Cisco Prime Infrastructure Classic View
Configuration Guide for Wireless Devices
Software Release 2.2
September 2014

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

Text Part Number: OL-32295-01
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 noninfringement 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.

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: www.cisco.com/go/trademarks. 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. (1110R)

Copyright © 2014 Cisco Systems, Inc.
All rights reserved.
## CONTENTS

### CHAPTER 1

**Cisco Prime Infrastructure Overview** 1-1

- Cisco Unified Network Components 1-2
- Cisco Wireless LAN Controller 1-2
- Virtual LAN Controllers 1-2
  - Features Not Supported by Virtual LAN Controllers 1-2
- Access Points 1-3
  - Embedded Access Points 1-3
- Access Point Communication Protocols 1-4
- Guidelines and Restrictions for Using CAPWAP 1-5
- WLAN Controller Autodiscovery 1-5
- The Controller Discovery Process 1-6
- Prime Infrastructure Services 1-6
  - Cisco Context-Aware Service Solution 1-7
  - Cisco Identity Service Engine Solution 1-7
  - Cisco Adaptive Wireless Intrusion Prevention Service 1-8

### CHAPTER 2

**Getting Started** 2-1

- Menu Bar 2-1
- Global Toolbar 2-2
  - Tools 2-2
  - Help 2-3
- Alarm Summary 2-3

### CHAPTER 3

**Configuring Security Solutions** 3-1

- Cisco Unified Wireless Network Solution Security 3-1
  - Layer 1 Solutions 3-2
  - Layer 2 Solutions 3-2
  - Layer 3 Solutions 3-2
  - Single Point of Configuration Policy Manager Solutions 3-2
- Rogue Access Point Solutions 3-3
  - Rogue Access Point Challenges 3-3
  - Tagging and Containing Rogue Access Points 3-3
Securing Your Network Against Rogue Access Points 3-3

Interpreting the Security Dashboard 3-4
Security Index 3-4
Malicious Rogue Access Points 3-5
Adhoc Rogues 3-6
CleanAir Security 3-6
Unclassified Rogue Access Points 3-7
Friendly Rogue Access Points 3-7
Access Point Threats or Attacks 3-8
MFP Attacks 3-8
Attacks Detected 3-8
Recent Rogue AP Alarms 3-8
Recent Adhoc Rogue Alarm 3-8
Most Recent Security Alarms 3-8

Rogue Access Points, Ad hoc Events, and Clients 3-9
Classifying Rogue Access Points 3-9
Rogue Access Point Classification Types 3-10
Adhoc Rogue 3-12

Rogue Access Point Location, Tagging, and Containment 3-12
Detecting Access Points on a Network 3-13
Viewing Rogue Access Points by Controller 3-14

Working with Alarms 3-15
Monitoring Rogue Alarm Events 3-16
Viewing Rogue AP Event Details 3-17
Monitoring Adhoc Rogue Events 3-18
Viewing Adhoc Rogue Event Details 3-18

Security Overview 3-19
Security Vulnerability Assessment 3-19
Security Index 3-20
Top Security Issues 3-21

Switch Port Tracing 3-27
Integrated Security Solutions 3-27

Using Prime Infrastructure to Convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 Mode 3-28
Configuring a Firewall for Prime Infrastructure 3-29
Access Point Authorization 3-29
Management Frame Protection (MFP) 3-30
Guidelines for Using MFP 3-31
Configuring Intrusion Detection Systems (IDS) 3-32
Viewing IDS Sensors 3-32
Configuring IDS Signatures 3-32
Uploading IDS Signatures 3-34
Downloading IDS Signatures 3-35
Enabling or Disabling IDS Signatures 3-36
Enabling Web Login 3-37
Downloading Customized Web Authentication 3-38
Connecting to the Guest WLAN 3-39
Certificate Signing Request (CSR) Generation 3-40

PERFORMING MAINTENANCE OPERATIONS 4-1
Information About Maintenance Operations 4-1
Performing System Tasks 4-1
Adding a Controller to the Prime Infrastructure Database 4-1
Using Prime Infrastructure to Update System Software 4-2
Downloading Vendor Device Certificates 4-3
Downloading Vendor CA Certificates 4-4
Using Prime Infrastructure to Enable Long Preambles for SpectraLink NetLink Phones 4-5
Creating an RF Calibration Model 4-5
Performing Prime Infrastructure Operations 4-6
Verifying the Status of Prime Infrastructure 4-6
Stopping Prime Infrastructure 4-6
Backing Up the Prime Infrastructure Database 4-7
Scheduling Automatic Backups 4-7
Performing a Manual Backup 4-8
Restoring the Prime Infrastructure Database 4-8
Restoring the Prime Infrastructure Database in a High Availability Environment 4-9
Upgrading WCS to Prime Infrastructure 4-9
Upgrading Prime Infrastructure in a High Availability Environment 4-10
Upgrading the Network 4-10
Reinitializing the Database 4-10
Recovering the Prime Infrastructure Password 4-11
Performing Disk Cleanup 4-11

MONITORING DEVICES 5-1
Information About Monitoring 5-1
Monitoring Controllers 5-1
Searching Controllers 5-2
Viewing a List of Controllers 5-2
Configuring the Controller List Display 5-3
Monitoring System Parameters 5-3
  Monitoring System Summary 5-4
  Monitoring Spanning Tree Protocol 5-5
  Monitoring CLI Sessions 5-7
  Monitoring DHCP Statistics 5-8
  Monitoring WLANs 5-9
Monitoring Ports 5-9
  Monitoring General Ports 5-9
  Monitoring CDP Interface Neighbors 5-14
Monitoring Controller Security 5-15
  Monitoring RADIUS Authentication 5-15
  Monitoring RADIUS Accounting 5-17
  Monitoring Management Frame Protection 5-19
  Monitoring Rogue AP Rules 5-20
  Monitoring Guest Users 5-22
Monitoring Controller Mobility 5-23
  Monitoring Mobility Stats 5-23
Monitoring Controller 802.11a/n 5-25
  Monitoring 802.11a/n Parameters 5-25
  Monitoring 802.11a/n RRM Groups 5-27
Monitoring Controllers 802.11b/g/n 5-29
  Monitoring 802.11b/g/n Parameters 5-29
  Monitoring 802.11b/g/n RRM Groups 5-30
Monitoring Controllers IPv6 5-32
  Monitoring Neighbor Bind Counter Statistics 5-32
Monitoring mDNS Service Provider Information 5-33
Monitoring Third Party Controllers 5-33
Monitoring Switches 5-34
  Searching Switches 5-34
  Viewing the Switches 5-34
    Configuring the Switch List Page 5-34
  Monitoring Switch System Parameters 5-35
    Viewing Switch Summary Information 5-35
    Viewing Switch Memory Information 5-36
    Viewing Switch Environment Information 5-37
    Viewing Switch Module Information 5-37
    Viewing Switch VLAN Information 5-38
    Viewing Switch VTP Information 5-38
    Viewing Switch Physical Ports Information 5-38
Contents

