiple RADIUS Servers](#), on page 377
- [Configuring 802.1X Security for WLAN with Split Authentication and Authorization Servers](#), on page 378
- [Configuring Web Authentication for WLAN with Split Authentication and Authorization Servers](#), on page 383
- [Verifying Split Authentication and Authorization Configuration](#), on page 385
- [Configuration Examples](#), on page 385

## Information About Authentication and Authorization Between Multiple RADIUS Servers

Cisco Embedded Wireless Controller on Catalyst Access Points uses the approach of request and response transaction with a single RADIUS server that combines both authentication and authorization. You can split the authentication and authorization on the controller between multiple RADIUS servers.

A RADIUS sever can assume the role of either an authentication server, authorization server, or both. In cases where there are disparate RADIUS servers for authentication and authorization, the Session Aware Networking (SANet) component on the embedded wireless controller now allows authentication on one server and authorization on another when a client joins the embedded wireless controller.

Authentication can be done using the Cisco ISE, Cisco DNAC, Free RADIUS, or any third-party RADIUS Server. After successful authentication from an authentication server, the embedded wireless controller relays attributes received from the authentication server to another RADIUS sever designated as authorization server.

The authorization server then performs the following:

- Processes received attributes with the other policies or rules defined on the server.
- Derives attributes as part of the authorization response and returns it to the embedded wireless controller.



---

**Note** In a split authentication and authorization configuration, both servers must be available and must successfully authenticate and authorize with an ACCESS-ACCEPT for a session to be accepted by the embedded wireless controller.

---

# Configuring 802.1X Security for WLAN with Split Authentication and Authorization Servers

## Configuring Explicit Authentication and Authorization Server List (GUI)

### Procedure

---

- Step 1** Choose **Configuration > Security > AAA**.
- Step 2** On the **Authentication Authorization and Accounting** page, click the **Servers/Groups** tab.
- Step 3** Click the type of AAA server you want to configure from the following options:
- RADIUS
  - TACACS+
  - LDAP
- In this procedure, the RADIUS server configuration is described.
- Step 4** With the **RADIUS** option selected, click **Add**.
- Step 5** Enter a name for the RADIUS server and the IPv4 or IPV6 address of the server.
- Step 6** Enter the authentication and encryption key to be used between the device and the key string RADIUS daemon running on the RADIUS server. You can choose to use either a PAC key or a non-PAC key.
- Step 7** Enter the server timeout value; valid range is 1 to 1000 seconds.
- Step 8** Enter a retry count; valid range is 0 to 100.
- Step 9** Leave the **Support for CoA** field in **Enabled** state.
- Step 10** Click **Save & Apply to Device**.
- Step 11** On the **Authentication Authorization and Accounting** page, with **RADIUS** option selected, click the **Server Groups** tab.
- Step 12** Click **Add**.
- Step 13** In the **Create AAA RADIUS Server Group** window that is displayed, enter a name for the RADIUS server group.
- Step 14** From the **MAC-Delimiter** drop-down list, choose the delimiter to be used in the MAC addresses that are sent to the RADIUS servers.
- Step 15** From the **MAC Filtering** drop-down list, choose a value based on which to filter MAC addresses.
- Step 16** To configure dead time for the server group and direct AAA traffic to alternative groups of servers that have different operational characteristics, in the **Dead-Time** field, enter the amount of time, in minutes, after which a server is assumed to be dead.

- Step 17** Choose the servers that you want to include in the server group from the **Available Servers** list and move them to the **Assigned Servers** list.
- Step 18** Click **Save & Apply to Device**.

## Configuring Explicit Authentication Server List (GUI)

### Procedure

- Step 1** Choose **Configuration > Security > AAA > Servers/Groups**.
- Step 2** Choose **RADIUS > Servers** tab.
- Step 3** Click **Add** to add a new server or click an existing server.
- Step 4** Enter the **Name**, the **Server Address**, **Key**, **Confirm Key**, **Auth Port** and **Acct Port**. Check the **PAC Key** checkbox and enter the **PAC key** and **Confirm PAC Key**.
- Step 5** Click **Apply to Device**.
- Step 6** Choose **RADIUS > Server Groups** and click **Add** to add a new server group or click an existing server group.
- Step 7** Enter the **Name** of the server group and choose the servers that you want to include in the server group, from the **Available Servers** list and move them to the **Assigned Servers** list.
- Step 8** Click **Apply to Device**.

## Configuring Explicit Authentication Server List (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>radius server</b> <i>server-name</i>  <b>Example:</b> Device(config)# <b>radius server</b> <b>free-radius-authc-server</b>	Specifies the RADIUS server name.
<b>Step 4</b>	<b>address ipv4</b> <i>address</i> <b>auth-port</b> <i>auth_port_number</i> <b>acct-port</b> <i>acct_port_number</i>  <b>Example:</b>	Specifies the RADIUS server parameters.

	Command or Action	Purpose
	Device(config-radius-server)# <b>address</b> ipv4 9.2.62.56 <b>auth-port</b> 1812 <b>acct-port</b> 1813	
<b>Step 5</b>	[pac] <b>key</b> <i>key</i> <b>Example:</b> Device(config-radius-server)# <b>key</b> cisco	Specify the authentication and encryption key used between the Device and the key string RADIUS daemon running on the RADIUS server.
<b>Step 6</b>	<b>exit</b> <b>Example:</b> Device(config-radius-server)# <b>exit</b>	Returns to the configuration mode.
<b>Step 7</b>	<b>aaa group server radius</b> <i>server-group</i> <b>Example:</b> Device(config)# <b>aaa group server radius</b> <b>authc-server-group</b>	Creates a radius server-group identification.
<b>Step 8</b>	<b>server name</b> <i>server-name</i> <b>Example:</b> Device(config)# <b>server name</b> <b>free-radius-authc-server</b>	Configures the server name.
<b>Step 9</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.  For more information, see <b>Configuring AAA for External Authentication</b> .

## Configuring Explicit Authorization Server List (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Security > AAA > Servers/Groups**.
  - Step 2** Choose **RADIUS > Servers** tab.
  - Step 3** Click **Add** to add a new server or click an existing server.
  - Step 4** Enter the **Name**, the **Server Address**, **Key**, **Confirm Key**, **Auth Port** and **Acct Port**. Check the **PAC Key** checkbox and enter the **PAC key** and **Confirm PAC Key**.
  - Step 5** Click **Apply to Device**.
  - Step 6** Choose **RADIUS > Server Groups** and click **Add** to add a new server group or click an existing server group.
  - Step 7** Enter the **Name** of the server group and choose the servers that you want to include in the server group, from the **Available Servers** list and move them to the **Assigned Servers** list.
  - Step 8** Click **Apply to Device**.
-



## Configuring Explicit Authorization Server List (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>radius server <i>server-name</i></b> <b>Example:</b> Device(config)# radius server cisco-dnac-authz-server	Specifies the RADIUS server name.
<b>Step 4</b>	<b>address ipv4 <i>address</i> auth-port <i>auth_port_number</i> acct-port <i>acct_port_number</i></b> <b>Example:</b> Device(config-radius-server)# address ipv4 9.4.62.32 auth-port 1812 acct-port 1813	Specifies the RADIUS server parameters.
<b>Step 5</b>	<b>[pac] key <i>key</i></b> <b>Example:</b> Device(config-radius-server)# pac key cisco	Specify the authorization and encryption key used between the Device and the key string RADIUS daemon running on the RADIUS server.
<b>Step 6</b>	<b>exit</b> <b>Example:</b> Device(config-radius-server)# exit	Returns to the configuration mode.
<b>Step 7</b>	<b>aaa group server radius <i>server-group</i></b> <b>Example:</b> Device(config)# aaa group server radius authz-server-group	Creates a radius server-group identification.
<b>Step 8</b>	<b>server name <i>server-name</i></b> <b>Example:</b> Device(config)# server name cisco-dnac-authz-server	
<b>Step 9</b>	<b>end</b> <b>Example:</b> Device(config)# end	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring Authentication and Authorization List for 802.1X Security (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** Click **Add**.
- Step 3** In the **General** tab, enter the **Profile Name**, the **SSID**, and the **WLAN ID**.
- Step 4** In the **Security > AAA** tab, choose the Authentication list from the **Authentication List** drop-down list.
- Step 5** Click **Apply to Device**.
- 

## Configuring Authentication and Authorization List for 802.1X Security

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>wlan wlan-name wlan-id SSID-name</b> <b>Example:</b> Device(config)# wlan wlan-foo 222 foo-ssid	Enters WLAN configuration sub-mode. <ul style="list-style-type: none"> <li>• <i>wlan-name</i>: Is the name of the configured WLAN.</li> <li>• <i>wlan-id</i>: Is the wireless LAN identifier. Range is from 1 to 512.</li> <li>• <i>SSID-name</i>: Is the SSID name which can contain 32 alphanumeric characters.</li> </ul> <p><b>Note</b> If you have already configured this command, enter <b>wlan wlan-name</b> command.</p>
<b>Step 4</b>	<b>security dot1x authentication-list            authenticate-list-name</b> <b>Example:</b> Device(config-wlan)# security dot1x authentication-list authc-server-group	Enables authentication list for dot1x security.

	Command or Action	Purpose
<b>Step 5</b>	<b>security dot1x authorization-list</b> <i>authorize-list-name</i>  <b>Example:</b> Device(config-wlan) # <b>security dot1x</b> <b>authorization-list authz-server-group</b>	Specifies authorization list for dot1x security.  For more information on the <b>Cisco Digital Network Architecture Center (DNAC)</b> , see the <b>DNAC documentation</b> .
<b>Step 6</b>	<b>end</b>  <b>Example:</b> Device(config-wlan) # <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring Web Authentication for WLAN with Split Authentication and Authorization Servers

### Configuring Authentication and Authorization List for Web Authentication (GUI)

#### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
  - Step 2** Click **Add**.
  - Step 3** In the **General** tab, enter the **Profile Name**, the **SSID**, and the **WLAN ID**.
  - Step 4** In the **Security > Layer2** tab, uncheck the **WPA Policy**, **AES** and **802.1x** check boxes.
  - Step 5** Check the **MAC Filtering** check box to enable the feature. With MAC Filtering enabled, choose the Authorization list from the **Authorization List** drop-down list.
  - Step 6** In the **Security > AAA** tab, choose the Authentication list from the **Authentication List** drop-down list.
  - Step 7** Click **Apply to Device**.
- 

### Configuring Authentication and Authorization List for Web Authentication

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode.  Enter your password if prompted.

	Command or Action	Purpose
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<b>wlan wlan-name wlan-id SSID-name</b> <b>Example:</b> Device(config)# <code>wlan wlan-bar 1 bar-ssid</code>	Enters WLAN configuration sub-mode.  <ul style="list-style-type: none"> <li>• <i>wlan-name</i>: Is the name of the configured WLAN.</li> <li>• <i>wlan-id</i>: Is the wireless LAN identifier.</li> <li>• <i>SSID-name</i>: Is the SSID name which can contain 32 alphanumeric characters.</li> </ul> <b>Note</b> If you have already configured this command, enter <code>wlan wlan-name</code> command.
<b>Step 4</b>	<b>no security wpa</b> <b>Example:</b> Device(config-wlan)# <code>no security wpa</code>	Disables WPA security.
<b>Step 5</b>	<b>no security wpa akm dot1x</b> <b>Example:</b> Device(config-wlan)# <code>no security wpa akm dot1x</code>	Disables security AKM for dot1x.
<b>Step 6</b>	<b>no security wpa wpa2</b> <b>Example:</b> Device(config-wlan)# <code>no security wpa wpa2</code>	Disables WPA2 security.
<b>Step 7</b>	<b>security web-auth {authentication-list authenticate-list-name   authorization-list authorize-list-name}</b> <b>Example:</b> Device(config-wlan)# <code>security web-auth authentication-list authc-server-group</code>	Enables authentication or authorization list for dot1x security.  <b>Note</b> You get to view the following error, if you do not disable WPA security, AKM for dot1x, and WPA2 security:  <i>% switch-1:dbm:wireless:web-auth cannot be enabled. Invalid WPA/WPA2 settings.</i>
<b>Step 8</b>	<b>end</b> <b>Example:</b> Device(config-wlan)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

# Verifying Split Authentication and Authorization Configuration

To view the WLAN details, use the following command:

```
Device# show run wlan
wlan wlan-foo 2 foo-ssid
security dot1x authentication-list authc-server-group
security dot1x authorization-list authz-server-group

wlan wlan-bar 3 bar-ssid
security web-auth authentication-list authc-server-group
security web-auth authorization-list authz-server-group
```

To view the AAA authentication and server details, use the following command:

```
Device# show run aaa
!
aaa authentication dot1x default group radius
username cisco privilege 15 password 0 cisco
!
!
radius server free-radius-authc-server
 address ipv4 9.2.62.56 auth-port 1812 acct-port 1813
 key cisco
!
radius server cisco-dnac-authz-server
 address ipv4 9.4.62.32 auth-port 1812 acct-port 1813
 pac key cisco
!
!
aaa new-model
aaa session-id common
!
```

To view the authentication and authorization list for 802.1X security, use the following command:

```
Device# show wlan name wlan-foo | sec 802.1x
802.1x authentication list name      : authc-server-group
802.1x authorization list name     : authz-server-group
           802.1x                   : Enabled
```

To view the authentication and authorization list for web authentication, use the following command:

```
Device# show wlan name wlan-bar | sec Webauth
Webauth On-mac-filter Failure      : Disabled
Webauth Authentication List Name   : authc-server-group
Webauth Authorization List Name    : authz-server-group
Webauth Parameter Map              : Disabled
```

## Configuration Examples

### Configuring Cisco Embedded Wireless Controller on Catalyst Access Points for Authentication with a Third-Party RADIUS Server: Example

This example shows how to configure Cisco Embedded Wireless Controller on Catalyst Access Points for authentication with a third-party RADIUS server:

```
Device(config)# radius server free-radius-authc-server
Device(config-radius-server)# address ipv4 9.2.62.56 auth-port 1812 acct-port 1813
```

```
Device(config-radius-server)# key cisco
Device(config-radius-server)# exit
Device(config)# aaa group server radius authc-server-group
Device(config)# server name free-radius-authc-server
Device(config)# end
```

### **Configuring Cisco Embedded Wireless Controller on Catalyst Access Points for Authorization with Cisco ISE or DNAC: Example**

This example shows how to configure Cisco Embedded Wireless Controller on Catalyst Access Points for authorization with Cisco ISE or DNAC:

```
Device(config)# radius server cisco-dnac-authz-server
Device (config-radius-server)# address ipv4 9.4.62.32 auth-port 1812 acct-port 1813
Device (config-radius-server)# pac key cisco
Device (config-radius-server)# exit
Device(config)# aaa group server radius authz-server-group
Device(config)# server name cisco-dnac-authz-server
Device(config)# end
```



## CHAPTER 44

# Secure LDAP

---

- [Information About SLDAP, on page 387](#)
- [Prerequisite for Configuring SLDAP, on page 389](#)
- [Restrictions for Configuring SLDAP, on page 389](#)
- [Configuring SLDAP, on page 389](#)
- [Configuring an AAA Server Group \(GUI\), on page 390](#)
- [Configuring a AAA Server Group, on page 391](#)
- [Configuring Search and Bind Operations for an Authentication Request, on page 392](#)
- [Configuring a Dynamic Attribute Map on an SLDAP Server, on page 393](#)
- [Verifying the SLDAP Configuration, on page 393](#)

## Information About SLDAP

### Transport Layer Security (TLS)

The Transport Layer Security (TLS) is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. TLS relies upon certificates, public keys, and private keys to prove the identity of clients.

The certificates are issued by the Certificate Authorities (CAs).

Each certificate includes the following:

- The name of the authority that issued it.
- The name of the entity to which the certificate was issued.
- The public key of the entity.
- The timestamps of the entity that indicate the expiration date of the certificate.

You can find the TLS support for LDAP in the RFC2830 which is an extension to the LDAP protocol.

### LDAP Operations

*Bind*

The bind operation is used to authenticate a user to the server. It is used to start a connection with the LDAP server. LDAP is a connection-oriented protocol. The client specifies the protocol version and authentication information.

LDAP supports the following binds:

- **Authenticated bind**—An authenticated bind is performed when a root Distinguished Name (DN) and password are available.
- **Anonymous bind**—In the absence of a root DN and password, an anonymous bind is performed.

In LDAP deployments, the search operation is performed first and the bind operation later. This is because, if a password attribute is returned as part of the search operation, the password verification can be done locally on an LDAP client. Thus, there is no need to perform an extra bind operation. If a password attribute is not returned, the bind operation can be performed later. Another advantage of performing a search operation first and a bind operation later is that the DN received in the search result can be used as the user DN instead of forming a DN by prefixing the username (cn attribute) with the base DN. All entries stored in an LDAP server have a unique DN.

The DN consists of two parts:

- **Relative Distinguished Name (RDN)**
- **Location in the LDAP server where the record resides.**

Most of the entries that you store in an LDAP server will have a name, and the name is frequently stored in the Common Name (cn) attribute. Because every object has a name, most objects you store in an LDAP will use their cn value as the basis for their RDN.

### *Search*

A search operation is used to search the LDAP server. The client specifies the starting point (base DN) of the search, the search scope (either the object, its children, or the subtree rooted at the object), and a search filter.

For authorization requests, the search operation is directly performed without a bind operation. The LDAP server can be configured with certain privileges for the search operation to succeed. This privilege level is established with the bind operation.

An LDAP search operation can return multiple user entries for a specific user. In such cases, the LDAP client returns an appropriate error code to AAA. To avoid these errors, you must configure appropriate search filters to match a single entry.

### *Compare*

The compare operation is used to replace a bind request with a compare request for an authentication. The compare operation helps to maintain the initial bind parameters for the connection.

## **LDAP Dynamic Attribute Mapping**

The Lightweight Directory Access Protocol (LDAP) is a powerful and flexible protocol for communication with AAA servers. LDAP attribute maps provide a method to cross-reference the attributes retrieved from a server to Cisco attributes supported by the security appliances.

When a user authenticates a security appliance, the security appliance, in turn, authenticates the server and uses the LDAP protocol to retrieve the record for that user. The record consists of LDAP attributes associated with fields displayed on the user interface of the server. Each attribute retrieved includes a value that was entered by the administrator who updates the user records.



## Prerequisite for Configuring SLDAP

If you are using a secure Transport Layer Security (TLS) secure connection, you must configure the X.509 certificates.

## Restrictions for Configuring SLDAP

- LDAP referrals are not supported.
- Unsolicited messages or notifications from the LDAP server are not handled.
- LDAP authentication is not supported for interactive (terminal) sessions.

## Configuring SLDAP

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# enable	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ldap server name</b> <b>Example:</b> Device(config)# ldap server server1	Defines a Lightweight Directory Access Protocol (LDAP) server and enters LDAP server configuration mode.
<b>Step 4</b>	<b>ipv4 ipv4-address</b> <b>Example:</b> Device(config-ldap-server)# ipv4 9.4.109.20	Specifies the LDAP server IP address using IPv4.
<b>Step 5</b>	<b>timeout retransmit seconds</b> <b>Example:</b> Device(config-ldap-server)# timeout retransmit 20	Specifies the number of seconds the embedded wireless controller waits for a reply to an LDAP request before retransmitting the request.
<b>Step 6</b>	<b>bind authenticate root-dn password [0 string   7 string] string</b> <b>Example:</b>	Specifies a shared secret text string used between the embedded wireless controller and an LDAP server.

	Command or Action	Purpose
	<pre>Device(config-ldap-server)# bind authenticate root-dn CN=ldapipv6user,CN=Users,DC=ca,DC=ssh2,DC=com password Cisco12345</pre>	<p>Use the <b>0</b> line option to configure an unencrypted shared secret.</p> <p>Use the <b>7</b> line option to configure an encrypted shared secret.</p>
<b>Step 7</b>	<p><b>base-dn</b> <i>string</i></p> <p><b>Example:</b></p> <pre>Device(config-ldap-server)# base-dn CN=Users,DC=ca,DC=ssh2,DC=com</pre>	Specifies the base Distinguished Name (DN) of the search.
<b>Step 8</b>	<p><b>mode secure</b> [<b>no- negotiation</b>]</p> <p><b>Example:</b></p> <pre>Device(config-ldap-server)# mode secure no- negotiation</pre>	Configures LDAP to initiate the TLS connection and specifies the secure mode.
<b>Step 9</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-ldap-server)# end</pre>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring an AAA Server Group (GUI)

Configuring a device to use AAA server groups helps you to group existing server hosts, select a subset of the configured server hosts and use them for a particular service. A server group is used with a global server-host list. The server group lists the IP addresses of the selected server hosts.

You can create the following server groups:

### Procedure

#### Step 1

#### RADIUS

- Choose **Services > Security > AAA > Server Groups > RADIUS**.
- Click the **Add** button. The **Create AAA Radius Server Group** dialog box appears.
- Enter a name for the RADIUS server group in the **Name** field.
- Choose a desired delimiter from the **MAC-Delimiter** drop-down list. The available options are colon, hyphen, and single-hyphen.
- Choose a desired filter from the **MAC-Filtering** drop-down list. The available options are mac and Key.
- Enter a value in the **Dead-Time (mins)** field to make a server non-operational. You must specify a value between 1 and 1440.
- Choose any of the available servers from the **Available Servers** list and move them to the **Assigned Servers** list by clicking the **>** button.
- Click the **Save & Apply to Device** button.

#### Step 2

#### TACACS+

- Choose **Services > Security > AAA > Server Groups > TACACS+**.

- b) Click the **Add** button. The **Create AAA Tacacs Server Group** dialog box appears.
- c) Enter a name for the TACACS server group in the **Name** field.
- d) Choose any of the available servers from the **Available Servers** list and move them to the **Assigned Servers** list by clicking the > button.
- e) Click the **Save & Apply to Device** button.

### Step 3 LDAP

- a) Choose **Services > Security > AAA > Server Groups > LDAP**.
- b) Click the **Add** button. The **Create AAA Ldap Server Group** dialog box appears.
- c) Enter a name for the LDAP server group in the **Name** field.
- d) Choose any of the available servers from the **Available Servers** list and move them to the **Assigned Servers** list by clicking the > button.
- e) Click the **Save & Apply to Device** button.

## Configuring a AAA Server Group

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# enable	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>aaa new-model</b> <b>Example:</b> Device(config)# aaa new-model	Enables AAA.
<b>Step 4</b>	<b>aaa group server ldap <i>group-name</i></b> <b>Example:</b> Device(config)# aaa group server ldap name1	Defines the AAA server group with a group name and enters LDAP server group configuration mode. All members of a group must be of the same type, that is, RADIUS, LDAP, or TACACS+.
<b>Step 5</b>	<b>server <i>name</i></b> <b>Example:</b> Device(config-ldap-sg)# server server1	Associates a particular LDAP server with the defined server group. Each security server is identified by its IP address and UDP port number.
<b>Step 6</b>	<b>exit</b> <b>Example:</b>	Exits LDAP server group configuration mode.

	Command or Action	Purpose
	Device(config-ldap-sg) # <b>exit</b>	

## Configuring Search and Bind Operations for an Authentication Request

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# enable	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>aaa new-model</b> <b>Example:</b> Device(config)# <b>aaa new-model</b>	Enables AAA.
<b>Step 4</b>	<b>ldap server name</b> <b>Example:</b> Device(config)# <b>ldap server server1</b>	Defines a Lightweight Directory Access Protocol (LDAP) server and enters LDAP server configuration mode.
<b>Step 5</b>	<b>authentication bind-first</b> <b>Example:</b> Device(config-ldap-server)# <b>authentication bind-first</b>	Configures the sequence of search and bind operations for an authentication request.
<b>Step 6</b>	<b>authentication compare</b> <b>Example:</b> Device(config-ldap-server)# <b>authentication compare</b>	Replaces the bind request with the compare request for authentication.
<b>Step 7</b>	<b>exit</b> <b>Example:</b> Device(config-ldap-server)# <b>exit</b>	Exits LDAP server group configuration mode.

# Configuring a Dynamic Attribute Map on an SLDAP Server

You must create LDAP attribute maps that map your existing user-defined attribute names and values to Cisco attribute names and values that are compatible with the security appliance. You can then bind these attribute maps to LDAP servers or remove them as required.



**Note** To use the attribute mapping features correctly, you need to understand the Cisco LDAP and user-defined attribute names and values.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# enable	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ldap attribute-map <i>map-name</i></b> <b>Example:</b> Device(config)# ldap attribute-map map1	Configures a dynamic LDAP attribute map and enters attribute-map configuration mode.
<b>Step 4</b>	<b>map type <i>ldap-attr-type aaa-attr-type</i></b> <b>Example:</b> Device(config-attr-map)# map type department supplicant-group	Defines an attribute map.
<b>Step 5</b>	<b>exit</b> <b>Example:</b> Device(config-attr-map)# exit	Exits attribute-map configuration mode.

## Verifying the SLDAP Configuration

To view details about the default LDAP attribute mapping, use the following command:

```
Device# show ldap attributes
```

To view the LDAP server state information and various other counters for the server, use the following command:

```
Device# show ldap server
```





## CHAPTER 45

# RADIUS DTLS

---

- [Information About RADIUS DTLS, on page 395](#)
- [Prerequisites, on page 397](#)
- [Configuring RADIUS DTLS Server, on page 397](#)
- [Configuring DTLS Dynamic Author, on page 402](#)
- [Enabling DTLS for Client, on page 402](#)
- [Verifying the RADIUS DTLS Server Configuration, on page 405](#)
- [Clearing RADIUS DTLS Specific Statistics, on page 405](#)

## Information About RADIUS DTLS

The Remote Authentication Dial-In User Service (RADIUS) is a client or server protocol that provides centralized security for users attempting to gain management access to a network. The RADIUS protocol is a widely deployed authentication and authorization protocol that delivers a complete Authentication, Authorization, and Accounting (AAA) solution.

### RADIUS DTLS Port

The RADIUS port (DTLS server) is used for authentication and accounting. The default DTLS server port is 2083.

You can change the RADIUS DTLS port number using `dtls port port_number`. For more information, see the [Configuring RADIUS DTLS Port Number](#) section.

### Shared Secret

You can use `radius/dtls` as the shared secret, if you have enabled DTLS for a specific server.

### Handling PAC for CTS Communication

You can download PAC from ISE for CTS communication. Once the PAC is downloaded, you need to encrypt all the CTS attributes with the PAC key instead of the shared secret.

The ISE then decrypts these attributes using PAC.

### Session Management

The RADIUS client purely depends on the response from the DTLS server. If the session is ideal for ideal timeout, then the session must be closed.

In case of invalid responses, the sessions must be deleted.

If you need to send the radius packets over DTLS, the DTLS session needs to be re-established with the specific server.

### Load Balancing

Multiple DTLS servers and load balancing methods are configured.

You need to select the AAA server to which the request needs to be sent. Then use the DTLS context of the specific server to encrypt the RADIUS packet and send it back.

### Connection Timeout

After the encrypted RADIUS packet is sent, you need to start the retransmission timer. If you do not get a response before the retransmission timer expires, the packet is re-encrypted and re-transmitted.

You can continue for number of times as per the **dtls retries** configuration or till the default value. Once the number of tries exceeds the limit, the server becomes unavailable and responses are sent back to the AAA clients.



---

**Note** The default connection timeout is 5 seconds.

---

### Connection Retries

As the RADIUS DTLS is UDP based, you need to retry the connection after a specific timeout interval for a specific number of retries.

After all retries are exhausted, the DTLS connection performs the following:

- Is marked as unsuccessful.
- Looks up for the next available server for processing the RADIUS requests.



---

**Note** The default connection retries is 5.

---

### Idle Timeout

When the idle timer expires and no transactions exists since the last idle timeout, the DTLS session remains closed.

After you establish the DTLS session, you can start the idle timer. If you start the idle timer for 30 seconds and one of the RADIUS DTLS packet is sent, then after 30 seconds, the idle timer expires and checks for number of RADIUS DTLS transactions.

If the idle timer value exceeds zero, the idle timer resets the transaction counter and restarts the timer.






---

**Note** The default idle timeout is 60 seconds.

---

### Handling Server and Server Group Failover

You can configure RADIUS servers with and without DTLS. It is recommended to create AAA server groups with DTLS enabled servers and non-DTLS servers. However, you will not find any such restriction while configuring AAA server groups.

Suppose you choose a DTLS server, the DTLS server establishes connection and RADIUS request packet is sent to the DTLS server. If the DTLS server does not respond after all RADIUS retries, it would fall over to the next configured server in the same server group. If the next server is a DTLS server, the processing of the RADIUS request packet continues with the next server. If the next server is a non-DTLS server, the processing of RADIUS request packet does not happen in that server group. Then the server group failover occurs and the same sequence continues with the next server group, if the next server group is available.




---

**Note** You need to use either only DTLS or non-DTLS servers in a server group.

---

## Prerequisites

### Support for IOS and BINOS AAA

The AAA server runs in IOS and BINOS platforms. Once you complete the RADIUS DTLS support in IOS, the same needs to be ported to BINOS.

## Configuring RADIUS DTLS Server

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device# enable	Enters privileged EXEC mode.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>radius server</b> <i>server-name</i>  <b>Example:</b> Device(config)# radius server R1	Specifies the RADIUS server name.

	Command or Action	Purpose
<b>Step 4</b>	<b>dtls</b> <b>Example:</b> Device(config-radius-server) # <b>dtls</b>	Configures DTLS parameters.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config-radius-server) # <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring RADIUS DTLS Connection Timeout

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# <b>enable</b>	Enters privileged EXEC mode.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>radius server</b> <i>server-name</i> <b>Example:</b> Device(config) # <b>radius server R1</b>	Specifies the RADIUS server name.
<b>Step 4</b>	<b>dtls connectiontimeout</b> <i>timeout</i> <b>Example:</b> Device(config-radius-server) # <b>dtls connectiontimeout 1</b>	Configures RADIUS DTLS connection timeout. Here, <i>timeout</i> refers to the DTLS connection timeout value. The valid range is from 1 to 65535.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config-radius-server) # <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring RADIUS DTLS Idle Timeout

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b>	Enters privileged EXEC mode.

	Command or Action	Purpose
	Device# enable	
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>radius server</b> <i>server-name</i> <b>Example:</b> Device(config)# <b>radius server</b> R1	Specifies the RADIUS server name.
<b>Step 4</b>	<b>dtls idletimeout</b> <i>idle_timeout</i> <b>Example:</b> Device(config-radius-server)# <b>dtls idletimeout</b> 2	Configures RADIUS DTLS idle timeout. Here, <i>idle_timeout</i> refers to the DTLS idle timeout value. The valid range is from 1 to 65535.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config-radius-server)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring Source Interface for RADIUS DTLS Server

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# enable	Enters privileged EXEC mode.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>radius server</b> <i>server-name</i> <b>Example:</b> Device(config)# <b>radius server</b> R1	Specifies the RADIUS server name.
<b>Step 4</b>	<b>dtls ip</b> { <b>radius source-interface</b> <i>Ethernet-Internal interface_number</i> <b>Example:</b> Device(config-radius-server)# <b>dtls ip radius source-interface</b> <b>Ethernet-Internal</b> 0	Configures source interface for RADIUS DTLS server. Here, <ul style="list-style-type: none"> <li><i>interface_number</i> refers to the Ethernet-Internal interface number. The default value is 0.</li> </ul>

	Command or Action	Purpose
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Device(config-radius-server) # <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring RADIUS DTLS Port Number

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device# <b>enable</b>	Enters privileged EXEC mode.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>radius server</b> <i>server-name</i>  <b>Example:</b> Device(config)# <b>radius server R1</b>	Specifies the RADIUS server name.
<b>Step 4</b>	<b>dtls port</b> <i>port_number</i>  <b>Example:</b> Device(config-radius-server) # <b>dtls port</b> <b>2</b>	Configures RADIUS DTLS port number. Here, <i>port_number</i> refers to the DTLS port number.
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Device(config-radius-server) # <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring RADIUS DTLS Connection Retries

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device# <b>enable</b>	Enters privileged EXEC mode.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b>	Enters global configuration mode.

	Command or Action	Purpose
	Device# <code>configure terminal</code>	
<b>Step 3</b>	<b>radius server</b> <i>server-name</i> <b>Example:</b> Device(config)# <code>radius server R1</code>	Specifies the RADIUS server name.
<b>Step 4</b>	<b>dtls retries</b> <i>retry_number</i> <b>Example:</b> Device(config-radius-server)# <code>dtls retries 3</code>	Configures RADIUS connection retries. Here, <i>retry_number</i> refers to the DTLS connection retries. The valid range is from 1 to 65535.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config-radius-server)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring RADIUS DTLS Trustpoint

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# <code>enable</code>	Enters privileged EXEC mode.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<b>radius server</b> <i>server-name</i> <b>Example:</b> Device(config)# <code>radius server R1</code>	Specifies the RADIUS server name.
<b>Step 4</b>	<b>dtls trustpoint</b> { <i>client LINE dtls</i>   <i>server LINE dtls</i> } <b>Example:</b> Device(config-radius-server)# <code>dtls trustpoint client client1 dtls</code> Device(config-radius-server)# <code>dtls trustpoint server server1 dtls</code>	Configures trustpoint for client and server.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config-radius-server)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring DTLS Dynamic Author

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# enable	Enters privileged EXEC mode.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>aaa server radius dynamic-author</b> <b>Example:</b> Device(config)# <b>aaa server radius dynamic-author</b>	Configures local server profile for RFC 3576 support.
<b>Step 4</b>	<b>dtls</b> <b>Example:</b> Device(config-locsvr-da-radius)# <b>dtls</b>	Configures DTLS source parameters.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config-locsvr-da-radius)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Enabling DTLS for Client

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# enable	Enters privileged EXEC mode.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>aaa server radius dynamic-author</b> <b>Example:</b>	Configures local server profile for RFC 3576 support.

	Command or Action	Purpose
	Device(config)# <b>aaa server radius dynamic-author</b>	
<b>Step 4</b>	<b>client IP_addr dtls</b>  <b>Example:</b> Device(config-locsvr-da-radius)# <b>client 10.104.49.14 dtls</b>	Enables DTLS for the client.
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Device(config-locsvr-da-radius)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring Client Trustpoint for DTLS

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device# enable	Enters privileged EXEC mode.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>aaa server radius dynamic-author</b>  <b>Example:</b> Device(config)# <b>aaa server radius dynamic-author</b>	Configures local server profile for RFC 3576 support.
<b>Step 4</b>	<b>client IP_addr dtls {client-tp client-tp-name   server-tp server-tp-name}</b>  <b>Example:</b> Device(config-locsvr-da-radius)# <b>client 10.104.49.14 dtls client-tp client_tp_name</b>	Configures client trustpoint for DTLS.
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Device(config-locsvr-da-radius)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring DTLS Idle Timeout

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# enable	Enters privileged EXEC mode.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>aaa server radius dynamic-author</b> <b>Example:</b> Device(config)# <b>aaa server radius dynamic-author</b>	Configures local server profile for RFC 3576 support.
<b>Step 4</b>	<b>client <i>IP_addr</i> dtls idletimeout <i>timeout-interval</i> {<b>client-tp</b> <i>client_tp_name</i>   <b>server-tp</b> <i>server_tp_name</i>}</b> <b>Example:</b> Device(config-locsvr-da-radius)# <b>client 10.104.49.14 dtls idletimeout 62 client-tp dtls_ise</b>	Configures DTLS idle time. Here, <i>timeout-interval</i> refers to the idle timeout interval. The valid range is from 60 to 600.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config-locsvr-da-radius)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring Server Trustpoint for DTLS

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# enable	Enters privileged EXEC mode.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.



	Command or Action	Purpose
<b>Step 3</b>	<b>aaa server radius dynamic-author</b> <b>Example:</b> Device(config)# <b>aaa server radius dynamic-author</b>	Configures local server profile for RFC 3576 support.
<b>Step 4</b>	<b>client IP_addr dtls server-tp server_tp_name</b> <b>Example:</b> Device(config-locsvr-da-radius)# <b>client 10.104.49.14 dtls server-tp dtls_client</b>	Configures server trust point.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config-locsvr-da-radius)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Verifying the RADIUS DTLS Server Configuration

To view information about the DTLS enabled servers, use the following command:

```
Device# show aaa servers
DTLS: Packet count since last idletimeout 1,
Send handshake count 3,
Handshake Success 1,
Total Packets Transmitted 1,
Total Packets Received 1,
Total Connection Resets 2,
Connection Reset due to idle timeout 0,
Connection Reset due to No Response 2,
Connection Reset due to Malformed packet 0,
```

## Clearing RADIUS DTLS Specific Statistics

To clear the radius DTLS specific statistics, use the following command:

```
Device# clear aaa counters servers radius {<server-id> | all}
```



**Note** Here, *server-id* refers to the server ID displayed by **show aaa servers**. The valid range is from 0 to 2147483647.





## CHAPTER 46

# MAC Authentication Bypass

- [MAC Authentication Bypass, on page 407](#)
- [Configuring 802.11 Security for WLAN \(GUI\), on page 409](#)
- [Configuring 802.11 Security for WLAN \(CLI\), on page 410](#)
- [Configuring AAA for External Authentication, on page 410](#)
- [Configuring AAA for Local Authentication \(GUI\), on page 412](#)
- [Configuring AAA for Local Authentication \(CLI\), on page 412](#)
- [Configuring MAB for Local Authentication, on page 413](#)
- [Configuring MAB for External Authentication \(GUI\), on page 414](#)
- [Configuring MAB for External Authentication \(CLI\), on page 414](#)

## MAC Authentication Bypass

You can configure the embedded wireless controller to authorize clients based on the client MAC address by using the MAC authentication bypass (MAB) feature.

When MAB is enabled, the embedded wireless controller uses the MAC address as the client identity. The authentication server has a database of client MAC addresses that are allowed network access. After detecting a client, the embedded wireless controller waits for a packet from the client. The embedded wireless controller sends the authentication server a RADIUS-access/request frame with a username and password based on the MAC address. If authorization succeeds, the embedded wireless controller grants the client access to the network. If authorization fails, the embedded wireless controller assigns the port to the guest WLAN, if one is configured.

Clients that were authorized with MAC authentication bypass can be re-authenticated. The re-authentication process is the same as that for clients that were authenticated. During re-authentication, the port remains in the previously assigned WLAN. If re-authentication is successful, the embedded wireless controller keeps the port in the same WLAN. If re-authentication fails, the embedded wireless controller assigns the port to the guest WLAN, if one is configured.

### MAB Configuration Guidelines

- MAB configuration guidelines are the same as the 802.1x authentication guidelines.
- When MAB is disabled from a port after the port has been authorized with its MAC address, the port state is not affected.

- If the port is in the unauthorized state and the client MAC address is not in the authentication-server database, the port remains in the unauthorized state. However, if the client MAC address is added to the database, the switch can use MAC authentication bypass to re-authorize the port.
- If the port is in the authorized state, the port remains in this state until re-authorization occurs.
- You can configure a timeout period for hosts that are connected by MAB but are inactive. The valid range is from 1 to 65535, in seconds.




---

**Note** If wlan-profile-name is configured for a user, guest user authentication is allowed only from that WLAN. If wlan-profile-name is not configured for a user, guest user authentication is allowed on any WLAN.

---

If you want the client to connect to SSID1, but not to SSID2 using mac-filtering, ensure that you configure **aaa-override** in the policy profile.

In the following example, when a client with MAC address 1122.3344.0001 tries to connect to a WLAN, the request is sent to the local RADIUS server, which checks the presence of the client MAC address in its attribute list (FILTER\_1 and FILTER\_2). If the client MAC address is listed in an attribute list (FILTER\_1), the client is allowed to join the WLAN (WLAN\_1) that is returned as *ssid attribute* from the RADIUS server. The client is rejected, if the client MAC address is not listed in the attribute list.

#### Local RADIUS Server Configuration

```
!Configures an attribute list as FILTER_2
aaa attribute list FILTER_2
!Defines an attribute type that is to be added to an attribute list.
attribute type ssid "WLAN_2"

!Username with the MAC address is added to the filter
username 1122.3344.0002 mac aaa attribute list FILTER_2

!
aaa attribute list FILTER_1
attribute type ssid "WLAN_1"
username 1122.3344.0001 mac aaa attribute list FILTER_1
```

#### Controller Configuration

```
! Sets authorization to the local radius server
aaa authorization network MLIST_MACFILTER local

!A WLAN with the SSID WLAN_2 is created and MAC filtering is set along with security
parameters.
wlan WLAN_2 2 WLAN_2
mac-filtering MLIST_MACFILTER
no security wpa
no security wpa wpa2 ciphers

!WLAN with the SSID WLAN_1 is created and MAC filtering is set along with security parameters.
wlan WLAN_1 1 WLAN_1
mac-filtering MLIST_MACFILTER
no security wpa
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
security web-auth
security web-auth authentication-list WEBAUTH

! Policy profile to be associated with the above WLANs
```

```
wireless profile policy MAC_FILTER_POLICY
aaa-override
vlan 504
no shutdown
```

## Configuring 802.11 Security for WLAN (GUI)

### Procedure

---

- Step 1** Choose **Configuration** > **Tags & Profiles** > **WLANs**.
- Step 2** Click **Add** to create WLANs.  
The **Add WLAN** page is displayed.
- Step 3** In the **Security** tab, you can configure the following:
- Layer2
  - Layer3
  - AAA
- Step 4** In the **Layer2** tab, you can configure the following:
- a) Choose the **Layer2 Security Mode** from the following options:
    - None—No Layer 2 security.
    - WPA + WPA2—Wi-Fi Protected Access.
    - Static WEP—Static WEP encryption parameters.
  - b) Enable **MAC Filtering** if required. MAC Filtering is also known as MAC Authentication Bypass (MAB).
  - c) In the **Protected Management Frame** section, choose the **PMF** as *Disabled*, *Optional*, or *Required*. By default, the PMF is disabled.
  - d) In the **WPA Parameters** section, choose the following options, if required:
    - WPA Policy
    - WPA2 Policy
    - WPA2 Encryption
  - e) Choose an option for **Auth Key Mgmt**.
  - f) Choose the appropriate status for **Fast Transition** between APs.
  - g) Check the **Over the DS** check box to enable Fast Transition over a distributed system.
  - h) Enter the **Reassociation Timeout** value, in seconds. This is the time after which a fast transition reassociation times out.
  - i) Click **Save & Apply to Device**.
- Step 5** In the **Layer3** tab, you can configure the following:
- a) Check the **Web Policy** check box to use the web policy.
  - b) Choose the required **Webauth Parameter Map** value from the drop-down list.

- c) Choose the required **Authentication List** value from the drop down list.
- d) In the **Show Advanced Settings** section, check the **On Mac Filter Failure** check box.
- e) Enable the **Conditional Web Redirect** and **Splash Web Redirect**.
- f) Choose the appropriate IPv4 and IPv6 ACLs from the drop-down lists.
- g) Click **Save & Apply to Device**.

**Step 6**

In the **AAA** tab, you can configure the following:

- a) Choose an authentication list from the drop-down.
- b) Check the **Local EAP Authentication** check box to enable local EAP authentication on the WLAN. Also, choose the required **EAP Profile Name** from the drop-down list.
- c) Click **Save & Apply to Device**.

## Configuring 802.11 Security for WLAN (CLI)

Follow the procedure below to configure 802.11 security for WLAN:

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>wlan</b> <i>profile-name wlan-id ssid</i>  <b>Example:</b> Device(config)# wlan ha-wlan-dot1x-test 3 ha-wlan-dot1x-test	Configures the WLAN profile.
<b>Step 2</b>	<b>security dot1x authentication-list</b> <i>auth-list-name</i>  <b>Example:</b> Device(config-wlan)# security dot1x authentication-list default	Enables security authentication list for dot1x security.
<b>Step 3</b>	<b>no shutdown</b>  <b>Example:</b> Device(config-wlan)# no shutdown	Enables the WLAN.

## Configuring AAA for External Authentication

Follow the procedure given below to configure AAA for external authentication.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>radius server</b> <i>server-name</i>  <b>Example:</b>	Sets the radius server.

	Command or Action	Purpose
	<code>Device(config)# radius server ISE</code>	
<b>Step 2</b>	<b>address {ipv4   ipv6}radius-server-ip-address</b> <b>auth-port auth-port-no acct-port acct-port-no</b>  <b>Example:</b> <code>Device(config-radius-server)# address</code> <code>ipv4 9.2.58.90 auth-port 1812 acct-port</code> <code>1813</code>	Specifies the radius server address.
<b>Step 3</b>	<b>key key</b>  <b>Example:</b> <code>Device(config-radius-server)# key any123</code>	Sets the per-server encryption key.
<b>Step 4</b>	<b>exit</b>  <b>Example:</b> <code>Device(config-locsvr-da-radius)# exit</code>	Returns to the configuration mode.
<b>Step 5</b>	<b>aaa local authentication default</b> <b>authorization default</b>  <b>Example:</b> <code>Device(config)# aaa local authentication</code> <code>default authorization default</code>	Selects the default local authentication and authorization.
<b>Step 6</b>	<b>aaa new-model</b>  <b>Example:</b> <code>Device(config)# aaa new-model</code>	Creates a AAA authentication model. Enable new access control commands and functions.
<b>Step 7</b>	<b>aaa session-id common</b>  <b>Example:</b> <code>Device(config)# aaa session-id common</code>	Creates common session ID.
<b>Step 8</b>	<b>aaa authentication dot1x default group</b> <b>radius</b>  <b>Example:</b> <code>Device(config)# aaa authentication dot1x</code> <code>default group radius</code>	Configures authentication for the default dot1x method.
<b>Step 9</b>	<b>aaa authorization network default group</b> <b>radius</b>  <b>Example:</b> <code>Device(config)# aaa authorization</code> <code>network default group radius</code>	Configures authorization for network services.
<b>Step 10</b>	<b>dot1x system-auth-control</b>  <b>Example:</b> <code>Device(config)# dot1x</code> <code>system-auth-control</code>	Enables SysAuthControl.

## Configuring AAA for Local Authentication (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
  - Step 2** On the **Wireless Networks** page, click **Add**.
  - Step 3** In the **Add WLAN** window that is displayed, select **Security > AAA**.
  - Step 4** Select a value from the **Authentication List** drop-down.
  - Step 5** Check the **Local EAP Authentication** check box to enable local EAP authentication on the WLAN.
  - Step 6** Select a value from the **EAP Profile Name** drop-down.
  - Step 7** Click **Save & Apply to Device**.
- 

## Configuring AAA for Local Authentication (CLI)

Follow the procedure given below to configure AAA for local authentication.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>aaa authentication dot1x default local</b> <b>Example:</b> Device(config)# aaa authentication dot1x default local	Configures to use the default local RADIUS server.
<b>Step 2</b>	<b>aaa authorization network default local</b> <b>Example:</b> Device(config)# aaa authorization network default local	Configures authorization for network services.
<b>Step 3</b>	<b>aaa authorization credential-download            default local</b> <b>Example:</b> Device(config)# aaa authorization credential-download default local	Configures default database to download credentials from local server.
<b>Step 4</b>	<b>username mac-address mac</b> <b>Example:</b> Device(config)# username abcdabcdabcd mac	For MAC filtering using username, use the <b>username abcdabcdabcd mac</b> command.
<b>Step 5</b>	<b>aaa local authentication default authorization            default</b>	Configures the local authentication method list.



	Command or Action	Purpose
	<b>Example:</b> Device(config)# aaa local authentication default authorization default	
<b>Step 6</b>	<b>aaa new-model</b> <b>Example:</b> Device(config)# aaa new-model	Creates a AAA authentication model. Enable new access control commands and functions.
<b>Step 7</b>	<b>aaa session-id common</b> <b>Example:</b> Device(config)# aaa session-id common	Creates common session ID.

## Configuring MAB for Local Authentication

Follow the procedure given below to configure MAB for local authentication.

### Before you begin

Configure AAA local authentication.

Configure the username for WLAN configuration (local authentication) using **username mac-address mac** command.



**Note** The mac-address must be in the following format: *abcdabcdabcd*

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>wlan profile-name wlan-id</b> <b>Example:</b> wlan CR1_SSID_mab-local-default 1 CR1_SSID_mab-local-default	Specifies the WLAN name and ID.
<b>Step 2</b>	<b>mac-filtering default</b> <b>Example:</b> Device(config-wlan)# mac-filtering default	Sets MAC filtering support for the WLAN.
<b>Step 3</b>	<b>no security wpa</b> <b>Example:</b> Device(config-wlan)# no security wpa	Disables WPA security.

	Command or Action	Purpose
<b>Step 4</b>	<b>no security wpa akm dot1x</b>  <b>Example:</b> Device(config-wlan)# no security wpa akm dot1x	Disables security AKM for dot1x.
<b>Step 5</b>	<b>no security wpa wpa2</b>  <b>Example:</b> Device(config-wlan)# no security wpa wpa2	Disables WPA2 security.
<b>Step 6</b>	<b>no security wpa wpa2 ciphers aes</b>  <b>Example:</b> Device(config-wlan)# no security wpa wpa2 ciphers aes	Disables WPA2 ciphers for AES.
<b>Step 7</b>	<b>no shutdown</b>  <b>Example:</b> Device(config-wlan)# no shutdown	Enables the WLAN.

## Configuring MAB for External Authentication (GUI)

### Before you begin

Configure AAA external authentication.

### Procedure

- 
- Step 1** Choose **Configuration > Wireless > WLANs**.
  - Step 2** On the **Wireless Networks** page, click the name of the WLAN.
  - Step 3** In the **Edit WLAN** window, click the **Security** tab.
  - Step 4** In the **Layer2** tab, check the **MAC Filtering** check box to enable the feature.
  - Step 5** With MAC Filtering enabled, choose the **Authorization List** from the drop-down list.
  - Step 6** Save the configuration.
- 

## Configuring MAB for External Authentication (CLI)

Follow the procedure given below to configure MAB for external authentication.