Viewing Switch Sensor Information  5-39
Viewing Switch Spanning Tree Information  5-39
Viewing Switch Stacks Information  5-40
Viewing Switch NMSP and Location Information  5-40

Monitoring Switch Interfaces  5-41
  Monitoring Switch Ethernet Interfaces  5-41
  Monitoring Switch IP Interfaces  5-42
  Monitoring Switch VLAN Interfaces  5-42
  Monitoring Switch EtherChannel Interfaces  5-43

Monitoring Switch Clients  5-43

Monitoring Access Points  5-43
  Searching Access Points  5-44
  Viewing a List of Access Points  5-44
    Configuring the Access Point List Display  5-45
    Configuring the List of Access Points Display  5-47

Generating a Report for Access Points  5-48
  Monitoring Traffic Load  5-50
  Monitoring Dynamic Power Control  5-51
  Monitoring Access Points Noise  5-52
  Monitoring Access Points Interference  5-52
  Monitoring Access Points Coverage (RSSI)  5-53
  Monitoring Access Points Coverage (SNR)  5-53
  Monitoring Access Points Up/Down Statistics  5-53
  Monitoring the Access Points Voice Statistics  5-54
  Monitoring the Access Points Voice TSM Table  5-54
  Monitoring the Access Points Voice TSM Reports  5-56
  Monitoring Access Points 802.11 Counters  5-56
  Monitoring Access Points AP Profile Status  5-57
  Monitoring Access Points Radio Utilization  5-57
  Monitoring Access Points Traffic Stream Metrics  5-57
  Monitoring Access Points Tx Power and Channel

Monitoring VoIP Calls  5-58
  Monitoring Voice Statistics  5-58
  Monitoring Air Quality  5-58

Monitoring Access Points Details  5-58
  General Tab  5-58
  Interfaces Tab  5-65
  CDP Neighbors Tab  5-67
  Current Associated Clients Tab  5-67
  SSID Tab  5-68
## Contents

### Monitoring Chokepoints 5-115
- Performing a Chokepoint Search 5-115

### Monitoring Interferers 5-116
- Monitoring AP Detected Interferers 5-116
- Monitoring AP Detected Interferer Details 5-117
- Monitoring AP Detected Interferer Details Location History 5-118
- Configuring the Search Results Display 5-118

### Monitoring Spectrum Experts 5-119
- Spectrum Experts Summary 5-119
- Interferers Summary 5-120
- Interferers Search 5-120
- Spectrum Experts Details 5-121

### Monitoring WiFi TDOA Receivers 5-121

### Monitoring Media Streams 5-122

### Monitoring Radio Resource Management (RRM) 5-123
- Channel Change Notifications 5-123
- Transmission Power Change Notifications 5-124
- RF Grouping Notifications 5-124
- Viewing the RRM Dashboard 5-124

### Monitoring Clients and Users 5-126

### Monitoring Alarms 5-126
- Alarms and Events Overview 5-126
- Viewing List of Alarms 5-127
- Filtering Alarms 5-128
- Viewing Alarm Details 5-129
- Viewing Events Related to Alarms 5-130
- Modifying Alarms 5-130
  - Specifying Email Notifications for Alarms 5-130
- Modifying the Alarm Browser 5-131
- Viewing the Alarm Summary 5-131
- Modifying Alarm Settings 5-132
  - Modifying Alarm Count Refresh Rate 5-132
  - Configuring Alarm Severity Levels 5-132
- Working with Alarms 5-133
- Monitoring Access Point Alarms 5-135
- Monitoring Air Quality Alarms 5-135
- Monitoring CleanAir Security Alarms 5-136
- Monitoring Email Notifications 5-137
- Monitoring Severity Configurations 5-137
Monitoring Cisco Adaptive wIPS Alarms 5-138
Monitoring Cisco Adaptive wIPS Alarm Details 5-139
Monitoring Events 5-141
Searching Events 5-143
Monitoring Failure Objects 5-143
Monitoring Events for Rogue APs 5-143
Monitoring Events for Ad hoc Rogues 5-144
Monitoring Cisco Adaptive wIPS Events 5-145
Monitoring CleanAir Air Quality Events 5-146
Viewing Air Quality Event Details 5-146
Monitoring Interferer Security Risk Events 5-146
Viewing Interferer Security Risk Event Details 5-147
Monitoring Health Monitor Events 5-147
Viewing Health Monitor Event Details 5-148
Working with Events 5-148
Monitoring Site Maps 5-149
Monitoring Google Earth Maps 5-149

CHAPTER 6  Monitoring Maps 6-1
About Maps 6-1
Adding a Campus Map 6-2
Adding a Building to a Campus Map 6-3
Adding a Standalone Building 6-5
Adding Floor Areas 6-6
Adding Floor Areas to a Campus Building 6-6
Adding Floor Plans to a Standalone Building 6-9
Configuring Floor Settings 6-11
Import Map and AP Location Data 6-23
Monitoring Floor Area 6-24
Panning and Zooming with Next Generation Maps 6-24
Adding Access Points to a Floor Area 6-25
Placing Access Points 6-27
Using the Automatic Hierarchy to Create Maps 6-28
Using the Map Editor 6-31
Guidelines for Using the Map Editor 6-31
Guidelines for Placing Access Points 6-32
Guidelines for Inclusion and Exclusion Areas on a Floor 6-33
Opening the Map Editor 6-34
Map Editor Icons 6-34
Using the Map Editor to Draw Coverage Areas 6-35
Using the Map Editor to Draw Obstacles 6-36
Defining an Inclusion Region on a Floor 6-36
Defining an Exclusion Region on a Floor 6-37
Defining a Rail Line on a Floor 6-38
Adding an Outdoor Area 6-39
Using Chokepoints to Enhance Tag Location Reporting 6-40
Adding Chokepoints to the Prime Infrastructure Database 6-40
Adding a Chokepoint to a Prime Infrastructure Map 6-41
Positioning Chokepoints 6-42
Configuring Wi-Fi TDOA Receivers 6-43
Adding Wi-Fi TDOA Receivers to the Prime Infrastructure Database 6-43
Adding Wi-Fi TDOA Receivers to a Map 6-43
Positioning Wi-Fi TDOA Receivers 6-44
Managing RF Calibration Models 6-45
Accessing Current Calibration Models 6-45
Applying Calibration Models to Maps 6-46
Viewing Calibration Model Properties 6-46
Viewing Calibration Model Details 6-46
Creating New Calibration Models 6-47
Starting Calibration Process 6-47
Calibrating 6-49
Apply the Model to the Floor 6-50
Deleting Calibration Models 6-50
Managing Location Presence Information 6-50
Searching Maps 6-51
Using the Map Editor 6-52
Opening the Map Editor 6-52
Using the Map Editor to Draw Polygon Areas 6-53
Defining an Inclusion Region on a Floor 6-53
Defining an Exclusion Region on a Floor 6-55
Defining a Rail Line on a Floor 6-55
Inspecting Location Readiness and Quality 6-56
Inspecting Location Readiness 6-57
Inspecting Location Quality Using Calibration Data 6-57
Inspecting VoWLAN Readiness 6-58
Troubleshooting Voice RF Coverage Issues 6-58
Monitoring Mesh Networks Using Maps 6-59
## Contents