### Before you begin

Configure AAA external authentication.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>wlan</b> <i>wlan-name wlan-id ssid-name</i> <b>Example:</b> <pre>wlan CR1_SSID_mab-ext-radius 3 CR1_SSID_mab-ext-radius</pre>	Specifies the WLAN name and ID.
<b>Step 2</b>	<b>mac-filtering</b> <i>list-name</i> <b>Example:</b> <pre>Device(config-wlan)# mac-filtering ewlc-radius</pre>	Sets the MAC filtering parameters. Here, <i>ewlc-radius</i> is an example for the <i>list-name</i>
<b>Step 3</b>	<b>no security wpa</b> <b>Example:</b> <pre>Device(config-wlan)# no security wpa</pre>	Disables WPA security.
<b>Step 4</b>	<b>no security wpa akm dot1x</b> <b>Example:</b> <pre>Device(config-wlan)# no security wpa akm dot1x</pre>	Disables security AKM for dot1x.
<b>Step 5</b>	<b>no security wpa wpa2</b> <b>Example:</b> <pre>Device(config-wlan)# no security wpa wpa2</pre>	Disables WPA2 security.
<b>Step 6</b>	<b>mab request format attribute</b> {1 <b>groupsize</b> <i>size separator separator</i> [ <b>lowercase</b>   <b>uppercase</b> ]   2 {0   7   <b>LINE</b> } <b>LINE</b> <i>password</i>   32 <b>vlan access-vlan</b> } <b>Example:</b> <pre>Device(config)# mab request format attribute 1 groupsize 4 separator</pre>	Optional. Configures the delimiter while using MAC filtering in a WLAN. Here, <b>1-</b> Specifies the username format used for MAB requests. <b>groupsize size-</b> Specifies the number of hex digits per group. The valid values range from 1 to 12. <b>separator separator-</b> Specifies how to separate groups. The separators are comma, semicolon, and full stop. <b>lowercase-</b> Specifies the username in lowercase format. <b>uppercase-</b> Specifies the username in uppercase format. <b>2-</b> Specifies the global password used for all the MAB requests. <b>0-</b> Specifies the unencrypted password.

	Command or Action	Purpose
		<p>7- Specifies the hidden password.</p> <p><b>LINE</b>- Specifies the encrypted or unencrypted password.</p> <p><i>password</i>- LINE password.</p> <p><b>32</b>- Specifies the NAS-Identifier attribute.</p> <p><b>vlan</b>- Specifies a VLAN.</p> <p><b>access-vlan</b>- Specifies the configured access VLAN.</p>
<b>Step 7</b>	<p><b>no security wpa wpa2 ciphers aes</b></p> <p><b>Example:</b></p> <pre>Device(config-wlan)# no security wpa wpa2 ciphers aes</pre>	Disables WPA2 ciphers for AES.
<b>Step 8</b>	<p><b>no shutdown</b></p> <p><b>Example:</b></p> <pre>Device(config-wlan)# no shutdown</pre>	Enables the WLAN.



## CHAPTER 47

# Dynamic Frequency Selection

---

- [Information About Dynamic Frequency Selection, on page 417](#)
- [Configuring Dynamic Frequency Selection \(GUI\), on page 417](#)
- [Configuring Dynamic Frequency Selection, on page 417](#)
- [Verifying DFS, on page 418](#)

## Information About Dynamic Frequency Selection

Dynamic Frequency Selection (DFS) is the process of detecting radar signals and automatically setting the frequency on a DFS-enabled 5.0-GHz (802.11a/h) radio to avoid interference with the radar signals. Radios configured for use in a regulatory domain must not interfere with radar systems.

In normal DFS, when a radar signal is detected on any of the channels in the 40-MHz or 80-MHz bandwidth, the whole channel is blocked. With Flex DFS, if the radar signals are not detected on the secondary channel, the AP is moved to a secondary channel with a reduction in the bandwidth, usually, by half.

## Configuring Dynamic Frequency Selection (GUI)

### Procedure

---

- Step 1** Choose **Configuration > Wireless > Mesh > Profiles**
  - Step 2** Choose a profile.
  - Step 3** In **General** tab, check the **Full sector DFS status** check box.
  - Step 4** Click **Update & Apply to Device**.
- 

## Configuring Dynamic Frequency Selection

Follow the procedure given below to configure DFS:

**Before you begin**

- The corresponding AP must be on one of the DFS channels.
- Shut down the radio before applying the configuration changes.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>no ap dot11 5ghz dtpc</b> <b>Example:</b> Device(config)# no ap dot11 5ghz dtpc	Disables the 802.11a Dynamic Transmit Power Control (DTPC) setting.
<b>Step 3</b>	<b>ap dot11 5ghz channelswitch mode <i>mode-num</i></b> <b>Example:</b> Device(config)# ap dot11 5ghz channelswitch mode 1	Configures the 802.11h channel switch mode.
<b>Step 4</b>	<b>ap dot11 5ghz power-constraint <i>value</i></b> <b>Example:</b> Device(config)# ap dot11 5ghz power-constraint 12	Configures the 802.11h power-constraint value.
<b>Step 5</b>	<b>ap dot11 5ghz smart-dfs</b> <b>Example:</b> Device(config)# ap dot11 5ghz smart-dfs	Configures nonoccupancy time for the radar interference channel.

## Verifying DFS

Use the following commands to verify the DFS configuration:

To display the 802.11h configuration, use the following command:

```
Device# show wireless dot11h
```

To display the auto-rF information for 802.11h configuration, use the following command:

```
Device# show ap auto-rf dot11 5ghz
```

To display the auto-rF information for a Cisco AP, use the following command:

```
Device# show ap name ap1 auto-rf dot11 5gh
```



## CHAPTER 48

# Managing Rogue Devices

- [Rogue Detection](#), on page 419
- [Rogue Location Discovery Protocol \(RLDP\)](#), on page 429
- [Rogue Detection Security Level](#), on page 435
- [Setting Rogue Detection Security-level](#), on page 436
- [Wireless Service Assurance Rogue Events](#), on page 437

## Rogue Detection

### Rogue Devices

Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain-text or other denial-of-service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as usernames and passwords. The hacker can then transmit a series of Clear to Send (CTS) frames. This action mimics an access point, informing a particular client to transmit, and instructing all the other clients to wait, which results in legitimate clients being unable to access network resources. Wireless LAN service providers have a strong interest in banning rogue access points from the air space.

Because rogue access points are inexpensive and readily available, employees sometimes plug unauthorized rogue access points into existing LANs and build ad hoc wireless networks without their IT department's knowledge or consent. These rogue access points can be a serious breach of network security because they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions. There is an increased chance of enterprise security breach when wireless users connect to access points in the enterprise network.

The following are some guidelines to manage rogue devices:

- The access points are designed to serve associated clients. These access points spend relatively less time performing off-channel scanning: about 50 milliseconds on each channel. If you want to detect a large number of rogue APs and clients with high sensitivity, a monitor mode access point must be used. Alternatively, you can reduce the scan intervals from 180 seconds to a lesser value, for example, 120 or 60 seconds, ensuring that the radio goes off-channel more frequently, which improves the chances of rogue detection. However, the access point continues to spend about 50 milliseconds on each channel.

- Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect many rogue devices.
- Client card implementation might mitigate the effectiveness of containment. This normally happens when a client might quickly reconnect to the network after receiving a "de-association/de-authentication" frame, so it might still be able to pass some traffic. However, the browsing experience of the rogue client would be badly affected when it is contained.
- It is possible to classify and report rogue access points by using rogue states and user-defined classification rules that enable rogues to automatically move between states.
- Each controller limits the number of rogue containments to three and six per radio for access points in the monitor mode.
- When manual containment is performed using configuration, the rogue entry is retained even after the rogue entry expires.
- When a rogue entry expires, the managed access points are instructed to stop any active containment on it.
- When Validate Rogue Clients Against AAA is enabled, the controller requests the AAA server for rogue client validation only once. As a result, if rogue client validation fails on the first attempt then the rogue client will not be detected as a threat any more. To avoid this, add the valid client entries in the authentication server before enabling Validate Rogue Clients Against AAA.

### Restrictions on Rogue Detection

- Rogue containment is not supported on DFS channels.

A rogue access point is moved to a contained state either automatically or manually. The controller selects the best available access point for containment and pushes the information to the access point. The access point stores the list of containments per radio. For auto containment, you can configure the controller to use only the monitor mode access point. The containment operation occurs in the following two ways:

- The container access point goes through the list of containments periodically and sends unicast containment frames. For rogue access point containment, the frames are sent only if a rogue client is associated.
- Whenever a contained rogue activity is detected, containment frames are transmitted.

Individual rogue containment involves sending a sequence of unicast disassociation and deauthentication frames.

## AP Impersonation Detection

The various methods to detect AP impersonation are:

- AP impersonation can be detected if a managed AP reports itself as Rogue. This method is always enabled and no configuration is required.
- AP impersonation detection is based on MFP.

Infrastructure MFP protects 802.11 session management functions by adding message integrity check (MIC) information elements, to the management frames sent by APs (and not those sent by clients), which are then validated by other APs in the network. If infrastructure MFP is enabled, the managed APs check if the MIC



information elements are present and if MIC information elements are as expected. If either of these conditions is not fulfilled, the managed AP sends rogue AP reports with updated AP authentication failure counter.

## Configuring Rogue Detection (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > AP Join**.
  - Step 2** Click the **AP Join Profile Name** to edit the AP join profile properties.
  - Step 3** In the **Edit AP Join Profile** window, click the **Rogue AP** tab.
  - Step 4** Check the **Rogue Detection** check box to enable rogue detection.
  - Step 5** In the **Rogue Detection Minimum RSSI** field, enter the RSSI value.
  - Step 6** In the **Rogue Detection Transient Interval** field, enter the interval in seconds.
  - Step 7** In the **Rogue Detection Report Interval** field, enter the report interval value in seconds.
  - Step 8** In the **Rogue Detection Client Number Threshold** field, enter the threshold for rogue client detection.
  - Step 9** Check the **Auto Containment on FlexConnect Standalone** check box to enable auto containment.
  - Step 10** Click **Update & Apply to Device**.
- 

## Configuring Rogue Detection (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ap profile <i>profile-name</i> rogue detection min-transient-time <i>time in seconds</i></b>  <b>Example:</b> Device(config)# <code>ap profile profile1</code>  Device(config)# <code>rogue detection min-transient-time 120</code>	Specify the time interval at which rogues have to be consistently scanned for by APs after the first time the rogues are scanned.  Valid range for the time in sec parameter is 120 seconds to 1800 seconds, and the default value is 0.

	Command or Action	Purpose
		<p><b>Note</b> This feature is applicable to all AP modes.</p> <p>Using the transient interval values, you can control the time interval at which APs should scan for rogues. APs can also filter the rogues based on their transient interval values.</p> <p>This feature has the following advantages:</p> <ul style="list-style-type: none"> <li>• Rogue reports from APs to the controller are shorter</li> <li>• Transient rogue entries are avoided in the controller</li> </ul> <p>Unnecessary memory allocation for transient rogues are avoided</p>
<b>Step 3</b>	<p><b>ap profile <i>profile-name</i> rogue detection containment {auto-rate   flex-rate}</b></p> <p><b>Example:</b></p> <pre>Device(config)# ap profile profile1 Device(config)# rogue detection containment flex-rate</pre>	Specifies the rogue containment options. The <b>auto-rate</b> option enables auto-rate for containment of rogues. The <b>flex-rate</b> option enables rogue containment of standalone flexconnect APs.
<b>Step 4</b>	<p><b>ap profile <i>profile-name</i> rogue detection enable</b></p> <p><b>Example:</b></p> <pre>Device(config)# ap profile profile1</pre>	Enables rogue detection on all APs.
<b>Step 5</b>	<p><b>ap profile <i>profile-name</i> rogue detection report-interval <i>time in seconds</i></b></p> <p><b>Example:</b></p> <pre>Device(config)# ap profile profile1 Device(config)# rogue detection report-interval 120</pre>	<p>Configures rogue report interval for monitor mode Cisco APs.</p> <p>The valid range for reporting the interval in seconds is 10 seconds to 300 seconds.</p>

## Configuring RSSI Deviation Notification Threshold for Rogue APs (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p>	Enters global configuration mode.

	Command or Action	Purpose
	Device# <code>configure terminal</code>	
<b>Step 2</b>	<b>wireless wps rogue ap notify-rssi-deviation</b>  <b>Example:</b> Device(config)# <code>wireless wps rogue ap notify-rssi-deviation</code>	Configures RSSI deviation notification threshold for Rogue APs.
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Device(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring Management Frame Protection (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Security > Wireless Protection Policies**.
  - Step 2** In the **Rogue Policy** tab, under the **MFP Configuration** section, check the **Global MFP State** check box and the **AP Impersonation Detection** check box to enable the global MFP state and the AP impersonation detection, respectively.
  - Step 3** In the **MFP Key Refresh Interval** field, specify the refresh interval in hours.
  - Step 4** Click **Apply**.
- 

## Configuring Management Frame Protection (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless wps mfp</b>  <b>Example:</b> Device(config)# <code>wireless wps mfp</code>	Configures a management frame protection.
<b>Step 3</b>	<b>wireless wps mfp {ap-impersonation   key-refresh-interval}</b>  <b>Example:</b> Device(config)# <code>wireless wps mfp ap-impersonation</code>	Configures ap impersonation detection (or) MFP key refresh interval in hours.  key-refresh-interval—Refers to the MFP key refresh interval in hours. The valid range is from 1 to 24. Default value is 24.

	Command or Action	Purpose
	Device(config)# wireless wps mfp key-refresh-interval	
<b>Step 4</b>	<b>end</b>  <b>Example:</b> Device(config)# end	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.

## Verifying Management Frame Protection

To verify if the Management Frame Protection (MFP) feature is enabled or not, use the following command:

```
Device# show wireless wps summary
Client Exclusion Policy
  Excessive 802.11-association failures : unknown
  Excessive 802.11-authentication failures: unknown
  Excessive 802.1x-authentication      : unknown
  IP-theft                             : unknown
  Excessive Web authentication failure  : unknown
  Failed Qos Policy                    : unknown

Management Frame Protection
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection     : Disabled
  Key refresh interval           : 15
```

To view the MFP details, use the following command:

```
Device# show wireless wps mfp summary
Management Frame Protection
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection     : Disabled
  Key refresh interval           : 15
```

## Verifying Rogue Events

To verify the rogue event history, run the **show wireless wps rogue ap detailed** command:

```
Device# show wireless wps rogue ap detailed d8b1.901c.3cfd

Rogue Event history

Timestamp                #Times Class/State Event                Ctx
-----
---
05/01/2020 08:37:03.55645 41616 Mal/CPend FSM_GOTO                ContPending (NotContYet)
0x0
05/01/2020 08:37:03.55427 28163 Mal/CPend EXPIRE_TIMER_START    1200s
0x0
05/01/2020 08:37:03.55380 28163 Mal/CPend RECV_REPORT           38ed.18cf.83e0/1
0x0
05/01/2020 08:36:54.659136 7356 Mal/CPend NO_OP_UPDATE
0x0
05/01/2020 08:36:33.347132 3185 Mal/CPend CHANNEL_CHANGE      e4aa.5d44.fec0/2,36->40
0x0
05/01/2020 08:25:19.573720 247 Mal/CPend LRAD_EXPIRE           7c21.0e41.0700/0
0x0
```

```

04/30/2020 07:55:37.977450 2 Mal/CPend PMF_CONTAINMENT ContPending (PMFDetected) 0x0
04/30/2020 07:55:37.977242 1 Unc/Alert INIT_TIMER_DONE 0xab9800439e00024f
0x0
04/30/2020 07:52:33.600332 1 Unk/Init INIT_TIMER_START 180s
0x0
04/30/2020 07:52:33.600326 1 Unk/Init CREATE
0x0

```

To verify the impersonations detected due to authentication errors, use the following command:

```
Device# show wireless wps rogue ap detailed
```

```

Rogue BSSID : 0062.ecf3.8d30
Last heard Rogue SSID : rogueA
802.11w PMF required : No
Is Rogue an impersonator : Yes
Is Rogue on Wired Network : No
Classification : Malicious
Manually Contained : No
State : Threat
First Time Rogue was Reported : 01/07/2020 15:51:01
Last Time Rogue was Reported : 01/08/2020 08:08:35

Number of clients : 0

Reported By
  AP Name : AP38ED.18CE.45E0
  MAC Address : 38ed.18cf.83e0
  Detecting slot ID : 0
  Radio Type : dot11g, dot11n - 2.4 GHz
  SSID : rogueA
  Channel : 6 (From DS)
  Channel Width : 20 MHz
  RSSI : -33 dBm
  SNR : 52 dB
  ShortPreamble : Disabled
  Security Policy : WPA2/WPA/FT
  Last reported by this AP : 01/08/2020 08:02:53
  Authentication Failure Count : 237

```

## Verifying Rogue Detection

This section describes the new command for rogue detection.

The following command can be used to verify rogue detection on the device.

**Table 10: Verifying Adhoc Rogues Information**

Command	Purpose
<b>show wireless wps rogue adhoc detailed</b> <i>mac_address</i>	Displays the detailed information for an Adhoc rogue.
<b>show wireless wps rogue adhoc summary</b>	Displays a list of all Adhoc rogues.

Table 11: Verifying Rogue AP Information

Command	Purpose
<b>show wireless wps rogue ap clients</b> <i>mac_address</i>	Displays the list of all rogue clients associated with a rogue.
<b>show wireless wps rogue ap custom summary</b>	Displays the custom rogue AP information.
<b>show wireless wps rogue ap detailed</b> <i>mac_address</i>	Displays the detailed information for a rogue AP.
<b>show wireless wps rogue ap friendly summary</b>	Displays the friendly rogue AP information.
<b>show wireless wps rogue ap list</b> <i>mac_address</i>	Displays the list of rogue APs detected by a given AP.
<b>show wireless wps rogue ap malicious summary</b>	Displays the malicious rogue AP information.
<b>show wireless wps rogue ap summary</b>	Displays a list of all Rogue APs.
<b>show wireless wps rogue ap unclassified summary</b>	Displays the unclassified rogue AP information.

Table 12: Verifying Rogue Auto-Containment Information

Command	Purpose
<b>show wireless wps rogue auto-contain</b>	Displays the rogue auto-containment information.

Table 13: Verifying Classification Rule Information

Command	Purpose
<b>show wireless wps rogue rule detailed</b> <i>rule_name</i>	Displays the detailed information for a classification rule.
<b>show wireless wps rogue rule summary</b>	Displays the list of all rogue rules.

Table 14: Verifying Rogue Statistics

Command	Purpose
<b>show wireless wps rogue stats</b>	Displays the rogue statistics.

Table 15: Verifying Rogue Client Information

Command	Purpose
<b>show wireless wps rogue client detailed</b> <i>mac_address</i>	Displays detailed information for a Rogue client.
<b>show wireless wps rogue client summary</b>	Displays a list of all the Rogue clients.

Table 16: Verifying Rogue Ignore List

Command	Purpose
<code>show wireless wps rogue ignore-list</code>	Displays the rogue ignore list.

## Examples: Rogue Detection Configuration

This example shows how to configure the minimum RSSI that a detected rogue AP needs to be at, to have an entry created in the device:

```
Device# wireless wps rogue ap notify-min-rssi 100
```

This example shows how to configure the classification interval:

```
Device# configure terminal
Device(config)#
Device(config)#
Device(config)# end
Device# show wireless wps rogue client /show wireless wps rogue ap summary
```

## Configuring Rogue Policies (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Security > Wireless Protection Policies**.
  - Step 2** In the **Rogue Policies** tab, use the **Rogue Detection Security Level** drop-down to select the security level.
  - Step 3** In the **Expiration timeout for Rogue APs (seconds)** field, enter the timeout value.
  - Step 4** Select the **Validate Rogue Clients against AAA** check box to validate rogue clients against AAA server.
  - Step 5** Select the **Validate Rogue APs against AAA** check box to validate rogue access points against AAA server.
  - Step 6** In the **Rogue Polling Interval (seconds)** field, enter the interval to poll the AAA server for rogue information.
  - Step 7** Select the **Detect and Report Adhoc Networks** check box to enable detection of rogue adhoc networks.
  - Step 8** In the **Rogue Detection Client Number Threshold** field, enter the threshold to generate SNMP trap.
  - Step 9** In the **Auto Contain** section, enter the following details.
  - Step 10** Use the **Auto Containment Level** drop-down to select the level.
  - Step 11** Select the **Auto Containment only for Monitor Mode APs** check box to limit the auto-containment only to monitor mode APs.
  - Step 12** Select the **Rogue on Wire** check box to limit the auto-containment only to rogue APs on wire.
  - Step 13** Select the **Using our SSID** check box to limit the auto-containment only to rogue APs using one of the SSID configured on the controller.
  - Step 14** Select the **Adhoc Rogue AP** check box to limit the auto-containment only to adhoc rogue APs.
  - Step 15** Click **Apply**.
-

## Configuring Rogue Policies (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless wps rogue ap timeout <i>number of seconds</i></b> <b>Example:</b> Device(config)# <code>wireless wps rogue ap timeout 250</code>	Configures the expiration time for rogue entries, in seconds. Valid range for the time in seconds 240 seconds to 3600 seconds.
<b>Step 3</b>	<b>wireless wps rogue client notify-min-rssi <i>RSSI threshold</i></b> <b>Example:</b> Device(config)# <code>wireless wps rogue client notify-min-rssi -128</code>	Configures the minimum RSSI notification threshold for rogue clients. Valid range for the RSSI threshold in dB is -128 - dB to -70 dB.
<b>Step 4</b>	<b>wireless wps rogue client notify-min-deviation <i>RSSI threshold</i></b> <b>Example:</b> Device(config)# <code>wireless wps rogue client notify-min-deviation 4</code>	Configures the RSSI deviation notification threshold for rogue clients. Valid range for the RSSI threshold in dB is 0 dB to 10 dB.
<b>Step 5</b>	<b>wireless wps rogue ap aaa polling-interval <i>AP AAA Interval</i></b> <b>Example:</b> Device(config)# <code>wireless wps rogue ap aaa polling-interval 120</code>	Configures rogue AP AAA validation interval. The valid range for the AP AAA interval in seconds is 60 seconds to 86400 seconds.
<b>Step 6</b>	<b>wireless wps rogue adhoc</b> <b>Example:</b> Device(config)# <code>wireless wps rogue adhoc</code>	Enables detecting and reporting adhoc rogue (IBSS).
<b>Step 7</b>	<b>wireless wps rogue client client-threshold <i>threshold</i></b> <b>Example:</b> Device(config)# <code>wireless wps rogue client client-threshold 100</code>	Configures the rogue client per a rogue AP SNMP trap threshold. The valid range for the threshold is 0 to 256.



# Rogue Location Discovery Protocol (RLDP)

## Rogue Location Discovery Protocol

Rogue Location Discovery Protocol (RLDP) is an active approach, which is used when rogue AP has no authentication (Open Authentication) configured. This mode, which is disabled by default, instructs an active AP to move to the rogue channel and connect to the rogue as a client. During this time, the active AP sends de-authentication messages to all connected clients and then shuts down the radio interface. Then, it associates to the rogue AP as a client. The AP then tries to obtain an IP address from the rogue AP and forwards a User Datagram Protocol (UDP) packet (port 6352) that contains the local AP and rogue connection information to the controller through the rogue AP. If the controller receives this packet, the alarm is set to notify the network administrator that a rogue AP was discovered on the wired network with the RLDP feature. RLDP has 100 % accuracy in rogue AP detection. It detects Open APs and NAT APs.

Following are some guidelines to manage RLDP:

- Rogue Location Discovery Protocol (RLDP) detects rogue access points that are configured for open authentication.
- RLDP detects rogue access points that use a broadcast Basic Service Set Identifier (BSSID), that is, the access point broadcasts its Service Set Identifier in beacons.
- RLDP detects only those rogue access points that are on the same network. If an access list in the network prevents the sending of RLDP traffic from the rogue access point to the embedded wireless controller, RLDP does not work.
- RLDP does not work on 5-GHz Dynamic Frequency Selection (DFS) channels.
- If RLDP is enabled on mesh APs, and the APs perform RLDP tasks, the mesh APs are dissociated from the embedded wireless controller. The workaround is to disable RLDP on mesh APs.
- If RLDP is enabled on non-monitor APs, client connectivity outages occur when RLDP is in process.

The following steps describe the functioning of RLDP:

1. Identify the closest Unified AP to the rogue using signal strength values.
2. The AP then connects to the rogue as a WLAN client, attempting three associations before timing out.
3. If association is successful, the AP then uses DHCP to obtain an IP address.
4. If an IP address was obtained, the AP (acting as a WLAN client) sends a UDP packet to each of the embedded wireless controller's IP addresses.
5. If the embedded wireless controller receives even one of the RLDP packets from the client, that rogue is marked as on-wire.



---

**Note** The RLDP packets are unable to reach the embedded wireless controller if filtering rules are placed between the embedded wireless controller's network and the network where the rogue device is located.

---

The embedded wireless controller continuously monitors all the nearby access points and automatically discovers and collects information on rogue access points and clients. When the embedded wireless controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP), if RLDP is enabled, to determine if the rogue is attached to your network.

Embedded Wireless Controller initiates RLDP on rogue devices that have open . If RLDP uses FlexConnect or local mode access points, then clients are disconnected for that moment. After the RLDP cycle, the clients are reconnected to the access points. As and when rogue access points are seen , the RLDP process is initiated.

You can configure the embedded wireless controller to use RLDP on all the access points or only on the access points configured for the monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded radio frequency (RF) space, allowing monitoring without creating unnecessary interference and without affecting the regular data access point functionality. If you configure the embedded wireless controller to use RLDP on all the access points, the embedded wireless controller always chooses the monitor access point for RLDP operation if a monitor access point and a local (data) access point are both nearby. If RLDP determines that the rogue is on your network, you can choose to contain the detected rogue either manually or automatically.

RLDP detects on wire presence of the rogue access points that are configured with open authentication only once, which is the default retry configuration. Retries can be configured using the .

You can initiate or trigger RLDP from embedded wireless controller in three ways:

1. Enter the RLDP initiation command manually from the embedded wireless controller CLI.
2. Schedule RLDP from the embedded wireless controller CLI.
3. Auto RLDP. You can configure auto RLDP on embedded wireless controller either from embedded wireless controller CLI or GUI but keep in mind the following guidelines:
  - The auto RLDP option can be configured only when the rogue detection security level is set to custom.
  - Either auto RLDP or schedule of RLDP can be enabled at a time.

### Restrictions for RLDP

- RLDP only works with open rogue APs broadcasting their SSID with authentication and encryption disabled.
- RLDP requires that the Managed AP acting as a client is able to obtain an IP address via DHCP on the rogue network.
- Manual RLDP can be used to attempt an RLDP trace on a rogue multiple number of times.
- During RLDP process, the AP is unable to serve clients. This negatively impacts performance and connectivity for local mode APs. To avoid this case, RLDP can be selectively enabled for Monitor Mode AP only.
- RLDP does not attempt to connect to a rogue AP operating in a 5GHz DFS channel.
- RLDP is supported only on Cisco IOS APs.

## Configuring RLDP for Generating Alarms (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Security > Wireless Protection Policies**.
- Step 2** In the **RLDP** tab, use the **Rogue Location Discovery Protocol** drop-down to select one of the following options:
- Disable**: Disables RLDP on all the access points. **Disable** is the default option.
  - All APs**: Enables RLDP on all APs.
  - Monitor Mode APs**: Enables RLDP only on APs in the monitor mode.
- Note** The **Schedule RLDP** check box is enabled only if the **Disable** option is selected. The Schedule RLDP check box remains disabled when you select the **All APs** option or the **Monitor Mode APs** option.
- Step 3** In the **Retry Count** field, specify the number of retries that should be attempted. The range allowed is between 1 and 5.
- Step 4** Click **Apply**.
- 

## Configuring an RLDP for Generating Alarms (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless wps rogue ap rldp alarm-only</b> <b>&lt;monitor-ap-only&gt;</b> <b>Example:</b> Device(config)# <code>wireless wps rogue ap rldp alarm-only</code> Device(config)# <code>wireless wps rogue ap rldp alarm-only monitor-ap-only</code>	Enables RLDP to generate alarms. In this method, the RLDP is always enabled. The <b>monitor-ap-only</b> keyword is optional. The command with just the <b>alarm-only</b> keyword enables RLDP without any restriction on the AP mode. The command with <b>alarm-only</b> <b>&lt;monitor-ap-only&gt;</b> keyword enables RLDP in monitor mode access points only.
<b>Step 3</b>	<b>end</b> <b>Example:</b> Device(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring a Schedule for RLDP (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Security > Wireless Protection Policies**.
- Step 2** In the **RLDP** tab, choose the following options from the **Rogue Location Discovery Protocol** drop-down list:
- **Disable (default)**: Disables RLDP on all the access points.
- Step 3** In the **Retry Count** field, specify the number of retries that should be attempted. Provide a valid range between 1 to 5.
- Step 4** Check the **Schedule RLDP** check box and then specify the days, start time, and end time for the process to take place.
- Step 5** Click **Apply**.
- 

## Configuring a Schedule for RLDP (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless wps rogue ap rldp schedule day <i>day</i> start <i>start-time</i> end <i>end-time</i></b>  <b>Example:</b> Device(config)# <code>wireless wps rogue ap rldp schedule day Monday start 10:10:01 end 12:00:00</code>	Enables RLDP based on a scheduled day, start time, and end time.  Here, <i>day</i> is the day when the RLDP scheduling can be done. The values are Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday.  <i>start-time</i> is the start time for scheduling RLDP for the day. You need to enter start time in <b>HH:MM:SS</b> format.  <i>end-time</i> is the end time for scheduling RLDP for the day. You need to enter end time in <b>HH:MM:SS</b> format.
<b>Step 3</b>	<b>wireless wps rogue ap rldp schedule</b>  <b>Example:</b> Device(config)# <code>wireless wps rogue ap rldp schedule</code>	Enables the schedule.

	Command or Action	Purpose
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring an RLDP for Auto-Contain (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Security > Wireless Protection Policies**.
- Step 2** In the **Rogue Policies** tab, under the **Auto Contain** section, check the **Rogue on Wire** checkbox.
- Step 3** Click **Apply**.
- 

## Configuring an RLDP for Auto-Contain (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless wps rogue ap rldp auto-contain [monitor-ap-only]</b> <b>Example:</b> Device(config)# <b>wireless wps rogue ap rldp auto-contain</b> Device(config)# <b>wireless wps rogue ap rldp auto-contain monitor-ap-only</b>	Enables RLDP to perform auto-contain. In this method, the RLDP is always enabled. The <b>monitor-ap-only</b> keyword is optional. The command with just the <b>auto-contain</b> keyword enables RLDP without any restriction on the AP mode. The command with <b>auto-contain &lt;monitor-ap-only&gt;</b> keyword enables RLDP in monitor mode access points only.
<b>Step 3</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring RLDP Retry Times on Rogue Access Points (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Security > Wireless Protection Policies**.
- Step 2** On the **Wireless Protection Policies** page, click the **RLDP** tab.
- Step 3** Enter the RLDP retry attempt value for rogue access points in the **Retry Count** field.  
The valid range is between 1 and 5.
- Step 4** Save the configuration.
- 

## Configuring RLDP Retry Times on Rogue Access Points (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless wps rogue ap rldp retries</b> <i>num-entries</i>  <b>Example:</b> Device(config)# <code>wireless wps rogue ap rldp retries 2</code>	Enables RLDP retry times on rogue access points.  Here, <i>num-entries</i> is the number of RLDP retry times for each of the rogue access points.  The valid range is 1 to 5.
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Device(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Verifying Rogue AP RLDP

The following commands can be used to verify rogue AP RLDP:

*Table 17: Verifying Rogue AP Information*

Command	Purpose
<code>show wireless wps rogue ap rldp detailed</code> <i>mac_address</i>	Displays the RLDP details for a rogue AP.
<code>show wireless wps rogue ap rldp in progress</code>	Displays the list of in-progress RLDP.

<code>show wireless wps rogue ap rldp summary</code>	Displays the summary of RLDP scheduling information.
--	--

## Rogue Detection Security Level

The rogue detection security level configuration allows you to set rogue detection parameters.

The available security levels are:

- Critical: Basic rogue detection for highly sensitive deployments.
- High: Basic rogue detection for medium-scale deployments.
- Low: Basic rogue detection for small-scale deployments.
- Custom: Default security-level, where all detection parameters are configurable.



**Note** When in Critical, High or Low, some rogue parameters are fixed and cannot be configured.

The following table shows parameter details for the three predefined levels:

**Table 18: Rogue Detection: Predefined Levels**

Parameter	Critical	High	Low
Cleanup Timer	3600	1200	240
AAA Validate Clients	Disabled	Disabled	Disabled
Adhoc Reporting	Enabled	Enabled	Enabled
Monitor-Mode Report Interval	10 seconds	30 seconds	60 seconds
Minimum RSSI	-128 dBm	-80 dBm	-80 dBm
Transient Interval	600 seconds	300 seconds	120 seconds
Auto Contain Works only on Monitor Mode APs.	Disabled	Disabled	Disabled
Auto Contain Level	1	1	1
Auto Contain Same-SSID	Disabled	Disabled	Disabled
Auto Contain Valid Clients on Rogue AP	Disabled	Disabled	Disabled
Auto Contain Adhoc	Disabled	Disabled	Disabled

Parameter	Critical	High	Low
Containment Auto-Rate	Enabled	Enabled	Enabled
Validate Clients with CMX	Enabled	Enabled	Enabled
Containment FlexConnect	Enabled	Enabled	Enabled
RLDP	Monitor-AP if RLDP scheduling is disabled.	Monitor-AP if RLDP scheduling is disabled	Disabled
Auto Contain RLDP	Disabled	Disabled	Disabled

## Setting Rogue Detection Security-level

Follow the procedure given below to set the rogue detection security-level:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters the global configuration mode.
<b>Step 2</b>	<b>wireless wps rogue security-level custom</b> <b>Example:</b> Device(config)# wireless wps rogue security-level custom	Configures rogue detection security level as custom.
<b>Step 3</b>	<b>wireless wps rogue security-level low</b> <b>Example:</b> Device(config)# wireless wps rogue security-level low	Configures rogue detection security level for basic rogue detection setup for small-scale deployments.
<b>Step 4</b>	<b>wireless wps rogue security-level high</b> <b>Example:</b> Device(config)# wireless wps rogue security-level high	Configures rogue detection security level for rogue detection setup for medium-scale deployments.
<b>Step 5</b>	<b>wireless wps rogue security-level critical</b> <b>Example:</b> Device(config)# wireless wps rogue security-level critical	Configures rogue detection security level for rogue detection setup for highly sensitive deployments.



# Wireless Service Assurance Rogue Events

Wireless Service Assurance (WSA) rogue events, supported in Release 16.12.x and later releases, consist of telemetry notifications for a subset of SNMP traps. WSA rogue events replicate the same information that is part of the corresponding SNMP trap.

For all the exported events, the following details are provided to the wireless service assurance (WSA) infrastructure:

- MAC address of the rogue AP
- Details of the managed AP and the radio that detected the rogue AP with strongest RSSI
- Event-specific data such as SSID, channel for potential honeypot event, and MAC address of the impersonating AP for impersonation event

The WSA rogue events feature can scale up to four times the maximum number of supported APs and half of the maximum number of supported clients.

The WSA rogue events feature is supported on Cisco DNA Center and other third-party infrastructure.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>network-assurance enable</b>  <b>Example:</b> Device# network-assurance enable	Enables wireless service assurance.
<b>Step 3</b>	<b>wireless wps rogue network-assurance enable</b>  <b>Example:</b> Device# wireless wps rogue network-assurance enable	Enables wireless service assurance for rogue devices. This ensures that the WSA rogue events are sent to the event queue.

## Monitoring Wireless Service Assurance Rogue Events

### Procedure

- show wireless wps rogue stats

#### Example:

```
Device# show wireless wps rogue stats
```

```
WSA Events
Total WSA Events Triggered      : 9
  ROGUE_POTENTIAL_HONEYPOT_DETECTED : 2
  ROGUE_POTENTIAL_HONEYPOT_CLEARED  : 3
  ROGUE_AP_IMPERSONATION_DETECTED   : 4
```

```
Total WSA Events Enqueued      : 6
  ROGUE_POTENTIAL_HONEYPOT_DETECTED : 1
  ROGUE_POTENTIAL_HONEYPOT_CLEARED  : 2
  ROGUE_AP_IMPERSONATION_DETECTED   : 3
```

In this example, nine events have been triggered, but only six of them have been enqueued. This is because three events were triggered before the WSA rogue feature was enabled.

- **show wireless wps rogue stats internal**

**show wireless wps rogue ap detailed** *rogue-ap-mac-addr*

These commands show information related to WSA events into the event history.



## CHAPTER 49

# Classifying Rogue Access Points

- [Information About Classifying Rogue Access Points, on page 439](#)
- [Guidelines and Restrictions for Classifying Rogue Access Points, on page 440](#)
- [How to Classify Rogue Access Points, on page 441](#)
- [Monitoring Rogue Classification Rules, on page 446](#)
- [Examples: Classifying Rogue Access Points, on page 447](#)

## Information About Classifying Rogue Access Points

The embedded wireless controller software enables you to create rules that can organize and display rogue access points as Friendly, Malicious, or Unclassified.

By default, none of the classification rules are used. You need to enable them. Therefore, all unknown access points are categorized as Unclassified. When you create or change a rule, configure conditions, and enable it, all rogue access points are then reclassified. Whenever you change a rule, it is applied to all the access points (friendly, malicious, and unclassified).



### Note

- Rule-based rogue classification does not apply to ad hoc rogues and rogue clients.
- You can configure up to 64 rogue classification rules per embedded wireless controller.

When the embedded wireless controller receives a rogue report from one of its managed access points, it responds as follows:

- If the unknown access point is in the friendly MAC address list, the embedded wireless controller classifies the access point as Friendly.
- If the unknown access point is not in the friendly MAC address list, the embedded wireless controller starts applying the rogue classification rules to the access point.
- 
- If the rogue access point matches the configured rules criteria, the embedded wireless controller classifies the rogue based on the classification type configured for that rule.
- If the rogue access point does not match any of the configured rules, the rogue remains unclassified.

The embedded wireless controller repeats the previous steps for all the rogue access points.

- If the rogue access point is detected on the same wired network, the embedded wireless controller marks the rogue state as Threat and classifies it as Malicious automatically, even if there are no configured rules. You can then manually contain the rogue to change the rogue state to Contained. If the rogue access point is not available on the network, the embedded wireless controller marks the rogue state as Alert. You can then manually contain the rogue.
- If desired, you can manually move the access point to a different classification type and rogue state.

Table 19: Classification Mapping

Rule-Based Classification Type	Rogue State
Friendly	<ul style="list-style-type: none"> <li>• Internal—If the unknown access point poses no threat to WLAN security, you can manually configure it as Friendly, Internal. An example of this would be the access points in your lab network.</li> <li>• External—If the unknown access point is outside the network and poses no threat to WLAN security, you can manually configure it as Friendly, External. An example of this would be the access point in your neighboring coffee shop.</li> <li>• Alert—</li> </ul>
Malicious	<ul style="list-style-type: none"> <li>• Alert—</li> <li>• Threat—The unknown access point is found to be on the network and poses a threat to WLAN security.</li> <li>• Contained—The unknown access point is contained.</li> </ul>
Unclassified	<ul style="list-style-type: none"> <li>• Alert—</li> <li>• Contained—The unknown access point is contained.</li> </ul>

As mentioned earlier, the embedded wireless controller can automatically change the classification type and rogue state of an unknown access point based on user-defined rules. Alternatively, you can manually move the unknown access point to a different classification type and rogue state.

## Guidelines and Restrictions for Classifying Rogue Access Points

- Classifying Custom type rogues is tied to rogue rules. Therefore, it is not possible to manually classify a rogue as Custom. Custom class change can occur only when rogue rules are used.
- Some are sent for containment by rule and every 30 minutes for rogue classification change.
- Rogue rules are applied on every incoming new rogue report in the embedded wireless controller in the order of their priority.
- After a rogue satisfies a rule and is classified, it does not move down the priority list for the same report.
- If a rogue AP is classified as friendly

- Until the controller discovers all the APs through neighbor reports from APs, the rogue APs are kept in unconfigured state for three minutes after they are detected. After 3 minutes, the rogue policy is applied on the rogue APs and the APs are moved to unclassified, friendly, malicious, or custom class. Rogue APs kept in unconfigured state means that no rogue policy has yet been applied on them.
- When a rogue BSSID is submitted for a containment on Cisco Catalyst 9800 Series Wireless Controller, if the controller has enough resources, it will contain. The APs that detect the particular contained rogue AP starts broadcasting the DEAUTH packets.

Wireless client connected to the contained rogue BSSID will disconnect once DEAUTH packets are received. However, when the client assumes being in a connected state, repeatedly tries to reconnect and the wireless client's user browsing experience would be badly affected.

Also, in a high RF environment like that of a stadium, though DEAUTH packets are broadcasted, client does not receive all of them because of RF disturbance. In this scenario, the client may not be fully disconnected but will be affected badly.

## How to Classify Rogue Access Points

### Classifying Rogue Access Points and Clients Manually (GUI)

#### Procedure

- 
- Step 1** Choose **Monitoring > Wireless > Rogues**.
  - Step 2** In the **Unclassified** tab, select an AP to view the detail in the lower pane.
  - Step 3** Use the **Class Type** drop-down to set the status.
  - Step 4** Click **Apply**.
- 

### Classifying Rogue Access Points and Clients Manually (CLI)

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless wps rogue adhoc {alert mac-addr   auto-contain   contain mac-addr containment-level   internal mac-addr   external mac-addr}</b>  <b>Example:</b>	Detects and reports the ad hoc rogue.  Enter one of these options after you enter the <b>adhoc</b> keyword: <ul style="list-style-type: none"> <li>• <b>alert</b>—Sets the ad hoc rogue access point to alert mode. If you choose this option,</li> </ul>

	Command or Action	Purpose
	<pre>Device(config)# wireless wps rogue adhoc alert 74a0.2f45.c520</pre>	<p>enter the MAC address for the <i>mac-addr</i> parameter.</p> <ul style="list-style-type: none"> <li>• <b>auto-contain</b>—Sets the automatically containing ad hoc rogue to auto-contain mode.</li> <li>• <b>contain</b>—Sets the containing ad hoc rogue access point to contain mode. If you choose this option, enter the MAC address for the <i>mac-addr</i> parameter and containment level for the <i>containment-level</i> parameter. The valid range for <i>containment-level</i> is from 1 to 4.</li> <li>• <b>external</b>—Sets the ad hoc rogue access point as <b>external</b>. If you choose this option, enter the MAC address for the <i>mac-addr</i> parameter.</li> <li>• <b>internal</b>—Sets the ad hoc rogue access point as <b>internal</b>. If you choose this option, enter the MAC address for the <i>mac-addr</i> parameter.</li> </ul>
<b>Step 3</b>	<pre>wireless wps rogue ap {friendly mac-addr state [external   internal]   malicious mac-addr state [alert   contain containment-level]}</pre> <p><b>Example:</b></p> <pre>Device(config)# wireless wps rogue ap malicious 74a0.2f45.c520 state contain 3</pre>	<p>Configures the rogue access points.</p> <p>Enter one of the following options after the <b>ap</b> keyword:</p> <ul style="list-style-type: none"> <li>• <b>friendly</b>—Configures the friendly rogue access points. If you choose this option, enter the MAC address for the <i>mac-addr</i> parameter. After that enter the <b>state</b> keyword followed by either of these options: <b>internal</b> or <b>external</b>. If you select an <b>internal</b> option, it indicates that you trust a foreign access point. If you select an <b>external</b> option, it indicates that you acknowledge the presence of a rogue access point.</li> <li>• <b>malicious</b>—Configures the malicious rogue access points. If you choose this option, enter the MAC address for the <i>mac-addr</i> parameter. After that enter the <b>state</b> keyword followed by either of these options: <b>alert</b> or <b>contain</b>.</li> <li>• <b>alert</b>—Sets the malicious rogue access point to <b>alert</b> mode.</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• <b>contain</b>—Sets the malicious rogue access point to <b>contain</b> mode. If you choose this option, enter the containment level for the <i>containment-level</i> parameter. The valid range is from 1 to 4.</li> </ul>
<b>Step 4</b>	<p><b>wireless wps rogue client</b> {<b>contain</b> <i>mac-addr</i> <i>containment-level</i>}</p> <p><b>Example:</b></p> <pre>Device(config)# wireless wps rogue client contain 74a0.2f45.c520 2</pre>	<p>Configures the rogue clients.</p> <p>Enter the following option after you enter the <b>client</b> keyword:</p> <p><b>contain</b>—Contains the rogue client. After you choose this option, enter the MAC address for the <i>mac-addr</i> parameter and the containment level for <i>containment-level</i> parameter. The valid range for <i>containment-level</i> is from 1 to 4.</p>
<b>Step 5</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config)# end</pre>	<p>Returns to privileged EXEC mode.</p> <p>Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.</p>

## Configuring Rogue Classification Rules (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Security > Wireless Protection Policies**.
- Step 2** In the **Wireless Protection Policies** page, choose **Rogue AP Rules** tab.
- Step 3** On the **Rogue AP Rules** page, click the name of the **Rule** or click **Add** to create a new one.
- Step 4** In the **Add/Edit Rogue AP Rule** window that is displayed, enter the name of the rule in the **Rule Name** field.
- Step 5** Choose the rule type from the following **Rule Type** drop-down list options:
- Friendly
  - Malicious
  - Unclassified
  - Custom
-

## Configuring Rogue Classification Rules (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless wps rogue rule <i>rule-name</i> priority <i>priority</i></b> <b>Example:</b> Device (config)# <b>wireless wps rogue rule rule_3 priority 3</b>	Creates or enables a rule. While creating a rule, you must enter the priority for the rule.  <b>Note</b> After creating a rule, you can edit the rule and change the priority only for the rogue rules that are disabled. You cannot change the priority for the rogue rules that are enabled. While editing, changing the priority for a rogue rule is optional.
<b>Step 3</b>	<b>classify {friendly state {alert   external   internal}   malicious state {alert   contained} }</b> <b>Example:</b> Device (config)# <b>wireless wps rogue rule rule_3 priority 3</b> Device (config-rule)# <b>classify friendly</b>	<ul style="list-style-type: none"> <li>• <b>friendly</b>—Configures the friendly rogue access points. After that enter the <b>state</b> keyword followed by either of these options: <b>alert</b>, <b>internal</b>, or <b>external</b>. If you select an <b>internal</b> option, it indicates that you trust a foreign access point. If you select an <b>external</b> option, it indicates that you acknowledge the presence of a rogue access point.</li> <li>• <b>malicious</b>—Configures the malicious rogue access points. After that enter the state keyword followed by either of these options: <b>alert</b> or <b>contained</b>.</li> <li>• <b>alert</b>—Sets the malicious rogue access point to alert mode.</li> <li>• <b>contained</b>—Sets the malicious rogue access point to contained mode.</li> </ul>
<b>Step 4</b>	<b>condition {client-count   duration   encryption   infrastructure   rssi   ssid}</b> <b>Example:</b> Device (config)# <b>wireless wps rogue rule rule_3 priority 3</b> Device (config-rule)# <b>condition client-count 5</b>	Adds the following conditions to a rule, which the rogue access point must meet:  <ul style="list-style-type: none"> <li>• <b>client-count</b>—Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, the access point could be classified as Malicious. If you choose this option, enter the minimum number</li> </ul>



	Command or Action	Purpose
		<p>of clients to be associated to the rogue access point for the parameter. The valid range is from 1 to 10 (inclusive), and the default value is 0.</p> <ul style="list-style-type: none"> <li>• <b>duration</b>—Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period for the parameter. The valid range is from 0 to 3600 seconds (inclusive), and the default value is 0 seconds.</li> <li>• <b>encryption</b>—Requires that the advertised WLAN does not have encryption enabled. You can choose <b>any</b> for any type of encryption, <b>off</b> for no encryption, <b>wpa1</b> for WPA encryption, <b>wpa2</b> for WPA2 encryption, <b>wpa3-owe</b> for WPA3 OWE encryption, or <b>wpa3-sae</b> for WPA3 SAE encryption.</li> <li>• <b>infrastructure</b>—Requires the SSID to be known to the controller.</li> <li>• <b>rss</b>i—The valid range is from -95 to -50 dBm (inclusive).</li> <li>• <b>ssid</b>—Requires the rogue access point to have a specific SSID. You could specify up to 25 different SSIDs. You should specify an SSID that is not managed by the controller. If you choose this option, enter the SSID for the parameter.</li> <li>• <b>wildcard-ssid</b>—Allows you to specify an expression that could match an SSID string. You can specify up to 25 of these SSIDs.</li> </ul>
<b>Step 5</b>	<b>match {all   any}</b> <b>Example:</b> <pre>Device(config)# wireless wps rogue rule rule_3 priority 3 Device(config-rule)# match all</pre>	Specifies whether a detected rogue access point must meet all or any of the conditions specified by the rule for the rule to be matched and the rogue access point to adopt the classification type of the rule.
<b>Step 6</b>	<b>default</b> <b>Example:</b> <pre>Device(config)# wireless wps rogue rule rule_3 priority 3</pre>	Sets a command to its default.

	Command or Action	Purpose
	Device (config-rule) # <b>default</b>	
<b>Step 7</b>	<b>exit</b> <b>Example:</b> Device (config) # <b>wireless wps rogue rule rule_3 priority 3</b> Device (config-rule) # <b>exit</b> Device (config) #	Exits the sub-mode.
<b>Step 8</b>	<b>shutdown</b> <b>Example:</b> Device (config) # <b>wireless wps rogue rule rule_3 priority 3</b> Device (config-rule) # <b>shutdown</b>	Disables a particular rogue rule. In this example, the rule <b>rule_3</b> is disabled.
<b>Step 9</b>	<b>end</b> <b>Example:</b> Device (config) # <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.
<b>Step 10</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 11</b>	<b>wireless wps rogue rule shutdown</b> <b>Example:</b> Device (config) # <b>wireless wps rogue rule shutdown</b>	Disables all the rogue rules.
<b>Step 12</b>	<b>end</b> <b>Example:</b> Device (config) # <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Monitoring Rogue Classification Rules

You can monitor the rogue classification rules using the following commands:

*Table 20: Commands for Monitoring Rogue Classification Rules*

Command	Purpose
<b>show wireless wps rogue rule detailed</b>	Displays detailed information of a classification rule.
<b>show wireless wps rogue rule summary</b>	Displays a summary of the classification rules.