- Monitoring Mesh Link Statistics Using Maps 6-59
- Monitoring Mesh Access Points Using Maps 6-60
- Monitoring Mesh Access Point Neighbors Using Maps 6-62
- Viewing the Mesh Network Hierarchy 6-62
- Using Mesh Filters to Modify Map Display of Maps and Mesh Links 6-63
- Monitoring Tags Using Maps 6-65
- Using Planning Mode 6-65
  - Accessing Planning Mode 6-66
  - Using Planning Mode to Calculate Access Point Requirements 6-67
- Refresh Options 6-70
- Creating a Network Design 6-71
  - Designing a Network 6-71
- Importing or Exporting WLSE Map Data 6-73
- Monitoring Device Details 6-74
  - Floor View Navigation 6-76
  - Understanding RF Heatmap Calculation 6-77
- Monitoring Google Earth Maps 6-78
  - Creating an Outdoor Location Using Google Earth 6-78
    - Understanding Geographical Coordinates for Google Earth 6-78
    - Creating and Importing Coordinates in Google Earth (KML File) 6-79
    - Creating and Importing Coordinates as a CSV File 6-81
  - Importing a File into Prime Infrastructure 6-82
  - Viewing Google Earth Maps 6-83
    - Viewing Google Earth Map Details 6-83
    - Adding Google Earth Location Launch Points to Access Point Pages 6-84
- Google Earth Settings 6-84

### Chapter 7

#### Managing User Accounts 7-1

- Managing the Prime Infrastructure User Accounts 7-1
  - Configuring the Prime Infrastructure User Accounts 7-2
  - Deleting the Prime Infrastructure User Accounts 7-3
- Changing Passwords 7-4
  - Changing the Root User Password using CLI 7-4
- Monitoring Active Sessions 7-4
- Viewing or Editing User Account Information 7-5
  - Setting the Lobby Ambassador Defaults 7-5
- Viewing or Editing Group Information 7-6
  - Editing the Guest User Credentials 7-7
- Viewing the Audit Trail 7-7
Audit Trail Details Page  7-8
Creating Guest User Accounts  7-8
Managing the Prime Infrastructure Guest User Accounts  7-9
  Scheduling the Prime Infrastructure Guest User Accounts  7-10
  Printing or E-mailing the Prime Infrastructure Guest User Details  7-11
  Saving Guest Accounts on a Device  7-11
  Editing the Guest User Credentials  7-12
Adding a New User  7-12
  Adding User Names, Passwords, and Groups  7-12
  Assigning a Virtual Domain  7-13
Managing Lobby Ambassador Accounts  7-14
  Creating a Lobby Ambassador Account  7-14
  Editing a Lobby Ambassador Account  7-16
  Logging in to the Prime Infrastructure User Interface as a Lobby Ambassador  7-16
  Logging the Lobby Ambassador Activities  7-17

CHAPTER 8
Configuring Mobility Groups  8-1
  Information About Mobility  8-1
  Symmetric Tunneling  8-5
  Overview of Mobility Groups  8-5
  When to Include Controllers in a Mobility Group  8-7
  Messaging among Mobility Groups  8-8
Configuring Mobility Groups  8-8
  Prerequisites  8-8
  Setting the Mobility Scalability Parameters  8-10
Mobility Anchors  8-11
Configuring Multiple Country Codes  8-11
Configuring Controller Config Groups  8-12
  Adding New Group  8-12
  Configuring Config Groups  8-13
  Adding or Removing Controllers from a Config Group  8-14
  Adding or Removing Templates from the Config Group  8-14
  Applying or Scheduling Config Groups  8-15
  Auditing Config Groups  8-15
  Rebooting Config Groups  8-16
Reporting Config Groups  8-16
Download Software  8-17
  Downloading IDS Signatures  8-17
Configuring Devices 9-1

Configuring Controllers 9-1
- Understanding the Controller Audit Report 9-3
- Adding Controllers 9-4
- Bulk Update of Controller Credentials 9-7
- Removing Controllers from the Prime Infrastructure 9-8
- Rebooting Controllers 9-8
- Downloading Software to Controllers 9-9
  - Downloading Software (FTP) 9-9
  - Downloading Software (TFTP) 9-11
  - Configuring IPaddr Upload Configuration/Logs from the Controller 9-13
- Downloading IDS Signatures 9-14
- Downloading a Customized WebAuthentication Bundle to a Controller 9-15
- Downloading a Vendor Device Certificate 9-16
- Downloading a Vendor CA Certificate 9-17
- Saving the Configuration to Flash 9-18
- Refreshing the Configuration from the Controller 9-18
- Discovering Templates from the Controller 9-19
- Updating Credentials in the Prime Infrastructure 9-19
- Viewing Templates Applied to a Controller 9-20
- Using the Audit Now Feature 9-21
- Viewing the Latest Network Audit Report 9-22

Configuring Existing Controllers 9-23
- Replacing an Old Controller Model with a New Model 9-24

Configuring Controllers Properties 9-24
- Configuring Controller System Parameters 9-25
  - Managing General System Properties for Controllers 9-26
  - Configuring Controller System Commands 9-32
  - Restoring Factory Defaults 9-34
  - Setting the Controller Time and Date 9-34
  - Uploading Configuration/Logs from Controllers 9-35
  - Downloading Configurations to Controllers 9-35
  - Downloading Software to a Controller 9-36
  - Downloading a Web Admin Certificate to a Controller 9-37
  - Downloading IDS Signatures 9-37
  - Downloading a Customized Web Auth Bundle to a Controller 9-38
- Configuring Controller System Interfaces 9-39