## Examples: Classifying Rogue Access Points

This example shows how to classify a rogue AP with MAC address 00:11:22:33:44:55 as malicious and mark it for being contained by 2 managed APs:

```
Device# configure terminal
Device(config)# wireless wps rogue ap malicious 0011.2233.4455 state contain 2
```

This example shows how to create a rule that can categorize a rogue AP that is using SSID **my-friendly-ssid**, and it is seen for at least for 1000 seconds as friendly internal:

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# condition ssid my-friendly-ssid
Device(config-rule)# condition duration 1000
Device(config-rule)# match all
Device(config-rule)# classify friendly state internal
```

This example shows how to apply a condition that a rogue access point must meet:

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# condition client-count 5
Device(config-rule)# condition duration 1000
Device(config-rule)# end
```





## CHAPTER 50

# Configuring Secure Shell

- [Information About Configuring Secure Shell](#) , on page 449
- [Prerequisites for Configuring Secure Shell](#), on page 451
- [Restrictions for Configuring Secure Shell](#), on page 452
- [How to Configure SSH](#), on page 452
- [Monitoring the SSH Configuration and Status](#), on page 455

## Information About Configuring Secure Shell

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

## SSH and Device Access

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

## SSH Servers, Integrated Clients, and Supported Versions

The Secure Shell (SSH) Integrated Client feature is an application that runs over the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco device to make a secure, encrypted connection to another Cisco device or to any other device running the SSH server. This connection provides functionality similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for secure communication over an unsecured network.

The SSH server and SSH integrated client are applications that run on the switch. The SSH server works with the SSH client supported in this release and with non-Cisco SSH clients. The SSH client works with publicly and commercially available SSH servers. The SSH client supports the ciphers of Data Encryption Standard (DES), 3DES, and password authentication.

The switch supports an SSHv1 or an SSHv2 server.

The switch supports an SSHv1 client.



---

**Note** The SSH client functionality is available only when the SSH server is enabled.

---

User authentication is performed like that in the Telnet session to the device. SSH also supports the following user authentication methods:

- TACACS+
- RADIUS
- Local authentication and authorization

## SSH Configuration Guidelines

Follow these guidelines when configuring the switch as an SSH server or SSH client:

- An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.
- If the SSH server is running on an active switch and the active switch fails, the new active switch uses the RSA key pair generated by the previous active switch.
- If you get CLI error messages after entering the **crypto key generate rsa** global configuration command, an RSA key pair has not been generated. Reconfigure the hostname and domain, and then enter the **crypto key generate rsa** command.
- When generating the RSA key pair, the message No host name specified might appear. If it does, you must configure a hostname by using the **hostname** global configuration command.
- When generating the RSA key pair, the message No domain specified might appear. If it does, you must configure an IP domain name by using the **ip domain-name** global configuration command.
- When configuring the local authentication and authorization authentication method, make sure that AAA is disabled on the console.

## Secure Copy Protocol Overview

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying switch configurations or switch image files. SCP relies on Secure Shell (SSH), an application and a protocol that provides a secure replacement for the Berkeley r-tools.

For SSH to work, the switch needs an RSA public/private key pair. This is the same with SCP, which relies on SSH for its secure transport.

Because SSH also relies on AAA authentication, and SCP relies further on AAA authorization, correct configuration is necessary.

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.
- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.



---

**Note** When using SCP, you cannot enter the password into the copy command. You must enter the password when prompted.

---

## Secure Copy Protocol

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying device configurations or switch image files. The behavior of SCP is similar to that of remote copy (rcp), which comes from the Berkeley r-tools suite, except that SCP relies on SSH for security. SCP also requires that authentication, authorization, and accounting (AAA) authorization be configured so the device can determine whether the user has the correct privilege level. To configure the Secure Copy feature, you should understand the SCP concepts.

## SFTP Support

SFTP client support is introduced from Cisco IOS XE Gibraltar 16.10.1 release onwards. SFTP client is enabled by default and no separate configuration required.

The SFTP procedures can be invoked using the **copy** command, which is similar to that of **scp** and **tftp** commands. A typical file download procedure using **sftp** command can be carried out as shown below:

```
copy sftp://user :password @server-ip/file-name flash0:// file-name
```

For more details on the **copy** command, see the following URL:

[https://www.cisco.com/c/m/en\\_us/techdoc/dc/reference/cli/nxos/commands/fund/copy.html](https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/fund/copy.html)

## Prerequisites for Configuring Secure Shell

The following are the prerequisites for configuring the switch for secure shell (SSH):

- For SSH to work, the switch needs an Rivest, Shamir, and Adleman (RSA) public/private key pair. This is the same with Secure Copy Protocol (SCP), which relies on SSH for its secure transport.
- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.
- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.
- SCP relies on SSH for security.
- SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level.
- A user must have appropriate authorization to use SCP.
- A user who has appropriate authorization can use SCP to copy any file in the Cisco IOS File System (IFS) to and from a switch by using the **copy** command. An authorized administrator can also do this from a workstation.
- The Secure Shell (SSH) server requires an IPsec (Data Encryption Standard [DES] or 3DES) encryption software image; the SSH client requires an IPsec (DES or 3DES) encryption software image.)

- Configure a hostname and host domain for your device by using the **hostname** and **ip domain-name** commands in global configuration mode.

## Restrictions for Configuring Secure Shell

The following are restrictions for configuring the device for secure shell.

- The switch supports Rivest, Shamir, and Adelman (RSA) authentication.
- SSH supports only the execution-shell application.
- The SSH server and the SSH client are supported only on Data Encryption Standard (DES) (56-bit) and 3DES (168-bit) data encryption software. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.
- The device supports the Advanced Encryption Standard (AES) encryption algorithm with a 128-bit key, 192-bit key, or 256-bit key. However, symmetric cipher AES to encrypt the keys is not supported.
- When using SCP, you cannot enter the password into the **copy** command. You must enter the password when prompted.
- The login banner is not supported in Secure Shell Version 1. It is supported in Secure Shell Version 2.
- The **-l** keyword and **userid** :{number} {ip-address} delimiter and arguments are mandatory when configuring the alternative method of Reverse SSH for console access.
- To authenticate clients with freeradius over RADSEC, you should generate an RSA key longer than 1024 bit. Use the **crypto key generate rsa general-keys exportable label label-name** command to achieve this.

## How to Configure SSH

### Setting Up the Device to Run SSH

Follow the procedure given below to set up your device to run SSH:

#### Before you begin

Configure user authentication for local or remote access.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# Device# <b>configure terminal</b>	Enters global configuration mode.



	Command or Action	Purpose
<b>Step 2</b>	<b>hostname</b> <i>hostname</i> <b>Example:</b> Device(config)# <b>hostname</b> <i>your_hostname</i>	Configures a hostname and IP domain name for your device.  <b>Note</b> Follow this procedure only if you are configuring the device as an SSH server.
<b>Step 3</b>	<b>ip domain name</b> <i>domain_name</i> <b>Example:</b> Device(config)# <b>ip domain name</b> <i>your_domain</i>	Configures a host domain for your device.
<b>Step 4</b>	<b>crypto key generate rsa</b> <b>Example:</b> Device(config)# <b>crypto key generate rsa</b>	Enables the SSH server for local and remote authentication on the device and generates an RSA key pair. Generating an RSA key pair for the device automatically enables SSH.  We recommend that a minimum modulus size of 1024 bits.  When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use.  <b>Note</b> Follow this procedure only if you are configuring the device as an SSH server.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Exits configuration mode.

## Configuring the SSH Server

Follow the procedure given below to configure the SSH server:



**Note** This procedure is only required if you are configuring the device as an SSH server.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>	Enters global configuration mode.

	Command or Action	Purpose
	Device# <code>configure terminal</code>	
<b>Step 2</b>	<p><b>ip ssh version [2]</b></p> <p><b>Example:</b></p> <pre>Device(config)# ip ssh version 2</pre>	(Optional) Configures the device to run SSH Version 2.
<b>Step 3</b>	<p><b>ip ssh {timeout <i>seconds</i>   authentication-retries <i>number</i>}</b></p> <p><b>Example:</b></p> <pre>Device(config)# ip ssh timeout 90 authentication-retries 2</pre>	<p>Configures the SSH control parameters:</p> <ul style="list-style-type: none"> <li>Specify the time-out value in seconds; the default is 120 seconds. The range is 0 to 120 seconds. This parameter applies to the SSH negotiation phase. After the connection is established, the device uses the default time-out values of the CLI-based sessions.</li> <li>By default, up to five simultaneous, encrypted SSH connections for multiple CLI-based sessions over the network are available (session 0 to session 4). After the execution shell starts, the CLI-based session time-out value returns to the default of 10 minutes.</li> <li>Specify the number of times that a client can re-authenticate to the server. The default is 3; the range is 0 to 5.</li> </ul> <p>Repeat this step when configuring both parameters.</p>
<b>Step 4</b>	<p>Use one or both of the following:</p> <ul style="list-style-type: none"> <li><code>line vty <i>line_number</i> [ <i>ending_line_number</i>]</code></li> <li><code>transport input ssh</code></li> </ul> <p><b>Example:</b></p> <pre>Device(config)# line vty 1 10</pre> <p>or</p> <pre>Device(config-line)# transport input ssh</pre>	<p>(Optional) Configures the virtual terminal line settings.</p> <ul style="list-style-type: none"> <li>Enters line configuration mode to configure the virtual terminal line settings. For <i>line_number</i> and <i>ending_line_number</i>, specify a pair of lines. The range is 0 to 15.</li> <li>Specifies that the device prevent non-SSH Telnet connections. This limits the router to only SSH connections.</li> </ul>

	Command or Action	Purpose
		<p><b>Note</b> If the Virtual Terminal (VTY) lines are exhausted, Telnet or SSH will fail. You can either disconnect the Telnet or SSH sessions to free up the VTY lines, or follow the recovery steps given below to clear VTY lines and reload Telnet or SSH:</p> <pre>Device# configure terminal Device(config)# clear line <i>line number</i></pre>
<b>Step 5</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-line)# end</pre>	Returns to privileged EXEC mode.

## Monitoring the SSH Configuration and Status

This table displays the SSH server configuration and status.

**Table 21: Commands for Displaying the SSH Server Configuration and Status**

Command	Purpose
<b>show ip ssh</b>	Shows the version and configuration information for the SSH server.
<b>show ssh</b>	Shows the status of the SSH server.





# CHAPTER 51

## Private Shared Key

---

- [Information About Private Preshared Key, on page 457](#)
- [Configuring a PSK in a WLAN \(CLI\), on page 458](#)
- [Configuring a PSK in a WLAN \(GUI\), on page 459](#)
- [Applying a Policy Profile to a WLAN \(GUI\), on page 460](#)
- [Applying a Policy Profile to a WLAN \(CLI\), on page 460](#)
- [Verifying a Private PSK, on page 460](#)

## Information About Private Preshared Key

With the advent of Internet of Things (IoT), the number of devices that connect to the internet has increased manifold. Not all of these devices support the 802.1x supplicant and need an alternate mechanism to connect to the internet. One of the security mechanisms, WPA-PSK, could be considered as an alternative. With the current configuration, the PSK is the same for all the clients that connect to the same WLAN. In certain deployments, such as educational institutions, this results in the key being shared to unauthorized users leading to security breach. This necessitates the need to provision unique PSKs for different clients on a large scale.

Identity PSKs are unique PSKs created for individuals or groups of users on the same SSID. No complex configuration is required for the clients. It provides the same simplicity of PSK, making it ideal for IoT, Bring your own device (BYOD), and guest deployments. The default password for PSK SSID is *password*.

Identity PSKs are supported on most devices, in which 802.1X is not, enabling stronger security for IoT. It is possible to easily revoke access, for a single device or individual without affecting everyone else. Thousands of keys can easily be managed and distributed through the AAA server.



---

**Note** Special characters, such as '<' and '>' are not supported in SSID Preshared key.

---



---

**Note** PSK supports whitespace in passwords (before or after or in-between) within double quotes only; single quotes for whitespaces are not supported.

---

### IPSK Solution

During client authentication, the AAA server authorizes the client MAC address and sends the passphrase (if configured) as part of the Cisco-AV pair list. The Embedded Wireless Controller receives this as part of the RADIUS response and processes this further for the computation of PSKs.

When a client sends an association request to the SSID broadcast by the corresponding access point, the Embedded Wireless Controller forms the RADIUS request packet with the particular mac address of the client and relays to the RADIUS server.

The RADIUS server performs the authentication and checks whether the client is allowed or not and sends either ACCESS-ACCEPT or ACCESS-REJECT as response to the WLC.

To support Identity PSKs, in addition to sending the authentication response, the authentication server also provides the AV pair passphrase for this specific client. This is used for the computation of the PMK.

The RADIUS server might also provide additional parameters, such as username, VLAN, Quality of Service (QoS), and so on, in the response, that is specific to this client. For multiple devices owned by a single user, the passphrase can remain the same.



**Note** When the PSK length is less than 15 characters in Federal Information Processing Standard (FIPS), the controller allows the WLAN configuration but displays the following error message on the console:

**"AP is allowed to join but corresponding WLAN will not be pushed to the access point"**

## Configuring a PSK in a WLAN (CLI)

Follow the procedure given below to configure a PSK in a WLAN:

### Before you begin

- Security should be configured for a pre-shared key (PSK) in a WLAN.
- If there is no override from the AAA server, the value on the corresponding WLAN is considered for authentication.
- In Federal Information Processing Standard (FIPS) and common criteria mode, ensure that the PSK WLAN has a minimum of 15 ASCII characters, else APs won't join the controller.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wlan wlan-name wlan-id ssid</b>  <b>Example:</b> Device(config)# wlan test-profile 4 abc	Configures the WLAN and SSID.

	Command or Action	Purpose
<b>Step 3</b>	<b>no security wpa akm dot1x</b> <b>Example:</b> Device(config-wlan)# no security wpa akm dot1x	Disables security AKM for dot1x.
<b>Step 4</b>	<b>security wpa akm psk</b> <b>Example:</b> Device(config-wlan)# security wpa akm psk	Configures the security type PSK.
<b>Step 5</b>	<b>security wpa akm psk set-key ascii/hex key</b> <b>Example:</b> Device(config-wlan)# security wpa akm psk set-key ascii 0	Configures the PSK authenticated key management (AKM) shared key.
<b>Step 6</b>	<b>security wpa akm psk</b> <b>Example:</b> Device(config-wlan)# security wpa akm psk	Configures PSK support.
<b>Step 7</b>	<b>mac-filtering auth-list-name</b> <b>Example:</b> Device(config-wlan)# mac-filtering test1	Specifies MAC filtering in a WLAN.

## Configuring a PSK in a WLAN (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** On the **Wireless Networks** page, click **Security** tab.
- Step 3** In the **Layer 2** window that is displayed, go to the **WPA Parameters** section.
- Step 4** From the **Auth Key Mgmt** drop-down, select the PSK format and type.
- Step 5** Enter the Pre-Shared Key in hexadecimal characters.
- If you selected the PSK format as HEX, the key length must be exactly 64 characters.
  - If you selected the PSK format as ASCII, the key length must be in the range of 8-63 characters.
- Note that once you have configured the key, these details are not visible even if you click on the eye icon next to the preshared key box, due to security reasons.
- Step 6** Click **Save & Apply to Device**.
-

## Applying a Policy Profile to a WLAN (GUI)

### Procedure

- 
- Step 1** Choose **Configuration** > **Tags & Profiles** > **Tags**.
  - Step 2** On the **Manage Tags** page, click **Policy** tab.
  - Step 3** Click **Add** to view the **Add Policy Tag** window.
  - Step 4** Enter a name and description for the policy tag.
  - Step 5** Click **Add** to map WLAN and policy.
  - Step 6** Choose the WLAN profile to map with the appropriate policy profile, and click the tick icon.
  - Step 7** Click **Save & Apply to Device**.
- 

## Applying a Policy Profile to a WLAN (CLI)

Follow the procedure given below to apply policy profile to a WLAN:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile policy <i>policy-profile-name</i></b>  <b>Example:</b> Device(config)# wireless profile policy policy-iot	Configures the default policy profile.
<b>Step 3</b>	<b>aaa-override</b>  <b>Example:</b> Device(config-wireless-policy)# aaa-override	Configures AAA override to apply policies coming from the AAA server or ISE the Cisco Identify Services Engine (ISE) server.

## Verifying a Private PSK

Use the following **show** commands to verify the configuration of a WLAN and a client:

```
Device# show wlan id 2
```

```
WLAN Profile Name      : test_ppsk
```



```

=====
Identifier                               : 2
Network Name (SSID)                      : test_ppsk
Status                                    : Enabled
Broadcast SSID                           : Enabled
Universal AP Admin                        : Disabled
Max Associated Clients per WLAN           : 0
Max Associated Clients per AP per WLAN    : 0
Max Associated Clients per AP Radio per WLAN : 0
Number of Active Clients                  : 0
Exclusionlist Timeout                     : 60
CHD per WLAN                             : Enabled
Interface                                 : default
Multicast Interface                       : Unconfigured
WMM                                        : Allowed
WifiDirect                               : Invalid
Channel Scan Defer Priority:
  Priority (default)                      : 4
  Priority (default)                      : 5
  Priority (default)                      : 6
Scan Defer Time (msecs)                  : 100
Media Stream Multicast-direct            : Disabled
CCX - AironetIe Support                   : Enabled
CCX - Diagnostics Channel Capability      : Disabled
Peer-to-Peer Blocking Action             : Disabled
Radio Policy                             : All
DTIM period for 802.11a radio             : 1
DTIM period for 802.11b radio            : 1
Local EAP Authentication                  : Disabled
Mac Filter Authorization list name      : test1
Accounting list name                      : Disabled
802.1x authentication list name           : Disabled
Security
  802.11 Authentication                   : Open System
  Static WEP Keys                         : Disabled
  802.1X                                  : Disabled
  Wi-Fi Protected Access (WPA/WPA2)      : Enabled
    WPA (SSN IE)                         : Disabled
    WPA2 (RSN IE)                        : Enabled
      TKIP Cipher                        : Disabled
      AES Cipher                          : Enabled
    Auth Key Management
      802.1x                             : Disabled
      PSK                                : Enabled
      CCKM                                : Disabled
      FT dot1x                            : Disabled
      FT PSK                              : Disabled
      PMF dot1x                           : Disabled
      PMF PSK                             : Disabled
    CCKM TSF Tolerance                    : 1000
    FT Support                            : Disabled
      FT Reassociation Timeout            : 20
      FT Over-The-DS mode                 : Enabled
    PMF Support                           : Disabled
      PMF Association Comeback Timeout    : 1
      PMF SA Query Time                   : 200
  Web Based Authentication                 : Disabled
  Conditional Web Redirect                 : Disabled
  Splash-Page Web Redirect                 : Disabled
  Webauth On-mac-filter Failure            : Disabled
  Webauth Authentication List Name         : Disabled
  Webauth Parameter Map                   : Disabled
  Tkip MIC Countermeasure Hold-down Timer : 60
Call Snooping                             : Disabled

```

```

Passive Client                : Disabled
Non Cisco WGB                 : Disabled
Band Select                   : Disabled
Load Balancing                : Disabled
Multicast Buffer               : Disabled
Multicast Buffer Size          : 0
IP Source Guard                : Disabled
Assisted-Roaming
  Neighbor List                : Disabled
  Prediction List              : Disabled
  Dual Band Support            : Disabled
IEEE 802.11v parameters
  Directed Multicast Service   : Disabled
  BSS Max Idle                 : Disabled
  Protected Mode               : Disabled
  Traffic Filtering Service    : Disabled
  BSS Transition               : Enabled
  Disassociation Imminent     : Disabled
  Optimised Roaming Timer     : 40
  Timer                         : 200
  WNM Sleep Mode               : Disabled
802.11ac MU-MIMO              : Disabled

```

Device# **show wireless client mac-address a886.adb2.05f9 detail**

```

Client MAC Address : a886.adb2.05f9
Client IPv4 Address : 9.9.58.246
Client Username : A8-86-AD-B2-05-F9
AP MAC Address : c025.5c55.e400
AP Name: saurabh-3600
AP slot : 1
Client State : Associated
Policy Profile : default-policy-profile
Flex Profile : default-flex-profile
Wireless LAN Id : 6
Wireless LAN Name: SSS_PPSK
BSSID : c025.5c55.e40f
Connected For : 280 seconds
Protocol : 802.11n - 5 GHz
Channel : 60
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Session Timeout : 320 sec (Remaining time: 40 sec)
Input Policy Name :
Input Policy State : None
Input Policy Source : None
Output Policy Name :
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs : BK, BE, VI, VO
Fastlane Support : Disabled
Power Save : OFF
Current Rate : m22
Supported Rates : 9.0,18.0,36.0,48.0,54.0
Mobility:
  Move Count : 0
  Mobility Role : Local
  Mobility Roam Type : None

```

```

Mobility Complete Timestamp : 09/27/2017 16:32:25 IST
Policy Manager State: Run
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 280 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : PSK
AAA override passphrase: Yes
Management Frame Protection : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN : 58
Access VLAN : 58
Anchor VLAN : 0
WFD capable : No
Manged WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Interface      : capwap_90000005
  IIF ID         : 0x90000005
  Device Type    : Apple-Device
  Protocol Map   : 0x000001
  Authorized     : TRUE
  Session timeout : 320
  Common Session ID: 1F3809090000005DC30088EA
  Acct Session ID : 0x00000000
  Auth Method Status List
    Method : MAB
      SM State      : TERMINATE
      Authen Status : Success
  Local Policies:
    Service Template : wlan_svc_default-policy-profile (priority 254)
    Absolute-Timer   : 320
    VLAN             : 58
  Server Policies:
  Resultant Policies:
    VLAN             : 58
    Absolute-Timer   : 320
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PECC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Central
FlexConnect Central Association : No
Client Statistics:
  Number of Bytes Received : 59795
  Number of Bytes Sent : 21404
  Number of Packets Received : 518
  Number of Packets Sent : 274
  Number of EAP Id Request Msg Timeouts :
  Number of EAP Request Msg Timeouts :
  Number of EAP Key Msg Timeouts :
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -32 dBm

```

```
Signal to Noise Ratio : 58 dB  
Fabric status : Disabled
```



# CHAPTER 52

## Multi-Preshared Key

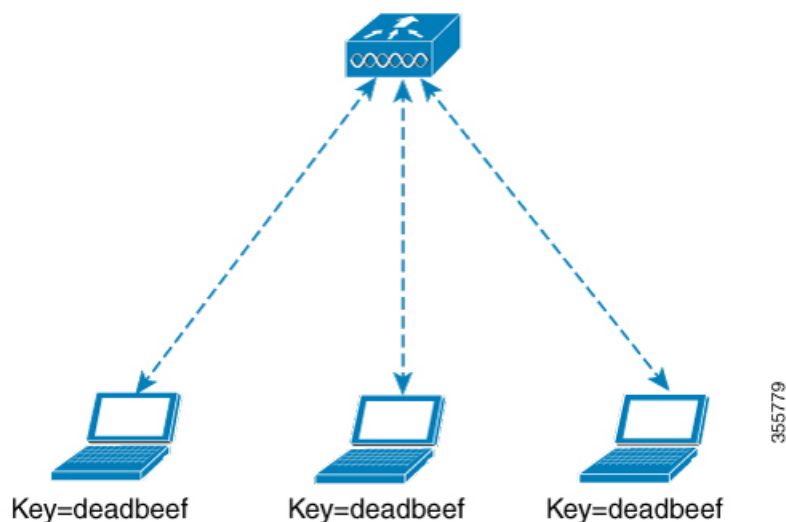
- [Information About Multi-Preshared Key, on page 465](#)
- [Restrictions on Multi-PSK, on page 466](#)
- [Configuring Multi-Preshared Key \(GUI\), on page 466](#)
- [Configuring Multi-Preshared Key \(CLI\), on page 469](#)
- [Verifying Multi-PSK Configurations, on page 470](#)

### Information About Multi-Preshared Key

Multi-PSK feature supports multiple PSKs simultaneously on a single SSID. You can use any of the configured PSKs to join the network. This is different from the Identity PSK (iPSK), wherein unique PSKs are created for individuals or groups of users on the same SSID.

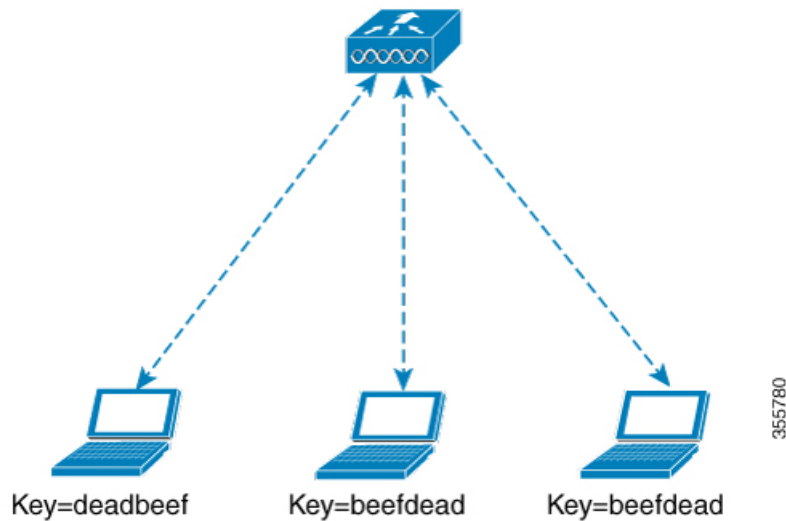
In a traditional PSK, all the clients joining the network use the same password as shown in the below figure.

**Figure 11: Traditional PSK**



But with multi-PSK, client can use any of the configured pre-shared keys to connect to the network as shown in the below figure.

Figure 12: Multi-PSK



In Multi-PSK, two passwords are configured (deadbeef and beefdead) for the same SSID. In this scenario, clients can connect to the network using either of the passwords.

## Restrictions on Multi-PSK

- Central authentication is supported in local, flex, and fabric modes only.
- In central authentication flex mode, the standalone AP allows client join with the highest priority PSK (*priority 0* key). New clients that do not use the highest priority PSK are rejected during the standalone mode.
- Multi-PSK does not support local authentication.

## Configuring Multi-Preshared Key (GUI)

### Procedure

- 
- Step 1** Choose **Configuration** > **Tags & Profiles** > **WLANs**.
  - Step 2** On the **Wireless Networks** page, click the name of the WLAN.
  - Step 3** In the **Edit WLAN** window, click the **Security** tab.
  - Step 4** In the **Layer2** tab, choose the **Layer2 Security Mode** from the following options:
    - None: No Layer 2 security
    - 802.1X: WEP 802.1X data encryption type
    - WPA + WPA2: Wi-Fi Protected Access
    - Static WEP: Static WEP encryption parameters
    - Static WEP+802.1X: Both Static WEP and 802.1X parameters

Parameters	Description
<b>802.1X</b>	
WEP Key Size	Choose the key size. The available values are <i>None</i> , <i>40 bits</i> , and <i>104 bits</i> .
<b>WPA + WPA2</b>	
Protected Management Frame	Choose from the following options: <ul style="list-style-type: none"> <li>• Disabled</li> <li>• Optional</li> <li>• Required</li> </ul>
WPA Policy	Check the check box to enable WPA policy.
WPA Encryption	Choose the WPA encryption standard. A WPA encryption standard must be specified if you have enabled WPA policy.
WPA2 Policy	Check the check box to enable WPA2 policy.
WPA2 Encryption	Choose the WPA2 encryption standard. A WPA encryption standard must be specified if you have enabled WPA policy.
Auth Key Mgmt	Choose the rekeying mechanism from the following options: <ul style="list-style-type: none"> <li>• 802.1X</li> <li>• FT + 802.1X</li> <li>• PSK: You must specify the PSK format and a preshared key</li> <li>• Cisco Centralized Key Management: You must specify a Cisco Centralized Key Management Timestamp Tolerance value</li> <li>• 802.1X + Cisco Centralized Key Management: You must specify a Cisco Centralized Key Management Timestamp Tolerance value</li> <li>• FT + 802.1X + Cisco Centralized Key Management: You must specify a Cisco Centralized Key Management Timestamp Tolerance value</li> </ul>
<b>Static WEP</b>	

Parameters	Description
Key Size	Choose the key size from the following options: <ul style="list-style-type: none"> <li>• 40 bits</li> <li>• 104 bits</li> </ul>
Key Index	Choose a key index from 1 to 4. One unique WEP key index can be applied to each WLAN. As there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer2 encryption.
Key Format	Choose the encryption key format as either ASCII or HEX.
Encryption Key	Enter an encryption key that is 13 characters long.
<b>Static WEP + 802.1X</b>	
Key Size	Choose the key size from the following options: <ul style="list-style-type: none"> <li>• 40 bits</li> <li>• 104 bits</li> </ul>
Key Index	Choose a key index from 1 to 4. One unique WEP key index can be applied to each WLAN. As there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer2 encryption.
Key Format	Choose the encryption key format as either ASCII or HEX.
Encryption Key	Enter an encryption key that is 13 characters long.
WEP Key Size	Choose from the following options: <ul style="list-style-type: none"> <li>• None</li> <li>• 40 bits</li> <li>• 104 bits</li> </ul>

**Step 5** Click **Save & Apply to Device**.

---



## Configuring Multi-Preshared Key (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wlan wlan-name wlan-id ssid</b> <b>Example:</b> Device(config)# <code>wlan mywlan 1 SSID_name</code>	Configures WLAN and SSID.
<b>Step 3</b>	<b>no security wpa akm dot1x</b> <b>Example:</b> Device(config-wlan)# <code>no security wpa akm dot1x</code>	Disables security AKM for dot1x.
<b>Step 4</b>	<b>security wpa akm psk</b> <b>Example:</b> Device(config-wlan)# <code>security wpa akm psk</code>	Configures PSK.
<b>Step 5</b>	<b>security wpa wpa2 mpsk</b> <b>Example:</b> Device(config-wlan)# <code>security wpa wpa2 mpsk</code>	Configures multi-PSK.
<b>Step 6</b>	<b>priority priority_value set-key {ascii [0   8] pre-shared-key   hex [0   8] pre-shared-key}</b> <b>Example:</b> Device(config-mpsk)# <code>priority 0 set-key ascii 0 deadbeef</code>	Configures PSK priority and all its related passwords. The <i>priority_value</i> ranges from 0 to 4. <b>Note</b> You need to configure <b>priority 0</b> key for multi-PSK.
<b>Step 7</b>	<b>no shutdown</b> <b>Example:</b> Device(config-mpsk)# <code>no shutdown</code>	Enables WLAN.
<b>Step 8</b>	<b>exit</b> <b>Example:</b> Device(config-wlan)# <code>exit</code>	Exits WLAN configuration mode and returns to configuration mode.

	Command or Action	Purpose
<b>Step 9</b>	<b>end</b>  <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Verifying Multi-PSK Configurations

To verify the configuration of a WLAN and a client, use the following command:

```

Device# show wlan id 8
WLAN Profile Name      : wlan_8
=====
Identifier              : 8
Network Name (SSID)    : ssid_8
Status                  : Enabled
Broadcast SSID         : Enabled
Universal AP Admin     : Disabled
Max Associated Clients per WLAN : 0
Max Associated Clients per AP per WLAN : 0
Max Associated Clients per AP Radio per WLAN : 200
Number of Active Clients : 0
CHD per WLAN           : Enabled
Multicast Interface    : Unconfigured
WMM                     : Allowed
WifiDirect              : Invalid
Channel Scan Defer Priority:
  Priority (default)    : 5
  Priority (default)    : 6
Scan Defer Time (msecs) : 100
Media Stream Multicast-direct : Disabled
CCX - AironetIe Support : Enabled
CCX - Diagnostics Channel Capability : Disabled
Peer-to-Peer Blocking Action : Disabled
Radio Policy           : All
DTIM period for 802.11a radio : 1
DTIM period for 802.11b radio : 1
Local EAP Authentication : Disabled
Mac Filter Authorization list name : Disabled
Mac Filter Override Authorization list name : Disabled
Accounting list name   :
802.1x authentication list name : Disabled
802.1x authorization list name : Disabled
Security
  802.11 Authentication : Open System
  Static WEP Keys       : Disabled
  802.1X                 : Disabled
  Wi-Fi Protected Access (WPA/WPA2/WPA3) : Enabled
    WPA (SSN IE)        : Disabled
    WPA2 (RSN IE)       : Enabled
      MP SK              : Enabled
      AES Cipher         : Enabled
      CCMP256 Cipher     : Disabled
      GCMP128 Cipher     : Disabled
      GCMP256 Cipher     : Disabled
    WPA3 (WPA3 IE)      : Disabled
  Auth Key Management
    802.1x               : Disabled
    PSK                  : Enabled

```

```

CCKM : Disabled
FT dot1x : Disabled
FT PSK : Disabled
FT SAE : Disabled
PMF dot1x : Disabled
PMF PSK : Disabled
SAE : Disabled
OWE : Disabled
SUITEB-1X : Disabled
SUITEB192-1X : Disabled
CCKM TSF Tolerance : 1000
FT Support : Adaptive
  FT Reassociation Timeout : 20
  FT Over-The-DS mode : Enabled
PMF Support : Disabled
  PMF Association Comeback Timeout : 1
  PMF SA Query Time : 200
Web Based Authentication : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled
Webauth Authentication List Name : Disabled
Webauth Authorization List Name : Disabled
Webauth Parameter Map : Disabled
Tkip MIC Countermeasure Hold-down Timer : 60
Non Cisco WGB : Disabled
Band Select : Enabled
Load Balancing : Disabled
Multicast Buffer : Disabled
Multicast Buffer Size : 0
IP Source Guard : Disabled
Assisted-Roaming
  Neighbor List : Disabled
  Prediction List : Disabled
  Dual Band Support : Disabled
IEEE 802.11v parameters
  Directed Multicast Service : Disabled
  BSS Max Idle : Disabled
    Protected Mode : Disabled
  Traffic Filtering Service : Disabled
  BSS Transition : Enabled
    Disassociation Imminent : Disabled
    Optimised Roaming Timer : 40
    Timer : 200
  WNM Sleep Mode : Disabled
802.11ac MU-MIMO : Disabled
802.11ax paramters
  OFDMA Downlink : unknown
  OFDMA Uplink : unknown
  MU-MIMO Downlink : unknown
  MU-MIMO Uplink : unknown
  BSS Color : unknown
  Partial BSS Color : unknown
  BSS Color Code :

```

To view the WLAN details, use the following command:

```

Device# show run wlan
wlan wlan_8 8 ssid_8
  security wpa psk set-key ascii 0 deadbeef
  no security wpa akm dot1x
  security wpa akm psk
  security wpa wpa2 mpsk
  priority 0 set-key ascii 0 deadbeef
  priority 1 set-key ascii 0 deaddead

```

```
priority 2 set-key ascii 0 d123d123
priority 3 set-key hex 0 023456789012345678901234567890123456789012345678901234
priority 4 set-key hex 0 1234567890123456789012345678901234567890123456789012345678901234
no shutdown
```



## CHAPTER 53

# Multiple Authentications for a Client

- [Information About Multiple Authentications for a Client, on page 473](#)
- [Configuring Multiple Authentications for a Client, on page 474](#)
- [Verifying Multiple Authentication Configurations, on page 480](#)

## Information About Multiple Authentications for a Client

Multiple Authentication feature is an extension of Layer 2 and Layer 3 security types supported for client join.



**Note** You can enable both L2 and L3 authentication for a given SSID.



**Note** The Multiple Authentication feature is applicable for regular clients only.

## Information About Supported Combination of Authentications for a Client

The Multiple Authentications for a Client feature supports multiple combination of authentications for a given client configured in the WLAN profile.

The following table outlines the supported combination of authentications:

Layer 2	Layer 3	Supported
MAB	CWA	Yes
MAB Failure	LWA	Yes
802.1X	CWA	Yes
PSK	CWA	Yes
iPSK + MAB	CWA	Yes
iPSK	LWA	No

MAB Failure + PSK	LWA	No
MAB Failure + PSK	CWA	No

From 16.10.1 onwards, 802.1X configurations on WLAN support web authentication configurations with WPA or WPA2 configuration.

The feature also supports the following AP modes:

- Local
- FlexConnect
- Fabric

## Configuring Multiple Authentications for a Client

### Configuring WLAN for 802.1X and Local Web Authentication (GUI)

#### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** Select the required WLAN from the list of WLANs displayed.
- Step 3** Choose **Security > Layer2** tab.
- Step 4** Select the security method from the **Layer 2 Security Mode** drop-down list.
- Step 5** In the **Auth Key Mgmt**, check the **802.1x** check box.
- Step 6** Check the **MAC Filtering** check box to enable the feature.
- Step 7** After MAC Filtering is enabled, from the **Authorization List** drop-down list, choose an option.
- Step 8** Choose **Security > Layer3** tab.
- Step 9** Check the **Web Policy** check box to enable web authentication policy.
- Step 10** From the **Web Auth Parameter Map** and the **Authentication List** drop-down lists, choose an option.
- Step 11** Click **Update & Apply to Device**.
- 

### Configuring WLAN for 802.1X and Local Web Authentication (CLI)

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	<b>wlan</b> <i>profile-name</i> <i>wlan-id</i> <i>SSID_Name</i> <b>Example:</b> Device(config)# <b>wlan wlan-test 3 ssid-test</b>	Enters WLAN configuration sub-mode. <ul style="list-style-type: none"> <li>• <i>profile-name</i>: Profile name of the configured WLAN.</li> <li>• <i>wlan-id</i>: Wireless LAN identifier. Range is from 1 to 512.</li> <li>• <i>SSID_Name</i>: SSID that can contain 32 alphanumeric characters.</li> </ul> <b>Note</b> If you have already configured this command, enter the <b>wlan profile-name</b> command.
<b>Step 3</b>	<b>security dot1x authentication-list</b> <i>auth-list-name</i> <b>Example:</b> Device(config-wlan)# <b>security dot1x authentication-list default</b>	Enables security authentication list for dot1x security. The configuration is similar for all dot1x security WLANs.
<b>Step 4</b>	<b>security web-auth</b> <b>Example:</b> Device(config-wlan)# <b>security web-auth</b>	Enables web authentication.
<b>Step 5</b>	<b>security web-auth authentication-list</b> <i>authenticate-list-name</i> <b>Example:</b> Device(config-wlan)# <b>security web-auth authentication-list default</b>	Enables authentication list for dot1x security.
<b>Step 6</b>	<b>security web-auth parameter-map</b> <i>parameter-map-name</i> <b>Example:</b> Device(config-wlan)# <b>security web-auth parameter-map WLAN1_MAP</b>	Maps the parameter map. <b>Note</b> If a parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
<b>Step 7</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wlan)# <b>no shutdown</b>	Enables the WLAN.

### Example

```
wlan wlan-test 3 ssid-test
security dot1x authentication-list default
security web-auth
security web-auth authentication-list default
```

```
security web-auth parameter-map WLAN1_MAP
no shutdown
```

## Configuring WLAN for Preshared Key (PSK) and Local Web Authentication (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** Select the required WLAN.
- Step 3** Choose **Security > Layer2** tab.
- Step 4** Select the security method from the **Layer 2 Security Mode** drop-down list.
- Step 5** In the Auth Key Mgmt, uncheck the **802.1x** check box.
- Step 6** Check the **PSK** check box.
- Step 7** Enter the **Pre-Shared Key** and choose the PSK Format from the **PSK Format** drop-down list and the PSK Type from the **PSK Type** drop-down list.
- Step 8** Choose **Security > Layer3** tab.
- Step 9** Check the **Web Policy** checkbox to enable web authentication policy.
- Step 10** Choose the Web Auth Parameter Map from the **Web Auth Parameter Map** drop-down list and the authentication list from the **Authentication List** drop-down list.
- Step 11** Click **Update & Apply to Device**.
- 

## Configuring WLAN for Preshared Key (PSK) and Local Web Authentication

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wlan profile-name wlan-id SSID_Name</b> <b>Example:</b> Device(config)# <b>wlan wlan-test 3 ssid-test</b>	Enters WLAN configuration sub-mode. <ul style="list-style-type: none"> <li>• <i>profile-name</i>- Is the profile name of the configured WLAN.</li> <li>• <i>wlan-id</i> - Is the wireless LAN identifier. Range is from 1 to 512.</li> <li>• <i>SSID_Name</i> - Is the SSID which can contain 32 alphanumeric characters.</li> </ul>



	Command or Action	Purpose
		<b>Note</b> If you have already configured this command, enter <code>wlan profile-name</code> command.
<b>Step 3</b>	<b>security wpa psk set-key</b> <i>ascii/hex key password</i>  <b>Example:</b> Device(config-wlan) # <b>security wpa psk set-key ascii 0 PASSWORD</b>	Configures the PSK shared key.
<b>Step 4</b>	<b>no security wpa akm dot1x</b>  <b>Example:</b> Device(config-wlan) # <b>no security wpa akm dot1x</b>	Disables security AKM for dot1x.
<b>Step 5</b>	<b>security wpa akm psk</b>  <b>Example:</b> Device(config-wlan) # <b>security wpa akm psk</b>	Configures the PSK support.
<b>Step 6</b>	<b>security web-auth</b>  <b>Example:</b> Device(config-wlan) # <b>security web-auth</b>	Enables web authentication for WLAN.
<b>Step 7</b>	<b>security web-auth authentication-list</b> <i>authenticate-list-name</i>  <b>Example:</b> Device(config-wlan) # <b>security web-auth authentication-list webauth</b>	Enables authentication list for dot1x security.
<b>Step 8</b>	<b>security web-auth parameter-map</b> <i>parameter-map-name</i>  <b>Example:</b> (config-wlan) # <b>security web-auth parameter-map WLAN1_MAP</b>	Configures the parameter map.  <b>Note</b> If parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.

### Example

```
wlan wlan-test 3 ssid-test
 security wpa psk set-key ascii 0 PASSWORD
 no security wpa akm dot1x
 security wpa akm psk
 security web-auth
 security web-auth authentication-list webauth
 security web-auth parameter-map WLAN1_MAP
```

## Configuring WLAN for PSK or Identity Preshared Key (iPSK) and Central Web Authentication (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** Select the required WLAN.
- Step 3** Choose **Security > Layer2** tab.
- Step 4** Select the security method from the **Layer 2 Security Mode** drop-down list.
- Step 5** In the **Auth Key Mgmt**, uncheck the **802.1x** check box.
- Step 6** Check the **PSK** check box.
- Step 7** Enter the **Pre-Shared Key** and choose the PSK Format from the **PSK Format** drop-down list and the PSK Type from the **PSK Type** drop-down list.
- Step 8** Check the **MAC Filtering** check box to enable the feature.
- Step 9** With MAC Filtering enabled, choose the Authorization List from the **Authorization List** drop-down list.
- Step 10** Choose **Security > Layer3** tab.
- Step 11** Check the **Web Policy** checkbox to enable web authentication policy.
- Step 12** Choose the Web Auth Parameter Map from the **Web Auth Parameter Map** drop-down list and the authentication list from the **Authentication List** drop-down list.
- Step 13** Click **Update & Apply to Device**.
- 

## Configuring WLAN for PSK or Identity Preshared Key (iPSK) and Central Web Authentication

### Configuring WLAN

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wlan profile-name wlan-id SSID_Name</b> <b>Example:</b> Device(config)# <code>wlan wlan-test 3 ssid-test</code>	Enters WLAN configuration sub-mode. <ul style="list-style-type: none"> <li>• <i>profile-name</i> - Is the profile name of the configured WLAN.</li> <li>• <i>wlan-id</i> - Is the wireless LAN identifier. Range is from 1 to 512.</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• <i>SSID_Name</i> - Is the SSID which can contain 32 alphanumeric characters.</li> </ul> <p><b>Note</b> If you have already configured this command, enter <b>wlan profile-name</b> command.</p>
<b>Step 3</b>	<b>no security wpa akm dot1x</b> <b>Example:</b> Device(config-wlan) # <b>no security wpa akm dot1x</b>	Disables security AKM for dot1x.
<b>Step 4</b>	<b>security wpa psk set-key <i>ascii/hex key password</i></b> <b>Example:</b> Device(config-wlan) # <b>security wpa psk set-key ascii 0 PASSWORD</b>	Configures the PSK AKM shared key.
<b>Step 5</b>	<b>mac-filtering <i>auth-list-name</i></b> <b>Example:</b> Device(config-wlan) # <b>mac-filtering test-auth-list</b>	Sets the MAC filtering parameters.

**Example**

```
wlan wlan-test 3 ssid-test
no security wpa akm dot1x
security wpa psk set-key ascii 0 PASSWORD
mac-filtering test-auth-list
```

**Applying Policy Profile to a WLAN****Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile policy <i>policy-profile-name</i></b> <b>Example:</b> Device(config) # <b>wireless profile policy policy-iot</b>	Configures the default policy profile.

	Command or Action	Purpose
<b>Step 3</b>	<b>aaa-override</b> <b>Example:</b> Device(config-wireless-policy)# <b>aaa-override</b>	Configures AAA override to apply policies coming from the AAA or ISE servers.
<b>Step 4</b>	<b>nac</b> <b>Example:</b> Device(config-wireless-policy)# <b>nac</b>	Configures NAC in the policy profile.
<b>Step 5</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wireless-policy)# <b>no shutdown</b>	Shutdown the WLAN.
<b>Step 6</b>	<b>end</b> <b>Example:</b> Device(config-wireless-policy)# <b>end</b>	Returns to privileged EXEC mode.

**Example**

```
wireless profile policy policy-iot
aaa-override
nac
no shutdown
```

## Verifying Multiple Authentication Configurations

**Layer 2 Authentication**

After L2 authentication (Dot1x) is complete, the client is moved to *Webauth Pending* state.

To verify the client state after L2 authentication, use the following commands:

```
Device# show wireless client summary
Number of Local Clients: 1
MAC Address  AP Name  WLAN  State  Protocol  Method  Role
-----
58ef.68b6.aa60  ewlc1_ap_1  3  Webauth Pending  11n(5)  Dot1x  Local
Number of Excluded Clients: 0

Device# show wireless client mac-address <mac_address> detail

Auth Method Status List

Method: Dot1x
Webauth State: Init
Webauth Method: Webauth
Local Policies:
Service Template: IP-Adm-V6-Int-ACL-global (priority 100)
```

```

URL Redirect ACL: IP-Adm-V6-Int-ACL-global
Service Template: IP-Adm-V4-Int-ACL-global (priority 100)
URL Redirect ACL: IP-Adm-V4-Int-ACL-global
Service Template: wlan_svc_default-policy-profile_local (priority 254)
Absolute-Timer: 1800
VLAN: 50

```

```
Device# show platform software wireless-client chassis active R0
```

ID	MAC Address	WLAN	Client	State
0xa0000003	58ef.68b6.aa60	3		L3 Authentication

```
Device# show platform software wireless-client chassis active F0
```

ID	MAC Address	WLAN	Client	State	AOM ID	Status
0xa0000003	58ef.68b6.aa60	3		L3		Authentication. 730.

```
Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
summary
```

Client Type Abbreviations:

RG - REGULAR BLE - BLE  
HL - HALO LI - LWFL INT

Auth State Abbreviations:

UK - UNKNOWN IP - LEARN IP IV - INVALID  
L3 - L3 AUTH RN - RUN

Mobility State Abbreviations:

UK - UNKNOWN IN - INIT  
LC - LOCAL AN - ANCHOR  
FR - FOREIGN MT - MTE  
IV - INVALID

EoGRE Abbreviations:

N - NON EOGRE Y - EOGRE

CPP IF_H	DP IDX	MAC Address	VLAN	CT	MCVL	AS	MS	E	WLAN	POA
0X49	0XA0000003	58ef.68b6.aa60	50	RG	0	L3	LC	N	wlan-test	0x90000003

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath summary
```

Vlan	DP IDX	MAC Address	VLAN	CT	MCVL	AS	MS	E	WLAN	POA
0X49	0xa0000003	58ef.68b6.aa60	50	RG	0	L3	LC	N	wlan-test	0x90000003

### Layer 3 Authentication

Once L3 authentication is successful, the client is moved to *Run* state.

To verify the client state after L3 authentication, use the following commands:

```
Device# show wireless client summary
```

Number of Local Clients: 1

MAC Address	AP Name	WLAN	State	Protocol	Method	Role
58ef.68b6.aa60	ewlcl_ap_1	3	Run	11n(5)	Web Auth	Local

Number of Excluded Clients: 0

```

Device# show wireless client mac-address 58ef.68b6.aa60 detail

Auth Method Status List

Method: Web Auth
Webauth State: Authz
Webauth Method: Webauth
Local Policies:
Service Template: wlan_svc_default-policy-profile_local (priority 254)
Absolute-Timer: 1800
VLAN: 50

Server Policies:

Resultant Policies:
VLAN: 50
Absolute-Timer: 1800

```

```
Device# show platform software wireless-client chassis active R0
```

ID	MAC Address	WLAN	Client State
0xa0000001	58ef.68b6.aa60	3	Run

```
Device# show platform software wireless-client chassis active f0
```

ID	MAC Address	WLAN	Client State	AOM ID.	Status
0xa0000001	58ef.68b6.aa60.	3	Run	11633	Done

```
Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
summary
```

Client Type Abbreviations:

RG - REGULAR    BLE - BLE  
HL - HALO        LI - LWFL INT

Auth State Abbreviations:

UK - UNKNOWN    IP - LEARN    IP IV - INVALID  
L3 - L3 AUTH    RN - RUN

Mobility State Abbreviations:

UK - UNKNOWN    IN - INIT  
LC - LOCAL       AN - ANCHOR  
FR - FOREIGN    MT - MTE  
IV - INVALID

EoGRE Abbreviations:

N - NON EOGRE    Y - EOGRE

CPP IF_H	DP IDX	MAC Address	VLAN	CT	MCVL	AS	MS	E	WLAN	POA
0X49	0XA0000003	58ef.68b6.aa60	50	RG	0	RN	LC	N	wlan-test	0x90000003

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath summary
```

Vlan	pal_if_hdl	mac	Input Uidb	Output Uidb
50	0xa0000003	58ef.68b6.aa60	95929	95927

## Verifying PSK+Webauth Configuration

```
Device# show wlan summary
```

```
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 12:08:32.941 CEST Tue Oct 6 2020
```

Number of WLANs: 1

ID Profile Name SSID Status Security

---

23 Gladius1-PSKWEBAUTH Gladius1-PSKWEBAUTH UP [WPA2][PSK][AES],[Web Auth]







## CHAPTER 54

# Information About Cisco Umbrella WLAN

---

The Cisco Umbrella WLAN provides a cloud-delivered network security service at the Domain Name System (DNS) level, with automatic detection of both known and emergent threats.

This feature allows you to block sites that host malware, bot networks, and phishing before they actually become malicious.

Cisco Umbrella WLAN provides the following:

- Policy configuration per user group at a single point.
- Policy configuration per network, group, user, device, or IP address.

The following is the policy priority order:

1. Local policy
  2. AP group
  3. WLAN
- Visual security activity dashboard in real time with aggregated reports.
  - Schedule and send reports through email.
  - Support up to 60 content categories, with a provision to add custom allowed list and blocked list entries.

This feature does not work in the following scenarios:

- If an application or host use an IP address directly, instead of using DNS to query domain names.
- If a client is connected to a web proxy and does not send a DNS query to resolve the server address.
- [Registering Embedded Wireless Controller to Cisco Umbrella Account, on page 486](#)
- [Configuring Cisco Umbrella WLAN, on page 487](#)
- [Verifying the Cisco Umbrella Configuration, on page 493](#)

# Registering Embedded Wireless Controller to Cisco Umbrella Account

## Before you Begin

- You should have an account with Cisco Umbrella.
- You should have an API token from Cisco Umbrella.

The embedded wireless controller is registered to Cisco Umbrella server using the Umbrella parameter map. Each of the Umbrella parameter map must have an API token. The Cisco Umbrella responds with the device ID for the embedded wireless controller. The device ID has a 1:1 mapping with the Umbrella parameter map name.

## Fetching API token for Embedded Wireless Controller from Cisco Umbrella Dashboard

From Cisco Umbrella dashboard, verify that your embedded wireless controller shows up under Device Name, along with their identities.

## Applying the API Token on Embedded Wireless Controller

Registers the Cisco Umbrella API token on the network.

## DNS Query and Response

Once the device is registered and Umbrella parameter map is configured on WLAN, the DNS queries from clients joining the WLAN are redirected to the Umbrella DNS resolver.



---

**Note** This is applicable for all domains not configured in the local domain RegEx parameter map.

---

The queries and responses are encrypted based on the DNSCrypt option in the Umbrella parameter map.

For more information on the Cisco Umbrella configurations, see the [Integration for ISR 4K and ISR 1100 – Security Configuration Guide](#).

## Limitations and Considerations

The limitations and considerations for this feature are as follows:

- You will be able to apply the wireless Cisco Umbrella profiles to wireless entities, such as, WLAN or AP groups, if the device registration is successful.
- In case of L3 mobility, the Cisco Umbrella must be applied on the anchor embedded wireless controller always.
- When two DNS servers are configured under DHCP, two Cisco Umbrella server IPs are sent to the client from DHCP option 6. If only one DNS server is present under DHCP, only one Cisco Umbrella server IP is sent as part of DHCP option 6.

# Configuring Cisco Umbrella WLAN

To configure Cisco Umbrella on the embedded wireless controller, perform the following:

- You must have the API token from the Cisco Umbrella dashboard.
- You must have the root certificate to establish HTTPS connection with the Cisco Umbrella registration server: [api.opendns.com](http://api.opendns.com). You must import the root certificate from **digicert.com** to the embedded wireless controller using the **crypto pki trustpool import terminal** command.

## Importing CA Certificate to the Trust Pool

### Before you begin

The following section covers details about how to fetch the root certificate and establish HTTPS connection with the Cisco Umbrella registration server:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	Perform either of the following tasks: <ul style="list-style-type: none"> <li>• <b>crypto pki trustpool import url url</b>                Device(config)# <code>crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b</code>                Imports the root certificate directly from the Cisco website.  <b>Note</b> The Trustpool bundle contains the root certificate of <i>digicert.com</i> together with other CA certificates.</li> <li>• <b>crypto pki trustpool import terminal</b>                Device(config)# <code>crypto pki trustpool import terminal</code>                Imports the root certificate by executing the import terminal command.</li> <li>• Enter PEM-formatted CA certificate from the following location: See the Related Information section to download the CA certificate.</li> </ul>	

	Command or Action	Purpose
	<pre>-----BEGIN CERTIFICATE----- MIIEGjCCAgAwgCqjUIMwKPKlVA3NBjchc9MBAQIAMSQDQq EwUeEMGALKHMFCraNcrQ85jRkEVMQEESSRzGraNcrQ1Z8MA HjDQDEdchq2VcHhG9Vgjn9dEQA6QMDhJOMAMIEB0MDhMj MELNlM83ZABjNBAVMRGEADQ8E8hVQ2VcHhMKA8jNEMIEB Z2DZC0IEMjB8Dg10hJ2ZDw9q0EMIEF7N8jchkc9MBAQIAMS CjCAwAELZ8wNlBNs0BZlUMNl7jR85jRkEVMQEESSRzGraN E8h92wIHlQIHC8hE8Mf5HjLlE855VQE8Kw6at9f0rTCR80R0 Vf0L99qj1M86LUNwRALE/3-klJlnWkCra85jRkEVMQEESSRz nuh9j85j1hE8P3LUNQ8E85j7C4HyE8K83Nec0L6W8Q8j40 K67S9h808jZ8eacicq7CPUTT4k7QDA85jRkEVMQEESSRzGra Eldcupp8e8q2j8570rMBAL8jQMA85jRkEVMQEESSRzGraNcr ALd8E8/CAwAELZ8wNlBNs0BZlUMNl7jR85jRkEVMQEESSRz R8E8wE8E8jR8E8P8Q8jC8jRkEVMQEESSRzGraNcrQ1Z8MA JmN8E8E8E8P8Q8jC8jRkEVMQEESSRzGraNcrQ1Z8MAZ2XCR8v Y8E8jR8E8h8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8 R8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8 R8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8 35H8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8 U8E8P8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8 5q8E8S8K8M8g8Q8jCA8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8 Y8E8S8wA8p838x8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8jR8E8 SaZMkE4f97Q= -----END CERTIFICATE-----</pre> <p>Imports the root certificate by pasting the CA certificate from the <b>digicert.com</b>.</p>	
<b>Step 3</b>	<p><b>quit</b></p> <p><b>Example:</b></p> <pre>Device(config)# quit</pre>	<p>Imports the root certificate by entering the <b>quit</b> command.</p> <p><b>Note</b> You will receive a message after the certificate has been imported.</p>

## Creating a Local Domain RegEx Parameter Map

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 2</b>	<p><b>parameter-map type regex</b></p> <p><i>parameter-map-name</i></p> <p><b>Example:</b></p> <pre>Device(config)# parameter-map type regex dns_w1</pre>	Creates a regex parameter map.
<b>Step 3</b>	<p><b>pattern</b> <i>regex-pattern</i></p>	Configures the regex pattern to match.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device(config-profile)# pattern www.google.com</pre>	<p><b>Note</b> The following patterns are supported:</p> <ul style="list-style-type: none"> <li>• Begins with . *. For example: <b>. *facebook . com</b></li> <li>• Begins with . * and ends with * . For example: <b>*google*</b></li> <li>• Begins with * . For example: <b>*facebook . com</b></li> <li>• Begins with * and ends with *. For example: <b>*google*</b></li> <li>• Ends with *. For example: <b>www . facebook*</b></li> <li>• No special character. For example: <b>www . facebook . com</b></li> </ul>
<b>Step 4</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-profile)# end</pre>	<p>Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.</p>

## Configuring Parameter Map Name in WLAN (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Policy**.
- Step 2** Click on the Policy Profile Name. The **Edit Policy Profile** window is displayed.
- Step 3** Choose the **Advanced** tab.
- Step 4** In the **Umbrella** settings, from the **Umbrella Parameter Map** drop-down list, choose the parameter map.
- Step 5** Enable or disable **Flex DHCP Option for DNS** and **DNS Traffic Redirect** toggle buttons.
- Step 6** Click **Update & Apply to Device**.
-

## Configuring the Umbrella Parameter Map

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>parameter-map type umbrella global</b>  <b>Example:</b> Device(config)# <code>parameter-map type umbrella global</code>	Creates an umbrella global parameter map.
<b>Step 3</b>	<b>token <i>token-value</i></b>  <b>Example:</b> Device(config-profile)# <code>token 5XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</code>	Configures an umbrella token.
<b>Step 4</b>	<b>local-domain <i>regex-parameter-map-name</i></b>  <b>Example:</b> Device(config-profile)# <code>local-domain dns_w1</code>	Configures local domain RegEx parameter map.
<b>Step 5</b>	<b>resolver {IPv4 X.X.X.X   IPv6 X:X:X:X::X}</b>  <b>Example:</b> Device(config-profile)# <code>resolver IPv6 10:1:1:1::10</code>	Configures the Anycast address. The default address is applied when there is no specific address configured.
<b>Step 6</b>	<b>end</b>  <b>Example:</b> Device(config-profile)# <code>end</code>	Returns to privileged EXEC mode.

## Enabling or Disabling DNSCrypt (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Security > Threat Defence > Umbrella**.
  - Step 2** Enter the **Registration Token** received from Umbrella. Alternatively, you can click on **Click here to get your Token** to get the token from Umbrella.
  - Step 3** Enter the **Whitelist Domains** that you want to exclude from filtering.
  - Step 4** Check or uncheck the **Enable DNS Packets Encryption** check box to encrypt or decrypt the DNS packets.
  - Step 5** Click **Apply**.
-

## Enabling or Disabling DNScrypt

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>parameter-map type umbrella global</b> <b>Example:</b> Device(config)# <code>parameter-map type umbrella global</code>	Creates an umbrella global parameter map.
<b>Step 3</b>	<b>[no] dnsencrypt</b> <b>Example:</b> Device(config-profile)# <code>no dnsencrypt</code>	Enables or disables DNScrypt. By default, the DNScrypt option is enabled. <b>Note</b> Cisco Umbrella DNScrypt is not supported when DNS-encrypted responses are sent in the data-DTLS encrypted tunnel (either mobility tunnel or AP CAPWAP tunnel).
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config-profile)# <code>end</code>	Returns to privileged EXEC mode.

## Configuring Timeout for UDP Sessions

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>parameter-map type umbrella global</b> <b>Example:</b> Device(config)# <code>parameter-map type umbrella global</code>	Creates an umbrella global parameter map.
<b>Step 3</b>	<b>udp-timeout <i>timeout_value</i></b> <b>Example:</b> Device(config-profile)# <code>udp-timeout 2</code>	Configures timeout value for UDP sessions. The <i>timeout_value</i> ranges from 1 to 30 seconds.

	Command or Action	Purpose
		<b>Note</b> The <b>public-key</b> and <b>resolver</b> parameter-map options are automatically populated with the default values. So, you need not change them.
<b>Step 4</b>	<b>end</b>  <b>Example:</b> Device(config-profile)# <b>end</b>	Returns to privileged EXEC mode.

## Configuring Parameter Map Name in WLAN (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Policy**.
  - Step 2** Click on the Policy Profile Name. The **Edit Policy Profile** window is displayed.
  - Step 3** Choose the **Advanced** tab.
  - Step 4** In the **Umbrella** settings, from the **Umbrella Parameter Map** drop-down list, choose the parameter map.
  - Step 5** Enable or disable **Flex DHCP Option for DNS** and **DNS Traffic Redirect** toggle buttons.
  - Step 6** Click **Update & Apply to Device**.
- 

## Configuring Parameter Map Name in WLAN

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile policy <i>profile-name</i></b>  <b>Example:</b> Device(config)# <code>wireless profile policy default-policy-profile</code>	Creates policy profile for the WLAN.  The <i>profile-name</i> is the profile name of the policy profile.
<b>Step 3</b>	<b>umbrella-param-map <i>umbrella-name</i></b>  <b>Example:</b> Device(config-wireless-policy)# <code>umbrella-param-map global</code>	Configures the Umbrella OpenDNS feature for the WLAN.



	Command or Action	Purpose
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config-wireless-policy)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Verifying the Cisco Umbrella Configuration

To view the Umbrella configuration details, use the following command:

```
Device# show umbrella config
Umbrella Configuration
=====
Token: 5XXXXXXXXABXXXXXXFXXXXXXXXDXXXXXXXXXXABXX
API-KEY: NONE
OrganizationID: xxxxxxxx
Local Domain Regex parameter-map name: dns_bypass
DNSEncrypt: Not enabled
Public-key: NONE
UDP Timeout: 5 seconds
Resolver address:
1. 10.1.1.1
2. 5.5.5.5
3. XXXX:120:50::50
4. XXXX:120:30::30
```

To view the Umbrella DNSEncrypt details, use the following command:

```
Device# show umbrella dnscrypt
DNSEncrypt: Enabled
  Public-key: B111:XXXX:XXXX:XXXX:3E2B:XXXX:XXXX:XXxE:XXX3:3XXX:DXXX:XXXX:BXXX:XXXB:XXXX:FXXX

  Certificate Update Status: In Progress
```

To view the Umbrella global parameter map details, use the following command:

```
Device# show parameter-map type umbrella global
```

To view the regex parameter map details, use the following command:

```
Device# show parameter-map type regex <parameter-map-name>
```

To view the Umbrella details on the AP, use the following command:

```
AP#show client.opendns summary
Server-IP role
208.67.220.220 Primary
208.67.222.222 Secondary

Server-IP role
2620:119:53::53 Primary
2620:119:35::35 Secondary

Wlan Id DHCP OpenDNS Override Force Mode
0 true false
1 false false
...

15 false false
Profile-name Profile-id
vj-1 010a29b176b34108
```

```
global 010a57bf502c85d4
vj-2 010ae385ce6c1256
AP0010.10A7.1000#
```

Client to profile command

```
AP#show client opensns address 50:3e:aa:ce:50:17
Client-mac Profile-name
50:3E:AA:CE:50:17 vj-1
AP0010.10A7.1000#
```



## CHAPTER 55

# Locally Significant Certificates

- [Information About Locally Significant Certificates, on page 495](#)
- [Restrictions for Locally Significant Certificates, on page 496](#)
- [Provisioning Locally Significant Certificates, on page 497](#)
- [Verifying LSC Configuration, on page 505](#)
- [Configuring Management Trustpoint to LSC \(GUI\), on page 506](#)
- [Configuring Management Trustpoint to LSC \(CLI\), on page 506](#)

## Information About Locally Significant Certificates

This module explains how to configure the Cisco Embedded Wireless Controller on Catalyst Access Points and Lightweight Access Points (LAPs) to use the Locally Significant Certificate (LSC). If you choose the Public Key Infrastructure (PKI) with LSC, you can generate the LSC on the APs and embedded wireless controllers. You can then use the certificates to mutually authenticate the embedded wireless controller and the APs.

In Cisco embedded wireless controllers, you can configure the embedded wireless controller to use an LSC. Use an LSC if you want your own PKI to provide better security, have control of your Certificate Authority (CA), and define policies, restrictions, and usages on the generated certificates.

You need to provision the new LSC certificate on the embedded wireless controller and then the Lightweight Access Point (LAP) from the CA Server.

The LAP communicates with the embedded wireless controller using the CAPWAP protocol. Any request to sign the certificate and issue the CA certificates for LAP and embedded wireless controller itself must be initiated from the embedded wireless controller. The LAP does not communicate directly with the CA server. The CA server details must be configured on the embedded wireless controller and must be accessible.

The embedded wireless controller makes use of the Simple Certificate Enrollment Protocol (SCEP) to forward certReqs generated on the devices to the CA and makes use of SCEP again to get the signed certificates from the CA.

The SCEP is a certificate management protocol that the PKI clients and CA servers use to support certificate enrollment and revocation. It is widely used in Cisco and supported by many CA servers. In SCEP, HTTP is used as the transport protocol for the PKI messages. The primary goal of SCEP is the secure issuance of certificates to network devices. SCEP is capable of many operations, but for our release, SCEP is utilized for the following operations:

- CA and Router Advertisement (RA) Public Key Distribution

- Certificate Enrollment

## Certificate Provisioning in Controllers

The new LSC certificates, both CA and device certificates, must be installed on the controller.

With the help of SCEP, CA certificates are received from the CA server. During this point, there are no certificates in the controller. After the **get** operation of obtaining the CA certificates, are installed on the controller. The same CA certificates are also pushed to the APs when the APs are provisioned with LSCs.

## Device Certificate Enrollment Operation

For both the LAP and the controller that request a CA-signed certificate, the certRequest is sent as a PKCS#10 message. The certRequest contains the Subject Name, Public Key, and other attributes to be included in the X.509 certificate, and must be digitally signed by the Private Key of the requester. These are then sent to the CA, which transforms the certRequest into an X.509 certificate.

The CA that receives a PKCS#10 certRequest requires additional information to authenticate the requester's identity and verify if the request is unaltered. (Sometimes, PKCS#10 is combined with other approaches, such as PKCS#7 to send and receive the certificate request or response.)

The PKCS#10 is wrapped in a PKCS#7 Signed Data message type. This is supported as part of the SCEP client functionality, while the PKCSReq message is sent to the controller. Upon successful enrollment operation, both the CA and device certificates are available on the controller.

## Certificate Provisioning on Lightweight Access Point

In order to provision a new certificate on LAP, while in CAPWAP mode, the LAP must be able to get the new signed X.509 certificate. In order to do this, it sends a certRequest to the controller, which acts as a CA proxy and helps obtain the certRequest signed by the CA for the LAP.

The certReq and the certResponses are sent to the LAP with the LWAPP payloads.

Both the LSC CA and the LAP device certificates are installed in the LAP, and the system reboots automatically. The next time when the system comes up, because it is configured to use LSCs, the AP sends the LSC device certificate to the controller as part of the JOIN Request. As part of the JOIN Response, the controller sends the new device certificate and also validates the inbound LAP certificate with the new CA root certificate.

### What to Do Next

To configure, authorize, and manage certificate enrollment with the existing PKI infrastructure for controller and AP, you need to use the LSC provisioning functionality.

## Restrictions for Locally Significant Certificates

- LSC workflow is different in FIPS+WLANCC mode. CA server must support Enrollment over Secure Transport (EST) protocol and should be capable of issuing EC certificates in FIPS+WLANCC mode.
- Elliptic Curve Digital Signature Algorithm (ECDSA) cipher works only if both AP and controller are having EC certificates, provisioned with LSC.

- EC certificates (LSC-EC) can be provisioned only if CA server supports EST (and not SCEP).
- FIPS + CC security modes is required to be configured in order to provision EC certificate.

## Provisioning Locally Significant Certificates

### Configuring RSA Key for PKI Trustpoint

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>crypto key generate rsa [exportable]</b> <b>general-keys modulus <i>key_size</i> label <i>RSA_key</i></b>  <b>Example:</b> Device(config)# <code>crypto key generate rsa exportable general-keys modulus 2048 label lsc-tp</code>	Configures RSA key for PKI trustpoint. <b>exportable</b> is an optional keyword. You may or may not want to configure an exportable-key. If selected, you can export the key out of the box, if required <ul style="list-style-type: none"> <li>• <i>key_size</i>: Size of the key modulus. The valid range is from 2048 to 4096.</li> <li>• <i>RSA_key</i>: RSA key pair label.</li> </ul>
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Device(config)# <code>end</code>	Returns to privileged EXEC mode.

### Configuring PKI Trustpoint Parameters

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>crypto pki trustpoint <i>trustpoint_name</i></b>  <b>Example:</b> Device(config)# <code>crypto pki trustpoint microsoft-ca</code>	Creates a new trustpoint for an external CA server. Here, <i>trustpoint_name</i> refers to the trustpoint name.

	Command or Action	Purpose
<b>Step 3</b>	<b>enrollment url</b> <i>HTTP_URL</i> <b>Example:</b> Device (ca-trustpoint) # <b>enrollment url</b> <b>http://CA_server/certsrv/mscep/mscep.dll</b>	Specifies the URL of the CA on which your router should send certificate requests.  <b>url url:</b> URL of the file system where your router should send certificate requests. An IPv6 address can be added in the URL enclosed in brackets. For example: http://[2001:DB8:1:1::1]:80. For more enrollment method options, see the enrollment url (ca-trustpoint) command page.
<b>Step 4</b>	<b>subject-name</b> <i>subject_name</i> <b>Example:</b> Device (ca-trustpoint) # <b>subject-name</b> C=IN,  ST=KA, I=Bengaluru, O=Cisco, CN=eagle-eye/emailAddress=support@abc.com	Creates subject name parameters for the trustpoint.
<b>Step 5</b>	<b>rsakeypair</b> <i>RSA_key key_size</i> <b>Example:</b> Device (ca-trustpoint) # <b>rsakeypair</b> <b>ewlc-tp1</b>	Maps RSA key with that of the trustpoint. <ul style="list-style-type: none"> <li>• <i>RSA_key</i>: RSA key pair label.</li> <li>• <i>key_size</i>: Signature key length. Range is from 360 to 4096.</li> </ul>
<b>Step 6</b>	<b>revocation</b> {crl   none   oosp} <b>Example:</b> Device (ca-trustpoint) # <b>revocation none</b>	Checks revocation.
<b>Step 7</b>	<b>end</b> <b>Example:</b> Device (ca-trustpoint) # <b>end</b>	Returns to privileged EXEC mode.

## Authenticating and Enrolling a PKI Trustpoint (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Security > PKI Management**.
- Step 2** In the **PKI Management** window, click the **Trustpoints** tab.
- Step 3** In the **Add Trustpoint** dialog box, provide the following information:
- In the **Label** field, enter the RSA key label.
  - In the **Enrollment URL** field, enter the enrollment URL.
  - Check the **Authenticate** check box to authenticate the Public Certificate from the enrollment URL.
  - In the **Subject Name** section, enter the **Country Code**, **State**, **Location**, **Organisation**, **Domain Name**, and **Email Address**.

- e) Check the **Key Generated** check box to view the available RSA keypairs. Choose an option from the **Available RSA Keypairs** drop-down list.
- f) Check the **Enroll Trustpoint** check box.
- g) In the **Password** field, enter the password.
- h) In the **Re-Enter Password** field, confirm the password.
- i) Click **Apply to Device**.

The new trustpoint is added to the trustpoint name list.

## Authenticating and Enrolling the PKI Trustpoint with CA Server (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>crypto pki authenticate trustpoint_name</b> <b>Example:</b> Device (config)# <b>crypto pki authenticate microsoft-ca</b>	Fetches the CA certificate.
<b>Step 3</b>	<b>yes</b> <b>Example:</b> Device(config)# % Do you accept this certificate? [yes/no]: yes Trustpoint CA certificate accepted.	
<b>Step 4</b>	<b>crypto pki enroll trustpoint_name</b> <b>Example:</b> Device (config)# <b>crypto pki enroll microsoft-ca</b> % % Start certificate enrollment .. % Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it.	Enrolls the client certificate.
<b>Step 5</b>	<b>password</b> <b>Example:</b> Device (config)# <b>abcd123</b>	Enters a challenge password to the CA server.

	Command or Action	Purpose
<b>Step 6</b>	<b>password</b> <b>Example:</b> Device(config)# <b>abcd123</b>	Re-enters a challenge password to the CA server.
<b>Step 7</b>	<b>yes</b> <b>Example:</b> Device(config)# % <b>Include the router serial number in the subject name? [yes/no]: yes</b>	
<b>Step 8</b>	<b>no</b> <b>Example:</b> Device(config)# % <b>Include an IP address in the subject name? [no]: no</b>	
<b>Step 9</b>	<b>yes</b> <b>Example:</b> Device(config)# <b>Request certificate from CA? [yes/no]: yes</b> % <b>Certificate request sent to Certificate Authority</b> % <b>The 'show crypto pki certificate verbose client' command will show the fingerprint.</b>	
<b>Step 10</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode.

## Configuring AP Join Attempts with LSC Certificate (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Wireless > Access Points**.
  - Step 2** In the **All Access Points** window, click the LSC Provision name.
  - Step 3** From the **Status** drop-down list, choose a status to enable LSC.
  - Step 4** From the **Trustpoint Name** drop-down list, choose the trustpoint.
  - Step 5** In the **Number of Join Attempts** field, enter the number of retry attempts that will be permitted.
  - Step 6** Click **Apply**.
-



## Configuring AP Join Attempts with LSC Certificate (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ap lsc-provision join-attempt</b> <i>number_of_attempts</i> <b>Example:</b> Device(config)# <code>ap lsc-provision join-attempt 10</code>	Specifies the maximum number of AP join failure attempts with the newly provisioned LSC certificate.  When the number of AP joins exceed the specified limit, AP joins back with the Manufacturer Installed Certificate (MIC).
<b>Step 3</b>	<b>end</b> <b>Example:</b> Device(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring Subject-Name Parameters in LSC Certificate

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ap lsc-provision subject-name-parameter</b> <b>country</b> <i>country-str</i> <b>state</b> <i>state-str</i> <b>city</b> <i>city-str</i> <b>domain</b> <i>domain-str</i> <b>org</b> <i>org-str</i> <b>email-address</b> <i>email-addr-str</i> <b>Example:</b> Device(config)# <code>ap lsc-provision subject-name-parameter country India state Karnataka city Bangalore domain domain1 org Right email-address adc@gfe.com</code>	Specifies the attributes to be included in the subject-name parameter of the certificate request generated by an AP.
<b>Step 3</b>	<b>end</b> <b>Example:</b> Device(config)# <code>end</code>	Returns to privileged EXEC mode.

## Configuring Key Size for LSC Certificate

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ap lsc-provision key-size { 2048   3072   4096 }</b>  <b>Example:</b> Device (config) # <code>ap lsc-provision key-size 2048</code>	Specifies the size of keys to be generated for the LSC on AP.
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Device (config) # <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring Trustpoint for LSC Provisioning on an Access Point

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ap lsc-provision trustpoint <i>tp-name</i></b>  <b>Example:</b> Device (config) # <code>ap lsc-provision trustpoint microsoft-ca</code>	Specifies the trustpoint with which the LCS is provisioned to an AP.  <i>tp-name</i> : The trustpoint name.
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Device (config) # <code>end</code>	Returns to privileged EXEC mode.

## Configuring an AP LSC Provision List (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Wireless > Access Points**.

- Step 2** In the **All Access Points** window, click the corresponding LSC Provision name.
- Step 3** From the **Status** drop-down list, choose a status to enable LSC.
- Step 4** From the **Trustpoint Name** drop-down list, choose a trustpoint.
- Step 5** In the **Number of Join Attempts** field, enter the number of retry attempts that are allowed.
- Step 6** From the **Key Size** drop-down list, choose a key.
- Step 7** In the **Edit AP Join Profile** window, click the **CAPWAP** tab.
- Step 8** In the **Add APs to LSC Provision List** section, click **Select File** to upload the CSV file that contains AP details.
- Step 9** Click **Upload File**.
- Step 10** In the **AP MAC Address** field, enter the AP MAC address. and add them. (The APs added to the provision list are displayed in the **APs in provision List** .)
- Step 11** In the **Subject Name Parameters** section, enter the following details:
- **Country**
  - **State**
  - **City**
  - **Organisation**
  - **Department**
  - **Email Address**
- Step 12** Click **Apply**.

## Configuring an AP LSC Provision List (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>[no] ap lsc-provision mac-address mac-addr</b>  <b>Example:</b> Device(config)# no ap lsc-provision mac-address 001b.3400.02f0	Adds the AP to the LSC provision list.  <b>Note</b> You can provision a list of APs using the <b>ap lsc-provision provision-list</b> command.  (Or)  You can provision all the APs using the <b>ap lsc-provision</b> command.

	Command or Action	Purpose
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode.

## Configuring LSC Provisioning for all the APs (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Wireless > Access Points**.
- Step 2** In the **Access Points** window, expand the **LSC Provision** section.
- Step 3** Set **Status** to **Enabled** state.
- Note** If you set **Status** to **Provision List**, LSC provisioning will be configured only for APs that are a part of the provision list.
- Step 4** From the **Trustpoint Name** drop-down list, choose the appropriate trustpoint for all APs.
- Step 5** In the **Number of Join Attempts** field, enter the number of retry attempts that the APs can make to join the embedded wireless controller.
- Step 6** From the **Key Size** drop-down list, choose the appropriate key size of the certificate:
- 2048
  - 3072
  - 4096
- Step 7** In the **Add APs to LSC Provision List** section, click **Select File** to upload the CSV file that contains the AP details.
- Step 8** Click **Upload File**.
- Step 9** In the **AP MAC Address** field, enter the AP MAC address. (The APs that are added to the provision list are displayed in the **APs in Provision List** section.)
- Step 10** In the **Subject Name Parameters** section, enter the following details:
- a. **Country**
  - b. **State**
  - c. **City**
  - d. **Organization**
  - e. **Department**
  - f. **Email Address**
- Step 11** Click **Apply**.
-

## Configuring LSC Provisioning for All APs (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>[no] ap lsc-provision</b> <b>Example:</b> Device(config)# <code>no ap lsc-provision</code>	Enables LSC provisioning for all APs.  By default, LSC provisioning is disabled for all APs.
<b>Step 3</b>	<b>end</b> <b>Example:</b> Device(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring LSC Provisioning for the APs in the Provision List

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ap lsc-provision provision-list</b> <b>Example:</b> Device(config)# <code>ap lsc-provision provision-list</code>	Enables LSC provisioning for a set of APs configured in the provision list.
<b>Step 3</b>	<b>end</b> <b>Example:</b> Device(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Verifying LSC Configuration

To view the details of the wireless management trustpoint, use the following command:

```
Device# show wireless management trustpoint
```

```
Trustpoint Name : microsoft-ca
Certificate Info : Available
Certificate Type : LSC
```

```
Certificate Hash : 9e5623adba5307facf778e6ea2f5082877ea4beb
Private key Info : Available
```

To view the LSC provision-related configuration details for an AP, use the following command:

```
Device# show ap lsc-provision summary

AP LSC-provisioning : Disabled
Trustpoint used for LSC-provisioning : microsoft-ca
LSC Revert Count in AP reboots : 10

AP LSC Parameters :
Country : IN
State : KA
City : BLR
Orgn : ABC
Dept : ABC
Email : support@abc.com
Key Size : 2048

AP LSC-provision List : Enabled
Total number of APs in provision list: 3

Mac Address
-----
0038.df24.5fd0
2c5a.0f22.d4ca
e4c7.22cd.b74f
```

## Configuring Management Trustpoint to LSC (GUI)

### Procedure

---

- Step 1** Choose **Administration > Management > HTTP/HTTPS**.
  - Step 2** In the **HTTP Trust Point Configuration** section, set **Enable Trust Point** to the **Enabled** state.
  - Step 3** From the **Trust Points** drop-down list, choose the appropriate trustpoint.
  - Step 4** Save the configuration.
- 

## Configuring Management Trustpoint to LSC (CLI)

After LSC provisioning, the APs will automatically reboot and join at the LSC mode after bootup. Similarly, if you remove the AP LSC provisioning, the APs reboot and join at non-LSC mode.

In EWC, the internal APs will not automatically reboot. You should manually reboot the internal AP to make it work in LSC and non-LSC mode.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless management trustpoint</b> <i>trustpoint_name</i> <b>Example:</b> Device(config)# <code>wireless management trustpoint microsoft-ca</code>	Configures the management trustpoint to LSC. The internal AP will not be able to join before a reload, so follow the steps given below to reload the internal AP.
<b>Step 3</b>	<b>write memory</b> <b>Example:</b> Device(config)# <code>write memory</code>	Saves the configuration.
<b>Step 4</b>	<b>wireless ewc-ap ap reload</b> <b>Example:</b> Device(config)# <code>write memory</code>	Reloads the internal AP. This will also reload the controller on the AP.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.







## PART **VII**

### **Quality of Service**

- [Quality of Service, on page 511](#)
- [Wireless Auto-QoS, on page 539](#)
- [Native Profiling, on page 545](#)





## CHAPTER 56

# Quality of Service

---

- [Wireless QoS Overview, on page 511](#)
- [Wireless QoS Targets, on page 511](#)
- [Precious Metal Policies for Wireless QoS, on page 512](#)
- [Prerequisites for Wireless QoS, on page 513](#)
- [Restrictions for QoS on Wireless Targets, on page 513](#)
- [Metal Policy Format, on page 514](#)
- [How to apply Bi-Directional Rate Limiting, on page 521](#)
- [How to apply Per Client Bi-Directional Rate Limiting, on page 528](#)
- [How to Configure Wireless QoS, on page 532](#)

## Wireless QoS Overview

Quality of Service (QoS), provides the ability to prioritize the traffic by giving preferential treatment to specific traffic over the other traffic types. Without QoS, the device offers best-effort service for each packet, regardless of the packet contents or size. The device sends the packets without any assurance of reliability, delay bounds, or throughput.

A target is the entity where the policy is applied. Wireless QoS policies for SSID and client are applied in the upstream and (or) downstream direction. The flow of traffic from a wired source to a wireless target is known as downstream traffic. The flow of traffic from a wireless source to a wired target is known as upstream traffic.

The following are some of the specific features provided by wireless QoS:

- SSID and client policies on wireless QoS targets
- Marking and Policing (also known as Rate Limiting ) of wireless traffic

## Wireless QoS Targets

This section describes the various wireless QoS targets available on a device.

### SSID Policies

You can create QoS policies on SSID in both the ingress and egress directions. If not configured, there is no SSID policy applied.

The policy is applicable per AP per SSID.

You can configure policing and marking policies on SSID.

## Client Policies

Client policies are applicable in the ingress and egress direction. You can configure policing and marking policies on clients. AAA override is also supported.

## Supported QoS Features on Wireless Targets

This table describes the various features available on wireless targets.

*Table 22: QoS Features Available on Wireless Targets*

Target	Features	Direction Where Policies Are Applicable
SSID	<ul style="list-style-type: none"> <li>• Set</li> <li>• Police</li> <li>• Drop</li> </ul>	Upstream and downstream
Client	<ul style="list-style-type: none"> <li>• Set</li> <li>• Police</li> <li>• Drop</li> </ul>	Upstream and downstream



**Note** For Drop support, the Drop action is achieved by the following configuration:

```
police <rate>
  conform-action drop
  exceed-action drop
```

Direct **action drop** is not supported.

## Precious Metal Policies for Wireless QoS

The precious metal policies are system-defined policies that are available on the embedded wireless controller. They cannot be removed or changed.

The following policies are available:

- Platinum—Used for VoIP clients.
- Gold—Used for video clients.
- Silver— Used for traffic that can be considered best-effort.

- Bronze—Used for NRT traffic.

These policies are pre-configured. They cannot be modified.

For client metal policies, they can be pushed using AAA.

Based on the policies applied, the 802.11e (WMM), and DSCP fields in the packets are affected.

For more information about metal policies format see the [Metal Policy Format, on page 514](#) section.

For more information about DSCP to UP mapping, see the [Architecture for Voice, Video and Integrated Data \(AVVID\), on page 520](#) table.

## Prerequisites for Wireless QoS

Before configuring wireless QoS, you must have a thorough understanding of these items:

- Wireless concepts and network topologies.
- Understanding of QoS implementation.
- Modular QoS CLI (MQC). For more information on Modular QoS, see the [MQC](#) guide
- The types of applications used and the traffic patterns on your network.
- Bandwidth requirements and speed of the network.

## Restrictions for QoS on Wireless Targets

### General Restrictions

A target is an entity where a policy is applied. A policy can be applied to a wireless target, which can be an SSID or client target, in the downstream and/or upstream direction. Downstream indicates that traffic is flowing from the controller to the wireless client. Upstream indicates that traffic is flowing from wireless client to the controller.

- Hierarchical (Parent policy and child policy) QoS is not supported.
- One policy per target per direction is supported.
- Only BSSID and client targets are supported, on both directions.
- The following policy formats are supported:

- QoS Policy Action

- Police:

```
police [cir | rate] bps [conform-action action] [exceed-action action]
```

Policer action types are **transmit** or **drop**.

- Set:

```
set dscp  
set wlan user-priority
```




---

**Note** `set wlan user-priority` (downstream only; BSSID only)

---

- QoS Policy Classification

```
match [not] access-group
match [not] dscp
match [not] protocol
```

#### AP Side Restrictions

- In Cisco Embedded Wireless Controller, FlexConnect local switching, and SDA deployments, the QoS policies are enforced on the AP. Due to this AP-side restriction, police actions (e.g., rate limiting) are only enforced at a per flow (5-tuple) level and not per client.

## Metal Policy Format

### Metal Policy Format

Metal Policies are system defined, and you cannot change it or delete it. There are four levels of metal policy - Platinum, Gold, Silver, and Bronze.




---

**Note** Each metal policy defines a DSCP ceiling so that the DSCP or the UP marking does not exceed a certain value.

For Platinum the value is 46, Gold is AF41, Silver is 22, and Bronze is CS1.

---

Policy Name	Policy-map Format	Class-map Format
platinum	<pre> policy-map platinum   class cm-dscp-34     set dscp af41   class cm-dscp-45     set dscp 45   class cm-dscp-46     set dscp ef   class cm-dscp-47     set dscp 47 </pre>	<pre> class-map match-any cm-dscp-34   match dscp af41  class-map match-any cm-dscp-45   match dscp 45  class-map match-any cm-dscp-46   match dscp ef  class-map match-any cm-dscp-47   match dscp 47  class-map match-any cm-dscp-0   match dscp default </pre>
gold	<pre> policy-map gold   class cm-dscp-45     set dscp af41   class cm-dscp-46     set dscp af41   class cm-dscp-47     set dscp af41 </pre>	
silver	<pre> policy-map silver   class cm-dscp-34     set dscp default   class cm-dscp-45     set dscp default   class cm-dscp-46     set dscp default   class cm-dscp-47     set dscp default </pre>	
bronze	<pre> policy-map bronze   class cm-dscp-0     set dscp cs1   class cm-dscp-34     set dscp cs1   class cm-dscp-45     set dscp cs1   class cm-dscp-46     set dscp cs1   class cm-dscp-47     set dscp cs1 </pre>	

Policy Name	Policy-map Format	Class-map Format
platinum-up	<pre> policy-map platinum-up   class cm-dscp-set1-for-up-4     set dscp af41   class cm-dscp-set2-for-up-4     set dscp af41   class cm-dscp-for-up-5     set dscp af41   class cm-dscp-for-up-6     set dscp ef   class cm-dscp-for-up-7     set dscp ef </pre>	<pre> class-map match-any cm-dscp-for-up-0   match dscp default   match dscp cs2  class-map match-any cm-dscp-for-up-1   match dscp cs1  class-map match-any cm-dscp-set1-for-up-4   match dscp cs3   match dscp af31   match dscp af32   match dscp af33 </pre>
gold-up	<pre> policy-map gold-up   class cm-dscp-for-up-6     set dscp af41   class cm-dscp-for-up-7     set dscp af41 </pre>	<pre> class-map match-any cm-dscp-set2-for-up-4   match dscp af41   match dscp af42   match dscp af43 </pre>
silver-up	<pre> policy-map silver-up   class cm-dscp-set1-for-up-4     set dscp default   class cm-dscp-set2-for-up-4     set dscp default   class cm-dscp-for-up-5     set dscp default   class cm-dscp-for-up-6     set dscp default   class cm-dscp-for-up-7     set dscp default </pre>	<pre> class-map match-any cm-dscp-for-up-5   match dscp cs4   match dscp cs5  class-map match-any cm-dscp-for-up-6   match dscp 44   match dscp ef </pre>
bronze-up	<pre> policy-map bronze-up   class cm-dscp-for-up-0     set dscp cs1   class cm-dscp-for-up-1     set dscp cs1   class cm-dscp-set1-for-up-4     set dscp cs1   class cm-dscp-set2-for-up-4     set dscp cs1   class cm-dscp-for-up-5     set dscp cs1   class cm-dscp-for-up-6     set dscp cs1   class cm-dscp-for-up-7     set dscp cs1 </pre>	<pre> class-map match-any cm-dscp-for-up-7   match dscp cs6   match dscp cs7 </pre>



Policy Name	Policy-map Format	Class-map Format
clwmm-platinum	<pre> policy-map clwmm-platinum class voice-plat   set dscp ef class video-plat   set dscp af41 class class-default   set dscp default </pre>	<pre> class-map match-any voice-plat   match dscp ef class-map match-any video-plat   match dscp af41 class-map match-any voice-gold   match dscp ef class-map match-any video-gold   match dscp af41 </pre>
clwmm-gold	<pre> policy-map clwmm-gold class voice-gold   set dscp af41 class video-gold   set dscp af41 class class-default   set dscp default </pre>	
clnon-wmm-platinum	<pre> policy-map clnon-wmm-platinum class class-default   set dscp ef </pre>	
clnon-wmm-gold	<pre> policy-map clnon-wmm-gold class class-default   set dscp af41 </pre>	
clsilver	<pre> policy-map clsilver class class-default   set dscp default </pre>	
clbronze	<pre> policy-map clbronze class class-default   set dscp cs1 </pre>	

## Auto QoS Policy Format

Policy Name	Policy-map Format	Class-map Format
enterprise-avc	<pre> policy-map AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy class AutoQos-4.0-wlan-Voip-Data-Class   set dscp ef class AutoQos-4.0-wlan-Voip-Signal-Class   set dscp cs3 class AutoQos-4.0-wlan-Multimedia-Conf-Class   set dscp af41 class AutoQos-4.0-wlan-Transaction-Class   set dscp af21 class AutoQos-4.0-wlan-Bulk-Data-Class   set dscp af11 class AutoQos-4.0-wlan-Scavenger-Class   set dscp cs1 class class-default   set dscp default  policy-map AutoQos-4.0-wlan-ET-SSID-Output-Policy class AutoQos-4.0-RT1-Class   set dscp ef class AutoQos-4.0-RT2-Class   set dscp af31 class class-default           </pre>	

Policy Name	Policy-map Format	Class-map Format
		<pre> class-map match-any AutoQos-4.0-wlan-Voip-Data-Class      match dscp ef  class-map match-any AutoQos-4.0-wlan-Voip-Signal-Class      match protocol     skinny     match protocol     cisco-jabber-control     match protocol sip     match protocol     sip-tls  class-map match-any AutoQos-4.0-wlan-Multimedia-Conf-Class      match protocol     cisco-phone-video     match protocol     cisco-jabber-video     match protocol     ms-lync-video     match protocol     webex-media  class-map match-any AutoQos-4.0-wlan-Transaction-Class      match protocol     cisco-jabber-im     match protocol     ms-office-web-apps     match protocol     salesforce     match protocol sap  class-map match-any AutoQos-4.0-wlan-Bulk-Data-Class      match protocol ftp     match protocol     ftp-data     match protocol     ftps-data     match protocol cifs  class-map match-any AutoQos-4.0-wlan-Scavenger-Class      match protocol     netflix     match protocol     youtube     match protocol skype      match protocol     bittorrent  class-map match-any AutoQos-4.0-RTT1-Class match dscp ef                     </pre>

Policy Name	Policy-map Format	Class-map Format
		<pre>match dscp cs6 class-map match-any AutoQos-4.0-RT2-Class match dscp cs4 match dscp cs3 match dscp af41</pre>
voice	<pre>policy-map platinum-up class dscp-for-up-4 set dscp 34 class dscp-for-up-5 set dscp 34 class dscp-for-up-6 set dscp 46 class dscp-for-up-7 set dscp 46  policy-map platinum class cm-dscp-34 set dscp 34 class cm-dscp-46 set dscp 46</pre>	
guest	<pre>Policy Map AutoQos-4.0-wlan-GT-SSID-Output-Policy Class class-default set dscp default  Policy Map AutoQos-4.0-wlan-GT-SSID-Input-Policy Class class-default set dscp default</pre>	
port (only applies to Local Mode)	<pre>policy-map AutoQos-4.0-wlan-Port-Output-Policy class AutoQos-4.0-Output-CAPWAP-C-Class priority level 1 class AutoQos-4.0-Output-Voice-Class priority level 2 class class-default  ip access-list extended AutoQos-4.0-Output-Acl-CAPWAP-C permit udp any eq 5246 16666 any</pre>	<pre>class-map match-any AutoQos-4.0-Output-CAPWAP-C-Class  match access-group name AutoQos-4.0-Output-Acl-CAPWAP-C  class-map match-any AutoQos-4.0-Output-Voice-Class  match dscp ef</pre>

## Architecture for Voice, Video and Integrated Data (AVVID)

IETF DiffServ Service Class	DSCP	IEEE 802.11e	
		User Priority	Access Category
Network Control	(CS7) CS6	0	AC_BE
Telephony	EF	6	AC_VO
VOICE-ADMIT	44	6	AC_VO
Signaling	CS5	5	AC_VI

IETF DiffServ Service Class	DSCP	IEEE 802.11e	
		User Priority	Access Category
Multimedia Conferencing	AF41 AF42 AF43	4	AC_VI
Real-Time Interactive	CS4	5	AC_VI
Multimedia Streaming	AF31 AF32 AF33	4	AC_VI
Broadcast Video	CS3	4	AC_VI
Low-Latency Data	AF21 AF22 AF23	3	AC_BE
OAM	CS2	0	AC_BE
High-Throughput Data	AF11 AF12 AF13	2	AC_BK
Standard	DF	0	AC_BE
Low-Priority Data	CS1	1	AC_BK
Remaining	Remaining	0	

## How to apply Bi-Directional Rate Limiting

### Information about Bi-Directional Rate Limiting

Bi-Directional Rate Limiting (BDRL) feature defines rate limits on both upstream and downstream traffic. These rate limits are individually configured. The rate limits can be configured on WLAN directly instead of QoS profiles, which will override QoS profile values. The WLAN rate limiting will always supersede Global QoS setting for controller and clients.

BDRL feature defines throughput limits for clients on their wireless networks and allows setting a priority service to a particular set of clients.

The following four QoS profiles are available to configure the rate limits:

- Gold

- Platinum
- Silver
- Bronze

The QoS profile is applied to all clients on the associated SSID. Therefore all clients connected to the same SSID will have the same rate limits.

To configure BDRL, select the QoS profile and configure the various rate limiting parameters. When rate limiting parameters are set to 0, the rate limiting feature is not functional. Each WLAN has a QoS profile associated with it in addition to the configuration in the QoS profile.



**Note** BDRL in a mobility Anchor-Foreign setup must be configured both on Anchor and Foreign controller. As a best practice, it is recommended to perform identical configuration on both the controllers to avoid breakage of any feature.

BDRL is supported on Guest anchor scenarios. The feature is supported on IRCM guest scenarios with AireOS as Guest anchor or Guest Foreign. Cisco Catalyst 9800 Series Wireless Controller uses **Policing** option to rate limit the traffic.

To apply metal policy with BDRL, perform the following tasks:

- [Configure Metal Policy on SSID](#)
- [Configure Metal Policy on Client](#)
- [Configure Bi-Directional Rate Limiting for All Traffic, on page 524](#)
- [Configure Bi-Directional Rate Limiting Based on Traffic Classification, on page 524](#)
- [Apply Bi-Directional Rate Limiting Policy Map to Policy Profile, on page 526](#)
- [Apply Metal Policy with Bi-Directional Rate Limiting, on page 527](#)

## Prerequisites for Bi-Directional Rate Limiting

- Client metal policy is applied through AAA-override.
- You must specify the metal policy on ISE server.
- AAA-override must be enabled on policy profile.

## Configure Metal Policy on SSID

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>	Enters global configuration mode.

	Command or Action	Purpose
	Device# configure terminal	
<b>Step 2</b>	<b>wireless profile policy</b> <i>policy-profile-name</i> <b>Example:</b> Device(config)# wireless profile policy policy-profile1	Configures WLAN policy profile and enters wireless policy configuration mode.
<b>Step 3</b>	<b>description</b> <i>description</i> <b>Example:</b> Device(config-wireless-policy)# description policy-profile1	Adds a user defined description to the new wireless policy.
<b>Step 4</b>	<b>service-policy input</b> <i>input-policy</i> <b>Example:</b> Device(config-wireless-policy)# service-policy input platinum-up	Sets platinum policy for input.
<b>Step 5</b>	<b>service-policy output</b> <i>output-policy</i> <b>Example:</b> Device(config-wireless-policy)# service-policy output platinum	Sets platinum policy for output.

## Configure Metal Policy on Client

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile policy</b> <i>policy-profile-name</i> <b>Example:</b> Device(config)# wireless profile policy policy-profile1	Configures WLAN policy profile and enters wireless policy configuration mode.
<b>Step 3</b>	<b>description</b> <i>description</i> <b>Example:</b> Device(config-wireless-policy)# description profile with aaa override	Adds a user defined description to the new wireless policy.
<b>Step 4</b>	<b>aaa-override</b> <b>Example:</b>	Enables AAA override on the WLAN.

	Command or Action	Purpose
	Device(config-wireless-policy)# aaa-override	<b>Note</b> After AAA-override is enabled and ISE server starts sending policy, client policy defined in service-policy client will not take effect.

## Configure Bi-Directional Rate Limiting for All Traffic

Use the police action in the policy-map to configure BDRL.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>policy-map <i>policy-map</i></b>  <b>Example:</b> Device(config)# policy-map policy-sample 1	Creates a named object representing a set of policies that are to be applied to a set of traffic classes. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
<b>Step 3</b>	<b>class <i>class-map-name</i></b>  <b>Example:</b> Device(config-pmap)# class class-default	Associates a class map with the policy map, and enters policy-map class configuration mode.
<b>Step 4</b>	<b>police <i>rate</i></b>  <b>Example:</b> Device(config-pmap-c)# police 500000	Configures traffic policing (average rate, in bits per second). Valid values are 8000 to 200000000.