Downloading Customized WebAuth 8-18
Adding an Interface  9-40
Viewing Current Interface Details  9-41
Deleting a Dynamic Interface  9-42
Configuring Controller System Interface Groups  9-42
  Adding an Interface Group  9-42
  Deleting an Interface Group  9-43
  Viewing Interface Groups  9-44
NAC Integration  9-44
Configuring Wired Guest Access  9-47
Creating an Ingress Interface  9-49
Creating an Egress Interface  9-49
Configuring Controller Network Routes  9-49
  Viewing Existing Network Routes  9-50
Configuring Controller Spanning Tree Protocol Parameters  9-50
Configuring Controller Mobility Groups  9-51
Configuring Controller Network Time Protocol  9-53
Background Scanning on 1510s in Mesh Networks  9-54
Configuring Controller QoS Profiles  9-56
Configuring Controller DHCP Scopes  9-57
Configuring Controller User Roles  9-58
Configuring a Global Access Point Password  9-59
Configuring Global CDP  9-59
Configuring AP 802.1X Supplicant Credentials  9-60
Configuring Controller DHCP  9-61
Configuring Controller Multicast Mode  9-62
Configuring Access Point Timer Settings  9-63
Configuring Controller WLANs  9-64
  Viewing WLAN Details  9-65
    General Tab  9-65
    Security Tab  9-66
    QoS Tab  9-71
    Advanced Tab  9-72
    Policy Configuration Tab  9-77
    Configuring Mobile Concierge (802.11u)  9-77
  Adding a WLAN  9-79
  Deleting a WLAN  9-80
  Managing WLAN Status Schedules  9-80
    Mobility Anchors  9-81
    Configuring WLANs AP Groups  9-82
    Adding Access Point Groups  9-82
Deleting Access Point Groups  9-84
Auditing Access Point Groups  9-84
Configuring Policy on a Controller  9-85
Configuring FlexConnect Parameters  9-86
  Configuring FlexConnect AP Groups  9-86
  Auditing a FlexConnect Group  9-90
Configuring Security Parameters  9-90
  Configuring Controller File Encryption  9-90
  Configuring Controllers > IPaddr > Security > AAA  9-91
  Configuring AAA General Parameters  9-91
  Configuring AAA RADIUS Auth Servers  9-91
  Configuring AAA RADIUS Acct Servers  9-92
  Configuring AAA RADIUS Fallback Parameters  9-93
  Configuring AAA LDAP Servers  9-94
  Configuring AAA TACACS+ Servers  9-96
  Configuring AAA Local Net Users  9-96
  Configuring AAA MAC Filtering  9-97
  Configuring AAA AP/MSE Authorization  9-98
  Configuring AAA Web Auth Configuration  9-99
  Configuring AAA Password Policy  9-100
  Configuring Controllers > IPaddr > Security > Local EAP  9-100
  Configuring Local EAP General Parameters  9-101
  Configuring Local EAP Profiles  9-102
  Configuring Local EAP General EAP-FAST Parameters  9-103
  Configuring Local EAP General Network Users Priority  9-104
  Configuring User Login Policies  9-104
  Managing Manually Disabled Clients  9-104
  Configuring Access Control Lists  9-105
  Configuring IPaddr > Access Control List > listname Rules  9-105
  Configuring FlexConnect Access Control Lists  9-106
  Configuring CPU Access Control Lists  9-107
  Configuring the IDS Sensor List  9-108
  Configuring CA Certificates  9-108
  Configuring ID Certificates  9-109
  Configuring Controllers > IPaddr > Security > Web Auth Certificate  9-110
  Configuring Wireless Protection Policies  9-110
  Configuring Rogue Policies  9-111
  Configuring Rogue AP Rules  9-112
  Configuring Client Exclusion Policies  9-113
  Configuring IDS Signatures  9-113
Contents