## Configure Bi-Directional Rate Limiting Based on Traffic Classification

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>policy-map <i>policy-map</i></b>  <b>Example:</b>	Creates a named object representing a set of policies that are to be applied to a set of traffic classes. Policy-map names can contain



	Command or Action	Purpose
	<code>Device(config)# policy-map policy-sample2</code>	alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
<b>Step 3</b>	<b>class</b> <i>class-map-name</i> <b>Example:</b> <code>Device(config-pmap)# class class-sample-youtube</code>	Associates a class map with the policy map, and enters policy-map class configuration mode.
<b>Step 4</b>	<b>police</b> <i>rate</i> <b>Example:</b> <code>Device(config-pmap-c)# police 1000000</code>	Configures traffic policing (average rate, in bits per second). Valid values are 8000 to 200000000.
<b>Step 5</b>	<b>conform-action</b> <i>drop</i> <b>Example:</b> <code>Device(config-pmap-c-police)# conform-action drop</code>	Specifies the drop action to take on packets that conform to the rate limit.
<b>Step 6</b>	<b>exceed-action</b> <i>drop</i> <b>Example:</b> <code>Device(config-pmap-c-police)# exceed-action drop</code>	Specifies the drop action to take on packets that exceeds the rate limit.
<b>Step 7</b>	<b>exit</b> <b>Example:</b> <code>Device(config-pmap-c-police)# exit</code>	Exits the policy-map class configuration mode.
<b>Step 8</b>	<b>set dscp</b> <i>default</i> <b>Example:</b> <code>Device(config-pmap-c)# set dscp default</code>	Sets the DSCP value to default.
<b>Step 9</b>	<b>police</b> <i>rate</i> <b>Example:</b> <code>Device(config-pmap-c)# police 500000</code>	Configures traffic policing (average rate, in bits per second). Valid values are 8000 to 200000000.
<b>Step 10</b>	<b>exit</b> <b>Example:</b> <code>Device(config-pmap-c)# exit</code>	Exits the policy-map class configuration mode.
<b>Step 11</b>	<b>exit</b> <b>Example:</b> <code>Device(config-pmap)# exit</code>	Exits the policy-map configuration mode.
<b>Step 12</b>	<b>class-map</b> <i>match-any class-map-name</i> <b>Example:</b>	Selects a class map.

	Command or Action	Purpose
	Device(config)# class-map match-any class-sample-youtube	
<b>Step 13</b>	<b>match protocol</b> <i>protocol</i>  <b>Example:</b> Device(config-cmap)# match protocol youtube	Configures the match criteria for a class map on the basis of the specified protocol.

## Apply Bi-Directional Rate Limiting Policy Map to Policy Profile

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile policy</b> <i>policy-profile-name</i>  <b>Example:</b> Device(config)# wireless profile policy policy-profile3	Configures WLAN policy profile and enters wireless policy configuration mode.
<b>Step 3</b>	<b>description</b> <i>description</i>  <b>Example:</b> Device(config-wireless-policy)# description policy-profile3	Adds a user defined description to the new wireless policy.
<b>Step 4</b>	<b>service-policy client input</b> <i>input-policy</i>  <b>Example:</b> Device(config-wireless-policy)# service-policy client input platinum-up	Sets the input client service policy as platinum.
<b>Step 5</b>	<b>service-policy client output</b> <i>output-policy</i>  <b>Example:</b> Device(config-wireless-policy)# service-policy client output platinum	Sets the output client service policy as platinum.
<b>Step 6</b>	<b>service-policy input</b> <i>input-policy</i>  <b>Example:</b> Device(config-wireless-policy)# service-policy input platinum-up	Sets the input service policy as platinum.
<b>Step 7</b>	<b>service-policy output</b> <i>output-policy</i>  <b>Example:</b> Device(config-wireless-policy)# service-policy output platinum	Sets the output service policy as platinum.

## Apply Metal Policy with Bi-Directional Rate Limiting

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile policy <i>policy-profile-name</i></b> <b>Example:</b> Device(config)# wireless profile policy policy-profile3	Configures WLAN policy profile and enters wireless policy configuration mode.
<b>Step 3</b>	<b>description <i>description</i></b> <b>Example:</b> Device(config-wireless-policy)# description policy-profile3	Adds a user defined description to the new wireless policy.
<b>Step 4</b>	<b>service-policy client input <i>input-policy</i></b> <b>Example:</b> Device(config-wireless-policy)# service-policy client input platinum-up	Sets the input client service policy as platinum.
<b>Step 5</b>	<b>service-policy client output <i>output-policy</i></b> <b>Example:</b> Device(config-wireless-policy)# service-policy client output platinum	Sets the output client service policy as platinum.
<b>Step 6</b>	<b>service-policy input <i>input-policy</i></b> <b>Example:</b> Device(config-wireless-policy)# service-policy input platinum-up	Sets the input service policy as platinum.
<b>Step 7</b>	<b>service-policy output <i>output-policy</i></b> <b>Example:</b> Device(config-wireless-policy)# service-policy output platinum	Sets the output service policy as platinum.
<b>Step 8</b>	<b>exit</b> <b>Example:</b> Device(config-wireless-policy)# exit	Exits the policy configuration mode.
<b>Step 9</b>	<b>policy-map <i>policy-map</i></b> <b>Example:</b> Device(config)# policy-map policy-sample 1	Creates a named object representing a set of policies that are to be applied to a set of traffic classes. Policy map names can contain alphabetic, hyphen, or underscore characters,

	Command or Action	Purpose
		are case sensitive, and can be up to 40 characters.
<b>Step 10</b>	<b>class</b> <i>class-map-name</i> <b>Example:</b> Device(config-pmap)# class class-default	Associates a class map with the policy map, and enters configuration mode for the specified system class.
<b>Step 11</b>	<b>police</b> <i>rate</i> <b>Example:</b> Device(config-pmap-c)# police 500000	Configures traffic policing (average rate, in bits per second). Valid values are 8000 to 200000000.

## How to apply Per Client Bi-Directional Rate Limiting

### Information About Per Client Bi-Directional Rate Limiting

The Per Client Bi-Directional Rate Limiting feature adds bi-directional rate limiting for each wireless clients on 802.11ac Wave 2 APs in a Flex local switching configuration. Earlier, the Wave 2 APs supported only per-flow rate limiting for a wireless client. When wireless client starts multiple streams of traffic, the client-based rate limiting does not work as expected. This limitation is addressed by this feature.

For instance, if the controller is configured with QoS policy and you expect each client to have a rate limiting cap of 1000 kbps. Due to per-flow rate limiting on the AP, if the wireless client starts a Youtube stream and FTP stream, each of them will be rate limited at 1000 Kbps, therefore the client will be 2000 Kbps rates. This is not desirable.

#### Use Cases

The following are the use cases supported by the Per Client Bi-Directional Rate Limiting feature:

##### Use Case -1

###### Configuring only default class map

If policy map is configured only with default class map and mapped only to QoS client policy, AP does a per client rate limit to the client connected to AP.

##### Use Case-2

###### Changing from per client rate limit to per flow rate limit

If policy map is configured with another different class map along with a default class map and mapped to QoS client policy, AP performs per flow rate limit to client. As policy map has different class map along with the default class map. The per client rate limit values are cleared, if the AP has previously configured per client rate limit.

If the policy map has more than one class map, then additional class map is configured along with the default class map. So, the rate limit is applied from per client to per flow. The per client rate limit value is deleted from the rate info token bucket.

##### Use Case-3

### Changing from per flow rate limit to per client limit

If different class map is removed from policy map and policy map has only one default class map, AP performs a per client rate limit to client.

The following covers the high-level steps for Per Client Bi-Directional Rate Limiting feature:

1. Configure a policy map to WLAN through policy profile.
2. Map the QoS related policy map to WLAN.
3. Configure policy map with the default class map.
4. Configure different police rate value for class Default map.



---

**Note** If policy map has class Default with valid police rate value, AP applies that rate limit to the overall client data traffic flow.

---

5. Apply the policy map with class Default to QoS client policy in WLAN policy profile.

## Prerequisites for Per Client Bi-Directional Rate Limiting

- This feature is exclusive to QoS client policy, that is, the policy profile must have only QoS Policy or policy target as client.
- If policy map has class default with valid police rate value, AP applies that rate limit value to the overall client data traffic flow.

## Restrictions on Per Client Bi-Directional Rate Limiting

- If policy map has class map other than the class Default map, the per client rate limit does not work in AP.

## Configuring Per Client Bi-Directional Rate Limiting (GUI)

### Procedure

---

**Step 1** Choose **Configuration > Tags & Profiles > Policy**.

**Step 2** Click the Policy Profile Name.

The **Edit Policy Profile** window is displayed.

**Note** The **Edit Policy Profile** window is displayed and configured in default class map only.

**Step 3** Choose the **QOS And AVC** tab.

**Step 4** In the **QoS Client Policy** settings, choose the policies from the **Egress** and **Ingress** drop-down lists.

**Note** You need to apply the default policy map to the QoS Client Policy.

**Step 5** Click **Update & Apply to Device**.

## Verifying Per Client Bi-Directional Rate Limiting

To verify whether per client is applied in AP, use the following command:

```
Device# show rate-limit client
Config:
      mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out nrt_rate_in
      nrt_burst_out nrt_burst_in
A0:D3:7A:12:6C:5E 0 0 0 0 0 0 0
0 0 0
Statistics:
      name      up down
      Unshaped  0  0
      Client RT pass 697610 8200
      Client NRT pass 0 0
      Client RT drops 0 0
      Client NRT drops 0 16
      9 180 0
Per client rate limit:
      mac vap rate_out rate_in policy
A0:D3:7A:12:6C:5E 0 88 23 per_client_rate_2
```

## Configuring BDRL Using AAA Override

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile policy <i>profile-name</i></b>  <b>Example:</b> Device (config)# <b>wireless profile policy default-policy-profile</b>	Configures the WLAN policy profile and enters wireless policy configuration mode.
<b>Step 3</b>	<b>aaa-override</b>  <b>Example:</b> Device(config-wireless-policy)# <b>aaa</b>	Configures AAA override to apply policies coming from the AAA server or ISE the Cisco Identify Services Engine (ISE) server.  The following attributes are available in the RADIUS server: <ul style="list-style-type: none"> <li>Airespace-Data-Bandwidth-Average-Contract: 8001</li> <li>Airespace-Real-Time-Bandwidth-Average-Contract: 8002</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• Airespace-Data-Bandwidth-Burst-Contract: 8003</li> <li>• Airespace-Real-Time-Bandwidth-Burst-Contract: 8004</li> <li>• Airespace-Data-Bandwidth-Average-Contract-Upstream: 8005</li> <li>• Airespace-Real-Time-Bandwidth-Average-Contract-Upstream: 8006</li> <li>• Airespace-Data-Bandwidth-Burst-Contract-Upstream: 8007</li> <li>• Airespace-Real-Time-Bandwidth-Burst-Contract-Upstream: 8008</li> </ul> <p><b>Note</b> 8001, 8002, 8003, 8004, 8005, 8006, 8007, and 8008 are the desired rate-limit values configured as an example.</p>

## Verifying Bi-Directional Rate-Limit

To verify the bi-directional rate limit, use the following command:

```
Device# show wireless client mac-address E8-8E-00-00-00-71 detail
Client MAC Address : e88e.0000.0071
Client MAC Type    : Universally Administered Address
Client IPv4 Address : 100.0.7.94
Client Username    : e88e00000071
AP MAC Address     : 0a0b.0c00.0200
AP Name            : AP6B8B4567-0002
AP slot            : 0
Client State       : Associated
Policy Profile     : dnas_qos_profile_policy
Flex Profile       : N/A
Wireless LAN Id    : 10
WLAN Profile Name  : QoS_wlan
Wireless LAN Network Name (SSID): QoS_wlan
BSSID : 0a0b.0c00.0200
Connected For      : 28 seconds
Protocol           : 802.11n - 2.4 GHz
Channel            : 1
Client IIF-ID      : 0xa0000034
Association Id     : 10
Authentication Algorithm : Open System
Idle state timeout : N/A
Session Timeout    : 1800 sec (Remaining time: 1777 sec)
Session Warning Time : Timer not running
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name : None
Output Policy State : None
```

```

Output Policy Source : None
WMM Support          : Enabled
U-APSD Support       : Disabled
Fastlane Support     : Disabled
Client Active State  : In-Active
Power Save           : OFF
Supported Rates      : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0
AAA QoS Rate Limit Parameters:
  QoS Average Data Rate Upstream      : 8005 (kbps)
  QoS Realtime Average Data Rate Upstream : 8006 (kbps)
  QoS Burst Data Rate Upstream        : 8007 (kbps)
  QoS Realtime Burst Data Rate Upstream : 8008 (kbps)
  QoS Average Data Rate Downstream    : 8001 (kbps)
  QoS Realtime Average Data Rate Downstream : 8002 (kbps)
  QoS Burst Data Rate Downstream      : 80300 (kbps)
  QoS Realtime Burst Data Rate Downstream : 8004 (kbps)

```

To verify the rate-limit details from the AP terminal, use the following command

```

Device# show rate-limit client
Config:
mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out nrt_rate_in nrt_burst_out
  nrt_burst_in
00:1C:F1:09:85:E7 0 8001 8002 8003 8004 8005 8006 8007 8008
Statistics:
name up down
Unshaped 0 0
Client RT pass 0 0
Client NRT pass 0 0
Client RT drops 0 0
Client NRT drops 0 0
Per client rate limit:
mac vap rate_out rate_in policy

```

## How to Configure Wireless QoS

### Configuring a Policy Map with Class Map (GUI)

#### Procedure

- 
- Step 1** Choose **Configuration > Services > QoS**.
  - Step 2** Click **Add** to view the **Add QoS** window.
  - Step 3** In the text box next to the **Policy Name**, enter the name of the new policy map that is being added.
  - Step 4** Click **Add Class-Maps**.
  - Step 5** Configure **AVC** based policies or **User Defined** policies. To enable **AVC** based policies, and configure the following:
    - a) Choose either **Match Any** or **Match All**.
    - b) Choose the required **Mark Type**. If you choose **DSCP** or **User Priority**, you must specify the appropriate **Mark Value**.
    - c) Check the **Drop** check box to drop traffic from specific sources.

**Note** When **Drop** is enabled, the **Mark Type** and **Police(kbps)** options are disabled.



- d) Based on the chosen **Match Type**, select the required protocols from the **Available Protocol(s)** list and move them to the **Selected Protocol(s)** list. These selected protocols are the ones from which traffic is dropped.
- e) Click **Save**.

**Note** To add more Class Maps, repeat steps 4 and 5.

**Step 6** To enable **User-Defined** QoS policy, and the configure the following:

- a) Choose either **Match Any** or **Match All**.
- b) Choose either **ACL** or **DSCP** as the **Match Type** from the drop-down list, and then specify the appropriate **Match Value**.
- c) Choose the required **Mark Type** to associate with the mark label. If you choose *DSCP*, you must specify an appropriate **Mark Value**.
- d) Check the **Drop** check box to drop traffic from specific sources.

**Note** When **Drop** is enabled, the **Mark Type** and **Police(kbps)** options are disabled.

- e) Click **Save**.

**Note** To define actions for all the remaining traffic, in the Class Default, choose **Mark** and/or **Police(kbps)** accordingly.

**Step 7** Click **Save & Apply to Device**.

## Configuring a Class Map (CLI)

Follow the procedure given below to configure class maps for voice and video traffic:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>class-map</b> <i>class-map-name</i> <b>Example:</b> Device(config)# <b>class-map test</b>	Creates a class map.
<b>Step 3</b>	<b>match dscp</b> <i>dscp-value</i> <b>Example:</b> Device(config-cmap)# <b>match dscp 46</b>	Matches the DSCP value in the IPv4 and IPv6 packets. <b>Note</b> By default for the class map the value is match-all.

	Command or Action	Purpose
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config-cmap)# <b>end</b>	Exits the class map configuration and returns to the privileged EXEC mode.
<b>Step 5</b>	<b>show class-map class-map-name</b> <b>Example:</b> Device# show class-map class_map_name	Verifies the class map details.

## Configuring Policy Profile to Apply QoS Policy (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Policy**.
- Step 2** On the **Policy Profile** page, click the name of the policy profile.
- Step 3** In the **Edit Policy Profile** window, click the **QoS and AVC** tab.
- Step 4** Under **QoS SSID Policy**, choose the appropriate **Ingress** and **Egress** policies for WLANs.
- Note** The ingress policies can be differentiated from the egress policies by the suffix *-up*. For example, the Platinum ingress policy is named *platinum-up*.
- Step 5** Under **QoS Client Policy**, choose the appropriate **Ingress** and **Egress** policies for clients.
- Step 6** Click **Update & Apply to Device**.
- Note** Only custom policies are displayed under **QoS Client Policy**. AutoQoS policies are auto generated and not displayed for user selection.
- 

## Configuring Policy Profile to Apply QoS Policy (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile policy profile-policy</b> <b>Example:</b> Device(config)# wireless profile policy qostest	Configures WLAN policy profile and enters the wireless policy configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>service-policy client</b> {input   output} <i>policy-name</i>  <b>Example:</b>  Device(config-wireless-policy)# <b>service-policy client input</b> <b>policy-map-client</b>	Applies the policy. The following options are available. <ul style="list-style-type: none"> <li>• <b>input</b>—Assigns the client policy for ingress direction on the policy profile.</li> <li>• <b>output</b>—Assigns the client policy for egress direction on the policy profile.</li> </ul>
<b>Step 4</b>	<b>service-policy</b> {input   output} <i>policy-name</i>  <b>Example:</b>  Device(config-wireless-policy)# <b>service-policy input policy-map-ssid</b>	Applies the policy to the BSSID. The following options are available. <ul style="list-style-type: none"> <li>• <b>input</b>—Assigns the policy-map to all clients in WLAN.</li> <li>• <b>output</b>—Assigns the policy-map to all clients in WLAN.</li> </ul>
<b>Step 5</b>	<b>no shutdown</b>  <b>Example:</b>  Device(config-wireless-policy)# no shutdown	Enables the wireless policy profile.

## Applying Policy Profile to Policy Tag (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Tags**.
  - Step 2** On the **Manage Tags** page in the **Policy** tab, click **Add**.
  - Step 3** In the **Add Policy Tag** window that is displayed, enter a name and description for the policy tag.
  - Step 4** Map the required WLAN IDs and WLAN profiles with appropriate policy profiles.
  - Step 5** Click **Update & Apply to Device**.
- 

## Applying Policy Profile to Policy Tag (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b>	Enters global configuration mode.

	Command or Action	Purpose
	Device# <b>configure terminal</b>	
<b>Step 2</b>	<b>wireless tag policy</b> <i>policy-tag-name</i> <b>Example:</b> Device(config-policy-tag)# wireless tag policy qostag	Configures policy tag and enters the policy tag configuration mode.
<b>Step 3</b>	<b>wlan</b> <i>wlan-name</i> <b>policy</b> <i>profile-policy-name</i> <b>Example:</b> Device(config-policy-tag)# wlan test policy qostest	Maps a policy profile to a WLAN profile.
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config-policy-tag)# end	Saves the configuration and exits the configuration mode and returns to privileged EXEC mode.
<b>Step 5</b>	<b>show wireless tag policy summary</b> <b>Example:</b> Device# show wireless tag policy summary	Displays the configured policy tags.  <b>Note</b> To view the detailed information of a policy tag, use the <b>show wireless tag policy detailed</b> <i>policy-tag-name</i> command.

## Attaching Policy Tag to an AP

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>ap</b> <i>mac-address</i> <b>Example:</b> Device(config)# ap F866.F267.7DFB	Configures Cisco APs and enters the ap profile configuration mode.
<b>Step 3</b>	<b>policy-tag</b> <i>policy-tag-name</i> <b>Example:</b> Device(config-ap-tag)# policy-tag qostag	Maps a Policy tag to the AP.

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config-ap-tag)# end	Saves the configuration and exits the configuration mode and returns to privileged EXEC mode.
<b>Step 5</b>	<b>show ap tag summary</b> <b>Example:</b> Device# show ap tag summary	Displays the ap details and tags associated to it.





# CHAPTER 57

## Wireless Auto-QoS

- [Information About Auto QoS, on page 539](#)
- [How to Configure Wireless AutoQoS, on page 540](#)

### Information About Auto QoS

Wireless Auto QoS automates deployment of wireless QoS features. It has a set of predefined profiles which can be further modified by the customer to prioritize different traffic flows. Auto-QoS matches traffic and assigns each matched packet to qos-groups. This allows the output policy map to put specific qos-groups into specific queues, including into the priority queue.

#### AutoQoS Policy Configuration

*Table 23: AutoQoS Policy Configuration*

Mode	Client Ingress	Client Egress	BSSID Ingress	BSSID Egress	Port Ingress	Port Egress	Radio
Voice	N/A	N/A	P3	P4	N/A	P7	ACM on
Guest	N/A	N/A	P5	P6	N/A	P7	
Fastlane	N/A	N/A	N/A	N/A	N/A	P7	<code>edca-parameters fastlane</code>
Enterprise-avc	N/A	N/A	P1	P2	N/A	P7	
P1				AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy			
P2				AutoQos-4.0-wlan-ET-SSID-Output-Policy			
P3				platinum-up			
P4				platinum			
P5				AutoQos-4.0-wlan-GT-SSID-Input-Policy			

P6	AutoQos-4.0-wlan-GT-SSID-Output-Policy
P7	AutoQos-4.0-wlan-Port-Output-Policy

# How to Configure Wireless AutoQoS

## Configuring Wireless AutoQoS on Profile Policy

You can enable AutoQoS on a profile policy.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device# <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>wireless autoqos policy-profile <i>policy-name</i> mode { enterprise-avc   fastlane   guest   voice}</b>  <b>Example:</b> Device# <b>wireless autoqos policy-profile test-profile mode voice</b>	Configures AutoQoS wireless policy. <ul style="list-style-type: none"> <li>• <b>enterprise-avc</b>—Enables AutoQoS Wireless Enterprise AVC Policy.</li> <li>• <b>fastlane</b>—Enable AutoQoS Wireless Fastlane Policy.</li> <li>• <b>guest</b>—Enable AutoQoS Wireless Guest Policy.</li> <li>• <b>voice</b>—Enable AutoQoS Wireless Voice Policy.</li> </ul> <p><b>Note</b> AutoQoS MIB attribute does not support full functionality with service policy. Service policy must be configured manually. Currently, there is only support for AutoQoS mode.</p>

### What to do next



**Note** After enabling AutoQoS, we recommend that you wait for a few seconds for the policy to install and then try and modify the AutoQoS policy maps if required; or retry if the modification is rejected.



## Disabling Wireless AutoQoS

To globally disable Wireless AutoQoS:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# <code>enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>shutdown</b> <b>Example:</b> Device# <code>shutdown</code>	Shuts down the policy profile.
<b>Step 3</b>	<b>wireless autoqos disable</b> <b>Example:</b> Device# <code>wireless autoqos disable</code>	Globally disables wireless AutoQoS.
<b>Step 4</b>	<b>[no] shutdown</b> <b>Example:</b> Device# <code>no shutdown</code>	Enables the wireless policy profile.  <b>Note</b> Disabling Auto QoS does not reset global radio configurations like CAC and EDCA parameters.

## Rollback AutoQoS Configuration (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Services > QoS**.
  - Step 2** Click **Disable AutoQoS**.
  - Step 3** Click **Yes** to confirm.
- 

## Rollback AutoQoS Configuration

### Before you begin




---

**Note** AutoQoS MIB attribute does not support the full functionality with service policy. Currently, there is only support for AutoQoS mode. Service policy must be configured manually.

---

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>clear platform software autoqos config template { enterprise_avc   guest}</b> <b>Example:</b> Device# <b>clear platform software autoqos config template guest</b>	Resets AutoQoS configuration. <ul style="list-style-type: none"> <li>• enterprise-avc—Resets AutoQoS Enterprise AVC Policy Template.</li> <li>• guest—Resets AutoQoS Guest Policy Template.</li> </ul>

## Clearing Wireless AutoQoS Policy Profile (GUI)

**Procedure**

- 
- Step 1** Choose **Configuration > Tags & Profiles > Policy**.
- Step 2** Click on the **Policy Profile Name**.
- Step 3** Go to **QoS and AVC** tab.
- Step 4** From the **Auto Qos** drop-down list, choose **None**.
- Step 5** Click **Update & Apply to Device**.
- 

## Clearing Wireless AutoQoS Policy Profile

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>shutdown</b> <b>Example:</b> Device# <b>shutdown</b>	Shuts down the policy profile.
<b>Step 3</b>	<b>wireless autoqos policy-profile <i>policy-name</i> mode clear</b> <b>Example:</b>	Clears the configured AutoQoS wireless policy.

	Command or Action	Purpose
	Device# <code>wireless autoqos policy-profile test-profile mode clear</code>	
<b>Step 4</b>	<b>[no] shutdown</b>  <b>Example:</b> <code>no shutdown</code>	Enables the wireless policy profile.

## Viewing AutoQoS on policy profile

### Before you begin

Autoqos is supported on the local mode and flex mode. Autoqos configures a set of policies and radio configurations depending on the template. It is possible to override the service-policy that is configured by autoqos. The latest configuration takes effect, with AAA override policy being of highest priority.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> <code>Device#enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>show wireless profile policy detailed</b> <i>policy-profile-name</i>  <b>Example:</b> <code>Device# show wireless profile policy detailed testqos</code>	Shows policy-profile detailed parameters.





## CHAPTER 58

# Native Profiling

---

- [Information About Native Profiling, on page 545](#)
- [Creating a Class Map \(GUI\), on page 546](#)
- [Creating a Class Map \(CLI\), on page 546](#)
- [Creating a Service Template \(GUI\), on page 548](#)
- [Creating a Service Template \(CLI\), on page 549](#)
- [Creating a Parameter Map, on page 550](#)
- [Creating a Policy Map \(GUI\), on page 550](#)
- [Creating a Policy Map \(CLI\), on page 551](#)
- [Configuring Native Profiling in Local Mode, on page 553](#)
- [Verifying Native Profile Configuration, on page 553](#)

## Information About Native Profiling

You can profile devices based on HTTP and DHCP to identify the end devices on the network. You can configure device-based policies and enforce these policies per user or per device policy on the network.

Policies allow profiling of mobile devices and basic onboarding of the profiled devices to a specific VLAN. They also assign ACL and QoS or configure session timeouts.

You can configure policies as two separate components:

- Defining policy attributes as service templates that are specific to clients joining the network and applying policy match criteria
- Applying match criteria to the policy.



---

**Note** Before proceeding with the native profile configuration, ensure that HTTP Profiling and DHCP Profiling are enabled.

---

To configure Native Profiling, use one of the following procedures:

- Create a service template
- Create a class map



**Note** You can apply a service template using either a class map or parameter map.

- Create a parameter-map and associate the service template to parameter-map
  - Create a policy map
    1. If class-map has to be used: Associate the class-map to the policy-map and associate the service-template to the class-map.
    2. If parameter-map has to be used: Associate the parameter-map to the policy-map
  - Associate the policy-map to the policy profile.

## Creating a Class Map (GUI)

### Procedure

- 
- Step 1** Click **Configuration > Services > QoS**.
- Step 2** In the **Qos – Policy** area, click **Add** to create a new QoS Policy or click the one you want to edit.
- Step 3** Add **Add Class Map** and enter the details.
- Step 4** Click **Save**.
- Step 5** Click **Update and Apply to Device**.
- 

## Creating a Class Map (CLI)



**Note** Configuration of class maps via CLI offer more options and can be more granular than GUI.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>class-map type control subscriber</b> <b>match-any</b> <i>class-map-name</i>	Specifies the class map type and name.

	Command or Action	Purpose
	<b>Example:</b> Device(config)# class-map type control subscriber match-any cls_user	
<b>Step 3</b>	<b>match username <i>username</i></b> <b>Example:</b> Device(config-filter-control-classmap)# match username ciscoise	Specifies the class map attribute filter criteria.
<b>Step 4</b>	<b>class-map type control subscriber match-any <i>class-map-name</i></b> <b>Example:</b> Device(config)# class-map type control subscriber match-any cls_userrole	Specifies the class map type and name.
<b>Step 5</b>	<b>match user-role <i>user-role</i></b> <b>Example:</b> Device(config-filter-control-classmap)# match user-role engineer	Specifies the class map attribute filter criteria.
<b>Step 6</b>	<b>class-map type control subscriber match-any <i>class-map-name</i></b> <b>Example:</b> Device(config)# class-map type control subscriber match-any cls_oui	Specifies the class map type and name.
<b>Step 7</b>	<b>match oui <i>oui-address</i></b> <b>Example:</b> Device(config-filter-control-classmap)# match oui 48.f8.b3	Specifies the class map attribute filter criteria.
<b>Step 8</b>	<b>class-map type control subscriber match-any <i>class-map-name</i></b> <b>Example:</b> Device(config)# class-map type control subscriber match-any cls_mac	Specifies the class map type and name.
<b>Step 9</b>	<b>match mac-address <i>mac-address</i></b> <b>Example:</b> Device(config-filter-control-classmap)# match mac-address 0040.96b9.4a0d	Specifies the class map attribute filter criteria.
<b>Step 10</b>	<b>class-map type control subscriber match-any <i>class-map-name</i></b> <b>Example:</b> Device(config)# class-map type control subscriber match-any cls_devtype	Specifies the class map type and name.

	Command or Action	Purpose
<b>Step 11</b>	<b>match device-type</b> <i>device-type</i> <b>Example:</b> <pre>Device(config-filter-control-classmap)# match device-type windows</pre>	Specifies the class map attribute filter criteria.
<b>Step 12</b>	<b>match join-time-of-day</b> <i>start-time end-time</i> <b>Example:</b> <pre>Device(config-filter-control-classmap)# match join-time-of-day 10:30 12:30</pre>	<p>Specifies a match to the time of day.</p> <p>Here, join time is considered for matching. For example, if the match filter is set from 11:00 am to 2:00 pm, a device joining at 10:59 am is not considered, even if it acquires credentials after 11:00 am.</p> <p>Here,</p> <p><i>start-time</i> and <i>end-time</i> specifies the 24-hour format.</p> <p>Use the <b>show class-map type control subscriber name</b> <i>name</i> command to verify the configuration.</p> <p><b>Note</b> You should also disable AAA override for this command to work.</p>

## Creating a Service Template (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Security > Local Policy**.
- Step 2** On the **Local Policy** page, **Service Template** tab, click **ADD**.
- Step 3** In the **Create Service Template** window, enter the following parameters:
- **Service Template Name:** Enter a name for the template.
  - **VLAN ID:** Enter the VLAN ID for the template. Valid range is between 1 and 4094.
  - **Session Timeout (secs):** Sets the timeout duration for the template. Valid range is between 1 and 65535.
  - **Access Control List:** Choose the Access Control List from the drop-down list.
  - **Ingress QOS:** Choose the input QoS policy for the client from the drop-down list
  - **Egress QOS:** Choose the output QoS policy for the client from the drop-down list.
- Step 4** Click **Save & Apply to Device**.
-



# Creating a Service Template (CLI)

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>service-template <i>service-template-name</i></b> <b>Example:</b> Device(config)# service-template svcl	Enters service template configuration mode.
<b>Step 3</b>	<b>access-group <i>access-list-name</i></b> <b>Example:</b> Device(config-service-template)# access-group acl-auto	Specifies the access list to be applied.
<b>Step 4</b>	<b>vlan <i>vlan-id</i></b> <b>Example:</b> Device(config-service-template)# vlan 10	Specifies VLAN ID. Valid range is from 1-4094.
<b>Step 5</b>	<b>absolute-timer <i>timer</i></b> <b>Example:</b> Device(config-service-template)# absolute-timer 1000	Specifies session timeout value for a service template. Valid range is from 1-65535.
<b>Step 6</b>	<b>service-policy qos input <i>qos-policy</i></b> <b>Example:</b> Device(config-service-template)# service-policy qos input in_qos	Configures an input QoS policy for the client.
<b>Step 7</b>	<b>service-policy qos output <i>qos-policy</i></b> <b>Example:</b> Device(config-service-template)# service-policy qos output out_qos	Configures an output QoS policy for the client.

## Creating a Parameter Map

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>parameter-map type subscriber attribute-to-service <i>parameter-map-name</i></b>  <b>Example:</b> Device(config)# parameter-map type subscriber attribute-to-service param	Specifies the parameter map type and name.
<b>Step 3</b>	<b>map-indexmap device-type eq <i>filter-name</i></b>  <b>Example:</b> Device(config-parameter-map-filter)# 1 map device-type eq "windows" mac-address eq 3c77.e602.2f91 username eq "cisco"	Specifies the parameter map attribute filter criteria. Multiple filters are used in the example provided here.
<b>Step 4</b>	<b>map-indexservice-template <i>service-template-name</i> precedence <i>precedence-num</i></b>  <b>Example:</b> Device(config-parameter-map-filter-submode)# 1 service-template svcl precedence 150	Specifies the service template and its precedence.

## Creating a Policy Map (GUI)

### Procedure

- Step 1** Choose **Configuration > Security > Local Policy > Policy Map** tab..
- Step 2** Enter a name for the Policy Map in the **Policy Map Name** text field.
- Step 3** Click **Add**
- Step 4** Choose the service template from the **Service Template** drop-down list.
- Step 5** For the following parameters select the type of filter from the drop-down list and enter the required match criteria
  - Device Type
  - User Role
  - User Name

- OUI
- MAC Address

- Step 6** Click **Add Criteria**
- Step 7** Click **Update & Apply to Device**.

## Creating a Policy Map (CLI)

### Before you begin

Before removing a policy map or parameter map, you should remove it from the target or shut down the WLAN profile or delete the session.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>policy-map type control subscriber</b> <i>policy-map-name</i> <b>Example:</b> Device(config)# policy-map type control subscriber polmap5	Specifies the policy map type.
<b>Step 3</b>	<b>event identity-update match-all</b> <b>Example:</b> Device(config-event-control-policymap)# event identity-update match-all	Specifies the match criteria to the policy map.
<b>Step 4</b>	You can apply a service template using either a class map or a parameter map, as shown here. <ul style="list-style-type: none"> <li>• <i>class-num</i> <b>class</b> <i>class-map-name</i> <b>do-until-failure</b></li> <li>• <i>action-index</i> <b>activate service-template</b> <i>service-template-name</i></li> <li>• <i>action-index</i> <b>map attribute-to-service</b> <b>table</b> <i>parameter-map-name</i></li> </ul> <b>Example:</b> The following example shows how a class-map with a service-template has to be applied: Device(config-class-control-policymap)# 10 class cls_mac do-until-failure	Configures the local profiling policy class map number and specifies how to perform the action or activates the service template or maps an identity-update attribute to an auto-configured template.

	Command or Action	Purpose
	<pre>Device(config-action-control-policymap)# 10 activate service-template svcl</pre> <p><b>Example:</b></p> <p>The following example shows how a parameter map has to be applied (service template is already associated with the parameter map 'param' while creating it):</p> <pre>Device(config-action-control-policymap)#1 map attribute-to-service table param</pre>	
<b>Step 5</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-action-control-policymap)# end</pre>	Exits configuration mode.
<b>Step 6</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 7</b>	<p><b>wireless profile policy</b> <i>wlan-policy-profile-name</i></p> <p><b>Example:</b></p> <pre>Device(config)# wireless profile policy wlan-policy-profilename</pre>	<p>Configures a wireless policy profile.</p> <p><b>Caution</b> Do not configure aaa-override for native profiling under a named wireless profile policy. Native profiling is applied at a lower priority than AAA policy. If aaa-override is enabled, the AAA policies will override native profile policy.</p>
<b>Step 8</b>	<p><b>description</b> <i>profile-policy-description</i></p> <p><b>Example:</b></p> <pre>Device(config-wireless-policy)# description "default policy profile"</pre>	Adds a description for the policy profile.
<b>Step 9</b>	<p><b>dhcp-tlv-caching</b></p> <p><b>Example:</b></p> <pre>Device(config-wireless-policy)# dhcp-tlv-caching</pre>	Configures DHCP TLV caching on a WLAN.
<b>Step 10</b>	<p><b>http-tlv-caching</b></p> <p><b>Example:</b></p> <pre>Device(config-wireless-policy)# http-tlv-caching</pre>	Configures client HTTP TLV caching on a WLAN.
<b>Step 11</b>	<p><b>subscriber-policy-name</b> <i>policy-name</i></p> <p><b>Example:</b></p>	Configures the subscriber policy name.

	Command or Action	Purpose
	Device(config-wireless-policy) # subscriber-policy-name polmap5	
<b>Step 12</b>	<b>vlan <i>vlan-id</i></b>  <b>Example:</b> Device(config-wireless-policy) # vlan 1	Configures a VLAN name or VLAN ID.
<b>Step 13</b>	<b>no shutdown</b>  <b>Example:</b> Device(config-wireless-policy) # no shutdown	Saves the configuration.

## Configuring Native Profiling in Local Mode

To configure native profiling in the local mode, you must follow the steps described in [Creating a Policy Map \(CLI\), on page 551](#). In the policy profile, you must enable central switching as described in the step given below in order to configure native profiling.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>central switching</b>  <b>Example:</b> Device(config-wireless-policy) # central switching	Enables central switching.

## Verifying Native Profile Configuration

Use the following **show** commands to verify the native profile configuration:

```
Device# show wireless client device summary
```

```
Active classified device summary
MAC Address      Device-type      User-role
Protocol-map
-----
1491.82b8.f94b   Microsoft-Workstation   sales
                   9
1491.82bc.2fd5   Windows7-Workstation     sales
                   41
```

```
Device# show wireless client device cache
```

```
Cached classified device info
MAC Address      Device-type      User-role
Protocol-map
-----
```

```

2477.031b.aa18   Microsoft-Workstation
                9
30a8.db3b.a753   Un-Classified Device
                9
4400.1011.e8b5   Un-Classified Device
                9
980c.a569.7dd0   Un-Classified Device

Device# show wireless client mac-address 4c34.8845.e32c detail | s
Session Manager:
Interface :
IIF ID      : 0x90000002
Device Type : Microsoft-Workstation
Protocol Map : 0x000009
Authorized  : TRUE
Session timeout : 1800
Common Session ID: 78380209000000174BF2B5B9
Acct Session ID : 0
Auth Method Status List
  Method : MAB
  SM State : TERMINATE
  Authen Status : Success
Local Polices:
  Service Template : wlan_svc_C414.3CCA.0A51 (priority 254)
  Absolute-Timer : 1800
Server Polices:
Resultant Policies:
Filter-ID    : acl-auto
Input QOS    : in_qos
Output QOS   : out_qos
Idle timeout : 60 sec
VLAN         : 10
Absolute-Timer : 1000

```

Use the following **show** command to verify the class map details for a class map name:

```

Device# show class-map type control subscriber name test
Class-map          Action                               Exec Hit Miss Comp
-----
match-any test    match day Monday                                0    0    0    0
match-any test    match join-time-of-day 8:00 18:00             0    0    0    0
Key:
"Exec" - The number of times this line was executed
"Hit" - The number of times this line evaluated to TRUE
"Miss" - The number of times this line evaluated to FALSE
"Comp" - The number of times this line completed the execution of its
condition without a need to continue on to the end

```



# PART **VIII**

## **IPv6**

- [Information About IPv6 Client Address Learning, on page 557](#)
- [Information About IPv6 ACL, on page 567](#)







## CHAPTER 59

# Information About IPv6 Client Address Learning

Client Address Learning is configured on embedded wireless controller to learn the IPv4 and IPv6 address of wireless client, and the client's transition state maintained by the embedded wireless controller on association and timeout.

There are three ways for an IPv6 client to acquire IPv6 addresses:

- Stateless Address Auto-Configuration (SLAAC)
- Stateful DHCPv6
- Static Configuration

In all of these methods, the IPv6 client always sends a neighbor solicitation Duplicate Address Detection (DAD) request to ensure that there is no duplicate IP address on the network. The embedded wireless controller snoops on the Neighbor Discovery Protocol (NDP) and DHCPv6 packets of the client to learn about its client IP addresses.

- [Address Assignment Using SLAAC](#) , on page 557
- [Stateful DHCPv6 Address Assignment](#), on page 558
- [Static IP Address Assignment](#), on page 559
- [Router Solicitation](#), on page 559
- [Router Advertisement](#), on page 559
- [Neighbor Discovery](#), on page 559
- [Neighbor Discovery Suppression](#), on page 560
- [Router Advertisement Guard](#), on page 560
- [Router Advertisement Throttling](#), on page 560
- [Prerequisites for IPv6 Client Address Learning](#), on page 561
- [Configuring IPv6 on Embedded Wireless Controller Interface](#), on page 561
- [Native IPv6](#), on page 562

## Address Assignment Using SLAAC

The most common method for IPv6 client address assignment is SLAAC, which provides simple plug-and-play connectivity, where clients self-assign an address based on the IPv6 prefix.

SLAAC is configured as follows:

- A host sends a Router Solicitation message.

- The host waits for a Router Advertisement message.
- The host take the first 64 bits of the IPv6 prefix from the Router Advertisement message and combines it with the 64 bit EUI-64 address (in the case of Ethernet, this is created from the MAC address) to create a global unicast message. The host also uses the source IP address, in the IP header, of the Router Advertisement message, as its default gateway.
- Duplicate Address Detection is performed by the IPv6 clients to ensure that random addresses that are picked do not collide with other clients.

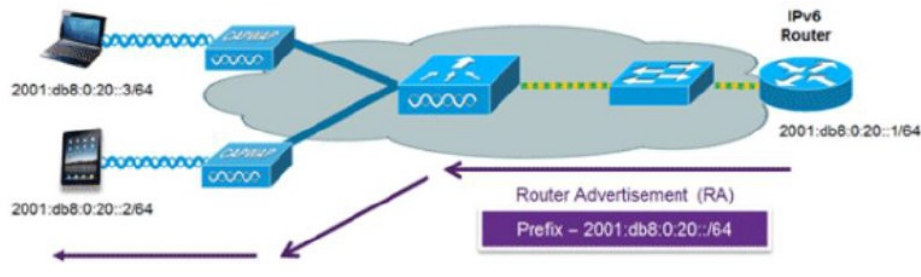


**Note** The choice of algorithm is up to the client and is often configurable.

The last 64 bits of the IPv6 address can be learned by using one of the following algorithms:

- EUI-64, which is based on the MAC address of the interface
- Private addresses that are randomly generated

**Figure 13: Address Assignment Using SLAAC**



The following Cisco IOS configuration commands from a Cisco-capable IPv6 router are used to enable SLAAC addressing and router advertisements:

```

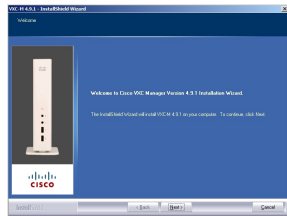
ipv6 unicast-routing
interface Vlan20
description IPv6-SLAAC
ip address 192.168.20.1 255.255.255.0
ipv6 address FE80:DB8:0:20::1 linklocal
ipv6 address 2001:DB8:0:20::1/64
ipv6 enable
end

```

## Stateful DHCPv6 Address Assignment

The use of DHCPv6 is not required for IPv6 client connectivity if SLAAC is already deployed. There are two modes of operation for DHCPv6, that is, Stateless and Stateful.

The DHCPv6 Stateless mode is used to provide clients with additional network information that is not available in the router advertisement, but not an IPv6 address, because this is already provided by SLAAC. This information includes the DNS domain name, DNS servers, and other DHCP vendor-specific options.

**Figure 14: Stateful DHCPv6 Address Assignment**

The following interface configuration is for a Cisco IOS IPv6 router implementing stateless DHCPv6 with SLAAC enabled:

```

ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateless
ip address 192.168.20.1 255.255.255.0
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPPOOL
ipv6 address 2001:DB8:0:20::1/64
end

```

## Static IP Address Assignment

Statically configured address on a client.

## Router Solicitation

A Router Solicitation message is issued by a host controller to facilitate local routers to transmit a Router Advertisement from which the controller can obtain information about local routing, or perform stateless auto configuration. Router Advertisements are transmitted periodically and the host prompts with an immediate Router Advertisement using a Router Solicitation such as - when it boots or following a restart operation.

## Router Advertisement

A Router Advertisement message is issued periodically by a router or in response to a Router Solicitation message from a host. The information contained in these messages is used by a host to perform stateless auto configuration and to modify its routing table.

## Neighbor Discovery

IPv6 Neighbor Discovery is a set of messages and processes that determine relationships between neighboring nodes. Neighbor Discovery replaces the Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP) Router Discovery, and ICMP Redirect used in IPv4.

IPv6 Neighbor Discovery inspection analyzes neighbor discovery messages in order to build a trusted binding table database, and IPv6 Neighbor Discovery packets that do not comply, are dropped. The neighbor binding table in the tracks each IPv6 address and its associated MAC address. Clients are removed from the table according to neighbor-binding timers.

## Neighbor Discovery Suppression

The IPv6 addresses of wireless clients are cached by a device. When the device receives an NS multicast looking for an IPv6 address, and if the target address is known to the device and belongs to one of its clients, the device will reply with an NA message on behalf of the client. At the end of this process, the equivalent of the ARP table of IPv4 is generated, but is more efficient because it uses fewer messages.



---

**Note** The device acts as a proxy and responds with NA, only when the **ipv6 nd suppress** command is configured.

---

If the device does not have the IPv6 address of a wireless client, the device does not respond with NA; instead, it forwards the NS packet to the wireless side. To resolve this, an NS Multicast Forwarding knob is provided. If this knob is enabled, the device gets the NS packet for the IPv6 address that it does not have (cache miss) and forwards it to the wireless side. This packet reaches the intended wireless client, and the client replies with NA.

Note that this cache miss scenario occurs rarely, and only very few clients who do not implement complete IPv6 stack may not advertise their IPv6 address during NDP.

## Router Advertisement Guard

- Port on which the frame is received
- IPv6 source address
- Prefix list
- Trusted or Untrusted ports for receiving the router advertisement guard messages
- Trusted/Untrusted IPv6 source addresses of the router advertisement sender
- Trusted/Untrusted Prefix list and Prefix ranges
- Router preference

## Router Advertisement Throttling

RA throttling allows the controller to enforce limits to the RA packets headed toward the wireless network. By enabling RA throttling, routers that send multiple RA packets can be trimmed to a minimum frequency that will still maintain an IPv6 client connectivity. If a client sends an RS packet, an RA is sent back to the client. This RA is allowed through the controller and unicast to the client. This process ensures that the new clients or roaming clients are not affected by the RA throttling.

# Prerequisites for IPv6 Client Address Learning

Before configuring IPv6 client address learning, configure the embedded wireless controller clients to support IPv6.

## Configuring IPv6 on Embedded Wireless Controller Interface

Follow the procedure given below to configure IPv6 on an interface:

### Before you begin

Enable IPv6 on the client and IPv6 support on the wired infrastructure.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. Enter your password, if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>interface GigabitEthernet0</b> <b>Example:</b> Device(config)# <b>interface GigabitEthernet0</b>	Creates the GigabitEthernet interface and enters interface configuration mode.
<b>Step 4</b>	<b>ip address fe80::1 link-local</b> <b>Example:</b> Device(config-if)# <b>ip address 198.51.100.1 255.255.255.0</b> Device(config-if)# <b>ipv6 address fe80::1 link-local</b> Device(config-if)# <b>ipv6 address 2001:DB8:0:1:FFFF:1234::5/64</b> Device(config-if)# <b>ipv6 address 2001:DB8:0:0:E000::F/64</b>	Configures IPv6 address on the GigabitEthernet interface using the link-local option.
<b>Step 5</b>	<b>ipv6 enable</b> <b>Example:</b> Device(config)# <b>ipv6 enable</b>	(Optional) Enables IPv6 on the GigabitEthernet interface.

	Command or Action	Purpose
Step 6	<b>end</b>  <b>Example:</b> Device(config)# <b>end</b>	Exits interface mode.

## Native IPv6

### Information About IPv6

IPv6 is a packet-based protocol used to exchange data, voice, and video traffic over digital networks. IPv6 is based on IP, but with a much larger address space, and improvements such as a simplified main header and extension headers. The architecture of IPv6 has been designed to allow existing IPv4 users to transition easily to IPv6 while continuing to use services such as end-to-end security, quality of service (QoS), and globally unique addresses. The larger IPv6 address space allows networks to scale and provide global reachability.



**Note** The features and functions that work on IPv4 networks with IPv4 addresses also work on IPv6 networks with IPv6 addresses.

#### General Guidelines

- You must configure the **ipv6 unicast-routing** command on the embedded wireless controller for the IPv6 feature to work.
- The Wireless Management interface should have only one static IPv6 address.
- Router advertisement should be suppressed on the wireless management interface and client VLANs (if IPv6 is configured on the client VLAN).
- Preferred mode is part of an AP join profile. When you configure the preferred mode as IPv6, an AP attempts to join over IPv6 first. If it fails, the AP falls back to IPv4.
- You should use MAC addresses for RA tracing of APs and clients.

#### Unsupported Features

- UDP Lite is not supported.
- AP sniffer over IPv6 is not supported.
- IPv6 is not supported for the HA port interface.
- Auto RF grouping over IPv6 is not supported. Only static RF grouping is supported.