- Configuring Controller Standard Signature Parameters 9-113
- Configuring Custom Signatures 9-117
- Configuring AP Authentication and MFP 9-118
- Configuring Cisco Access Points 9-118
  - Sniffer Feature 9-119
- Configuring 802.11 Parameters 9-120
  - Configuring General Parameters for an 802.11 Controller 9-121
  - Configuring Aggressive Load Balancing 9-122
  - Configuring Band Selection 9-123
  - Configuring Preferred Call 9-124
  - Configuring 802.11 Media Parameters 9-125
- Configuring RF Profiles (802.11) 9-125
- Configuring SIP Snooping 9-126
- Configuring 802.11a/n Parameters 9-127
  - Configuring 802.11a/n General Parameters 9-127
  - Configuring 802.11a/n RRM Thresholds 9-129
  - Configuring 802.11a/n RRM Intervals 9-129
  - Configuring 802.11a/n RRM Transmit Power Control 9-130
  - Configuring 802.11a/n RRM Dynamic Channel Allocation 9-131
  - Configuring 802.11a/n RRM Radio Grouping 9-132
  - Configuring 802.11a/n Media Parameters 9-132
  - Configuring 802.11a/n EDCA Parameters 9-135
  - Configuring 802.11a/n Roaming Parameters 9-135
  - Configuring 802.11a/n 802.11h Parameters 9-136
  - Configuring 802.11a/n High Throughput (802.11n) Parameters 9-137
  - Configuring 802.11a/n CleanAir Parameters 9-137
- Configuring 802.11b/g/n Parameters 9-139
  - Configuring 802.11b/g/n General Parameters 9-139
  - Configuring 802.11b/g/n RRM Thresholds 9-140
  - Configuring 802.11b/g/n RRM Intervals 9-141
  - Configuring 802.11b/g/n RRM Transmit Power Control 9-141
  - Configuring 802.11b/g/n RRM DCA 9-142
  - Configuring 802.11b/g/n RRM Radio Grouping 9-142
  - Configuring 802.11b/g/n Media Parameters 9-143
  - Configuring 802.11b/g/n EDCA Parameters 9-145
  - Configuring 802.11b/g/n Roaming Parameters 9-146
  - Configuring 802.11b/g/n High Throughput (802.11n) Parameters 9-147
  - Configuring 802.11b/g/n CleanAir Parameters 9-147
- Configuring Mesh Parameters 9-149
  - Client Access on 1524SB Dual Backhaul 9-150
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backhaul Channel Deselection Using the Prime Infrastructure</td>
<td>9-151</td>
</tr>
<tr>
<td>Configuring Port Parameters</td>
<td>9-152</td>
</tr>
<tr>
<td>Configuring Controllers Management Parameters</td>
<td>9-152</td>
</tr>
<tr>
<td>Configuring Trap Receivers</td>
<td>9-153</td>
</tr>
<tr>
<td>Configuring Trap Control Parameters</td>
<td>9-154</td>
</tr>
<tr>
<td>Configuring Telnet SSH Parameters</td>
<td>9-155</td>
</tr>
<tr>
<td>Configuring a Syslog for an Individual Controller</td>
<td>9-156</td>
</tr>
<tr>
<td>Configuring Multiple Syslog Servers</td>
<td>9-157</td>
</tr>
<tr>
<td>Configuring WEB Admin</td>
<td>9-157</td>
</tr>
<tr>
<td>Downloading Web Auth or Web Admin Certificate to the Controller</td>
<td>9-158</td>
</tr>
<tr>
<td>Configuring Local Management Users</td>
<td>9-158</td>
</tr>
<tr>
<td>Configuring Authentication Priority</td>
<td>9-159</td>
</tr>
<tr>
<td>Configuring Location Configurations</td>
<td>9-159</td>
</tr>
<tr>
<td>Configuring IPv6</td>
<td>9-161</td>
</tr>
<tr>
<td>Configuring Neighbor Binding Timers</td>
<td>9-161</td>
</tr>
<tr>
<td>Configuring RA Throttle Policy</td>
<td>9-162</td>
</tr>
<tr>
<td>Configuring RA Guard</td>
<td>9-162</td>
</tr>
<tr>
<td>Configuring Proxy Mobile IPv6</td>
<td>9-163</td>
</tr>
<tr>
<td>Configuring PMIP Global Configurations</td>
<td>9-163</td>
</tr>
<tr>
<td>Configuring LMA Configurations</td>
<td>9-164</td>
</tr>
<tr>
<td>Configuring PMIP Profile</td>
<td>9-164</td>
</tr>
<tr>
<td>Configuring mDNS</td>
<td>9-165</td>
</tr>
<tr>
<td>Configuring AVC Profiles</td>
<td>9-166</td>
</tr>
<tr>
<td>Configuring NetFlow</td>
<td>9-167</td>
</tr>
<tr>
<td>Configuring NetFlow Monitor</td>
<td>9-167</td>
</tr>
<tr>
<td>Configuring NetFlow Exporter</td>
<td>9-168</td>
</tr>
<tr>
<td>Configuring Third-Party Controllers and Access Points</td>
<td>9-168</td>
</tr>
<tr>
<td>Adding a Third-Party Controller</td>
<td>9-169</td>
</tr>
<tr>
<td>Viewing Third-Party Controller Operational Status</td>
<td>9-169</td>
</tr>
<tr>
<td>Viewing the Details of Third-Party Access Points</td>
<td>9-170</td>
</tr>
<tr>
<td>Removing Third-Party Access Points</td>
<td>9-170</td>
</tr>
<tr>
<td>Viewing Third-Party Access Point Operational Status</td>
<td>9-171</td>
</tr>
<tr>
<td>Configuring Access Points</td>
<td>9-171</td>
</tr>
<tr>
<td>Setting AP Failover Priority</td>
<td>9-172</td>
</tr>
<tr>
<td>Configuring Global Credentials for Access Points</td>
<td>9-173</td>
</tr>
<tr>
<td>Configuring Ethernet Bridging and Ethernet VLAN Tagging</td>
<td>9-174</td>
</tr>
<tr>
<td>Ethernet VLAN Tagging Guidelines</td>
<td>9-175</td>
</tr>
<tr>
<td>Enabling Ethernet Bridging and VLAN Tagging</td>
<td>9-177</td>
</tr>
<tr>
<td>Autonomous to Lightweight Migration Support</td>
<td>9-178</td>
</tr>
<tr>
<td>Adding Autonomous Access Points to the Prime Infrastructure</td>
<td>9-179</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Viewing Autonomous Access Points in Prime Infrastructure</td>
<td>9-183</td>
</tr>
<tr>
<td>Downloading Images to Autonomous Access Points (TFTP)</td>
<td>9-183</td>
</tr>
<tr>
<td>Downloading Images to Autonomous Access Points (FTP)</td>
<td>9-184</td>
</tr>
<tr>
<td>Supporting Autonomous Access Points in Work Group Bridge (WGB) mode</td>
<td>9-184</td>
</tr>
<tr>
<td>Configuring Access Point Details</td>
<td>9-184</td>
</tr>
<tr>
<td>Configuring an Ethernet Interface</td>
<td>9-193</td>
</tr>
<tr>
<td>Viewing the Deleted AP Jobs</td>
<td>9-193</td>
</tr>
<tr>
<td>Importing AP Configuration</td>
<td>9-194</td>
</tr>
<tr>
<td>Exporting AP Configuration</td>
<td>9-195</td>
</tr>
<tr>
<td>Configuring Access Points 802.11n Antenna</td>
<td>9-195</td>
</tr>
<tr>
<td>Configuring CDP</td>
<td>9-198</td>
</tr>
<tr>
<td>Configuring CDP on Access Points</td>
<td>9-198</td>
</tr>
<tr>
<td>Configuring Access Point Radios for Tracking Optimized Monitor Mode</td>
<td>9-199</td>
</tr>
<tr>
<td>Copying and Replacing Access Points</td>
<td>9-199</td>
</tr>
<tr>
<td>Removing Access Points</td>
<td>9-200</td>
</tr>
<tr>
<td>Scheduling and Viewing Radio Status</td>
<td>9-200</td>
</tr>
<tr>
<td>Scheduling Radio Status</td>
<td>9-200</td>
</tr>
<tr>
<td>Viewing Scheduled Tasks</td>
<td>9-201</td>
</tr>
<tr>
<td>Viewing Audit Status (for Access Points)</td>
<td>9-201</td>
</tr>
<tr>
<td>Filtering Alarms for Maintenance Mode Access Points</td>
<td>9-202</td>
</tr>
<tr>
<td>Placing an Access Point in Maintenance State</td>
<td>9-202</td>
</tr>
<tr>
<td>Removing an Access Point from Maintenance State</td>
<td>9-203</td>
</tr>
<tr>
<td>Searching Access Points</td>
<td>9-203</td>
</tr>
<tr>
<td>Viewing Mesh Link Details</td>
<td>9-204</td>
</tr>
<tr>
<td>Viewing or Editing Rogue Access Point Rules</td>
<td>9-204</td>
</tr>
<tr>
<td>Configuring Switches</td>
<td>9-205</td>
</tr>
<tr>
<td>Features Available by Switch Type</td>
<td>9-205</td>
</tr>
<tr>
<td>Viewing Switches</td>
<td>9-205</td>
</tr>
<tr>
<td>Viewing Switch Details</td>
<td>9-206</td>
</tr>
<tr>
<td>Modifying SNMP Parameters</td>
<td>9-207</td>
</tr>
<tr>
<td>Modifying Telnet/SSH Parameters</td>
<td>9-207</td>
</tr>
<tr>
<td>Adding Switches</td>
<td>9-208</td>
</tr>
<tr>
<td>Configuring SNMPv3 on Switches</td>
<td>9-209</td>
</tr>
<tr>
<td>Sample CSV File for Importing Switches</td>
<td>9-209</td>
</tr>
<tr>
<td>Configuring Switch NMSP and Location</td>
<td>9-210</td>
</tr>
<tr>
<td>Enabling and Disabling NMSP for Switches</td>
<td>9-211</td>
</tr>
<tr>
<td>Configuring a Switch Location</td>
<td>9-211</td>
</tr>
<tr>
<td>Configuring a Switch Port Location</td>
<td>9-211</td>
</tr>
<tr>
<td>Removing Switches</td>
<td>9-212</td>
</tr>
<tr>
<td>Refreshing Switch Configuration</td>
<td>9-212</td>
</tr>
</tbody>
</table>
Enabling Traps and Syslogs on Switches for Wired Client Discovery  9-213
   MAC Notification for Traps (Used for Non-Identity Client Discovery)  9-213
   Syslog Configuration  9-214
Configuring Unknown Devices  9-214
Configuring Spectrum Experts  9-215
   Adding a Spectrum Expert  9-215
   Monitoring Spectrum Experts  9-216
      Viewing Spectrum Experts Summary  9-216
      Viewing Interferers Summary  9-216
      Viewing Spectrum Experts Details  9-217
   OfficeExtend Access Point  9-217
      Licensing for an OfficeExtend Access Point  9-218
Configuring Link Latency Settings for Access Points  9-218
Configuring Chokepoints  9-219
   Configuring New Chokepoints  9-219
      Adding a Chokepoint to Prime Infrastructure Database  9-219
      Adding a Chokepoint to an Prime Infrastructure Map  9-220
      Removing a Chokepoint from an Prime Infrastructure Map  9-221
      Removing a Chokepoint from Prime Infrastructure  9-221
   Editing Current Chokepoints  9-222
Configuring Spectrum Experts  9-222
   Adding a Spectrum Expert  9-222
   Spectrum Experts Details  9-223
Configuring Wi-Fi TDOA Receivers  9-223
   Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting  9-223
   Adding Wi-Fi TDOA Receivers to Prime Infrastructure and Maps  9-224
   Viewing or Editing Current Wi-Fi TDOA Receivers  9-226
   Removing Wi-Fi TDOA Receivers from Prime Infrastructure and Maps  9-226
Configuring Scheduled Configuration Tasks  9-227
Configuring Auto Provisioning for Controllers  9-227
Configuring Redundancy on Controllers  9-228
Configuring wIPS Profiles  9-228
   Profile List  9-229
      Adding a Profile  9-229
      Profile Editor  9-230
      Deleting a Profile  9-232
      Applying a Current Profile  9-233
   Configure > wIPS > SSID Group List  9-233
   Global SSID Group List  9-234
CHAPTER 10
Managing Clients