## Configuring IPv6 Addressing

Follow the procedure given below to configure IPv6 addressing:



**Note** All the features and functions that work on IPv4 networks with IPv4 addresses will work on IPv6 networks with IPv6 addresses too.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ipv6 unicast-routing</b> <b>Example:</b> Device(config)# ipv6 unicast-routing	Configures IPv6 for unicasting.
<b>Step 3</b>	<b>interface GigabitEthernet0</b> <b>Example:</b> Device(config)# <b>interface</b> <b>GigabitEthernet0</b>	Creates the GigabitEthernet interface and enters interface configuration mode.
<b>Step 4</b>	<b>ipv6 address <i>ipv6-address</i></b> <b>Example:</b> Device(config-if)# ipv6 address FD09:9:2:49::53/64	Specifies a global IPv6 address.
<b>Step 5</b>	<b>ipv6 enable</b> <b>Example:</b> Device(config-if)# ipv6 enable	Enables IPv6 on the interface.
<b>Step 6</b>	<b>ipv6 nd ra suppress all</b> <b>Example:</b> Device(config-if)# ipv6 nd ra suppress all	Suppresses IPv6 router advertisement transmissions on the interface.
<b>Step 7</b>	<b>exit</b> <b>Example:</b> Device(config-if)# exit	Returns to global configuration mode.
<b>Step 8</b>	<b>wireless management interface</b> <b>gigabitEthernet <i>gigabitEthernet-interface-vlan 64</i></b> <b>Example:</b> Device(config)# wireless management interface gigabitEthernet vlan 64	Configures the ports that are connected to the supported APs with the wireless management interface.

	Command or Action	Purpose
<b>Step 9</b>	<b>ipv6 route</b> <i>ipv6-address</i>  <b>Example:</b> Device(config)# ipv6 route ::/0 FD09:9:2:49::1	Specifies IPv6 static routes.

## Creating an AP Join Profile (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > AP Join**.
  - Step 2** On the **AP Join Profile** window, click the **General** tab and click **Add**.
  - Step 3** In the **Name** field enter, a name for the AP join profile.
  - Step 4** (Optional) Enter a description for the AP join profile.
  - Step 5** Choose **CAPWAP > Advanced**.
  - Step 6** Under the **Advanced** tab, from the **Preferred Mode** drop-down list, choose **IPv6**. This sets the preferred mode of APs as IPv6.
  - Step 7** Click **Save & Apply to Device**.
- 

## Creating an AP Join Profile (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ap profile</b> <i>ap-profile</i>  <b>Example:</b> Device(config)# ap profile xyz-ap-profile	Configures an AP profile and enters AP profile configuration mode.
<b>Step 3</b>	<b>description</b> <i>ap-profile-name</i>  <b>Example:</b> Device(config-ap-profile)# description "xyz ap profile"	Adds a description for the AP profile.
<b>Step 4</b>	<b>preferred-mode</b> <b>ipv6</b>  <b>Example:</b>	Sets the preferred mode of APs as IPv6.



	Command or Action	Purpose
	Device(config-ap-profile)# preferred-mode ipv6	

## Configuring the Primary and Backup Embedded Wireless Controller (GUI)

### Before you begin

Ensure that you have configured an AP join profile prior to configuring the primary and backup embedded wireless controllers.

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > AP Join**.
  - Step 2** On the **AP Join Profile** window, click the AP join profile name.
  - Step 3** In the **Edit AP Join Profile** window, click the **CAPWAP** tab.
  - Step 4** In the **High Availability** tab, under **Backup Controller Configuration**, check the **Enable Fallback** check box.
  - Step 5** Enter the primary and secondary controller names and IP addresses.
  - Step 6** Click **Update & Apply to Device**.
- 

## Configuring Primary and Backup Controller (CLI)

Follow the procedure given below to configure the primary and secondary controllers for a selected AP:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ap profile profile-name</b> <b>Example:</b> Device(config)# ap profile yy-ap-profile	Configures an AP profile and enters AP profile configuration mode.
<b>Step 3</b>	<b>capwap backup primary</b> <i>primary-controller-name primary-controller-ip</i> <b>Example:</b>	Configures AP CAPWAP parameters with the primary backup controller's name.

	Command or Action	Purpose
	Device(config)# capwap backup primary WLAN-Controller-A 2001:DB8:1::1	<b>Note</b> You need to enable fast heartbeat for <b>capwap backup primary</b> and <b>capwap backup secondary</b> to work.  AP disconnection may occur if the link between the controller and AP is not reliable and fast heartbeat is enabled.
<b>Step 4</b>	<b>ap capwap backup secondary</b> <i>secondary-controller-name</i> <i>secondary-controller-ip</i>  <b>Example:</b> Device(config)# capwap backup secondary WLAN-Controller-B 2001:DB8:1::1	Configures AP CAPWAP parameters with the secondary backup controller's name.
<b>Step 5</b>	<b>syslog host ipaddress</b>  <b>Example:</b> Device(config)# syslog host 2001:DB8:1::1	Configures the system logging settings for the APs.
<b>Step 6</b>	<b>tftp-downgrade tftp-server-ip imagename</b>  <b>Example:</b> Device(config)# tftp-downgrade 2001:DB8:1::1 testimage	Initiates AP image downgrade from a TFTP server for all the APs.

## Verifying IPv6 Configuration

Use the following **show** command to verify the IPv6 configuration:

```
Device# show wireless interface summary
```

```
Interface Name   Interface Type  VLAN ID  IP Address      IP Netmask      NAT-IP Address  MAC
Address
-----
GigabitEthernet0 Management      0        0.0.0.0        255.255.255.0  0.0.0.0
d4c9.3ce6.b854
                                     fd09:9:2:49::54/64
```



## CHAPTER 60

# Information About IPv6 ACL

An access control list (ACL) is a set of rules used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the embedded wireless controller). ACLs are configured on the device and applied to the management interface, the AP-manager interface, any of the dynamic interfaces, or a WLAN to control data traffic to and from wireless clients or to the embedded wireless controller central processing unit (CPU) to control all traffic destined for the CPU.

You can also create a preauthentication ACL for web authentication. Such an ACL is used to allow certain types of traffic before authentication is complete.

IPv6 ACLs support the same options as IPv4 ACLs including source, destination, source and destination ports.



---

**Note** You can enable only IPv4 traffic in your network by blocking IPv6 traffic. That is, you can configure an IPv6 ACL to deny all IPv6 traffic and apply it on specific or all WLANs.

---

- [Understanding IPv6 ACLs, on page 567](#)
- [Types of ACL, on page 567](#)
- [Prerequisites for Configuring IPv6 ACL, on page 568](#)
- [Restrictions for Configuring IPv6 ACL, on page 568](#)
- [Configuring IPv6 ACLs, on page 569](#)
- [How To Configure an IPv6 ACL, on page 570](#)
- [Verifying IPv6 ACL, on page 573](#)
- [Configuration Examples for IPv6 ACL, on page 574](#)

## Understanding IPv6 ACLs

### Types of ACL

#### Per User IPv6 ACL

For the per-user ACL, the full access control entries (ACE) as the text strings are configured on the Cisco Secure Access Control Server (Cisco Secure ACS).

The ACE is not configured on the Controller Embedded Wireless Controller. The ACE is sent to the device in the `ACCESS-Accept` attribute and applies it directly for the client. When a wireless client roams into an foreign device, the ACEs are sent to the foreign device as an AAA attribute in the mobility Handoff message. Output direction, using per-user ACL is not supported.

## Filter ID IPv6 ACL

For the filter-Id ACL, the full ACEs and the `acl_name(filter-id)` is configured on the device and only the `filter-id` is configured on the Cisco Secure ACS.

The `filter-id` is sent to the device in the `ACCESS-Accept` attribute, and the device looks up the `filter-id` for the ACEs, and then applies the ACEs to the client. When the client L2 roams to the foreign device, only the `filter-id` is sent to the foreign device in the mobility Handoff message. Output filtered ACL, using per-user ACL is not supported. The foreign device has to configure the `filter-id` and ACEs beforehand.

## Downloadable IPv6 ACL

For the downloadable ACL (dACL), all the full ACEs and the `dac1` name are configured only on the Cisco Secure ACS.

The Cisco Secure ACS sends the `dac1` name to the device in its `ACCESS-Accept` attribute, which takes the `dac1` name and sends the `dACL` name back to the Cisco Secure ACS for the ACEs, using the `ACCESS-request` attribute.

## Prerequisites for Configuring IPv6 ACL

You can filter IP Version 6 (IPv6) traffic by creating IPv6 access control lists (ACLs) and applying them to interfaces similarly to the way that you create and apply IP Version 4 (IPv4) named ACLs. You can also create and apply input router ACLs to filter Layer 3 management traffic when the switch is running the Network Essentials license.

## Restrictions for Configuring IPv6 ACL

With IPv4, you can configure standard and extended numbered IP ACLs, named IP ACLs, and MAC ACLs. IPv6 supports only named ACLs.

The device supports most of the Cisco IOS-supported IPv6 ACLs with some exceptions:

- The device does not support matching on these keywords: **flowlabel**, **routing header**, and **undetermined-transport**.
- The device does not support reflexive ACLs (the **reflect** keyword).
- The device does not apply MAC-based ACLs on IPv6 frames.
- When configuring an ACL, there is no restriction on keywords entered in the ACL, regardless of whether or not they are supported on the platform. When you apply the ACL to an interface that requires hardware forwarding (physical ports or SVIs), the device checks to determine whether or not the ACL can be supported on the interface. If not, attaching the ACL is rejected.

- If an ACL is applied to an interface and you attempt to add an access control entry (ACE) with an unsupported keyword, the device does not allow the ACE to be added to the ACL that is currently attached to the interface

## Configuring IPv6 ACLs

Follow the procedure given below to filter IPv6 traffic:

1. Create an IPv6 ACL, and enter IPv6 access list configuration mode.
2. Configure the IPv6 ACL to block (deny) or pass (permit) traffic.
3. Apply the IPv6 ACL to the interface where the traffic needs to be filtered.
4. Apply the IPv6 ACL to an interface. For router ACLs, you must also configure an IPv6 address on the Layer 3 interface to which the ACL is applied.

## Default IPv6 ACL Configuration

There are no IPv6 ACLs configured or applied.

## Interaction with Other Features and Switches

- If an IPv6 router ACL is configured to deny a packet, the packet is not routed. A copy of the packet is sent to the Internet Control Message Protocol (ICMP) queue to generate an ICMP unreachable message for the frame.
- If a bridged frame is to be dropped due to a port ACL, the frame is not bridged.
- You can create both IPv4 and IPv6 ACLs on a switch or switch stack, and you can apply both IPv4 and IPv6 ACLs to the same interface. Each ACL must have a unique name; an error message appears if you try to use a name that is already configured.

You use different commands to create IPv4 and IPv6 ACLs and to attach IPv4 or IPv6 ACLs to the same Layer 2 or Layer 3 interface. If you use the wrong command to attach an ACL (for example, an IPv4 command to attach an IPv6 ACL), you receive an error message.

- You cannot use MAC ACLs to filter IPv6 frames. MAC ACLs can only filter non-IP frames.
- If the hardware memory is full, for any additional configured ACLs, packets are dropped to the CPU, and the ACLs are applied in software. When the hardware is full a message is printed to the console indicating the ACL has been unloaded and the packets will be dropped on the interface.

# How To Configure an IPv6 ACL

## Creating an IPv6 ACL

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>ipv6 access-list <i>acl_name</i></b> <b>Example:</b> Device# <b>ipv6 access-list access-list-name</b>	Use a name to define an IPv6 access list and enter IPv6 access-list configuration mode.
<b>Step 4</b>	<b>{deny permit} protocol</b> <b>Example:</b> <pre>{deny   permit} protocol {source-ipv6-prefix/prefix-length   any    host source-ipv6-address} [operator [port-number]](destination-ipv6-prefix/prefix-length    any  host destination-ipv6-address} [operator [port-number]][dscp value] [fragments][log] [log-input] [routing][sequence value] [time-range name]</pre>	Enter deny or permit to specify whether to deny or permit the packet if conditions are matched. These are the conditions: <ul style="list-style-type: none"> <li>• For protocol, enter the name or number of an Internet protocol: ahp, esp, icmp, ipv6, pcp, stcp, tcp, or udp, or an integer in the range 0 to 255 representing an IPv6 protocol number.</li> <li>• The source-ipv6-prefix/prefix-length or destination-ipv6-prefix/ prefix-length is the source or destination IPv6 network or class of networks for which to set deny or permit conditions, specified in hexadecimal and using 16-bit values between colons (see RFC 2373).</li> <li>• Enter any as an abbreviation for the IPv6 prefix ::/0.</li> <li>• For host source-ipv6-address or destination-ipv6-address, enter the source or destination IPv6 host address for which to set deny or permit conditions, specified</li> </ul>

	Command or Action	Purpose
		<p>in hexadecimal using 16-bit values between colons.</p> <ul style="list-style-type: none"> <li>• (Optional) For operator, specify an operand that compares the source or destination ports of the specified protocol. Operands are lt (less than), gt (greater than), eq (equal), neq (not equal), and range.</li> </ul> <p>If the operator follows the source-ipv6-prefix/prefix-length argument, it must match the source port. If the operator follows the destination-ipv6-prefix/prefix-length argument, it must match the destination port.</p> <ul style="list-style-type: none"> <li>• (Optional) The port-number is a decimal number from 0 to 65535 or the name of a TCP or UDP port. You can use TCP port names only when filtering TCP. You can use UDP port names only when filtering UDP.</li> <li>• (Optional) Enter dscp value to match a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.</li> <li>• (Optional) Enter fragments to check noninitial fragments. This keyword is visible only if the protocol is ipv6.</li> <li>• (Optional) Enter log to cause an logging message to be sent to the console about the packet that matches the entry. Enter log-input to include the input interface in the log entry. Logging is supported only for router ACLs.</li> <li>• (Optional) Enter routing to specify that IPv6 packets be routed.</li> <li>• (Optional) Enter sequence value to specify the sequence number for the access list statement. The acceptable range is from 1 to 4294967295</li> <li>• (Optional) Enter time-range name to specify the time range that applies to the deny or permit statement.</li> </ul>

	Command or Action	Purpose
Step 5	<p><b>{deny permit} tcp</b></p> <p><b>Example:</b></p> <pre>{deny   permit} tcp {source-ipv6-prefix/prefix-length   any    hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length    any   hostdestination-ipv6-address} [operator [port-number]][ack] [dscp value][established] [fin] [log][log-input] [neq {port   protocol}]  [psh] [range{port   protocol}] [rst][routing] [sequence value] [syn] [time-range name][urg]</pre>	<p>(Optional) Define a TCP access list and the access conditions.</p> <p>Enter tcp for Transmission Control Protocol. The parameters are the same as those described in Step 3, with these additional optional parameters:</p> <ul style="list-style-type: none"> <li>• ack—Acknowledgment bit set.</li> <li>• established—An established connection. A match occurs if the TCP datagram has the ACK or RST bits set.</li> <li>• fin—Finished bit set; no more data from sender.</li> <li>• neq {port   protocol}—Matches only packets that are not on a given port number.</li> <li>• psh—Push function bit set.</li> <li>• range {port   protocol}—Matches only packets in the port number range.</li> <li>• rst—Reset bit set.</li> <li>• syn—Synchronize bit set.</li> <li>• urg—Urgent pointer bit set.</li> </ul>
Step 6	<p><b>{deny permit} udp</b></p> <p><b>Example:</b></p> <pre>{deny   permit} udp {source-ipv6-prefix/prefix-length   any    hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length    any   hostdestination-ipv6-address} [operator [port-number]][dscp value] [log][log-input] [neq {port   protocol}] [range {port  protocol}] [routing][sequence value][time-range name]</pre>	<p>(Optional) Define a UDP access list and the access conditions.</p> <p>Enter udp for the User Datagram Protocol. The UDP parameters are the same as those described for TCP, except that the operator [port] port number or name must be a UDP port number or name, and the established parameter is not valid for UDP.</p>
Step 7	<p><b>{deny permit} icmp</b></p> <p><b>Example:</b></p> <pre>{deny   permit} icmp {source-ipv6-prefix/prefix-length   any    hostsource-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length    any   hostdestination-ipv6-address} [operator [port-number]][icmp-type]</pre>	<p>(Optional) Define an ICMP access list and the access conditions.</p> <p>Enter icmp for Internet Control Message Protocol. The ICMP parameters are the same as those described for most IP protocols in Step 3a, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings:</p>



	Command or Action	Purpose
	[icmp-code] [icmp-message] [dscpvalue] [log] [log-input] [routing] [sequence value] [time-range name]	<ul style="list-style-type: none"> <li>• icmp-type—Enter to filter by ICMP message type, a number from 0 to 255.</li> <li>• icmp-code—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255.</li> <li>• icmp-message—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name. To see a list of ICMP message type names and code names, use the ? key or see command reference for this release.</li> </ul>
<b>Step 8</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.
<b>Step 9</b>	<b>show ipv6 access-list</b> <b>Example:</b> show ipv6 access-list	Verify the access list configuration.
<b>Step 10</b>	<b>copy running-config startup-config</b> <b>Example:</b> copy running-config startup-config	(Optional) Save your entries in the configuration file.

## Creating WLAN IPv6 ACL

## Verifying IPv6 ACL

## Displaying IPv6 ACLs

To display IPv6 ACLs, perform this procedure:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b>  Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<b>show access-list</b>  <b>Example:</b>  Device# <code>show access-lists</code>	Displays all access lists configured on the device
<b>Step 4</b>	<b>show ipv6 access-list <i>acl_name</i></b>  <b>Example:</b>  Device# <code>show ipv6 access-list</code> <code>[access-list-name]</code>	Displays all configured IPv6 access list or the access list specified by name.

## Configuration Examples for IPv6 ACL

### Example: Creating an IPv6 ACL

This example configures the IPv6 access list named CISCO. The first deny entry in the list denies all packets that have a destination TCP port number greater than 5000. The second deny entry denies packets that have a source UDP port number less than 5000. The second deny also logs all matches to the console. The first permit entry in the list permits all ICMP packets. The second permit entry in the list permits all other traffic. The second permit entry is necessary because an implicit deny -all condition is at the end of each IPv6 access list.



**Note** Logging is supported only on Layer 3 interfaces.

```
Device(config)# ipv6 access-list CISCO
Device(config-ipv6-acl)# deny tcp any any gt 5000
Device (config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Device(config-ipv6-acl)# permit icmp any any
Device(config-ipv6-acl)# permit any any
```

### Example: Displaying IPv6 ACLs

This is an example of the output from the **show access-lists** privileged EXEC command. The output shows all access lists that are configured on the switch or switch stack.

```
Device #show access-lists
Extended IP access list hello
10 permit ip any any
IPv6 access list ipv6
permit ipv6 any any sequence 10
```

This is an example of the output from the **show ipv6 access-lists** privileged EXEC command. The output shows only IPv6 access lists configured on the switch or switch stack.

```
Device# show ipv6 access-list
IPv6 access list inbound
permit tcp any any eq bgp (8 matches) sequence 10
permit tcp any any eq telnet (15 matches) sequence 20
permit udp any any sequence 30

IPv6 access list outbound
deny udp any any sequence 10
deny tcp any any eq telnet sequence 20
```





## PART **IX**

### **CleanAir**

- [Cisco CleanAir, on page 579](#)
- [Spectrum Intelligence, on page 593](#)





## CHAPTER 61

# Cisco CleanAir

- [Information About Cisco CleanAir, on page 579](#)
- [Prerequisites for CleanAir, on page 582](#)
- [Restrictions for CleanAir, on page 582](#)
- [How to Configure CleanAir, on page 583](#)
- [Verifying CleanAir Parameters, on page 590](#)
- [Configuration Examples for CleanAir, on page 591](#)
- [CleanAir FAQs, on page 592](#)

## Information About Cisco CleanAir

Cisco CleanAir is a solution designed to proactively manage the challenges of a shared wireless spectrum. It allows you to see all the users of a shared spectrum (both native devices and foreign interferers). It also enables the network to act upon this information. For example, you can manually remove the interfering device, or the system can automatically change the channel away from the interference. CleanAir provides spectrum management and Radio Frequency (RF) visibility.

A Cisco CleanAir system consists of CleanAir-enabled access points. These access points collect information about all the devices that operate in the industrial, scientific, and medical (ISM) bands, identify and evaluate the information as a potential interference source, and forward it to the embedded wireless controller. The controller embedded wireless controller controls the access points.

For every device operating in the unlicensed band, Cisco CleanAir provides information about what it is, how it is impacting your wireless network, and what actions you or your network should take. It simplifies RF.

Wireless LAN systems operate in unlicensed 2.4-GHz and 5-GHz ISM bands. Many devices, such as microwave ovens, cordless phones, and Bluetooth devices also operate in these bands and can negatively affect the Wi-Fi operations.

Some of the most advanced WLAN services, such as voice-over-wireless and IEEE 802.11 radio communications, might be significantly impaired by the interference caused by other legal users of the ISM bands. The integration of Cisco CleanAir functionality addresses this problem of RF interference.

## Cisco CleanAir-Related Terms

Table 24: CleanAir-Related Terms

Term	Description
AQI	Air Quality Index. The AQI is an indicator of air quality, based on the air pollutants. An AQI of 0 is bad and an AQI > 85 is good.
AQR	Air Quality Report. AQRs contain information about total interference from all the identified sources represented by AQI and the summary of the most severe interference categories. AQRs are sent every 15 minutes to the Mobility Controller and every 30 seconds in the Rapid mode.
DC	Duty Cycle. Percentage of time that the channel is utilized by a device.
EDRRM	Event-Driven RRM. EDRRM allows an access point in distress to bypass normal RRM intervals and immediately change channels.
IDR	Interference Device Reports that an access point sends to the embedded wireless controller.
ISI	Interference Severity Index. The ISI is an indicator of the severity of the interference.
RSSI	Received Signal Strength Indicator. RSSI is a measurement of the power present in a received radio signal. It is the power at which an access point sees the interferer device.

## Cisco CleanAir Components

The basic Cisco CleanAir architecture consists of Cisco CleanAir-enabled APs and device.

An access point equipped with Cisco CleanAir technology collects information about Wi-Fi interference sources processes it. The access point sends the Air Quality Report (AQR) and Interference Device Report (IDR) to the embedded wireless controller.

The controller controls and configures CleanAir-capable access points, and collects and processes spectrum data. The provides local user interfaces (GUI and CLI) to configure basic CleanAir features and services and display current spectrum information. The also detects, merges, and mitigates interference devices using RRM TPC and DCA For details, see Interference Device Merging.

The device performs the following tasks in a Cisco CleanAir system:

- Configures Cisco CleanAir capabilities on the access point.
- Provides interfaces ( CLI) for configuring Cisco CleanAir features and retrieving data.
- Displays spectrum data.
- Collects and processes AQRs from the access point and stores them in the air quality database. AQRs contain information about the total interference from all the identified sources represented by the Air Quality Index (AQI) and the summary for the most severe interference categories. The CleanAir system can also include unclassified interference information under per-interference type reports that enable you to take action in scenarios where interference because of unclassified interfering devices is more.
- Collects and processes IDRs from the access point and stores them in the interference device database.



## Interference Types that Cisco CleanAir can Detect

Cisco CleanAir .

Wi-Fi chip-based RF management systems share these characteristics:

- Any RF energy that cannot be identified as a Wi-Fi signal is reported as noise.
- Noise measurements that are used to assign a channel plan tend to be averaged over a period of time to avoid instability or rapid changes that can be disruptive to certain client devices.
- Averaging measurements reduces the resolution of the measurement. As such, a signal that disrupts clients might not look like it needs to be mitigated after averaging.
- All RF management systems available today are reactive in nature.

Cisco CleanAir is different and can positively identify not only the source of the noise but also its potential impact to a WLAN. Having this information allows you to consider the noise within the context of the network and make intelligent and, where possible, proactive decisions.



---

**Note** Spectrum event-driven RRM can be triggered only by Cisco CleanAir-enabled access points in local mode.

---

Spontaneous interference is interference that appears suddenly on a network, perhaps jamming a channel or a range of channels completely. The Cisco CleanAir spectrum event-driven RRM feature allows you to set a threshold for air quality (AQ) which, if exceeded, triggers an immediate channel change for the affected access point. Most RF management systems can avoid interference, but this information takes time to propagate through the system. Cisco CleanAir relies on AQ measurements to continuously evaluate the spectrum and can trigger a move within 30 seconds. For example, if an access point detects interference from a video camera, it can recover by changing channels within 30 seconds of the camera becoming active. Cisco CleanAir also identifies and locates the source of interference so that more permanent mitigation of the device can be performed at a later time.

Microwave Ovens, Outdoor Ethernet bridges are two classes of devices that qualify as persistent, since once detected, it is likely that these devices will continue to be a random problem and are not likely to move. For these types of devices we can tell RRM of the detection and Bias the affected channel so that RRM "remembers" that there is a high potential for client impacting interference for the Detecting AP on the detected channel. For more information, see [https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b\\_RRM\\_White\\_Paper/b\\_RRM\\_White\\_Paper\\_chapter\\_0100.html?bookSearch=true#id\\_15217](https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_RRM_White_Paper/b_RRM_White_Paper_chapter_0100.html?bookSearch=true#id_15217).

CleanAir PDA devices include:

- Microwave Oven
- WiMax Fixed
- WiMax Mobile
- Motorola Canopy

In the case of Bluetooth devices, Cisco CleanAir-enabled access points can detect and report interference only if the devices are actively transmitting. Bluetooth devices have extensive power-save modes. For example, interference can be detected when data or voice is being streamed between the connected devices.

## EDRRM and AQR Update Mode

EDRRM is a feature that allows an access point that is in distress to bypass normal RRM intervals and immediately change channels. A CleanAir access point always monitors AQ and reports the AQ every 15 minutes. AQ only reports classified interference devices. The key benefit of EDRRM is fast action time. If an interfering device is operating on an active channel and causes enough AQ degradation to trigger an EDRRM, then no clients will be able to use that channel or the access point. You must remove the access point from the channel. EDRRM is not enabled by default, you must first enable CleanAir and then enable EDRRM.

## Prerequisites for CleanAir

You can configure Cisco CleanAir only on CleanAir-enabled access points.

Only Cisco CleanAir-enabled access points using the following access point modes can perform Cisco CleanAir spectrum monitoring:

- **Local**—In this mode, each Cisco CleanAir-enabled access point radio provides air quality and interference detection reports for the current operating channel only. An AP can only measure air quality and interference when the AP is not busy transmitting Wi-Fi frames. This implies that CleanAir detections will be drastically lower if the AP is having a high channel utilization.
- **Monitor**—When Cisco CleanAir is enabled in monitor mode, the access point provides air quality and interference detection reports for all monitored channels.

The following options are available:

- **All**—All channels
- **DCA**—Channel selection governed by the DCA list
- **Country**—All channels are legal within a regulatory domain

## Restrictions for CleanAir

- Access points in monitor mode do not transmit Wi-Fi traffic or 802.11 packets. They are excluded from radio resource management (RRM) planning and are not included in the neighbor access point list. IDR clustering depends on the device's ability to detect neighboring in-network access points. Correlating interference device detections from multiple access points is limited between monitor-mode access points.
- For 4800 AP slot 1 5 GHz is dedicated and cannot be individually moved to monitor mode. However, slot 0 is XOR and can be moved to monitor as well as 2.4/5 GHz. Slot 2 is dedicated monitor and will operate in 5GHz and in AP monitor mode, slot 2 will be disabled because a monitor radio is already available in both 2.4/5GHz. 3700 AP has dedicated 2.4GHz (slot0) and 5GHz (slot1).
- Do not connect access points in SE connect mode directly to any physical port on the controller.
- CleanAir is not supported wherein the channel width is 160 MHz.

# How to Configure CleanAir

## Enabling CleanAir for the 2.4-GHz Band (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Radio Configurations > CleanAir**
  - Step 2** On the **CleanAir** page, click the **me2.4 GHz Band > General** tab.
  - Step 3** Check the **Enable CleanAir** checkbox.
  - Step 4** Click **Apply**.
- 

## Enabling CleanAir for the 2.4-GHz Band (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ap dot11 24ghz cleanair</b>  <b>Example:</b> Device(config)# <code>ap dot11 24ghz cleanair</code> Device(config)# <code>no ap dot11 24ghz cleanair</code>	Enables the CleanAir feature on the 802.11b network. Run the <b>no</b> form of this command to disable CleanAir on the 802.11b network.
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Device(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring Interference Reporting for a 2.4-GHz Device (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Radio Configurations > CleanAir**.
  - Step 2** Click the **2.4 GHz Band** tab.
  - Step 3** Choose the interference types and add them to the **Interference Types to detect** section.

The following interference types are available:

- BLE Beacon—Bluetooth low energy beacon
- Bluetooth Discovery
- Bluetooth Link
- Canopy
- Continuous Transmitter
- DECT-like Phone—Digital Enhanced Cordless Technology phone
- 802.11 FH—802.11 frequency hopping device
- WiFi Inverted—Device using spectrally inverted Wi-Fi signals
- Jammer
- Microwave Oven
- WiFi Invalid Channel—Device using nonstandard Wi-Fi channels
- TDD Transmitter
- Video Camera
- SuperAG—802.11 SuperAG device
- WiMax Mobile
- WiMax Fixed
- 802.15.4
- Microsoft Device
- SI\_FHSS

**Step 4** Click **Apply**.

## Configuring Interference Reporting for a 2.4-GHz Device (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>ap dot11 24ghz cleanair device {bt-discovery   bt-link   canopy   cont-tx   dect-like   fh   inv   jammer   mw-oven   nonstd   report  </b>	Configures the 2.4-GHz interference devices to report to the device. Run the <b>no</b> form of this command to disable the configuration.

Command or Action	Purpose
<p><b>superag   tdd-tx   video   wimax-fixed   wimax-mobile   xbox   zigbee }</b></p> <p><b>Example:</b></p> <pre>Device(config)# ap dot11 24ghz cleanair device bt-discovery  Device(config)# ap dot11 24ghz cleanair device bt-link  Device(config)# ap dot11 24ghz cleanair device canopy  Device(config)# ap dot11 24ghz cleanair device cont-tx  Device(config)# ap dot11 24ghz cleanair device dect-like  Device(config)# ap dot11 24ghz cleanair device fh  Device(config)# ap dot11 24ghz cleanair device inv  Device(config)# ap dot11 24ghz cleanair device jammer  Device(config)# ap dot11 24ghz cleanair device mw-oven  Device(config)# ap dot11 24ghz cleanair device nonstd  Device(config)# ap dot11 24ghz cleanair device report  Device(config)# ap dot11 24ghz cleanair device superag  Device(config)# ap dot11 24ghz cleanair device tdd-tx  Device(config)# ap dot11 24ghz cleanair device video  Device(config)# ap dot11 24ghz cleanair device wimax-fixed  Device(config)# ap dot11 24ghz cleanair device wimax-mobile  Device(config)# ap dot11 24ghz cleanair device xbox  Device(config)# ap dot11 24ghz cleanair device zigbee</pre>	<p>The following is a list of the keyword descriptions:</p> <ul style="list-style-type: none"> <li>• <b>bt-discovery</b>—Bluetooth discovery</li> <li>• <b>bt-link</b>—Bluetooth link</li> <li>• <b>canopy</b>—Canopy device</li> <li>• <b>cont-tx</b>—Continuous transmitter</li> <li>• <b>dect-like</b>—Digital Enhanced Cordless Communication-like phone</li> <li>• <b>fh</b>—802.11-frequency hopping device</li> <li>• <b>inv</b>—Device using spectrally inverted Wi-Fi signals</li> <li>• <b>jammer</b>—Jammer</li> <li>• <b>mw-oven</b>—Microwave oven</li> <li>• <b>nonstd</b>—Device using nonstandard Wi-Fi channels</li> <li>• <b>report</b>—Interference device reporting</li> <li>• <b>superag</b>—802.11 SuperAG device</li> <li>• <b>tdd-tx</b>—TDD transmitter</li> <li>• <b>video</b>—Video camera</li> <li>• <b>wimax-fixed</b>—WiMax Fixed</li> <li>• <b>wimax-mobile</b>—WiMax Mobile</li> <li>• <b>microsoft xbox</b>—Microsoft Xbox device</li> <li>• <b>zigbee</b>—802.15.4 device</li> </ul>

	Command or Action	Purpose
	Device(config)# <b>ap dot11 24ghz cleanair</b> device alarm	
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Enabling CleanAir for the 5-GHz Band (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Radio Configurations > CleanAir**
  - Step 2** On the **CleanAir** page, click the **me5 GHz Band > General** tab.
  - Step 3** Check the **Enable CleanAir** checkbox.
  - Step 4** Click **Apply**.
- 

## Enabling CleanAir for the 5-GHz Band (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>ap dot11 5ghz cleanair</b>  <b>Example:</b> Device(config)# <b>ap dot11 5ghz cleanair</b>  Device(config)# <b>no ap dot11 5ghz cleanair</b>	Enables the CleanAir feature on a 802.11a network. Run the <b>no</b> form of this command to disable CleanAir on the 802.11a network.
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring Interference Reporting for a 5-GHz Device (GUI)

### Procedure

- Step 1** Choose **Configuration** > **Radio Configurations** > **CleanAir**.
- Step 2** Click the **5 GHz Band** tab.
- Step 3** Choose the interference types and add them to the **Interference Types to detect** section.

The following interference types are available:

- Canopy
- Continuous Transmitter
- DECT-like Phone—Digital Enhanced Cordless Technology phone
- 802.11 FH—802.11 frequency hopping device
- WiFi Inverted—Device using spectrally inverted Wi-Fi signals
- Jammer
- WiFi Invalid Channel—Device using nonstandard Wi-Fi channels
- SuperAG—802.11 SuperAG device
- TDD Transmitter
- WiMax Mobile
- WiMax Fixed
- Video Camera

- Step 4** Click **Apply**.

## Configuring Interference Reporting for a 5-GHz Device (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<code>ap dot11 5ghz cleanair device {canopy   cont-tx   dect-like   inv   jammer   nonstd   report   superag   tdd-tx   video   wimax-fixed   wimax-mobile}</code>	Configures a 5-GHz interference device to report to the device. Run the <b>no</b> form of this command to disable interference device reporting.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device(config)#ap dot11 5ghz cleanair device canopy  Device(config)#ap dot11 5ghz cleanair device cont-tx  Device(config)#ap dot11 5ghz cleanair device dect-like  Device(config)#ap dot11 5ghz cleanair device inv  Device(config)#ap dot11 5ghz cleanair device jammer  Device(config)#ap dot11 5ghz cleanair device nonstd  Device(config)#ap dot11 5ghz cleanair device report  Device(config)#ap dot11 5ghz cleanair device superag  Device(config)#ap dot11 5ghz cleanair device tdd-tx  Device(config)#ap dot11 5ghz cleanair device video  Device(config)#ap dot11 5ghz cleanair device wimax-fixed  Device(config)#ap dot11 5ghz cleanair device wimax-mobile  Device(config)#ap dot11 5ghz cleanair device si_fhss  Device(config)#ap dot11 5ghz cleanair device alarm</pre>	<p>The following is a list of the keyword descriptions:</p> <ul style="list-style-type: none"> <li>• <b>canopy</b>—Canopy device</li> <li>• <b>cont-tx</b>—Continuous transmitter</li> <li>• <b>dect-like</b>—Digital Enhanced Cordless Communication-like phone</li> <li>• <b>fh</b>—802.11-frequency hopping device</li> <li>• <b>inv</b>—Device using spectrally-inverted Wi-Fi signals</li> <li>• <b>jammer</b>—Jammer</li> <li>• <b>nonstd</b>—Device using nonstandard Wi-Fi channels</li> <li>• <b>superag</b>—802.11 SuperAG device</li> <li>• <b>tdd-tx</b>—TDD transmitter</li> <li>• <b>video</b>—Video camera</li> <li>• <b>wimax-fixed</b>—WiMax fixed</li> <li>• <b>wimax-mobile</b>—WiMax mobile</li> </ul>
<b>Step 3</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config)# end</pre>	<p>Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.</p>



## Configuring Event Driven RRM for a CleanAir Event (GUI)

### Procedure

- Step 1** Choose **Configuration > Radio Configurations > RRM**. The **Radio Resource Management** page is displayed.
- Step 2** Click the **DCA** tab.
- Step 3** In the **Event Driven RRM** section, check the **EDRRM** check box to run RRM when CleanAir-enabled AP detects a significant level of interference.
- Step 4** Configure the **Sensitivity Threshold** level at which RRM has to be invoked from the following options:
- **Low**: Represents a decreased sensitivity to changes in the environment and its value is set at 35.
  - **Medium**: Represents medium sensitivity to changes in the environment at its value is set at 50.
  - **High**: Represents increased sensitivity to changes in the environment at its value is set at 60.
  - **Custom**: If you choose this option, you must specify a custom value in the **Custom Threshold** box.
- Step 5** To configure rogue duty cycle, check the **Rogue Contribution** check box and then specify the **Rogue Duty-Cycle** in terms of percentage. The default value of rogue duty cycle is 80 percent.
- Note** Rogue Contribution is a new component included in ED-RRM functionality. Rogue Contribution allows ED-RRM to trigger based on identified Rogue Channel Utilization, which is completely separate from CleanAir metrics. Rogue Duty Cycle comes from normal off channel RRM metrics, and invokes a channel change based on neighboring rogue interference. Because this comes from RRM metrics and not CleanAir, the timing - assuming normal 180 second off channel intervals - would be within 3 minutes or 180 seconds worst case. It is configured separately from CleanAir ED-RRM and is disabled by default. This allows the AP to become reactive to Wi-Fi interference that is not coming from own network and is measured at each individual AP.
- Step 6** Save the configuration.

## Configuring EDRRM for a CleanAir Event (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ap dot11 {24ghz   5ghz} rrm channel cleanair-event</b> <b>Example:</b> Device(config)# <code>ap dot11 24ghz rrm channel cleanair-event</code>	Enables EDRRM CleanAir event. Run the <b>no</b> form of this command to disable EDRRM.

	Command or Action	Purpose
	<code>Device(config)#no ap dot11 24ghz rrm channel cleanair-event</code>	
<b>Step 3</b>	<p><code>ap dot11 {24ghz   5ghz} rrm channel cleanair-event [sensitivity {high   low   medium}]</code></p> <p><b>Example:</b></p> <pre>Device(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high</pre>	<p>Configures the EDRRM sensitivity of the CleanAir event.</p> <p>The following is a list of the keyword descriptions:</p> <ul style="list-style-type: none"> <li>• <b>High</b>—Specifies the most sensitivity to non-Wi-Fi interference as indicated by the AQ value.</li> <li>• <b>Low</b>—Specifies the least sensitivity to non-Wi-Fi interference as indicated by the AQ value.</li> <li>• <b>Medium</b>—Specifies medium sensitivity to non-Wi-Fi interference as indicated by the AQ value.</li> </ul>
<b>Step 4</b>	<p><code>end</code></p> <p><b>Example:</b></p> <pre>Device(config)# end</pre>	<p>Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.</p>

## Verifying CleanAir Parameters

You can verify CleanAir parameters using the following commands:

*Table 25: Commands for verifying CleanAir*

Command Name	Description
<code>show ap dot11 24ghz cleanair device type all</code>	Displays all the CleanAir interferers for the 2.4-GHz band.
<code>show ap dot11 24ghz cleanair device type bt-discovery</code>	Displays CleanAir interferers of type BT Discovery for the 2.4-GHz band.
<code>show ap dot11 24ghz cleanair device type bt-link</code>	Displays CleanAir interferers of type BT Link for the 2.4-GHz band.
<code>show ap dot11 24ghz cleanair device type canopy</code>	Displays CleanAir interferers of type Canopy for the 2.4-GHz band.
<code>show ap dot11 24ghz cleanair device type cont-tx</code>	Displays CleanAir interferers of type Continuous transmitter for the 2.4-GHz band.
<code>show ap dot11 24ghz cleanair device type dect-like</code>	Displays CleanAir interferers of type DECT Like for the 2.4-GHz band.

Command Name	Description
show ap dot11 24ghz cleanair device type fh	Displays CleanAir interferers of type 802.11FH for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type inv	Displays CleanAir interferers of type Wi-Fi Inverted for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type jammer	Displays CleanAir interferers of type Jammer for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type mw-oven	Displays CleanAir interferers of type MW Oven for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type nonstd	Displays CleanAir interferers of type Wi-Fi inverted channel for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type superag	Displays CleanAir interferers of type SuperAG for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type tdd-tx	Displays CleanAir interferers of type TDD Transmit for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type video	Displays CleanAir interferers of type Video Camera for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type wimax-fixed	Displays CleanAir interferers of type WiMax Fixed for the 2.4-GHz band.

## Monitoring Interference Devices

When a CleanAir-enabled access point detects interference devices, detections of the same device from multiple sensors are merged together to create clusters. Each cluster is given a unique ID. Some devices conserve power by limiting the transmit time until actually needed, which results in the spectrum sensor to stop detecting the device temporarily. This device is then correctly marked as down. Such a device is correctly removed from the spectrum database. In cases when all the interferer detections for a specific device are reported, the cluster ID is kept alive for an extended period of time to prevent possible device-detection bouncing. If the same device is detected again, it is merged with the original cluster ID and the device-detection history is preserved.

For example, some bluetooth headsets operate on battery power. These devices employ methods to reduce power consumption, such as turning off the transmitter when not actually needed. Such devices can appear to come and go from the classification. To manage these devices, CleanAir keeps the cluster IDs for longer and they are remerged into a single record upon detection. This process smoothens the user records and accurately represents the device history.

## Configuration Examples for CleanAir

This example shows how to enable CleanAir on the 2.4-GHz band and an access point operating in the channel:

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

```
Device(config)#exit
Device#ap name TAP1 dot11 24ghz cleanair
Device#end
```

This example shows how to enable an EDRRM CleanAir event in the 2.4-GHz band and configure high sensitivity to non-Wi-Fi interference:

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

## CleanAir FAQs

- Q.** Multiple access points detect the same interference device. However, the device shows them as separate clusters or different suspected devices clustered together. Why does this happen?
- A.** Access points must be RF neighbors for the device to consider merging the devices that are detected by these access points. An access point takes time to establish neighbor relationships. A few minutes after the device reboots or after there is a change in the RF group, and similar events, clustering will not be very accurate.
- Q.** How do I view neighbor access points?
- A.** To view neighbor access points, use the **show ap ap\_name auto-rf dot11 {24ghz | 5ghz}** command.

This example shows how to display the neighbor access points:

```
Device#show ap name AS-5508-5-AP3 auto-rf dot11 24ghz
```

```
<snippet>
Nearby APs
  AP 0C85.259E.C350 slot 0      : -12 dBm on 1 (10.10.0.5)
  AP 0C85.25AB.CCA0 slot 0      : -24 dBm on 6 (10.10.0.5)
  AP 0C85.25C7.B7A0 slot 0      : -26 dBm on 11 (10.10.0.5)
  AP 0C85.25DE.2C10 slot 0      : -24 dBm on 6 (10.10.0.5)
  AP 0C85.25DE.C8E0 slot 0      : -14 dBm on 11 (10.10.0.5)
  AP 0C85.25DF.3280 slot 0      : -31 dBm on 6 (10.10.0.5)
  AP 0CD9.96BA.5600 slot 0      : -44 dBm on 6 (10.0.0.2)
  AP 24B6.5734.C570 slot 0      : -48 dBm on 11 (10.0.0.2)
<snippet>
```

- Q.** What are the AP debug commands available for CleanAir?
- A.** The AP debug commands for CleanAir are:

- 
-



## CHAPTER 62

# Spectrum Intelligence

---

- [Spectrum Intelligence, on page 593](#)
- [Configuring Spectrum Intelligence, on page 594](#)
- [Verifying Spectrum Intelligence Information, on page 594](#)

## Spectrum Intelligence

The Spectrum Intelligence feature scans for non-Wi-Fi radio interference on 2.4-GHz and 5-GHz bands. Spectrum intelligence provides basic functions to detect interferences of three types, namely microwave, continuous wave (like video bridge and baby monitor), wi-fi and frequency hopping (bluetooth and frequency-hopping spread spectrum (FHSS) cordless phone).

The following Cisco access points (APs) support Spectrum Intelligence feature:

- Cisco Catalyst 9115 Series Wi-Fi 6 APs
- Cisco Aironet 1852E/I APs
- Cisco Aironet 1832I APs
- Cisco Aironet 1815W/T/I/M APs
- Cisco Aironet 1810W/T APs
- Cisco Aironet 1800I/S APs
- Cisco Aironet 1542D/I APs



---

**Note** You must enable Spectrum Intelligence feature on the Cisco Aironet 1832 and 1852 series APs to get radio details, such as noise, air-quality, interference, and radio utilization on the Cisco DNA Center Assurance AP health.

---

### Restrictions

- SI APs only report a single interference type in Local mode.

- SI does not support high availability for air quality or interference reports. High Availability is not supported because interference report/device reported will not be copied to standby after switchover. We expect AP to send it again, if at all interferer is still there.
- Spectrum Intelligence detects only three types of devices:
  - Microwave
  - Continuous wave—(video recorder, baby monitor)
  - SI-FHSS—(Bluetooth, Frequency hopping Digital European Cordless Telecommunications (DECT) phones)

## Configuring Spectrum Intelligence

Follow the procedure given below to configure spectrum intelligence:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ap dot11 {24ghz   5ghz} SI</b> <b>Example:</b> Device(config)# ap dot11 24ghz SI	Configures the 2.4-GHz or 5-GHz Spectrum Intelligence feature on the 802.11a or 802.11b network.  Add <b>no</b> form of the command to disable SI on the 802.11a or 802.11b network.

## Verifying Spectrum Intelligence Information

Use the following commands to verify spectrum intelligence information:

To display the SI information for a 2.4-GHz or 5-GHz band, use the following command:

```
Device# show ap dot11 24ghz SI config

SI Solution..... : Enabled
Interference Device Settings:
  SI_FHSS..... : Enabled
Interference Device Types Triggering Alarms:
  SI_FHSS..... : Disabled
```

To display SI interferers of type Continuous transmitter for a 2.4-GHz band, use the following command:

```
Device# show ap dot11 24ghz SI device type cont_tx

DC      = Duty Cycle (%)
ISI     = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI    = Received Signal Strength Index (dBm)
```

DevID = Device ID  
 AP type = CA, clean air, SI spectrum intelligence

No	ClusterID	DevID	Type	AP Type	AP Name	ISI	RSSI	DC	Channel
	xx:xx:xx:xx	0014	BT	CA	myAP1	--	-69 00	133	
	xx:xx:xx:xx	0014	BT	SI	myAP1	--	-69 00	133	

To display 802.11a interference devices information for the given AP for 5-GHz, use the following command:

Device# **show ap dot11 5ghz SI device type ap**

DC = Duty Cycle (%)  
 ISI = Interference Severity Index (1-Low Interference, 100-High Interference)  
 RSSI = Received Signal Strength Index (dBm)  
 DevID = Device ID  
 AP type = CA, clean air, SI spectrum intelligence

No	ClusterID/BSSID	DevID	Type	AP Type	AP Name	ISI	RSSI	DC	Channel
-----									
-----									

To display all Cisco CleanAir interferers for a 2.4-GHz band, use the following command:

Device# **show ap dot11 24ghz cleanair device type all**







## PART **X**

### **WLAN**

- [WLANs, on page 599](#)
- [Network Access Server Identifier, on page 613](#)
- [DHCP for WLANs, on page 619](#)
- [WLAN Security, on page 621](#)
- [Peer-to-Peer Client Support, on page 625](#)
- [802.11r BSS Fast Transition, on page 627](#)
- [Assisted Roaming, on page 637](#)
- [802.11v, on page 641](#)
- [802.11w, on page 645](#)
- [Deny Wireless Client Session Establishment Using Calendar Profiles, on page 653](#)
- [Introduction to EoGRE, on page 663](#)





## CHAPTER 63

# WLANs

---

- [Information About WLANs, on page 599](#)
- [Prerequisites for WLANs, on page 602](#)
- [Restrictions for WLANs, on page 602](#)
- [How to Configure WLANs, on page 603](#)
- [Verifying WLAN Properties \(CLI\), on page 611](#)

## Information About WLANs

This feature enables you to control WLANs for lightweight access points. Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. All access points can advertise up to 16 WLANs. However, you can create up to 4096 WLANs and then selectively advertise these WLANs (using profiles and tags) to different APs for better manageability.

You can configure WLANs with different SSIDs or with the same SSID. An SSID identifies the specific wireless network that you want the controller to access.

## Band Selection

Band select enables client radios that are capable of dual-band (2.4 and 5-GHz) operations to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of 3 nonoverlapping channels. To prevent these sources of interference and improve overall network performance, configure band selection on the device.

## Off-Channel Scanning Deferral

A lightweight access point, in normal operational conditions, periodically goes off-channel and scans another channel. This is in order to perform RRM operations such as the following:

- Transmitting and receiving Neighbor Discovery Protocol (NDP) packets with other APs.
- Detecting rogue APs and clients.
- Measuring noise and interference.

During the off-channel period, which normally is about 70 milliseconds, the AP is unable to transmit or receive data on its serving channel. Therefore, there is a slight impact on its performance and some client transmissions might be dropped.

While the AP is sending and receiving important data, it is possible to configure off-channel scanning deferral so that the AP does not go off-channel and its normal operation is not impacted. You can configure off-channel scanning deferral on a per-WLAN basis, per WMM UP class basis, with a specified time threshold in milliseconds. If the AP sends or receives, on a particular WLAN, a data frame marked with the given UP class within the specified threshold, the AP defers its next RRM off-channel scan. For example, by default, off-channel scanning deferral is enabled for UP classes 4, 5, and 6, with a time threshold of 100 milliseconds. Therefore, when RRM is about to perform an off-channel scan, a data frame marked with UP 4, 5, or 6 is received within the last 100 milliseconds, RRM defers going off-channel. The AP radio does not go off-channel when a voice call sending and receiving audio samples are marked as UP class 6 for every active 20 milliseconds.

Off-channel scanning deferral does come with a tradeoff. Off-channel scanning can impact throughput by 2 percent or more, depending on the configuration, traffic patterns, and so on. Throughput can be slightly improved if you enable off-channel scanning deferral for all traffic classes and increase the time threshold. However, by not going off-channel, RRM can fail to identify AP neighbors and rogues, resulting in negative impact to security, DCA, TPC, and 802.11k messages.

## DTIM Period

In the 802.11 networks, lightweight access points broadcast a beacon at regular intervals, which coincides with the Delivery Traffic Indication Map (DTIM). After the access point broadcasts the beacon, it transmits any buffered broadcast and multicast frames based on the value set for the DTIM period. This feature allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

Typically, the DTIM value is set to 1 (to transmit broadcast and multicast frames after every beacon) or 2 (to transmit broadcast and multicast frames after every other beacon). For instance, if the beacon period of the 802.11 network is 100 ms and the DTIM value is set to 1, the access point transmits buffered broadcast and multicast frames for 10 times every second. If the beacon period is 100 ms and the DTIM value is set to 2, the access point transmits buffered broadcast and multicast frames for 5 times every second. Either of these settings are suitable for applications, including Voice Over IP (VoIP), that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (to transmit broadcast and multicast frames after every 255th beacon). The only recommended DTIM values are 1 and 2; higher DTIM values will likely cause communications problems.



---

**Note** A beacon period, which is specified in milliseconds on the device, is converted internally by the software to 802.11 Time Units (TUs), where 1 TU = 1.024 milliseconds. Depending on the AP model, the actual beacon period may vary slightly; for example, a beacon period of 100 ms may in practice equate to 104.448 ms.

---

## Session Timeouts

You can configure a WLAN with a session timeout. The session timeout is the maximum time for a client session to remain active before requiring reauthorization.

If a WLAN is configured with Layer 2 security, for example WPA2-PSK, and a Layer 3 authentication is also configured, the WLAN session timeout value is overridden with the 802.1X reauthentication timeout value. If APF reauthentication timeout value is greater than 65535, the WLAN session timeout is by default set to 65535; else, the configured 802.1X reauthentication timeout value is applied as the WLAN session timeout.

This section contains the following subsections:

## Cisco Client Extensions

The Cisco Client Extensions (CCX) software is licensed to manufacturers and vendors of third-party client devices. The CCX code resident on these clients enables them to communicate wirelessly with Cisco access points and to support Cisco features that other client devices do not, including those features that are related to increased security, enhanced performance, fast roaming, and power management.

- The software supports CCX versions 1 through 5, which enables devices and their access points to communicate wirelessly with third-party client devices that support CCX. CCX support is enabled automatically for every WLAN on the device and cannot be disabled. However, you can configure Aironet information elements (IEs).
- If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the device sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the device and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

## Peer-to-Peer Blocking

Peer-to-peer blocking is applied to individual WLANs, and each client inherits the peer-to-peer blocking setting of the WLAN to which it is associated. Peer-to-Peer enables you to have more control over how traffic is directed. For example, you can choose to have traffic bridged locally within the device, dropped by the device, or forwarded to the upstream VLAN.

Peer-to-peer blocking is supported for clients that are associated with local and central switching WLANs.



---

**Note** Peer-to-peer blocking feature is VLAN-based. WLANs using the same VLAN has an impact, if Peer-to-peer blocking feature is enabled.

---

This section contains the following subsections:

## Diagnostic Channel

You can choose a diagnostic channel to troubleshoot why the client is having communication problems with a WLAN. You can test the client and access points to identify the difficulties that the client is experiencing and allow corrective measures to be taken to make the client operational on the network. You can use the device GUI or CLI to enable the diagnostic channel, and you can use the device **diag-channel** CLI to run the diagnostic tests.




---

**Note** We recommend that you enable the diagnostic channel feature only for nonanchored SSIDs that use the management interface. CCX Diagnostic feature has been tested only with clients having Cisco ADU card

---

## Prerequisites for WLANs

- You can associate up to 16 WLANs with each policy tag.
- We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that devices properly route VLAN traffic.

## Restrictions for WLANs

- Do not configure PSK and CCKM in a WLAN, as this configuration is not supported and impacts client join flow.
- Ensure that TKIP or AES ciphers are enabled with WPA1 configuration, else ISSU may break during upgrade process.
- When you change the WLAN profile name, then FlexConnect APs (using AP-specific VLAN mapping) will become WLAN-specific. If FlexConnect Groups are configured, the VLAN mapping will become Group-specific.
- Do not enable IEEE 802.1X Fast Transition on Flex Local Authentication enabled WLAN, as client association is not supported with Fast Transition 802.1X key management.
- Peer-to-peer blocking does not apply to multicast traffic.
- In FlexConnect, peer-to-peer blocking configuration cannot be applied only to a particular FlexConnect AP or a subset of APs. It is applied to all the FlexConnect APs that broadcast the SSID.
- The WLAN name and SSID can have up to 32 characters.
- WLAN and SSID names support only the following ASCII characters:
  - Numerals: 48 through 57 hex (0 to 9)
  - Alphabets (uppercase): 65 through 90 hex (A to Z)
  - Alphabets (lowercase): 97 through 122 hex (a to z)
  - ASCII space: 20 hex
  - Printable special characters: 21 through 2F, 3A through 40, and 5B through 60 hex, that is: ! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } ~
- WLAN name cannot be a keyword; for example, if you try to create a WLAN with the name as 's' by entering the **wlan s** command, it results in shutting down all WLANs because 's' is used as a keyword for shutdown.

- You cannot map a WLAN to VLAN 0. Similarly, you cannot map a WLAN to VLANs 1002 to 1006.
- Dual stack clients with a static-IPv4 address is not supported.
- In a dual-stack with IPv4 and IPv6 configured in the Cisco 9800 controller, if an AP tries to join controller with IPv6 tunnel before its IPv4 tunnel gets cleaned, you would see a traceback and AP join will fail.
- When creating a WLAN with the same SSID, you must create a unique profile name for each WLAN.
- When multiple WLANs with the same SSID get assigned to the same AP radio, you must have a unique Layer 2 security policy so that clients can safely select between them.
- If the newly configured SSID is on a 5-GHz DFS channel, beaconing does not start immediately.
- RADIUS server overwrite is not configured on a per WLAN basis, but rather on a per AAA server group basis.
- Downloadable ACL (DAACL) is not supported in the FlexConnect mode or the local mode.

**Caution**

Some clients might not be able to connect to WLANs properly if they detect the same SSID with multiple security policies. Use this WLAN feature with care.

## How to Configure WLANs

### Creating WLANs (GUI)

#### Procedure

- 
- Step 1** In the **Configuration > Tags & Profiles > WLANs** page, click **Add**.  
The **Add WLAN** window is displayed.
- Step 2** Under the **General** tab and **Profile Name** field, enter the name of the WLAN. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.
- Step 3** Click **Save & Apply to Device**.
- 

### Creating WLANs (CLI)

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	<p><b>wlan</b> <i>profile-name</i> <i>wlan-id</i> [<i>ssid</i>]</p> <p><b>Example:</b></p> <pre>Device(config)# wlan mywlan 34 mywlan-ssid</pre>	<p>Specifies the WLAN name and ID:</p> <ul style="list-style-type: none"> <li>• For the <i>profile-name</i>, enter the profile name. The range is from 1 to 32 alphanumeric characters.</li> <li>• For the <i>wlan-id</i>, enter the WLAN ID. The range is from 1 to 512.</li> <li>• For the <i>ssid</i>, enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID.</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• You can create SSID using GUI or CLI. However, we recommend that you use CLI to create SSID.</li> <li>• By default, the WLAN is disabled.</li> </ul>
<b>Step 3</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config)# end</pre>	<p>Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.</p>

## Deleting WLANs (GUI)

### Procedure

- 
- Step 1** In the **Configuration > Tags & Profiles > WLANs** page, check the checkbox adjacent to the WLAN you want to delete.
- To delete multiple WLANs, select multiple WLANs checkboxes.
- Step 2** Click **Delete**.
- Step 3** Click **Yes** on the confirmation window to delete the WLAN.
-



## Deleting WLANs

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>no wlan wlan-name wlan-id ssid</b> <b>Example:</b> Device(config)# <b>no wlan test2</b>	Deletes the WLAN. The arguments are as follows: <ul style="list-style-type: none"> <li>• The <i>wlan-name</i> is the WLAN profile name.</li> <li>• The <i>wlan-id</i> is the WLAN ID.</li> <li>• The <i>ssid</i> is the WLAN SSID name configured for the WLAN.</li> </ul>
<b>Step 3</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Searching WLANs (CLI)

To verify the list of all WLANs configured on the controller, use the following show command:

```
Device# show wlan summary
Number of WLANs: 4
```

WLAN Profile Name	SSID	VLAN	Status
1 test1	test1-ssid	137	UP
3 test2	test2-ssid	136	UP
2 test3	test3-ssid	1	UP
45 test4	test4-ssid	1	DOWN

To use wild cards and search for WLANs, use the following show command:

```
Device# show wlan summary | include test-wlan-ssid
1 test-wlan test-wlan-ssid 137 UP
```

## Enabling WLANs (GUI)

### Procedure

- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** On the **WLANs** page, click the WLAN name.
- Step 3** In the **Edit WLAN** window, toggle the **Status** button to **ENABLED**.

**Step 4** Click **Update & Apply to Device**.

## Enabling WLANs (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wlan profile-name</b> <b>Example:</b> Device(config)# <code>wlan test4</code>	Enters WLAN configuration submode. The <i>profile-name</i> is the profile name of the configured WLAN.
<b>Step 3</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wlan)# <code>no shutdown</code>	Enables the WLAN.
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config-wlan)# <code>end</code>	Returns to privileged EXEC mode.

## Disabling WLANs (GUI)

### Procedure

- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** In the **WLANs** window, click the WLAN name.
- Step 3** In the **Edit WLAN** window, set the **Status** toggle button as **DISABLED**.
- Step 4** Click **Update & Apply to Device**.

## Disabling WLANs (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>	Enters global configuration mode.

	Command or Action	Purpose
	Device# <code>configure terminal</code>	
<b>Step 2</b>	<b>wlan</b> <i>profile-name</i> <b>Example:</b> Device(config)# <code>wlan test4</code>	Enters WLAN configuration submode. The <i>profile-name</i> is the profile name of the configured WLAN.
<b>Step 3</b>	<b>shutdown</b> <b>Example:</b> Device(config-wlan)# <code>shutdown</code>	Disables the WLAN.
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config-wlan)# <code>end</code>	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show wlan summary</b> <b>Example:</b> Device# <code>show wlan summary</code>	Displays the list of all WLANs configured on the device. You can search for the WLAN in the output.

## Configuring General WLAN Properties (CLI)

You can configure the following properties:

- Media stream
- Broadcast SSID
- Radio

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wlan</b> <i>profile-name</i> <b>Example:</b> Device(config)# <code>wlan test4</code>	Enters WLAN configuration submode. The <i>profile-name</i> is the profile name of the configured WLAN.
<b>Step 3</b>	<b>shutdown</b> <b>Example:</b> Device(config-wlan)# <code>shutdown</code>	Disables the WLAN.
<b>Step 4</b>	<b>broadcast-ssid</b> <b>Example:</b>	Broadcasts the SSID for this WLAN.

	Command or Action	Purpose
	Device(config-wlan)# <b>broadcast-ssid</b>	
<b>Step 5</b>	<b>radio {dot11a   dot11ag   dot11bg   dot11g}</b> <b>Example:</b> Device(config-wlan)# <b>radio dot11g</b>	Enables radios on the WLAN. The keywords are as follows: <ul style="list-style-type: none"> <li>• <b>dot11a</b>—Configures the WLAN on only 802.11a radio bands.</li> <li>• <b>dot11g</b>—Configures the WLAN on 802.11ag radio bands.</li> <li>• <b>dot11bg</b>—Configures the WLAN on only 802.11b/g radio bands (only 802.11b if 802.11g is disabled).</li> <li>• <b>dot11ag</b>— Configures the wireless LAN on 802.11g radio bands only.</li> </ul>
<b>Step 6</b>	<b>media-stream multicast-direct</b> <b>Example:</b> Device(config-wlan)# <b>media-stream multicast-direct</b>	Enables multicast VLANs on this WLAN.
<b>Step 7</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wlan)# <b>no shutdown</b>	Enables the WLAN.
<b>Step 8</b>	<b>end</b> <b>Example:</b> Device(config-wlan)# <b>end</b>	Returns to privileged EXEC mode.

## Configuring Advanced WLAN Properties (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wlan <i>profile-name</i></b> <b>Example:</b> Device(config)# <b>wlan test4</b>	Enters WLAN configuration submenu. The <i>profile-name</i> is the profile name of the configured WLAN.
<b>Step 3</b>	<b>chd</b> <b>Example:</b>	Enables coverage hole detection for this WLAN.

	Command or Action	Purpose
	Device(config-wlan) # <b>chd</b>	
<b>Step 4</b>	<b>ccx aironet-iesupport</b> <b>Example:</b> Device(config-wlan) # <b>ccx</b> <b>aironet-iesupport</b>	Enables support for Aironet IEs for this WLAN.
<b>Step 5</b>	<b>client association limit</b> { <i>clients-per-wlan</i>   <b>ap</b> <i>clients-per-ap-per-wlan</i>   <b>radio</b> <i>clients-per-ap-radio--per-wlan</i> } <b>Example:</b> Device(config-wlan) # <b>client association limit ap 400</b>	Sets the maximum number of clients, clients per AP, or clients per AP radio that can be configured on a WLAN.
<b>Step 6</b>	<b>ip access-group web</b> <i>acl-name</i> <b>Example:</b> Device(config-wlan) # <b>ip access-group web test-acl-name</b>	Configures the IPv4 WLAN web ACL. The variable <i>acl-name</i> specifies the user-defined IPv4 ACL name.
<b>Step 7</b>	<b>peer-blocking</b> [ <b>drop</b>   <b>forward-upstream</b> ] <b>Example:</b> Device(config-wlan) # <b>peer-blocking drop</b>	Configures peer to peer blocking parameters. The keywords are as follows: <ul style="list-style-type: none"> <li>• <b>drop</b>—Enables peer-to-peer blocking on the drop action.</li> <li>• <b>forward-upstream</b>—No action is taken and forwards packets to the upstream.</li> </ul>
<b>Step 8</b>	<b>channel-scan</b> { <b>defer-priority</b> { <b>0-7</b> }   <b>defer-time</b> { <b>0 - 6000</b> } } <b>Example:</b> Device(config-wlan) # <b>channel-scan defer-priority 6</b>	Sets the channel scan defer priority and defer time. The arguments are as follows: <ul style="list-style-type: none"> <li>• <b>defer-priority</b>—Specifies the priority markings for packets that can defer off-channel scanning. The range is from 0 to 7. The default is 3.</li> <li>• <b>defer-time</b>—Deferral time in milliseconds. The range is from 0 to 6000. The default is 100.</li> </ul>
<b>Step 9</b>	<b>end</b> <b>Example:</b> Device(config-wlan) # <b>end</b>	Returns to privileged EXEC mode.

## Configuring Advanced WLAN Properties (GUI)

### Before you begin

Ensure that you have configured an AP Join Profile prior to configuring the primary and backup controllers.

### Procedure

---

- Step 1** Choose **Configuration > Wireless > WLANs > Wireless Networks**.
- Step 2** In the **Wireless Networks** window, click **Add**.
- Step 3** Under the **Advanced** tab, check the **Coverage Hole Detection** check box.
- Step 4** Check the **Aironet IE** check box to enable Aironet IE on the WLAN.
- Step 5** Check the **Diagnostic Channel** check box to enable diagnostic channel on the WLAN.
- Step 6** From the **P2P Blocking Action** drop-down list, choose the required value.
- Step 7** Set the **Multicast Buffer** toggle button as enabled or disabled.
- Step 8** Check the **Media Stream Multicast-Direct** check box to enable the feature.
- Step 9** In the **Max Client Connections** section, specify the maximum number of client connections for the following:
- In the **Per WLAN** field, enter a value. The valid range is between 0 and 10000.
  - In the **Per AP Per WLAN** field, enter a value. The valid range is between 0 and 400.
  - In the **Per AP Radio Per WLAN** field, enter a value. The valid range is between 0 and 200.
- Step 10** In the **11v BSS Transition Support** section, perform the following configuration tasks:
- a) Check the **BSS Transition** check box to enable 802.11v BSS Transition support.
  - b) In the **Disassociation Imminent** field, enter a value. The valid range is between 0 and 3000.
  - c) In the **Optimized Roaming Disassociation Timer** field, enter a value. The valid range is between 0 and 40.
  - d) Select the check box to enable the following:
    - BSS Max Idle Service
    - BSS Max Idle Protected
    - Disassociation Imminent Service
    - Directed Multicast Service
    - Universal Admin
    - Load Balance
    - Band Select
    - IP Source Guard
- Step 11** From the **WMM Policy** drop-down list, choose the policy as Allowed, Disabled, or Required. By default, the WMM policy is Allowed.

- Step 12** In the **Off Channel Scanning Defer** section, choose the appropriate **Defer Priority** values and then specify the required Scan Defer Time value in milliseconds.
- Step 13** In the **Assisted Roaming (11k)** section, choose the appropriate status for the following:
- Prediction Optimization
  - Neighbor List
  - Dual-Band Neighbor List
- Step 14** In the **DTIM Period (in beacon intervals)** section, specify a value for 802.11a/n and 802.11b/g/n radios. The valid range is from 1 to 255.
- Step 15** Click **Save & Apply to Device**.
- 

## Verifying WLAN Properties (CLI)

To verify the WLAN properties based on the WLAN ID, use the following `show` command:

```
Device# show wlan id wlan-id
```

To verify the WLAN properties based on the WLAN name, use the following `show` command:

```
Device# show wlan name wlan-name
```

To verify the WLAN properties of all the configured WLANs, use the following `show` command:

```
Device# show wlan all
```

To verify the summary of all WLANs, use the following `show` command:

```
Device# show wlan summary
```

To verify the running configuration of a WLAN based on the WLAN name, use the following `show` command:

```
Device# show running-config wlan wlan-name
```

To verify the running configuration of all WLANs, use the following `show` command:

```
Device# show running-config wlan
```







## CHAPTER 64

# Network Access Server Identifier

---

- [Information About Network Access Server Identifier, on page 613](#)
- [Creating a NAS ID Policy\(GUI\), on page 614](#)
- [Creating a NAS ID Policy, on page 614](#)
- [Attaching a Policy to a Tag \(GUI\), on page 615](#)
- [Attaching a Policy to a Tag \(CLI\), on page 615](#)
- [Verifying the NAS ID Configuration, on page 616](#)

## Information About Network Access Server Identifier

Network access server identifier (NAS-ID) is used to notify the source of a RADIUS access request, which enables the RADIUS server to choose a policy for that request. You can configure one on each WLAN profile, or VLAN interface. The NAS-ID is sent to the RADIUS server by the embedded wireless controller through an authentication request to classify users to different groups. This enables the RADIUS server to send a customized authentication response.



---

**Note** The acct-session-id is sent with the RADIUS access request only when accounting is enabled on the policy profile.

---

If you configure a NAS-ID for a WLAN profile, it overrides the NAS-ID that is configured for the VLAN interface.

The following options can be configured for a NAS ID:

- sys-name (System Name)
- sys-ip (System IP Address)
- sys-mac (System MAC Address)
- ap-ip (AP's IP address)
- ap-name (AP's Name)
- ap-mac (AP's MAC Address)
- ap-eth-mac (AP's Ethernet MAC Address)

- ap-policy-tag (AP's policy tag name)
- ap-site-tag (AP's site tag name)
- ssid (SSID Name)
- ap-location (AP's Location)

## Creating a NAS ID Policy(GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Security > Wireless AAA Policy**.
- Step 2** On the **Wireless AAA Policy** page, click the name of the **Policy** or click **Add** to create a new one.
- Step 3** In the **Add/Edit Wireless AAA Policy** window that is displayed, enter the name of the policy in the **Policy Name** field.
- Step 4** Choose from one of the NAS ID options from the **Option 1** drop-down list.
- Step 5** Choose from one of the NAS ID options from the **Option 2** drop-down list.
- Step 6** Choose from one of the NAS ID options from the **Option 3** drop-down list.
- Step 7** Save the configuration.
- 

## Creating a NAS ID Policy

Follow the procedure given below to create NAS ID policy:

### Before you begin

- NAS ID can be a combination of multiple NAS ID options; the maximum options are limited to 3.
- The maximum length of the NAS ID attribute is 253. Before adding a new attribute, the attribute buffer is checked, and if there is no sufficient space, the new attribute is ignored.
- By default, a wireless aaa policy (default-aaa-policy) is created with the default configuration (sys-name). You can update this policy with various NAS ID options. However, the default-aaa-policy cannot be deleted.
- If a NAS ID is not configured, the default sys-name is considered as the NAS ID for all wireless-specific RADIUS packets (authentication and accounting) from the embedded wireless controller.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b>	Enters global configuration mode.

	Command or Action	Purpose
	Device# configure terminal	
<b>Step 2</b>	<b>wireless aaa policy <i>policy-name</i></b> <b>Example:</b> Device(config)# wireless aaa policy test	Configures a new AAA policy.
<b>Step 3</b>	<b>nas-id option1 sys-name</b> <b>Example:</b> Device(config-aaa-policy)# nas-id option1 sys-name	Configures NAS ID for option1.
<b>Step 4</b>	<b>nas-id option2 sys-ip</b> <b>Example:</b> Device(config-aaa-policy)# nas-id option2 sys-ip	Configures NAS ID for option2.
<b>Step 5</b>	<b>nas-id option3 sys-mac</b> <b>Example:</b> Device(config-aaa-policy)# nas-id option3 sys-mac	Configures NAS ID for option3.

## Attaching a Policy to a Tag (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Tags** page, click **Policy** tab.
  - Step 2** Click **Add** to view the **Add Policy Tag** window.
  - Step 3** Enter a name and description for the policy tag.
  - Step 4** Click **Add** to map WLAN profile and Policy profile.
  - Step 5** Choose the **WLAN Profile** to map with the appropriate **Policy Profile**, and click the tick icon.
  - Step 6** Click **Save & Apply to Device**.
- 

## Attaching a Policy to a Tag (CLI)

Follow the procedure given below to attach a NAS ID policy to a tag:

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile policy <i>policy-name</i></b> <b>Example:</b> Device(config)# wireless profile policy test1	Configures a WLAN policy profile.
<b>Step 3</b>	<b>aaa-policy <i>aaa-policy-name</i></b> <b>Example:</b> Device(config-wireless-policy)# aaa-policy policy-aaa	Configures a AAA policy profile.
<b>Step 4</b>	<b>exit</b> <b>Example:</b> Device(config-wireless-policy)# exit	Returns to global configuration mode.
<b>Step 5</b>	<b>wireless tag policy <i>policy-tag</i></b> <b>Example:</b> Device(config)# wireless tag policy policy-tag1	Configures a wireless policy tag.
<b>Step 6</b>	<b>wlan wlan1 policy <i>policy-name</i></b> <b>Example:</b> Device(config)# wlan wlan1 policy test1	Maps a WLAN profile to a policy profile.  <b>Note</b> You can also use the <b>ap-tag</b> option to configure a NAS ID for an AP group, which will override the NAS ID that is configured for a WLAN profile or the VLAN interface.

## Verifying the NAS ID Configuration

Use the following **show** command to verify the NAS ID configuration:

```
Device# show wireless profile policy detailed test1
```

```
Policy Profile Name      : test1
Description              :
Status                   : ENABLED
VLAN                     : 1
Client count             : 0
:
:
AAA Policy Params
  AAA Override           : DISABLED
```

```
NAC : DISABLED
AAA Policy name : test
```





## CHAPTER 65

# DHCP for WLANs

---

- [DHCP for WLANs, on page 619](#)

## DHCP for WLANs

DHCP packets sent by the wireless clients are released in their respective VLANs as broadcast by the AP and relies on the fact that the network gateway of that VLAN forwards the requests to the DHCP server.



---

**Note** Internal DHCP server is not supported in EWC.

---







## CHAPTER 66

# WLAN Security

---

- [Information About AAA Override, on page 621](#)
- [Prerequisites for Layer 2 Security, on page 621](#)
- [How to Configure WLAN Security, on page 622](#)

## Information About AAA Override

The AAA Override option of a WLAN enables you to configure the WLAN for identity networking. It enables you to apply VLAN tagging, Quality of Service (QoS), and Access Control Lists (ACLs) to individual clients based on the returned RADIUS attributes from the AAA server.

## Prerequisites for Layer 2 Security

WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on the information advertised in beacon and probe responses. The available Layer 2 security policies are as follows:

- None (open WLAN)
- WPA+WPA2



---

**Note**

- Although WPA and WPA2 cannot be used by multiple WLANs with the same SSID, you can configure two WLANs with the same SSID with WPA/TKIP with PSK and Wi-Fi Protected Access (WPA)/Temporal Key Integrity Protocol (TKIP) with 802.1X, or with WPA/TKIP with 802.1X or WPA/AES with 802.1X.
- A WLAN configured with TKIP support will not be enabled on an RM3000AC module.

- 
- Static WEP (not supported on Wave 2 APs)

# How to Configure WLAN Security

## Configuring Static WEP Layer 2 Security Parameters (CLI)

### Before you begin

You must have administrator privileges.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>end</b>  <b>Example:</b> Device(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring WPA + WPA2 Layer 2 Security Parameters (CLI)

### Before you begin

You must have administrator privileges.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>security wpa</b>  <b>Example:</b> Device(config-wlan)# <code>security wpa</code>	
<b>Step 3</b>	<b>security wpa wpa1</b>  <b>Example:</b> Device(config-wlan)# <code>security wpa wpa1</code>	Enables .
<b>Step 4</b>	<b>security wpa wpa1 ciphers [aes   tkip]</b>  <b>Example:</b>	Specifies the WPA1 cipher. Choose one of the following encryption types: <ul style="list-style-type: none"> <li>• <b>aes</b>—Specifies WPA/AES support.</li> </ul>

	Command or Action	Purpose
	Device(config-wlan) # <b>security wpa wpa1 ciphers aes</b>	<ul style="list-style-type: none"> <li>• <b>tkip</b>—Specifies WPA/TKIP support.</li> </ul>
<b>Step 5</b>	<b>security wpa wpa2</b> <b>Example:</b> Device(config-wlan) # <b>security wpa</b>	Enables WPA2.
<b>Step 6</b>	<b>security wpa wpa2 ciphers aes</b> <b>Example:</b>	Configure WPA2 cipher.
<b>Step 7</b>	<b>end</b> <b>Example:</b> Device(config) # <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.





## CHAPTER 67

# Peer-to-Peer Client Support

- [Information About Peer-to-Peer Client Support, on page 625](#)
- [Configure Peer-to-Peer Client Support, on page 625](#)

## Information About Peer-to-Peer Client Support

Peer-to-peer client support can be applied to individual WLANs, with each client inheriting the peer-to-peer blocking setting of the WLAN to which it is associated. The peer-to-Peer Client Support feature provides a granular control over how traffic is directed. For example, you can choose to have traffic bridged locally within a device, dropped by a device, or forwarded to the upstream VLAN.

Peer-to-peer blocking is supported for clients that are associated with the local switching WLAN.

### Restrictions

- Peer-to-peer blocking does not apply to multicast traffic.
- Peer-to-peer blocking is not enabled by default.
- In FlexConnect, peer-to-peer blocking configuration cannot be applied only to a particular FlexConnect AP or a subset of APs. It is applied to all the FlexConnect APs that broadcast the SSID.
- FlexConnect central switching clients supports peer-to-peer upstream-forward. However, this is not supported in the FlexConnect local switching. This is treated as peer-to-peer drop and client packets are dropped.

FlexConnect central switching clients supports peer-to-peer blocking for clients associated with different APs. However, for FlexConnect local switching, this solution targets only clients connected to the same AP. FlexConnect ACLs can be used as a workaround for this limitation.

## Configure Peer-to-Peer Client Support

Follow the procedure given below to configure Peer-to-Peer Client Support:

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wlan <i>profile-name</i></b> <b>Example:</b> Device(config)# wlan wlan1	Enters WLAN configuration submode. The <i>profile-name</i> is the profile name of the configured WLAN.
<b>Step 3</b>	<b>peer-blocking [drop   forward-upstream ]</b> <b>Example:</b> Device(config-wlan)# peer-blocking drop	Configures peer-to-peer blocking parameters. <b>drop</b> —Enables peer-to-peer blocking on the drop action. <b>forward-upstream</b> —Enables peer-to-peer blocking on the forward upstream action.
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config)# end	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show wlan id <i>wlan-id</i></b> <b>Example:</b> Device# show wlan id 12	Displays the details of the selected WLAN.



## CHAPTER 68

# 802.11r BSS Fast Transition

- [Information About 802.11r Fast Transition, on page 627](#)
- [Restrictions for 802.11r Fast Transition, on page 628](#)
- [Monitoring 802.11r Fast Transition \(CLI\), on page 629](#)
- [Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN \(CLI\), on page 630](#)
- [Configuring 802.11r Fast Transition in an Open WLAN \(GUI\), on page 631](#)
- [Configuring 802.11r Fast Transition in an Open WLAN \(CLI\), on page 632](#)
- [Configuring 802.11r Fast Transition on a PSK Security–Enabled WLAN \(CLI\), on page 633](#)
- [Disabling 802.11r Fast Transition \(GUI\), on page 634](#)
- [Disabling 802.11r Fast Transition \(CLI\), on page 634](#)

## Information About 802.11r Fast Transition

802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with a new AP is done even before the corresponding client roams to the target access point. This concept is called Fast Transition. The initial handshake allows a client and the access points to do the Pairwise Transient Key (PTK) calculation in advance. These PTK keys are applied to the client and the access points after the client responds to the reassociation request or responds to the exchange with new target AP.

The FT key hierarchy is designed to allow clients to make fast BSS transitions between APs without requiring reauthentication at every AP. WLAN configuration contains a new Authenticated Key Management (AKM) type called FT (Fast Transition).

### Client Roaming

For a client to move from its current AP to a target AP using the FT protocols, message exchanges are performed using one of the following methods:

- **Over-the-Air**—The client communicates directly with the target AP using IEEE 802.11 authentication with the FT authentication algorithm.
- **Over-the-Distribution System (DS)**—The client communicates with the target AP through the current AP. The communication between the client and the target AP is carried in FT action frames between the client and the current AP and is then sent through the device.

Figure 15: Message Exchanges when Over-the-Air Client Roaming is Configured

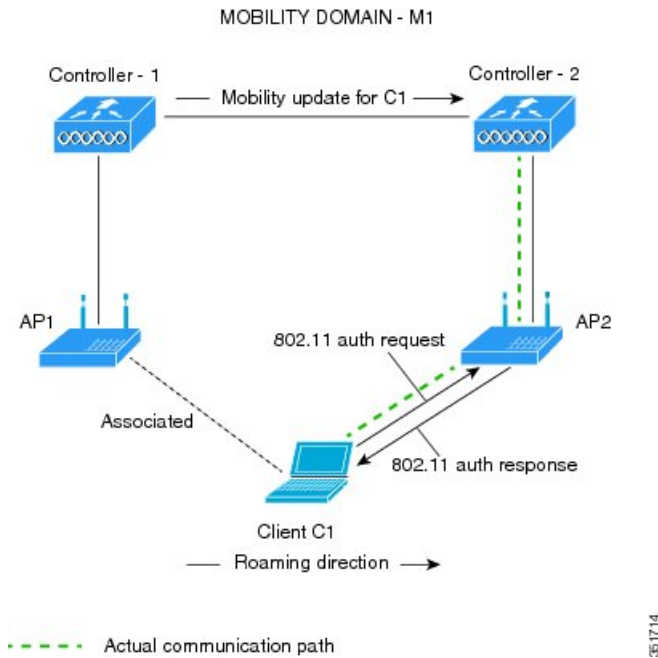
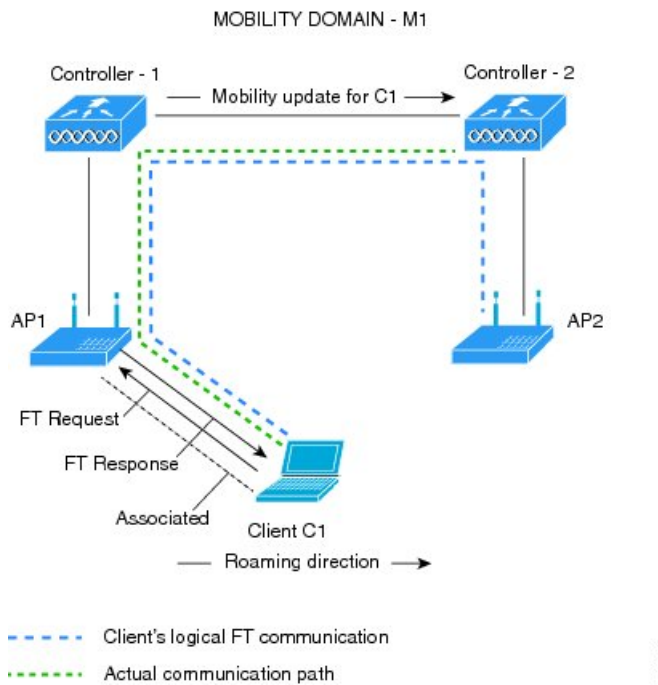


Figure 16: Message Exchanges when Over-the-DS Client Roaming is Configured



## Restrictions for 802.11r Fast Transition

- EAP LEAP method is not supported.



- Traffic Specification (TSPEC) is not supported for 802.11r fast roaming. Therefore, RIC IE handling is not supported.
- If WAN link latency exists, fast roaming is also delayed. Voice or data maximum latency should be verified. The Cisco WLC handles 802.11r Fast Transition authentication requests during roaming for both Over-the-Air and Over-the-DS methods.
- Legacy clients cannot associate with a WLAN that has 802.11r enabled if the driver of the supplicant that is responsible for parsing the Robust Security Network Information Exchange (RSN IE) is old and not aware of the additional AKM suites in the IE. Due to this limitation, clients cannot send association requests to WLANs. These clients, however, can still associate with non-802.11r WLANs. Clients that are 802.11r-capable can associate as 802.11i clients on WLANs that have both 802.11i and 802.11r Authentication Key Management Suites enabled.

The workaround is to enable or upgrade the driver of the legacy clients to work with the new 802.11r AKMs, after which the legacy clients can successfully associate with 802.11r-enabled WLANs.

Another workaround is to have two SSIDs with the same name, but with different security settings (FT and non-FT).

- Fast Transition resource-request protocol is not supported because clients do not support this protocol. Also, the resource-request protocol is an optional protocol.
- To avoid any Denial of Service (DoS) attack, each Cisco WLC allows a maximum of three Fast Transition handshakes with different APs.
- Non-802.11r-capable devices will not be able to associate with FT-enabled WLAN.
- We do not recommend 802.11r FT + PMF.
- We recommend 802.11r FT Over-the-Air roaming for FlexConnect deployments.

## Monitoring 802.11r Fast Transition (CLI)

The following command can be used to monitor 802.11r Fast Transition:

Command	Description
<code>show wlan name <i>wlan-name</i></code>	Displays a summary of the configured parameters on the WLAN.

Command	Description
<code>show wireless client mac-address mac-address</code>	<p>Displays the summary of the 802.11r authentication key management configuration on a client.</p> <pre> . . . . . . Client Capabilities   CF Pollable : Not implemented   CF Poll Request : Not implemented   Short Preamble : Not implemented   PBCC : Not implemented   Channel Agility : Not implemented   Listen Interval : 15   Fast BSS Transition : Implemented Fast BSS Transition Details : Client Statistics:   Number of Bytes Received : 9019   Number of Bytes Sent : 3765   Number of Packets Received : 130   Number of Packets Sent : 36   Number of EAP Id Request Msg Timeouts : 0   Number of EAP Request Msg Timeouts : 0   Number of EAP Key Msg Timeouts : 0   Number of Data Retries : 1   Number of RTS Retries : 0   Number of Duplicate Received Packets : 1   Number of Decrypt Failed Packets : 0   Number of Mic Failed Packets : 0   Number of Mic Missing Packets : 0   Number of Policy Errors : 0   Radio Signal Strength Indicator : -48 dBm   Signal to Noise Ratio : 40 dB . . . . . . </pre>

## Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wlan profile-name</b> <b>Example:</b> Device# <code>wlan test4</code>	Enters WLAN configuration submenu. The <i>profile-name</i> is the profile name of the configured WLAN.

	Command or Action	Purpose
<b>Step 3</b>	<b>client vlan</b> <i>vlan-name</i> <b>Example:</b> Device(config-wlan)# <b>client vlan 0120</b>	Associates the client VLAN to this WLAN.
<b>Step 4</b>	<b>security dot1x authentication-list default</b> <b>Example:</b> Device(config-wlan)# <b>security dot1x authentication-list default</b>	Enables security authentication list for dot1x security. The configuration is similar for all dot1x security WLANs.
<b>Step 5</b>	<b>security ft</b> <b>Example:</b> Device(config-wlan)# <b>security ft</b>	Enables 802.11r Fast Transition on the WLAN.
<b>Step 6</b>	<b>security wpa akm ft dot1x</b> <b>Example:</b> Device(config-wlan)# <b>security wpa akm ft dot1x</b>	Enables 802.1x security on the WLAN.
<b>Step 7</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wlan)# <b>no shutdown</b>	Enables the WLAN.
<b>Step 8</b>	<b>end</b> <b>Example:</b> Device(config-wlan)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-z</b> to exit global configuration mode

## Configuring 802.11r Fast Transition in an Open WLAN (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** Click **Add** to create WLANs.  
The **Add WLAN** page is displayed.
- Step 3** In the **Security > Layer2** tab, choose the appropriate status for **Fast Transition** between APs.
- Step 4** Click **Save & Apply to Device**.
-

## Configuring 802.11r Fast Transition in an Open WLAN (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wlan profile-name</b> <b>Example:</b> Device# <code>wlan test4</code>	Enters WLAN configuration submode. The <i>profile-name</i> is the profile name of the configured WLAN.
<b>Step 3</b>	<b>client vlan vlan-id</b> <b>Example:</b> Device(config-wlan)# <code>client vlan 0120</code>	Associates the client VLAN to the WLAN.
<b>Step 4</b>	<b>no security wpa</b> <b>Example:</b> Device(config-wlan)# <code>no security wpa</code>	Disables WPA security.
<b>Step 5</b>	<b>no security wpa akm dot1x</b> <b>Example:</b> Device(config-wlan)# <code>no security wpa akm dot1x</code>	Disables security AKM for dot1x.
<b>Step 6</b>	<b>no security wpa wpa2</b> <b>Example:</b> Device(config-wlan)# <code>no security wpa wpa2</code>	Disables WPA2 security.
<b>Step 7</b>	<b>no wpa wpa2 ciphers aes</b> <b>Example:</b> Device(config-wlan)# <code>no security wpa wpa2 ciphers aes</code>	Disables WPA2 ciphers for AES.
<b>Step 8</b>	<b>security ft</b> <b>Example:</b> Device(config-wlan)# <code>security ft</code>	Specifies the 802.11r Fast Transition parameters.
<b>Step 9</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wlan)# <code>shutdown</code>	Shuts down the WLAN.

	Command or Action	Purpose
Step 10	<b>end</b> <b>Example:</b> Device (config-wlan) # <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-z</b> to exit global configuration mode

## Configuring 802.11r Fast Transition on a PSK Security–Enabled WLAN (CLI)

### Procedure

	Command or Action	Purpose
Step 1	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>wlan profile-name</b> <b>Example:</b> Device# <b>wlan test4</b>	Enters WLAN configuration submode. The <i>profile-name</i> is the profile name of the configured WLAN.
Step 3	<b>client vlan vlan-name</b> <b>Example:</b> Device (config-wlan) # <b>client vlan 0120</b>	Associates the client VLAN to this WLAN.
Step 4	<b>no security wpa akm dot1x</b> <b>Example:</b> Device (config-wlan) # <b>no security wpa akm dot1x</b>	Disables security AKM for dot1x.
Step 5	<b>security wpa akm ft psk</b> <b>Example:</b> Device (config-wlan) # <b>security wpa akm ft psk</b>	Configures Fast Transition PSK support.
Step 6	<b>security wpa akm psk set-key {ascii {0   8}   hex {0   8}}</b> <b>Example:</b> Device (config-wlan) # <b>security wpa akm psk set-key ascii 0 test</b>	Configures PSK AKM shared key.
Step 7	<b>security ft</b> <b>Example:</b> Device (config-wlan) # <b>security ft</b>	Configures 802.11r Fast Transition.

	Command or Action	Purpose
<b>Step 8</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wlan)# <b>no shutdown</b>	Enables the WLAN.
<b>Step 9</b>	<b>end</b> <b>Example:</b> Device(config-wlan)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-z</b> to exit global configuration mode

## Disabling 802.11r Fast Transition (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
  - Step 2** On the **WLANs** page, click the WLAN name.
  - Step 3** In the **Edit WLAN** window, click the **Security > Layer2** tab.
  - Step 4** From the **Fast Transition** drop-down list, choose **Disabled**
  - Step 5** Click **Update & Apply to Device**.
- 

## Disabling 802.11r Fast Transition (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wlan <i>profile-name</i></b> <b>Example:</b> Device# <b>wlan test4</b>	Enters WLAN configuration submode. The <i>profile-name</i> is the profile name of the configured WLAN.
<b>Step 3</b>	<b>no security ft [over-the-ds   reassociation-timeout <i>timeout-in-seconds</i>]</b> <b>Example:</b> Device(config-wlan)# <b>no security ft over-the-ds</b>	Disables 802.11r Fast Transition on the WLAN.

	Command or Action	Purpose
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.







## CHAPTER 69

# Assisted Roaming

- [802.11k Neighbor List and Assisted Roaming, on page 637](#)
- [Restrictions for Assisted Roaming, on page 638](#)
- [How to Configure Assisted Roaming, on page 638](#)
- [Verifying Assisted Roaming, on page 639](#)
- [Configuration Examples for Assisted Roaming, on page 639](#)

## 802.11k Neighbor List and Assisted Roaming

The 802.11k standard allows an AP to inform 802.11k-capable clients of neighboring BSSIDs (APs in the same SSID). This can help the client to optimize its scanning and roaming behavior. Additionally, the Assisted Roaming Prediction Optimization feature can be used with non-802.11k clients, to discourage them from roaming to suboptimal APs.

### Prediction Based Roaming - Assisted Roaming for Non-802.11k Clients

You can optimize roaming for non-802.11k clients by generating a prediction neighbor list for each client without sending an 802.11k neighbor list request. When prediction based roaming enables a WLAN, after each successful client association/re-association, the same neighbor list optimization applies on the non-802.11k client to generate and store the neighbor list in the mobile station software data structure. Clients at different locations have different lists because the client probes are seen with different RSSI values by the different neighbors as the clients usually probe before any association or re-association. This list is created with the most updated probe data and predicts the next AP that the client is likely to roam to.

The wireless infrastructure discourages clients from roaming to those less desirable neighbors by denying association if the association request to an AP does not match the entries on the stored prediction neighbor list.

- Denial count: Maximum number of times a client is refused association.
- Prediction threshold: Minimum number of entries required in the prediction list for the assisted roaming feature to activate.

For more information, see [https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/Enterprise-Mobility-8-5-Design-Guide/Enterprise\\_Mobility\\_8-5\\_Deployment\\_Guide/Chapter-11.html#pgfid-1140097](https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/Enterprise-Mobility-8-5-Design-Guide/Enterprise_Mobility_8-5_Deployment_Guide/Chapter-11.html#pgfid-1140097).

## Restrictions for Assisted Roaming

- This feature is supported only on 802.11n capable indoor access points. For a single band configuration, a maximum of 6 neighbors are visible in a neighbor list. For dual band configuration, a maximum of 12 neighbors are visible.
- You can configure assisted roaming only using the device CLI.

## How to Configure Assisted Roaming

### Configuring Assisted Roaming (CLI)

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless assisted-roaming floor-bias dBm</b>  <b>Example:</b> Device(config)# <code>wireless assisted-roaming floor-bias 20</code>	Configures neighbor floor label bias. The valid range is from 5 to 25 dBm, and the default value is 15 dBm.
<b>Step 3</b>	<b>wlan wlan-id</b>  <b>Example:</b> Device(config)# <code>wlan wlan1</code>	Enters the WLAN configuration submode. The <i>wlan-name</i> is the profile name of the configured WLAN.
<b>Step 4</b>	<b>assisted-roaming neighbor-list</b>  <b>Example:</b> Device(wlan)# <code>assisted-roaming neighbor-list</code>	Configures an 802.11k neighbor list for a WLAN. By default, assisted roaming is enabled on the neighbor list when you create a WLAN. The <b>no</b> form of the command disables assisted roaming neighbor list.
<b>Step 5</b>	<b>assisted-roaming dual-list</b>  <b>Example:</b> Device(wlan)# <code>assisted-roaming dual-list</code>	Configures a dual-band 802.11k dual list for a WLAN. By default, assisted roaming is enabled on the dual list when you create a WLAN. The <b>no</b> form of the command disables assisted roaming dual list.

	Command or Action	Purpose
<b>Step 6</b>	<b>assisted-roaming prediction</b> <b>Example:</b> Device (wlan) # <b>assisted-roaming prediction</b>	Configures assisted roaming prediction list feature for a WLAN. By default, the assisted roaming prediction list is disabled.  <b>Note</b> A warning message is displayed and load balancing is disabled for the WLAN if load balancing is already enabled for the WLAN.
<b>Step 7</b>	<b>wireless assisted-roaming prediction-minimum count</b> <b>Example:</b> Device# <b>wireless assisted-roaming prediction-minimum</b>	Configures the minimum number of predicted APs required for the prediction list feature to be activated. The default value is 3.  <b>Note</b> If the number of the AP in the prediction assigned to the client is less than the number that you specify, the assisted roaming feature will not apply on this roam.
<b>Step 8</b>	<b>wireless assisted-roaming denial-maximum count</b> <b>Example:</b> Device# <b>wireless assisted-roaming denial-maximum 8</b>	Configures the maximum number of times a client can be denied association if the association request is sent to an AP does not match any AP on the prediction. The valid range is from 1 to 10, and the default value is 5.
<b>Step 9</b>	<b>end</b> <b>Example:</b> Device (config) # <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Verifying Assisted Roaming

The following command can be used to verify assisted roaming configured on a WLAN:

Command	Description
<b>show wlan id</b> <i>wlan-id</i>	Displays the WLAN parameters on the WLAN.

## Configuration Examples for Assisted Roaming

This example shows how to configure the neighbor floor label bias:

```
Device# configure terminal
Device(config)# wireless assisted-roaming floor-bias 10
Device(config)# end
Device# show wlan id 23
```

This example shows how to disable neighbor list on a specific WLAN:

```
Device# configure terminal
Device(config)# wlan test1
Device(config) (wlan)# no assisted-roaming neighbor-list
Device(config) (wlan)# end
Device# show wlan id 23
```

This example shows how to configure the prediction list on a specific WLAN:

```
Device# configure terminal
Device(config)# wlan test1
Device(config) (wlan)# assisted-roaming prediction
Device(config) (wlan)# end
Device# show wlan id 23
```

This example shows how to configure the prediction list based on assisted roaming prediction threshold and maximum denial count on a specific WLAN:

```
Device# configure terminal
Device(config)# wireless assisted-roaming prediction-minimum 4
Device(config)# wireless assisted-roaming denial-maximum 4
Device(config) (wlan)# end
Device# show wlan id 23
```



## CHAPTER 70

### 802.11v

---

- [Information About 802.11v, on page 641](#)
- [Prerequisites for Configuring 802.11v, on page 642](#)
- [Restrictions for 802.11v, on page 642](#)
- [Enabling 802.11v BSS Transition Management, on page 642](#)
- [Configuring 802.11v BSS Transition Management \(GUI\), on page 643](#)
- [Configuring 802.11v BSS Transition Management \(CLI\), on page 643](#)

## Information About 802.11v

The embedded wireless controller supports 802.11v amendment for wireless networks, which describes numerous enhancements to wireless network management.

One such enhancement is Network assisted Power Savings which helps clients to improve the battery life by enabling them to sleep longer. As an example, mobile devices typically use a certain amount of idle period to ensure that they remain connected to access points and therefore consume more power when performing the following tasks while in a wireless network.

Another enhancement is Network assisted Roaming which enables the WLAN to send requests to associated clients, advising the clients as to better APs to associate to. This is useful for both load balancing and in directing poorly connected clients.

## Enabling 802.11v Network Assisted Power Savings

Wireless devices consume battery to maintain their connection to the clients, in several ways:

- By waking up at regular intervals to listen to the access point beacons containing a DTIM, which indicates buffered broadcast or multicast traffic that the access point delivers to the clients.
- By sending null frames to the access points, in the form of keepalive messages— to maintain connection with access points.
- Devices also periodically listen to beacons (even in the absence of DTIM fields) to synchronize their clock to that of the corresponding access point.

All these processes consume battery and this consumption particularly impacts devices (such as Apple), because these devices use a conservative session timeout estimation, and therefore, wake up often to send keepalive messages. The 802.11 standard, without 802.11v, does not include any mechanism for the controller or the access points to communicate to wireless clients about the session timeout for the local client.

To save the power of clients due to the mentioned tasks in wireless network, the following features in the 802.11v standard are used:

- Directed Multicast Service
- Base Station Subsystem (BSS) Max Idle Period

### Directed Multicast Service

Using Directed Multicast Service (DMS), the client requests the access point to transmit the required multicast packet as unicast frames. This allows the client to receive the multicast packets it has ignored while in sleep mode and also ensures Layer 2 reliability. Furthermore, the unicast frame is transmitted to the client at a potentially higher wireless link rate which enables the client to receive the packet quickly by enabling the radio for a shorter duration, thus also saving battery power. Since the wireless client also does not have to wake up at each DTIM interval in order to receive multicast traffic, longer sleeping intervals are allowed.

### BSS Max Idle Period

The BSS Max Idle period is the timeframe during which an access point (AP) does not disassociate a client due to nonreceipt of frames from the connected client. This helps ensure that the client device does not send keepalive messages frequently. The idle period timer value is transmitted using the association and reassociation response frame from the access point to the client. The idle time value indicates the maximum time that a client can remain idle without transmitting any frame to an access point. As a result, the clients remain in sleep mode for a longer duration without transmitting the keepalive messages often. This in turn contributes to saving battery power.

## Prerequisites for Configuring 802.11v

- Applies for Apple clients like Apple iPad, iPhone, and so on, that run on Apple iOS version 7 or later.
- Supports local mode; also supports FlexConnect access points in central authentication modes only.