Client Dashlets on the General Dashboard

Client Dashboard
- Client Troubleshooting Dashlet
- Client Distribution Dashlet
  - Client Authentication Type Distribution
- Client Alarms and Events Summary Dashlet
- Client Traffic Dashlet
- Wired Client Speed Distribution Dashlet
- Top 5 SSIDs by Client Count
- Top 5 Switches by Switch Count
- Client Posture Status Dashlet
- Client Count By IP Address Type
- IPv6 Assignment Distribution
- User Auth Failure Count
- Client Protocol Distribution
- Client EAP Type Distribution
- Guest Users Count
- Client CCX Distribution
- Top N Client Count
- Client Mobility Status Distribution
- Client 11u Distribution
- 11u Client Count
- 11u Client Traffic
- PMIP Clients Distribution
- PMIP Client Count
- Top APs By Client Count
- Most Recent Client Alarms
Recent 5 Guest User Accounts 10-9
Latest 5 logged in Guest Users 10-9
Clients Detected by Context Aware Service 10-9
Monitoring Clients and Users 10-9
Filtering Clients and Users 10-10
Viewing Clients and Users 10-12
  Client Attributes 10-15
  Client IPv6 Addresses 10-16
  Client Statistics 10-17
  Client Association History 10-17
  Client Event Information 10-18
  Client Location Information 10-18
  Wired Location History 10-19
  Wireless Location History 10-19
  Client CCXv5 Information 10-19
Exporting Clients and Users 10-21
Client Troubleshooting 10-21
Tracking Clients 10-30
  Notification Settings 10-30
Identifying Unknown Users 10-31
  Configuring the Search Results Display 10-32
Enabling Automatic Client Troubleshooting 10-32
Viewing Client Details in the Access Point Page 10-33
Viewing Currently Associated Clients 10-33
Running Client Reports 10-33
Running ISE Reports 10-33
Specifying Client Settings 10-33
Receiving Radio Measurements for a Client 10-33
  Radio Measurement Results for a Client 10-34
Viewing Client V5 Statistics 10-35
Viewing Client Operational Parameters 10-36
Viewing Client Profiles 10-38
Disabling a Current Client 10-38
Removing a Current Client 10-39
Enabling Mirror Mode 10-39
Viewing a Map (High Resolution) of a Client Recent Location 10-39
Viewing a Map (High Resolution) of a Client Current Location 10-39
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running a Client Sessions Report for the Client</td>
</tr>
<tr>
<td>Viewing a Roam Reason Report for the Client</td>
</tr>
<tr>
<td>Viewing Detecting Access Point Details</td>
</tr>
<tr>
<td>Viewing Client Location History</td>
</tr>
<tr>
<td>Viewing Voice Metrics for a Client</td>
</tr>
</tbody>
</table>

**CHAPTER 11**

**Using Templates** 11-1

- Information About Templates 11-1
- Accessing the Controller Template Launch Pad 11-1
- Adding Controller Templates 11-2
- Deleting Controller Templates 11-2
- Applying Controller Templates 11-2
- Configuring Controller Templates 11-4
  - Configuring System Templates 11-4
    - Configuring General Templates 11-5
    - Configuring SNMP Community Controller Templates 11-7
    - Configuring an NTP Server Template 11-9
    - Configuring User Roles Controller Templates 11-9
    - Configuring AP Username Password Controller Templates 11-10
    - Configuring AP 802.1X Supplicant Credentials 11-11
    - Configuring a Global CDP Configuration Template 11-11
    - Configuring DHCP Templates 11-12
    - Configuring Dynamic Interface Templates 11-13
    - Configuring QoS Templates 11-15
    - Configuring AP Timers Templates 11-16
    - Configuring an Interface Group Template 11-17
    - Configuring a Traffic Stream Metrics QoS Template 11-17
  - Configuring WLAN Templates 11-18
    - Configuring WLAN Templates 11-19
    - Security Tab 11-21
    - QoS Tab 11-27
    - Advanced Tab 11-28
    - Policy Configuration Tab 11-33
    - Configuring Client Profiling 11-34
    - Configuring Mobile Concierge (802.11u) 11-35
    - Configuring WLAN AP Groups Templates 11-37
    - Adding Access Point Groups 11-37
    - Deleting Access Point Groups 11-39
Configuring Policy Configuration Templates 11-39
Configuring FlexConnect Templates 11-40
  Configuring FlexConnect AP Groups Templates 11-40
  Configuring FlexConnect Users 11-43
Configuring Security Templates 11-44
  Configuring a General Security Controller Template 11-44
  Configuring a File Encryption Template 11-45
  Configuring a RADIUS Authentication Template 11-45
  Configuring a RADIUS Accounting Template 11-47
  Configuring a RADIUS Fallback Template 11-48
  Configuring an LDAP Server Template 11-49
  Configuring a TACACS+ Server Template 11-50
  Configuring a Local EAP General Template 11-51
  Configuring a Local EAP Profile Template 11-52
  Configuring an EAP-FAST Template 11-53
  Configuring a Network User Priority Template 11-54
  Configuring a Local Network Users Template 11-54
Guest User Templates 11-55
  Configuring a User Login Policies Template 11-56
  Configuring a MAC Filter Template 11-57
  Configuring an Access Point or MSE Authorization Template 11-58
  Configuring a Manually Disabled Client Template 11-58
  Configuring a Client Exclusion Policies Template 11-59
  Configuring an Access Point Authentication and MFP Template 11-60
  Configuring a Web Authentication Template 11-61
  Configuring an External Web Auth Server Template 11-64
  Configuring a Security Password Policy Template 11-64
Configuring Security - Access Control Templates 11-64
  Configuring an Access Control List Template 11-65
  Configuring a FlexConnect Access Control List Template 11-67
  Configuring an ACL IP Groups Template 11-69
  Configuring an ACL Protocol Groups Template 11-70
Configuring Security - CPU Access Control List Templates 11-71
  Configuring a CPU Access Control List (ACL) Template 11-71
Configuring Security - Rogue Templates 11-72
  Configuring a Rogue Policies Template 11-72
  Configuring a Rogue AP Rules Template 11-73
  Configuring a Rogue AP Rule Groups Template 11-75
  Configuring a Friendly Access Point Template 11-76
  Configuring Ignored Rogue AP Templates 11-77
Configuring 802.11 Templates  11-78
   Configuring Load Balancing Templates  11-78
   Configuring Band Selection Templates  11-79
   Configuring Preferred Call Templates  11-79
   Configuring Media Stream for Controller Templates (802.11)  11-80
   Configuring RF Profiles Templates (802.11)  11-81
   Configuring SIP Snooping  11-83