## Restrictions for 802.11v

Client needs to support 802.11v BSS Transition.

## Enabling 802.11v BSS Transition Management

802.11v BSS Transition is applied in the following three scenarios:

- Solicited request—Client can send an 802.11v Basic Service Set (BSS) Transition Management Query before roaming for a better option of AP to reassociate with.
- Unsolicited Load Balancing request—If an AP is heavily loaded, it sends out an 802.11v BSS Transition Management Request to an associated client.
- Unsolicited Optimized Roaming request—If a client's RSSI and rate do not meet the requirements, the corresponding AP sends out an 802.11v BSS Transition Management Request to this client.



**Note** 802.11v BSS Transition Management Request is a suggestion (or advice) given to a client, which the client can choose to follow or ignore. To force the task of disassociating a client, turn on the disassociation-imminent function. This disassociates the client after a period if the client is not reassociated to another AP.

## Configuring 802.11v BSS Transition Management (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** Click **Add** to create WLANs.  
The **Add WLAN** page is displayed.
- Step 3** In the **Advanced** tab and **11v BSS Transition Support** section, select the **BSS Transition** check box to enable BSS transition per WLAN.
- Step 4** Enter the **Disassociation Imminent** value. The valid range is from 0 to 3000 TBTT.
- Step 5** Click **Save & Apply to Device**.
- 

## Configuring 802.11v BSS Transition Management (CLI)

802.11v BSS Transition is applied in the following three scenarios:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters the global configuration mode.
<b>Step 2</b>	<b>wlan <i>profile-name</i></b> <b>Example:</b> Device(config)# <code>wlan test-wlan</code>	Configures WLAN profile and enters the WLAN profile configuration mode.
<b>Step 3</b>	<b>shut</b> <b>Example:</b> Device(config-wlan)# <code>shut</code>	Shutdown the WLAN profile.
<b>Step 4</b>	<b>bss-transition</b> <b>Example:</b>	Configure BSS transition per WLAN.

	<b>Command or Action</b>	<b>Purpose</b>
	Device(config-wlan)# bss-transition	
<b>Step 5</b>	<b>bss-transition disassociation-imminent</b> <b>Example:</b> Device(config-wlan)# bss-transition disassociation-imminent	Configure BSS transition disassociation Imminent per WLAN.
<b>Step 6</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wlan)# no shutdown	Enables the WLAN profile.
<b>Step 7</b>	<b>end</b> <b>Example:</b> Device(config-wlan)# end	Return to privilege EXEC mode. Alternatively, you can press <b>CTRL + Z</b> to exit global configuration mode.





# CHAPTER 71

## 802.11w

---

- [Information About 802.11w, on page 645](#)
- [Prerequisites for 802.11w, on page 648](#)
- [Restrictions for 802.11w, on page 648](#)
- [How to Configure 802.11w, on page 649](#)
- [Disabling 802.11w, on page 650](#)
- [Monitoring 802.11w, on page 651](#)

### Information About 802.11w

Wi-Fi is a broadcast medium that enables any device to eavesdrop and participate either as a legitimate or rogue device. Management frames such as authentication, de-authentication, association, disassociation, beacons, and probes are used by wireless clients to initiate and tear down sessions for network services. Unlike data traffic, which can be encrypted to provide a level of confidentiality, these frames must be heard and understood by all clients and therefore must be transmitted as open or unencrypted. While these frames cannot be encrypted, they must be protected from forgery to protect the wireless medium from attacks. For example, an attacker could spoof management frames from an AP to attack a client associated with the AP.

The 802.11w protocol applies only to a set of robust management frames that are protected by the Protected Management Frames (PMF) service. These include Disassociation, De-authentication, and Robust Action frames.

Management frames that are considered as robust action and therefore protected are the following:

- Spectrum Management
- QoS
- DLS
- Block Ack
- Radio Measurement
- Fast BSS Transition
- SA Query
- Protected Dual of Public Action
- Vendor-specific Protected

When 802.11w is implemented in the wireless medium, the following occur:

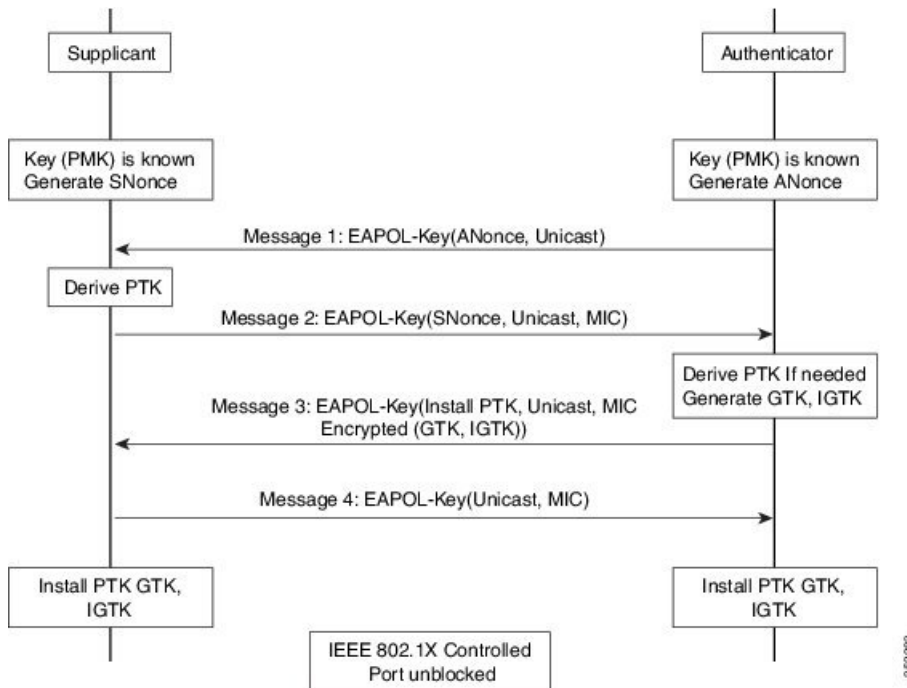
- Client protection is added by the AP adding cryptographic protection to de-authentication and disassociation frames preventing them from being spoofed in a DOS attack.
- Infrastructure protection is added by adding a Security Association (SA) tear down protection mechanism consisting of an Association Comeback Time and an SA-Query procedure preventing spoofed association request from disconnecting an already connected client.

802.11w has introduced a new IGTK Key, which is used to protect broadcast/multicast robust management frames:

- IGTK is a random value assigned by the authenticator STA (WLC) and used to protect MAC management protocol data units (MMPDUs) from that source STA.

When Management Frame Protection is negotiated, the AP encrypts the GTK and IGTK values in the EAPOL-Key frame, which is delivered in Message 3 of 4-way handshake.

**Figure 17: IGTK Exchange in 4-way Handshake**

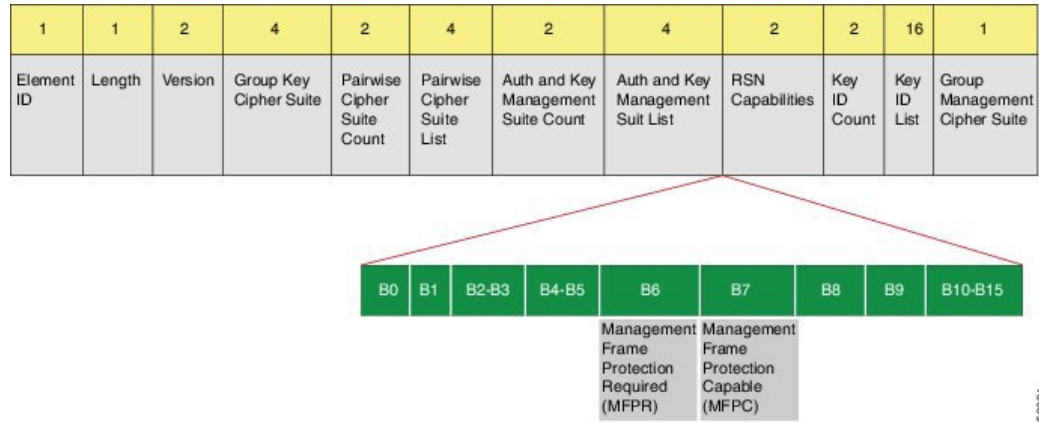


- If the AP later changes the GTK, it sends the new GTK and IGTK to the client using the Group Key Handshake .

802.11w defines a new Broadcast/Multicast Integrity Protocol (BIP) that provides data integrity and replay protection for broadcast/multicast robust management frames after successful establishment of an IGTKSA - It adds a MIC that is calculated using the shared IGTK key.

### 802.11w Information Elements (IEs)

Figure 18: 802.11w Information Elements

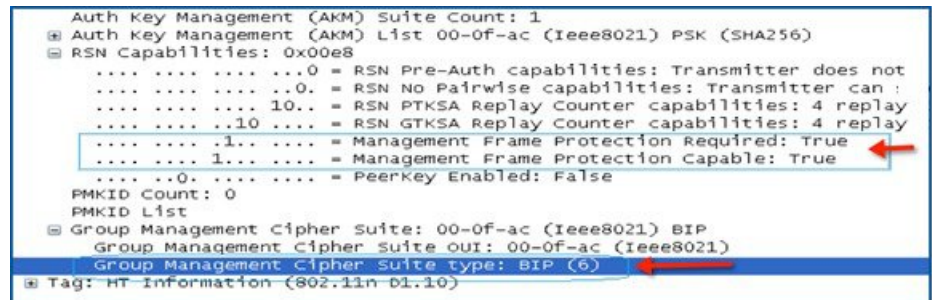


1. Modifications made in the RSN capabilities field of RSNIE.
  - a. Bit 6: Management Frame Protection Required (MFPR)
  - b. Bit 7: Management Frame Protection Capable (MFPC)
2. Two new AKM Suites, 5 and 6 are added for AKM Suite Selectors.
3. New Cipher Suite with type 6 is added to accommodate BIP.

The WLC adds this modified RSNIE in association and re-association responses and the APs add this modified RSNIE in beacons and probe responses.

The following Wireshark captures shows the RSNIE capabilities and the Group Management Cipher Suite elements.

Figure 19: 802.11w Information Elements



### Security Association (SA) Teardown Protection

SA teardown protection is a mechanism to prevent replay attacks from tearing down the session of an existing client. It consists of an Association Comeback Time and an SA-Query procedure preventing spoofed association requests from disconnecting an already connected client.

If a client has a valid security association, and has negotiated 802.11w, the AP shall reject another Association Request with status code 30. This status code stands for "Association request rejected temporarily; Try again later". The AP should not tear down or otherwise modify the state of the existing association until the SA-Query

procedure determines that the original SA is invalid and shall include in the Association Response an Association Comeback Time information element, specifying a comeback time when the AP would be ready to accept an association with this client.

The following capture shows the Association Reject message with status code 0x1e (30) and the Association comeback time set to 10 seconds.

**Figure 20: Association Reject with Comeback Time**

```

IEEE 802.11 wireless LAN management frame
  Fixed parameters (6 bytes)
    Capabilities Information: 0x0001
    status code: Association request rejected temporarily; try again later (0x001e)
    ..00 0000 0000 0000 = Association ID: 0x0000
  Tagged parameters (95 bytes)
    Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag: HT Capabilities (802.11n D1.10)
    Tag: HT Information (802.11n D1.10)
    Tag: Vendor Specific: Microsoft: WMM/WME: Parameter Element
    Tag: Timeout Interval
      Tag Number: Timeout Interval (56)
      Tag length: 5
      Timeout Interval Type: Association Comeback time (TUS) (3)
      Timeout Interval value: 10000
  
```

Following this, if the AP is not already engaged in an SA Query with the client, the AP shall issue an SA Query until a matching SA Query response is received or the Association Comeback time expires. An AP may interpret reception of a valid protected frame as an indication of a successfully completed SA Query.

If a SA QUERY response with a matching transaction identifier within the time period, the AP shall allow the association process to be started without starting additional SA Query procedures.

## Prerequisites for 802.11w

- To configure 802.11w feature for optional and mandatory, you must have WPA and AKM configured.



**Note** The RNS (Robust Secure Network) IE must be enabled with an AES Cipher.

- To configure 802.11w as mandatory, you must enable PMF AKM in addition to WPA AKM.

## Restrictions for 802.11w

- 802.11w cannot be applied on an open WLAN, WEP-encrypted WLAN, or a TKIP-encrypted WLAN.
- Cisco Catalyst 9800 Series Wireless Controller supports 802.11w + PMF combination for non-Apple clients. But Apple iOS version 11 and earlier require fix from the Apple iOS side to resolve the association issues.
- The controller will ignore disassociation or deauthentication frames sent by the clients if they are not using 802.11w PMF. The client entry will only get deleted immediately upon reception of such a frame if the client uses PMF. This is to avoid denial of service by malicious device since there is no security on those frames without PMF.

# How to Configure 802.11w

## Configuring 802.11w (GUI)

### Before you begin

WPA and AKM must be configured.

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** Click **Add** to create WLANs.  
The **Add WLAN** page is displayed.
- Step 3** In the **Security > Layer2** tab, navigate to the **Protected Management Frame** section.
- Step 4** Choose **PMF** as *Disabled*, *Optional*, or *Required*. By default, the PMF is *disabled*.  
If you choose **PMF** as *Optional* or *Required*, you get to view the following fields:
- **Association Comeback Timer**—Enter a value between 1 and 10 seconds to configure 802.11w association comeback time.
  - **SA Query Time**—Enter a value between 100 to 500 (milliseconds). This is required for clients to negotiate 802.11w PMF protection on a WLAN.
- Step 5** Click **Save & Apply to Device**.
- 

## Configuring 802.11w (CLI)

### Before you begin

WPA and AKM must be configured.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wlan profile-name wlan-id ssid</b> <b>Example:</b> Device(config)# wlan wlan-test 12 alpha	Configures a WLAN and enters configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>security wpa akm pmf dot1x</b> <b>Example:</b> Device(config-wlan)#security wpa akm pmf dot1x	Configures 802.1x support.
<b>Step 4</b>	<b>security pmf association-comeback comeback-interval</b> <b>Example:</b> Device(config-wlan)# security pmf association-comeback 10	Configures the 802.11w association comeback time.
<b>Step 5</b>	<b>security pmf mandatory</b> <b>Example:</b> Device(config-wlan)# security pmf mandatory	Requires clients to negotiate 802.11w PMF protection on a WLAN.
<b>Step 6</b>	<b>security pmf saquery-retry-time timeout</b> <b>Example:</b> Device(config-wlan)# security pmf saquery-retry-time 100	Time interval identified in milliseconds before which the SA query response is expected. If the device does not get a response, another SQ query is tried.

## Disabling 802.11w

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wlan profile-name wlan-id ssid</b> <b>Example:</b> Device(config)# wlan wlan-test 12 alpha	Configures a WLAN and enters configuration mode.
<b>Step 3</b>	<b>no security wpa akm pmf dot1x</b> <b>Example:</b> Device(config-wlan)# no security wpa akm pmf dot1x	Disables 802.1x support.
<b>Step 4</b>	<b>no security pmf association-comeback comeback-interval</b> <b>Example:</b> Device(config-wlan)# no security pmf association-comeback 10	Disables the 802.11w association comeback time.

	Command or Action	Purpose
<b>Step 5</b>	<b>no security pmf mandatory</b> <b>Example:</b> Device(config-wlan)# no security pmf mandatory	Disables client negotiation of 802.11w PMF protection on a WLAN.
<b>Step 6</b>	<b>no security pmf saquery-retry-time timeout</b> <b>Example:</b> Device(config-wlan)# no security pmf saquery-retry-time 100	Disables SQ query retry.

## Monitoring 802.11w

Use the following commands to monitor 802.11w.

### Procedure

#### Step 1 **show wlan name *wlan-name***

Displays the WLAN parameters on the WLAN. The PMF parameters are displayed.

```

. . . . .
. . . . .
Auth Key Management
    802.1x                : Disabled
    PSK                   : Disabled
    CCKM                   : Disabled
    FT dot1x              : Disabled
    FT PSK                 : Disabled
    FT SAE                 : Disabled
    Dot1x-SHA256          : Enabled
    PSK-SHA256            : Disabled
    SAE                    : Disabled
    OWE                    : Disabled
    SUITEB-1X             : Disabled
    SUITEB192-1X         : Disabled
CCKM TSF Tolerance      : 1000
FT Support              : Adaptive
    FT Reassociation Timeout : 20
    FT Over-The-DS mode     : Enabled
PMF Support              : Required
    PMF Association Comeback Timeout : 1
    PMF SA Query Time      : 500
. . . . .
. . . . .

```

#### Step 2 **show wireless client mac-address *mac-address* detail**

Displays the summary of the 802.11w authentication key management configuration on a client.

```

. . . . .
. . . . .
Policy Manager State: Run

```

```
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 497 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x-SHA256
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : Yes
EAP Type : LEAP
VLAN : 39
Multicast VLAN : 0
Access VLAN : 39
Anchor VLAN : 0
WFD capable : No
Manged WFD capable : No
. . . .
. . . .
```

---





## CHAPTER 72

# Deny Wireless Client Session Establishment Using Calendar Profiles

---

- [Information About Denial of Wireless Client Session Establishment, on page 653](#)
- [Configuring Daily Calendar Profile, on page 654](#)
- [Configuring Weekly Calendar Profile, on page 655](#)
- [Configuring Monthly Calendar Profile, on page 656](#)
- [Mapping a Daily Calendar Profile to a Policy Profile, on page 657](#)
- [Mapping a Weekly Calendar Profile to a Policy Profile, on page 658](#)
- [Mapping a Monthly Calendar Profile to a Policy Profile, on page 659](#)
- [Verifying Calendar Profile Configuration, on page 660](#)
- [Verifying Policy Profile Configuration, on page 661](#)

## Information About Denial of Wireless Client Session Establishment

Denial of client session establishment feature allows the controller to stop client session establishment based on a particular time. This helps control the network in efficient and controlled manner without any manual intervention.

In Embedded Wireless Controller, you can deny the wireless client session based on the following recurrences:

- Daily
- Weekly
- Monthly

The Calendar Profiles created are then mapped to the policy profile. By attaching the calendar profile to a policy profile, you will be able to create different recurrences for the policy profile using different policy tag.



**Note** You need to create separate Calendar Profile for Daily, Weekly, and Monthly sub-categories.

The following is the workflow for denial of wireless client session establishment feature:

- Create a calendar profile.
- Apply the calendar profile to a policy profile.



**Note** A maximum of 100 calendar profile configuration and 5 calendar profile association to policy profile is supported.

### Points to Remember

If you boot up your controller, the denial of client session establishment feature kicks in after a minute from the system boot up.

If you change the system time after the calendar profile is associated to a policy profile, you can expect a maximum of 30 second delay to adapt to the new clock timings.



**Note** You cannot use the **no action deny-client** command to disable action while associating the calendar profile to a policy profile.

If you want to disable the action command, you need to disassociate the calendar profile from the policy profile, and re-configure again.

## Configuring Daily Calendar Profile

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile calendar-profile name name</b>  <b>Example:</b> Device(config)# wireless profile calendar-profile name daily_calendar_profile	Configures a calendar profile.  Here, <i>name</i> refers to the name of the calendar profile.
<b>Step 3</b>	<b>start start_time end end_time</b>  <b>Example:</b>	Configures start and end time for the calendar profile.

	Command or Action	Purpose
	Device(config-calendar-profile)# start 09:00:00 end 17:00:00	Here,  <i>start_time</i> is the start time for the calendar profile. You need to enter start time in <b>HH:MM:SS</b> format.  <i>end_time</i> is the end time for the calendar profile. You need to enter end time in <b>HH:MM:SS</b> format.
<b>Step 4</b>	<b>recurrence daily</b>  <b>Example:</b> Device(config-calendar-profile)# recurrence daily	Configures daily recurrences for a calendar profile.
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Device(config-calendar-profile)# end	Returns to privileged EXEC mode.  Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.  <b>Note</b> When the calendar profile kicks in, the AP power profile rules (for example, radio state and USB device state) that are defined for the Ethernet speed are not applied and continue to be as per the fixed power profile.

## Configuring Weekly Calendar Profile

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile calendar-profile name name</b>  <b>Example:</b> Device(config)# wireless profile calendar-profile name weekly_calendar_profile	Configures a calendar profile.  Here, <i>name</i> refers to the name of the calendar profile.
<b>Step 3</b>	<b>start start_time end end_time</b>  <b>Example:</b> Device(config-calendar-profile)# start 18:00:00 end 19:00:00	Configures start and end time for the calendar profile.  Here,

	Command or Action	Purpose
		<p><i>start_time</i> is the start time for the calendar profile. You need to enter start time in <b>HH:MM:SS</b> format.</p> <p><i>end_time</i> is the end time for the calendar profile. You need to enter end time in <b>HH:MM:SS</b> format.</p>
<b>Step 4</b>	<p><b>recurrence weekly</b></p> <p><b>Example:</b></p> <pre>Device(config-calendar-profile)# recurrence weekly</pre>	Configures weekly recurrences for the calendar profile.
<b>Step 5</b>	<p><b>day {friday   monday   saturday   sunday   thursday   tuesday   wednesday}</b></p> <p><b>Example:</b></p> <pre>Device(config-calendar-profile)# day friday Device(config-calendar-profile)# day monday</pre>	<p>Configure days when the weekly calendar needs to be active.</p> <p><b>Note</b> You can configure multiple days using this command.</p>
<b>Step 6</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-calendar-profile)# end</pre>	<p>Returns to privileged EXEC mode.</p> <p>Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.</p>

## Configuring Monthly Calendar Profile

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 2</b>	<p><b>wireless profile calendar-profile name name</b></p> <p><b>Example:</b></p> <pre>Device(config)# wireless profile calendar-profile name monthly_calendar_profile</pre>	<p>Configures a calendar profile.</p> <p>Here, <i>name</i> refers to the name of the calendar profile.</p>
<b>Step 3</b>	<p><b>start start_time end end_time</b></p> <p><b>Example:</b></p> <pre>Device(config-calendar-profile)# start 18:00:00 end 19:00:00</pre>	<p>Configures start and end time for the calendar profile.</p> <p>Here,</p>

	Command or Action	Purpose
		<p><i>start_time</i> is the start time for the calendar profile. You need to enter start time in <b>HH:MM:SS</b> format.</p> <p><i>end_time</i> is the end time for the calendar profile. You need to enter end time in <b>HH:MM:SS</b> format.</p>
<b>Step 4</b>	<p><b>recurrence monthly</b></p> <p><b>Example:</b></p> <pre>Device(config-calendar-profile)# recurrence monthly</pre>	Configures monthly recurrences for the calendar profile.
<b>Step 5</b>	<p><b>date value</b></p> <p><b>Example:</b></p> <pre>Device(config-calendar-profile)# date 25</pre>	<p>Configures a date for the calendar profile.</p> <p><b>Note</b> If the requirement is to perform denial of service in certain timing, such as, 2, 10, and 25 of every month, all three days need to be configured using the <b>date</b> command. There is no range for date. You need to configure the dates as per your requirement.</p>
<b>Step 6</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-calendar-profile)# end</pre>	<p>Returns to privileged EXEC mode.</p> <p>Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.</p>

## Mapping a Daily Calendar Profile to a Policy Profile

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 2</b>	<p><b>wireless profile policy <i>profile-name</i></b></p> <p><b>Example:</b></p> <pre>Device(config)# wireless profile policy default-policy-profile</pre>	<p>Creates policy profile for the WLAN.</p> <p>The <i>profile-name</i> is the profile name of the policy profile.</p>
<b>Step 3</b>	<p><b>calendar-profile name <i>calendar-profile-name</i></b></p> <p><b>Example:</b></p>	Maps a calendar profile to a policy profile.

	Command or Action	Purpose
	<pre>Device(config-wireless-policy)# calendar-profile name daily_calendar_profile</pre>	<p>The <i>calendar-profile-name</i> is the name of the calendar profile name created in <a href="#">Configuring Daily Calendar Profile, on page 654</a>.</p> <p><b>Note</b> You need to disable Policy Profile before associating a calendar profile to a policy profile. The following needs to be done:</p> <pre>Device(config-wireless-policy)# shutdown</pre>
<b>Step 4</b>	<p><b>action deny-client</b></p> <p><b>Example:</b></p> <pre>Device(config-policy-profile-calender)# action deny-client</pre>	<p>Configures deny client session establishment during calendar profile interval.</p> <p><b>Note</b> Client associations are denied daily between timeslot 9:00:00 to 17:00:00. For start and end time details, see <a href="#">Configuring Daily Calendar Profile, on page 654</a>.</p>
<b>Step 5</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-policy-profile-calender)# end</pre>	<p>Returns to privileged EXEC mode.</p> <p>Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.</p>

## Mapping a Weekly Calendar Profile to a Policy Profile

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 2</b>	<p><b>wireless profile policy <i>profile-name</i></b></p> <p><b>Example:</b></p> <pre>Device(config)# wireless profile policy default-policy-profile</pre>	<p>Creates policy profile for the WLAN.</p> <p>The <i>profile-name</i> is the profile name of the policy profile.</p>
<b>Step 3</b>	<p><b>calendar-profile name <i>calendar-profile-name</i></b></p> <p><b>Example:</b></p> <pre>Device(config-wireless-policy)# calendar-profile name weekly_calendar_profile</pre>	<p>Maps a calendar profile to a policy profile.</p> <p>The <i>calendar-profile-name</i> is the name of the calendar profile name created in <a href="#">Configuring Weekly Calendar Profile, on page 655</a>.</p>

	Command or Action	Purpose
		<p><b>Note</b> You need to disable Policy Profile before associating a calendar profile to a policy profile. The following needs to be done:</p> <pre>Device(config-wireless-policy)# shutdown</pre>
<b>Step 4</b>	<p><b>action deny-client</b></p> <p><b>Example:</b></p> <pre>Device(config-policy-profile-calender)# action deny-client</pre>	<p>Configures deny client session establishment during calendar profile interval.</p> <p><b>Note</b> Client associations are denied daily between timeslot 9:00:00 to 17:00:00. For start and end time details, see <a href="#">Configuring Weekly Calendar Profile, on page 655</a>.</p> <p>On Monday and Tuesday, clients are denied between 17:30:00 and 19:00:00 besides regular time 9:00:00 to 17:00:00.</p> <p>On 25th of every month, clients are denied between 18:00:00 and 19:00:00 besides regular time 9:00:00 to 17:00:00.</p>
<b>Step 5</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-policy-profile-calender)# end</pre>	<p>Returns to privileged EXEC mode.</p> <p>Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.</p>

## Mapping a Monthly Calendar Profile to a Policy Profile

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 2</b>	<p><b>wireless profile policy <i>profile-name</i></b></p> <p><b>Example:</b></p> <pre>Device(config)# wireless profile policy default-policy-profile</pre>	<p>Creates policy profile for the WLAN.</p> <p>The <i>profile-name</i> is the profile name of the policy profile.</p>
<b>Step 3</b>	<p><b>calender-profile name <i>calendar-profile-name</i></b></p>	Maps a calender profile to a policy profile.

	Command or Action	Purpose
	<b>Example:</b> Device(config-wireless-policy)# calender-profile name monthly_calendar_profile	The <i>calendar-profile-name</i> is the name of the calendar profile name created in <a href="#">Configuring Monthly Calendar Profile, on page 656</a> .
<b>Step 4</b>	<b>action deny-client</b>  <b>Example:</b> Device(config-policy-profile-calender)# action deny-client	Configures deny client session establishment for the defined calendar profile interval.  <b>Note</b> Every day client associations are denied between timeslot 9:00:00 to 17:00:00. For start and end time details, see <a href="#">Configuring Monthly Calendar Profile, on page 656</a> .  On Monday and Tuesday, clients are denied between 17:30:00 and 19:00:00 besides regular time 9:00:00 to 17:00:00.  On 25th of every month, clients are denied between 18:00:00 and 19:00:00 besides regular time 9:00:00 to 17:00:00.
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Device(config-policy-profile-calender)# end	Returns to privileged EXEC mode.  Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Verifying Calendar Profile Configuration

To view the summary of calendar profiles, use the following command:

```
Device# show wireless profile calendar-profile summary
Number of Calendar Profiles: 3

Profile-Name
-----
monthly_25_profile
weekly_mon_profile
daily_calendar_profile
```

To view the calendar profile details for a specific profile name, use the following command:

```
Device# show wireless profile calendar-profile detailed daily_calendar_profile
Calendar profiles                : daily_calendar_profile
-----
Recurrence                       : DAILY
Start Time                       : 09:00:00
End Time                         : 17:00:00
```



## Verifying Policy Profile Configuration

To view the detailed parameters for a specific policy profile, use the following command:

```
Device# show wireless profile policy detailed default-policy-profile
Tunnel Profile
  Profile Name                : Not Configured
Calendar Profile
  Profile Name                : monthly_25_profile
  Wlan Enable                 : Not Configured
  Client Block                : Client Block Configured
-----
  Profile Name                : weekly_mon_profile
  Wlan Enable                 : Not Configured
  Client Block                : Client Block Configured
-----
  Profile Name                : daily_calendar_profile
  Wlan Enable                 : Not Configured
  Client Block                : Client Block Configured
-----
Fabric Profile
  Profile Name                : Not Configured
```

To view the configured calendar profile information under policy profile, use the following command:

```
Device# show wireless profile policy all
Tunnel Profile
Profile Name : Not Configured
Calendar Profile
Profile Name : daily_calendar_profile
Wlan Enable : Not Configured
Client Block : Client Block Configured
-----
Profile Name : weekly_calendar_profile
Wlan Enable : Not Configured
Client Block : Client Block Configured
-----
Fabric Profile
Profile Name : Not Configured
```




---

**Note** The anchor priority is always displayed as local. Priorities can be assigned on the foreign controller.

---





## CHAPTER 73

# Introduction to EoGRE

Ethernet over GRE (EoGRE) is an aggregation solution for grouping Wi-Fi traffic from hotspots. This solution enables customer premises equipment (CPE) devices to bridge the Ethernet traffic coming from an end-host, and encapsulate the traffic in Ethernet packets over an IP Generic Routing Encapsulation (GRE) tunnel. When the IP GRE tunnels are terminated on a service provider's broadband network gateway, the end-host traffic is forwarded and subscriber sessions are initiated.

### Client IPv6

### EoGRE for WLAN

To enable EoGRE for a WLAN, the wireless policy profile should be mapped to a tunnel profile, which may contain the following:

- AAA override: Allows you to bypass rule filtering for a client.
- Gateway RADIUS proxy: Allows forwarding of AAA requests to tunnel gateways.
- Tunnel rules: Defines the domain to use for each realm. They also define VLAN tagging for the client traffic towards tunnel gateways.
- DHCP option 82: Provides a set of predefined fields.

### EoGRE Deployment with Multiple Tunnel Gateways

The embedded wireless controller sends keepalive pings to the primary and secondary tunnel gateways and keeps track of the missed pings. When a certain threshold level is reached for the missed pings, switchover is performed and the secondary tunnel is marked as active. This switchover deauthenticates all the clients to enable them to rejoin the access points (APs). When the primary tunnel come back online, all the client traffic are reverted to the primary tunnel. However, this behavior depends on the type of redundancy.

### Load Balancing in EtherChannels

Load balancing of tunneled traffic over Etherchannels works by hashing the source or destination IP addresses or mac addresses of the tunnel endpoint pair. Because the number of tunnels is very limited when compared to clients (each tunnel carries traffic for many clients), the spreading effect of hashing is highly reduced and optimal utilization of Etherchannel links can be hard to achieve.

Using the EoGRE configuration model, you can use the *tunnel source* option of each tunnel interface to adjust the load-balancing parameters and spread tunnels across multiple links.

You can use different source interfaces on each tunnel for load balancing based on the source or destination IP address. For that choose the source interface IP address in such a way that traffic flows take different links for each src-dest IP pair. The following is an example with four ports:

```
Client traffic on Tunnel1 - Src IP: 40.143.0.72  Dest IP: 40.253.0.2
Client traffic on Tunnel2 - Src IP: 40.146.0.94  Dest IP: 40.253.0.6
Client traffic on Tunnel3 - Src IP: 40.147.0.74  Dest IP: 40.253.0.10
```

Use the **show platform software port-channel link-select interface port-channel 4 ipv4 src\_ip dest\_ip** command to determine the link that a particular flow will take.

- [EoGRE Configuration Overview, on page 664](#)
- [Create a Tunnel Gateway, on page 665](#)
- [Configuring a Tunnel Domain, on page 666](#)
- [Configuring EoGRE Global Parameters, on page 667](#)
- [Configuring a Tunnel Profile, on page 667](#)
- [Associating WLAN to a Wireless Policy Profile, on page 669](#)
- [Attaching a Policy Tag and a Site Tag to an AP, on page 669](#)
- [Verifying the EoGRE Tunnel Configuration, on page 670](#)

## EoGRE Configuration Overview

The EoGRE solution can be deployed in two different ways:

- Central-Switching: EoGRE tunnels connect the embedded wireless controller to the tunnel gateways.
- Flex or Local-Switching: EoGRE tunnels are initiated on the APs and terminated on the tunnel gateways.

To configure EoGRE, perform the following tasks:

1. Create a set of tunnel gateways.
2. Create a set of tunnel domains.
3. Create a tunnel profile with rules that define how to match clients to domains.
4. Create a policy profile and attach the tunnel profile to it.
5. Map the policy profile to WLANs using policy tags.



**Note** The EoGRE tunnel fallback to the secondary tunnel is triggered after the *max-skip-count* ping fails in the last measurement window. Based on the starting and ending instance of the measurement window, the fall-back may take more time than the duration that is configured.

**Table 26: EoGRE Authentication Methods**

Method Name	First Supported Release	Mode
PSK	17.2.1	Local/Flex (central authentication)
Open	16.12.1	Local/Flex (central authentication)

Method Name	First Supported Release	Mode
LWA	16.12.1	Local/Flex (central authentication)
Dot1x	16.12.1	Local/Flex (central authentication)
CWA	16.12.1	Local/Flex (central authentication)

## Create a Tunnel Gateway



**Note** In the Cisco Embedded Wireless Controller on Catalyst Access Points, a tunnel gateway is modeled as a tunnel interface.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>interface tunnel <i>tunnel_number</i></b>  <b>Example:</b> Device(config)# interface tunnel 21	Configures a tunnel interface and enters interface configuration mode.
<b>Step 3</b>	<b>tunnel source <i>source_intf</i></b>  <b>Example:</b> Device(config-if)# tunnel source 22	Sets the source address of the tunnel interface. The source interface can be VLAN, Gigabit Ethernet or loopback.
<b>Step 4</b>	<b>tunnel destination <i>tunnel-address</i></b>  <b>Example:</b> Device(config-if)# tunnel destination 10.11.12.13	Sets the destination address of the tunnel.
<b>Step 5</b>	<b>tunnel mode ethernet gre {ipv4   ipv6} p2p</b>  <b>Example:</b> Device(config-if)# tunnel mode ethernet gre ipv4 p2p	Sets the encapsulation mode of the tunnel to Ethernet over GRE IPv4 or Ethernet over GRE IPv6.

# Configuring a Tunnel Domain



**Note** Tunnel domains are a redundancy grouping of tunnels. The following configuration procedure specifies a primary and a secondary tunnel, along with a redundancy model.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>tunnel eogre domain <i>domain</i></b> <b>Example:</b> Device(config)# tunnel eogre domain doml	Configures EoGRE redundancy domain.
<b>Step 3</b>	<b>primary tunnel <i>primary-tunnel_intf</i></b> <b>Example:</b> Device(config-eogre-domain)# primary tunnel 21	Configures the primary tunnel.
<b>Step 4</b>	<b>secondary tunnel <i>secondary-tunnel_intf</i></b> <b>Example:</b> Device(config-eogre-domain)# secondary tunnel 22	Configures the secondary tunnel.
<b>Step 5</b>	<b>redundancy revertive</b> <b>Example:</b> Device(config-eogre-domain)# redundancy revertive	Sets the redundancy model as revertive.  When redundancy is set to revertive and the primary tunnel goes down, a switchover to secondary tunnel is performed. When the primary tunnel comes back up, a switchover to the primary tunnel is performed, because the primary tunnel has priority over the secondary tunnel.  When redundancy is not set to revertive, tunnels will have the same priority, and a switchover to the primary tunnel is not performed if the active tunnel is the secondary tunnel and the primary tunnel comes back up.

# Configuring EoGRE Global Parameters

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>tunnel eogre heartbeat interval <i>interval-value</i></b>  <b>Example:</b> Device(config)# tunnel eogre heartbeat interval 600	Sets EoGRE tunnel heartbeat periodic interval.
<b>Step 3</b>	<b>tunnel eogre heartbeat max-skip-count <i>skip-count</i></b>  <b>Example:</b> Device(config)# tunnel eogre heartbeat max-skip-count 7	Sets the maximum number of tolerable dropped heartbeats.  After reaching the maximum number of heartbeats that can be dropped, the tunnel is declared as down and a switchover is performed.
<b>Step 4</b>	<b>tunnel eogre source loopback <i>tunnel_source</i></b>  <b>Example:</b> Device(config)# tunnel eogre source loopback 12	Sets the tunnel EoGRE source interface.
<b>Step 5</b>	<b>tunnel eogre interface tunnel <i>tunnel-intf</i> aaa proxy key <i>key key-name</i></b>  <b>Example:</b> Device(config)# tunnel eogre interface tunnel 21 aaa proxy key 0 mykey	(Optional) Configures AAA proxy RADIUS key for the AAA proxy setup.  <b>Note</b> When the tunnel gateway is behaving as the AAA proxy server, only this step is required for the configuration.

## Configuring a Tunnel Profile

### Before you begin

Ensure that you define the destination VLAN on the controller. If you do not define the VLAN, clients will not be able to connect.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile policy <i>profile-policy-name</i></b> <b>Example:</b> Device(config)# wireless profile policy eogre_policy	Configures a WLAN policy profile.
<b>Step 3</b>	<b>tunnel-profile <i>tunnel-profile-name</i></b> <b>Example:</b> Device(config-wireless-policy)# tunnel-profile tunnell	Creates a tunnel profile.
<b>Step 4</b>	<b>exit</b> <b>Example:</b> Device(config-wireless-policy)# exit	Returns to global configuration mode.
<b>Step 5</b>	<b>wireless profile tunnel <i>tunnel-profile-name</i></b> <b>Example:</b> Device(config)# wireless profile tunnel wl-tunnel-1	Configures a wireless tunnel profile.
<b>Step 6</b>	<b>dhcp-opt82 enable</b> <b>Example:</b> Device(config-tunnel-profile)# dhcp-opt82 enable	Activates DHCP Option 82 for the tunneled clients.
<b>Step 7</b>	<b>dhcp-opt82 remote-id <i>remote-id</i></b> <b>Example:</b> Device(config-tunnel-profile)# dhcp-opt82 remote-id vlan	Configures Remote ID options.  Choose from the comma-separated list of options such as <b>ap-mac</b> , <b>ap-ethmac</b> , <b>ap-name</b> , <b>ap-group-name</b> , <b>flex-group-name</b> , <b>ap-location</b> , <b>vlan</b> , <b>ssid-name</b> , <b>ssid-type</b> , and <b>client-mac</b> .
<b>Step 8</b>	<b>aaa-override</b> <b>Example:</b> Device(config-tunnel-profile)# aaa-override	Enables AAA policy override.
<b>Step 9</b>	<b>gateway-radius-proxy</b> <b>Example:</b> Device(config-tunnel-profile)# gateway-radius-proxy	Enables the gateway RADIUS proxy.



	Command or Action	Purpose
<b>Step 10</b>	<b>gateway-accounting-radius-proxy</b> <b>Example:</b> Device(config-tunnel-profile)# gateway-accounting-radius-proxy	Enables the gateway accounting RADIUS proxy.
<b>Step 11</b>	<b>rule priority realm-filter realm domain domain-name vlan vlan-id</b> <b>Example:</b> Device(config-tunnel-profile)# rule 12 realm-filter realm domain dom1 vlan 5	Creates a rule to choose a domain, using the realm filter, for client Network Access Identifier (NAI), tunneling domain name, and destination VLAN.

## Associating WLAN to a Wireless Policy Profile

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless tag policy policy-tag-name</b> <b>Example:</b> Device(config)# wireless tag policy eogre_tag	Configures a policy tag and enters policy tag configuration mode.
<b>Step 3</b>	<b>wlan wlan-name policy profile-policy-name</b> <b>Example:</b> Device(config-policy-tag)# wlan eogre_open_eogre policy eogre_policy	Maps an EoGRE policy profile to a WLAN profile.
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config-policy-tag)# end	Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.

## Attaching a Policy Tag and a Site Tag to an AP

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>	Enters global configuration mode.

	Command or Action	Purpose
	Device# configure terminal	
<b>Step 2</b>	<b>ap mac-address</b> <b>Example:</b> Device(config)# ap 80E8.6FD4.0BB0	Configures an AP and enters AP profile configuration mode.
<b>Step 3</b>	<b>policy-tag policy-tag-name</b> <b>Example:</b> Device(config-ap-tag)# policy-tag eogre_tag	Maps the EoGRE policy tag to the AP.
<b>Step 4</b>	<b>site-tag site-tag-name</b> <b>Example:</b> Device(config-ap-tag)# site-tag sp-flex-site	Maps a site tag to the AP.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config-ap-tag)# end	Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.

## Verifying the EoGRE Tunnel Configuration

The `show tunnel eogre` command displays the EoGRE clients, domains, gateways, global-configuration, and manager information in the local mode.

To display the EoGRE domain summary in the local mode, use the following command:

```
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
```

To display the details of an EoGRE domain in the local mode, use the following command:

```
Device# show tunnel eogre domain detailed domain-name
```

```
Domain Name      : eogre_domain
Primary GW       : Tunnel1
Secondary GW     : Tunnel2
Active GW        : Tunnel1
Redundancy       : Non-Revertive
```

To view the EoGRE tunnel gateway summary and statistics in the local mode, use the following command:

```
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

```

To view the details of an EoGRE tunnel gateway in the local mode, use the following command:

```
Device# show tunnel eogre gateway detailed gateway-name
```

```

Gateway : Tunnel1
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                                : 1
  Transmitted Keepalives in last window : 2
  Received Keepalives in last window    : 2

```

To view the client summary of EoGRE in the local mode, use the following command:

```
Device# show tunnel eogre client summary
```

Client MAC	AP MAC	Domain	Tunnel	VLAN	Local
74da.3828.88b0	80e8.6fd4.9520	eogre_domain	N/A	2121	No

To view the details of an EoGRE global configuration in the local mode, use the following command:

```
Device# show tunnel eogre global-configuration
```

```

Heartbeat interval      : 60
Max Heartbeat skip count : 3
Source Interface        : (none)

```

To view the details of the global tunnel manager statistics in the local mode, use the following command:

```
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
  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

```

To view the tunnel manager statistics of a specific process instance in the local mode, use the following command:

```
Device# show tunnel eogre manager stats instance instance-number
```

```

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

```

The `show ap tunnel eogre` command displays the tunnel domain information, EoGRE events, and the tunnel gateway status on the APs, in the flex mode.

To view the summary information of an EoGRE tunnel gateway in the flex mode, use the following command:

```
Device# show ap tunnel eogre domain summary
```

AP MAC	Domain	Active Gateway
80e8.6fd4.9520	eogre_domain	Tunnell

To view the wireless tunnel profile summary, use the following command:

```
Device# show wireless profile tunnel summary
```

Profile Name	AAA-Override	AAA-Proxy	DHCP Opt82	Enabled
eogre_tunnel	No	No	Yes	Yes
eogre_tunnel_set	No	No	Yes	No
eogre_tunnel_snmp	No	No	No	No

To view a wireless tunnel profile's details, use the following command:

```
Device# show wireless profile tunnel detailed profile-name
```

```
Profile Name : eogre_tunnel
Status : Enabled
AAA-Proxy/Accounting-Proxy: Disabled / Disabled
AAA-Override : Disabled
DHCP Option82 : Enabled
Circuit-ID : ap-mac,ap-ethmac,ap-location,vlan
Remote-ID : ssid-name,ssid-type,client-mac,ap-name
```

Tunnel Rules

Priority	Realm	Vlan	Domain (Status/Primary GW/Secondary GW)
1	*	2121	eogre_domain (Enabled/Tunnell1/Tunnel2)

To view detailed information about an EoGRE tunnel domain's status, use the following command:

```
Device# show ap tunnel eogre domain detailed
```

```
Domain      : eogre_domain
AP MAC      : 80e8.6fd4.9520
Active GW   : Tunnell
```

To view the EoGRE events on an AP, use the following command:

```
Device# show ap tunnel eogre events
```

```
AP 80e8.6fd4.9520 Event history
Timestamp          #Times  Event                      RC Context
-----
02/18/2019 23:50:26.341 6      IAPP_STATS                 0 GW Tunnel2 uptime:0s
02/18/2019 23:49:40.222 2      CLIENT_JOIN                0 74da.3828.88b0, (eogre_domain/2121)
02/18/2019 23:48:43.549 1      CLIENT_LEAVE               0 74da.3828.88b0, (eogre_domain/2121)
02/18/2019 23:47:33.127 1      DOMAIN_STATUS              0 eogre_domain Active GW: Tunnell1
02/18/2019 23:47:33.124 4      AP_TUNNEL_STATUS           0 Tunnel2 Dn
```

```

02/18/2019 23:47:33.124 1      MSG_CLIENT_DEL      0 GW Tunnel2 (IP: 9.51.1.12)
02/18/2019 23:47:33.124 2      TUNNEL_ADD          0 GW Tunnel2
02/18/2019 23:47:33.120 3      MSG_CLIENT_DEL_PD   0 GW Tunnel1 (IP: 9.51.1.11)
02/18/2019 23:47:31.763 2      AP_DOMAIN_PUSH      0 Delete:eogre_domain_set, 0 GWs
02/18/2019 23:47:31.753 4      AP_VAP_PUSH         0 profile:'eogre_tunnel',
wlan:pyats_eogre

```

To view the summary information of the EoGRE tunnel gateway, use the following command:

```
Device# show ap tunnel eogre gateway summary
```

AP MAC	Gateway	Type	IP	State	Clients
80e8.6fd4.9520	Tunnel1	IPv4	9.51.1.11	Up	1
80e8.6fd4.9520	Tunnel2	IPv4	9.51.1.12	Down	0

To view detailed information about an EoGRE tunnel gateway, use the following command:

```
Device# show ap tunnel eogre gateway detailed gateway-name
```

```

Gateway : Tunnel1
Mode    : IPv4
IP      : 9.51.1.11
State   : Up
MTU     : 1476
Up Time: 14 hours 25 minutes 2 seconds
AP MAC  : 80e8.6fd4.9520

Clients
Total Number of Wireless Clients      : 1
Traffic
Total Number of Received Packets      : 6
Total Number of Received Bytes        : 2643
Total Number of Transmitted Packets    : 94
Total Number of Transmitted Bytes      : 20629
Total Number of Lost Keepalive         : 3

```

To view summary information about the EoGRE tunnel gateway status, use the following command:

```
Device# show ap tunnel eogre domain summary
```

AP MAC	Domain	Active Gateway
80e8.6fd4.9520	eogre_domain	Tunnel1

To view information about EoGRE events on an AP, use the following command:

```
Device# show ap name ap-name tunnel eogre events
```

```

AP 80e8.6fd4.9520 Event history
Timestamp          #Times  Event                      RC Context
-----
02/18/2019 23:50:26.341 6      IAPP_STATS                 0 GW Tunnel2 uptime:0s
02/18/2019 23:49:40.222 2      CLIENT_JOIN                 0 74da.3828.88b0, (eogre_domain/2121)
02/18/2019 23:48:43.549 1      CLIENT_LEAVE                 0 74da.3828.88b0, (eogre_domain/2121)

```



```

02/18/2019 23:47:33.127 1      DOMAIN_STATUS      0 eogre_domain Active GW: Tunnel1
02/18/2019 23:47:33.124 4      AP_TUNNEL_STATUS   0 Tunnel2 Dn
02/18/2019 23:47:33.124 1      MSG_CLIENT_DEL     0 GW Tunnel2 (IP: 9.51.1.12)
02/18/2019 23:47:33.124 2      TUNNEL_ADD         0 GW Tunnel2
02/18/2019 23:47:33.120 3      MSG_CLIENT_DEL_PD  0 GW Tunnel1 (IP: 9.51.1.11)
02/18/2019 23:47:31.763 2      AP_DOMAIN_PUSH     0 Delete:eogre_domain_set, 0 GWs
02/18/2019 23:47:31.753 4      AP_VAP_PUSH        0 profile:'eogre_tunnel',
wlan:pyats_eogre

```

To view the summary information about EoGRE tunnel domain's status on an AP, use the following command:

```
Device# show ap name ap-name tunnel eogre domain summary
```

```

AP MAC          Domain          Active Gateway
-----
80e8.6fd4.9520  eogre_domain

```

To view the detailed information about EoGRE tunnel domain on an AP, use the following command:

```
Device# show ap name ap-name tunnel eogre domain detailed
```

```

Domain Name      : eogre_domain
Primary GW       : Tunnel1
Secondary GW     : Tunnel2
Active GW        : Tunnel1
Redundancy       : Non-Revertive
AdminState       : Up

```

To view the summary information about EoGRE tunnel gateways on an AP, use the following command:

```
Device# show ap name ap-name tunnel eogre gateway summary
```

```

AP MAC          Gateway          Type IP          State Clients
-----
80e8.6fd4.9520  Tunnel1          IPv4 9.51.1.11    Up      1
80e8.6fd4.9520  Tunnel2          IPv4 9.51.1.12    Down    0

```

To view detailed information about an EoGRE tunnel gateway's status on an AP, use the following command:

```
Device# show ap name ap-name tunnel eogre gateway detailed gateway-name
```

```

Gateway : Tunnel2
Mode    : IPv4
IP      : 9.51.1.12
State   : Down
MTU     : 0
AP MAC  : 80e8.6fd4.9520

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
Total Number of Lost Keepalive         : 151
```