Configuring Radio Templates (802.11a/n)  11-83
   Configuring 802.11a/n Parameters Templates  11-83
   Configuring Media Parameters Controller Templates (802.11a/n)  11-85
   Configuring EDCA Parameters Through a Controller Template (802.11a/n)  11-88
   Configuring a Roaming Parameters Template (802.11a/n)  11-88
   Configuring an 802.11h Template  11-90
   Configuring a High Throughput Template (802.11a/n)  11-90
   Configuring CleanAir Controller Templates (802.11a/n)  11-91
   Configuring 802.11a/n RRM Templates  11-92

Configuring Radio Templates (802.11b/g/n)  11-96
   Configuring 802.11b/g/n Parameters Templates  11-97
   Configuring Media Parameters Controller Templates (802.11b/g/n)  11-99
   Configuring EDCA Parameters Controller Templates (802.11b/g/n)  11-101
   Configuring Roaming Parameters Controller Templates (802.11b/g/n)  11-102
   Configuring High Throughput (802.11n) Controller Templates (802.11b/g/n)  11-103
   Configuring CleanAir Controller Templates (802.11 b/g/n)  11-104
   Configuring 802.11b/g/n RRM Templates  11-105

Configuring Mesh Templates  11-110
   Configuring Mesh Setting Templates  11-110

Configuring Management Templates  11-111
   Configuring Trap Receiver Templates  11-111
   Configuring Trap Control Templates  11-111
   Configuring Telnet SSH Templates  11-113
   Configuring Legacy Syslog Templates  11-114
   Configuring Multiple Syslog Templates  11-114
   Configuring Local Management User Templates  11-115
   Configuring User Authentication Priority Templates  11-116

Configuring CLI Templates  11-116
   Applying a Set of CLI Commands  11-116

Configuring Location Configuration Templates  11-117

Configuring IPv6 Templates  11-118
   Configuring Neighbor Binding Timers Templates  11-119
   Configuring RA Throttle Policy Templates  11-119
Configuring RA Guard Templates 11-120
Configuring Proxy Mobile IPv6 Templates 11-120
Configuring PMIP Global Configurations 11-121
Configuring LMA Configurations 11-121
Configuring PMIP Profile 11-122
Configuring mDNS Templates 11-122
Configuring AVC Profiles Templates 11-124
Configuring NetFlow Templates 11-125
Configuring NetFlow Monitor Template 11-125
Configuring NetFlow Exporter Template 11-126
Configuring AP Configuration Templates 11-126
Configuring Lightweight Access Point Templates 11-127
Configuring a New Lightweight Access Point Template 11-127
Selecting Access Points for Template Deployment 11-133
Scheduling Template Deployment 11-133
Viewing the Status of the Template Deployment 11-134
Editing a Current Lightweight Access Point Template 11-134
Configuring Autonomous Access Point Templates 11-134
Configuring a New Autonomous Access Point Template 11-135
Applying an AP Configuration Template to an Autonomous Access Point 11-135
Configuring Switch Location Configuration Templates 11-136
Configuring Autonomous AP Migration Templates 11-137
Migrating an Autonomous Access Point to a Lightweight Access Point 11-137
Editing Current Autonomous AP Migration Templates 11-138
Viewing the Migration Analysis Summary 11-140
Adding/Modifying a Migration Template 11-140
Copying a Migration Template 11-142
Deleting Migration Templates 11-142
Viewing the Current Status of Cisco IOS Access Points 11-142
Disabling Access Points that are Ineligible 11-143

CHAPTER 12
Configuring FlexConnect 12-1
Information About FlexConnect 12-1
FlexConnect Authentication Process 12-2
FlexConnect Guidelines 12-4
Configuring FlexConnect 12-4
Configuring the Switch at the Remote Site 12-5
Configuring the Controller for FlexConnect 12-6
Configuring an Access Point for FlexConnect 12-8
Connecting Client Devices to the WLANs  12-9
FlexConnect Access Point Groups  12-9
FlexConnect Groups and Backup RADIUS Servers  12-10
FlexConnect Groups and CCKM  12-11
FlexConnect Groups and Local Authentication  12-11
Configuring FlexConnect Groups  12-11
Auditing a FlexConnect Group  12-13

**CHAPTER 13**

**Alarm and Event Dictionary**  13-1
What is an Event?  13-1
What is an Alarm?  13-1
Unsupported Traps  13-2

**CHAPTER 14**

**Reports**  14-1
Non Upgradable Reports from the WCS to Prime Infrastructure  14-1

**CHAPTER 15**

**Performing Administrative Tasks**  15-1

**CHAPTER 16**

**Prime Infrastructure Services**  16-1
Mobility Services  16-1
Location Service  16-1
wIPS  16-1
Mobile Concierge Service  16-2
CMX Analytics Service  16-2
CMX Connect and Engage Service  16-2
Cisco Context-Aware Mobility Solution  16-2
Cisco Prime Infrastructure  16-3
WLAN Controllers  16-3
Access Points  16-3
Cisco Mobility Services Engines  16-4
Accessing Services  16-4
Licensing Information for MSE  16-4
Viewing Current Mobility Services  16-5
Adding a Mobility Services Engine  16-6
Deleting an MSE License File  16-10
Deleting MSEs from Prime Infrastructure  16-10
Installing Device and wIPS License Files  16-11
Adding a Location Server  16-11
Synchronizing Services  16-12
Keeping Mobility Services Engines Synchronized 16-12
Synchronizing the Prime Infrastructure and a Mobility Services Engine 16-12
Synchronizing Controllers with Mobility Services Engines 16-14
Working with Third-Party Elements 16-15
Setting and Verifying the Timezone on a Controller 16-16
Configuring Smart Mobility Services Engine Database Synchronization 16-17
Out-of-Sync Alarms 16-18
Viewing Mobility Services Engine Synchronization Status 16-19
Viewing Synchronization History 16-19
Viewing Notification Statistics 16-20
Configuring High Availability 16-20
Managing System Properties for a Mobility Services Engine 16-20
Editing General Properties for a Mobility Services Engine 16-21
Editing NMSP Parameters for a Mobility Services Engine 16-23
Viewing Active Session Details for a Mobility Services Engine 16-24
Viewing and Adding Trap Destinations for a Mobility Services Engine 16-24
Editing Advanced Parameters for a Mobility Services Engine 16-26
Rebooting the Mobility Services Engine Hardware 16-27
Shutting Down the Mobility Services Engine Hardware 16-27
Clearing the Mobility Services Engine Database 16-27
Working with Logs 16-28
Managing User and Group Accounts for a Mobility Services Engine 16-29
Monitoring Status Information for a Mobility Services Engine 16-32
Viewing Server Events for a Mobility Services Engine 16-32
Viewing Audit Logs from a Mobility Services Engine 16-32
Viewing Prime Infrastructure Alarms for a Mobility Services Engine 16-33
Viewing Prime Infrastructure Events for a Mobility Services Engine 16-33
Viewing NMSP Connection Status for a Mobility Services Engine 16-33
Managing Maintenance for Mobility Services 16-35
Viewing or Editing Mobility Services Backup Parameters 16-35
Backing Up Mobility Services Engine Historical Data 16-35
Restoring Mobility Services Engine Historical Data 16-36
Downloading Software to a Mobility Services Engine Using the Prime Infrastructure 16-37
Configuring Partner System for a Mobility Services Engine 16-37
Qualcomm PDS Configuration 16-37
MSE-Qualcomm Configuration 16-38
Managing Cisco Adaptive wIPS Service Parameters 16-39
Managing Context-Aware Service Software Parameters 16-39
Context-Aware Service General Parameters 16-40
Context-Aware Service Administration Parameters 16-41
Modifying Tracking Parameters for Mobility Services  16-41
Filtering Parameters for Mobility Services  16-45
Modifying History Parameters for Mobility Services  16-48
Enabling Location Presence for Mobility Services  16-49
Importing Asset Information for Mobility Services  16-50
Exporting Asset Information for Mobility Services  16-50
Importing Civic Information for Mobility Services  16-51
Context-Aware Service Wired Parameters  16-51
Monitoring Interferers  16-54
Context-Aware Service Advanced Parameters  16-59
Modifying Northbound Notifications  16-59
Modifying Location Parameters for Mobility Services  16-60
Modifying Notification Parameters for Mobility Services  16-63
Viewing Partner Engine Status  16-64
Viewing Notification Information for Mobility Services  16-65
Viewing the Notifications Summary for Mobility Services  16-65
Viewing and Managing Notifications for Mobility Services  16-67
Viewing Notification Statistics  16-67
Mobile Concierge Service Parameters  16-68
Viewing the Configured Service Advertisements  16-68
Viewing Mobile Concierge Service Statistics  16-68
About Event Groups  16-69
Adding Event Groups  16-69
Deleting Event Groups  16-69
Working with Event Definitions  16-70
Adding Event Definitions  16-72
Deleting an Event Definition  16-76
Client Support on MSE  16-76
Searching a Wireless Client from the Prime Infrastructure on the MSE by IPv6 Address  16-76
Viewing the Clients Detected by the MSE  16-78
Upgrading from 5.0 to 6.0 or 7.0  16-83
Viewing the MSE Alarm Details  16-85
MSE License Overview  16-87
MSE License Structure Matrix  16-87
Sample an MSE License File  16-87
Revoking and Reusing an MSE License  16-88
Deploying the MSE Virtual Appliance  16-88
Adding a License File to the MSE Using the License Center  16-89
Viewing the MSE License Information using License Center  16-89
Removing a License File Using the License Center  16-90
| Contents |
|-----------------|----------------------|
| Auto Switch Port Tracing and Auto Containment of Rogue APs | 16-90 |
| Configuring Auto Switch Port Tracing Criteria on the Prime Infrastructure | 16-91 |
| Configuring Auto Containing Settings on the Prime Infrastructure | 16-91 |
| Location Assisted Client Troubleshooting from the Context Aware Dashboard | 16-92 |
| MSE Analytics Reports | 16-93 |
| Monitoring Maps | 16-93 |
| Disabling Mobility Services Engine Admin View | 16-93 |
| Mobile Concierge Service | 16-94 |
| Licensing for Mobile Concierge | 16-94 |
| Defining a Venue | 16-94 |
| Deleting the Venue | 16-95 |
| Defining a Provider with Policies | 16-95 |
| Deleting the Provider | 16-96 |
| Defining New Policies | 16-96 |
| Deleting New Policies | 16-97 |
| Adding Service Advertisements to the Floor Map | 16-98 |
| Creating Service Advertisements from the Floor Map | 16-98 |
| Viewing the Configured Service Advertisements | 16-99 |
| Viewing Mobile Concierge Service Statistics | 16-100 |
| Viewing the MSE Summary Page for Mobile Concierge License Information | 16-100 |
| Viewing Service Advertisements Synchronization Status | 16-100 |
| Adding a Mobile Concierge Service License Using the License Center | 16-101 |
| Mobile Concierge Reports | 16-101 |
| Identity Services | 16-102 |
| Viewing Identify Services | 16-102 |
| Adding an Identity Services Engine | 16-103 |
| Removing an Identity Services Engine | 16-103 |
| Mobility Services Engine Admin User Interface | 16-103 |
| Launching the MSE Admin User Interface | 16-104 |

**CHAPTER 17**

**Tools**

<table>
<thead>
<tr>
<th>Tools</th>
<th>17-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running Voice Audits</td>
<td>17-1</td>
</tr>
<tr>
<td>Running Voice Diagnostic</td>
<td>17-1</td>
</tr>
<tr>
<td>Configuring the Location Accuracy Tools</td>
<td>17-1</td>
</tr>
<tr>
<td>Configuring Audit Summary</td>
<td>17-2</td>
</tr>
<tr>
<td>Configuring Migration Analysis</td>
<td>17-2</td>
</tr>
<tr>
<td>Configuring TAC Case Attachments</td>
<td>17-2</td>
</tr>
</tbody>
</table>
wIPS Policy Alarm Encyclopedia     18-1

Security IDS/IPS Overview     18-1

Intrusion Detection—Denial of Service Attack     18-2

Denial of Service Attack Against Access Points     18-3
  Denial of Service Attack: Association Flood     18-3
  Denial of Service Attack: Association Table Overflow     18-4
  Denial of Service Attack: Authentication Flood     18-5
  Denial of Service Attack: EAPOL-Start Attack     18-6
  Denial of Service Attack: PS Poll Flood     18-6
  Denial of Service Attack: Probe Request Flood     18-7
  Denial of Service Attack: Re-association Request Flood     18-7
  Denial of Service Attack: Unauthenticated Association     18-8

Denial of Service Attack Against Infrastructure     18-9
  Denial of Service Attack: Beacon Flood     18-10
  Denial of Service Attack: MDK3-Destruction Attack     18-10
  Denial of Service Attack: CTS Flood     18-11
  Denial of Service Attack: Queensland University of Technology Exploit     18-11
  Denial of Service attack: RF Jamming     18-12
  Denial of Service: RTS Flood     18-13
  Denial of Service Attack: Virtual Carrier Attack     18-14

Denial of Service Attack Against Station     18-15
  Denial of Service Attack: Authentication-Failure Attack     18-16
  Denial of Service Attack: Block ACK Flood     18-17
  Denial of Service Attack: De-Auth Broadcast Flood     18-18
  Denial of Service Attack: De-Auth Flood     18-19
  Denial of Service Attack: Dis-Assoc Broadcast Flood     18-20
  Denial of Service Attack: Dis-Assoc Flood     18-22
  Denial of Service Attack: EAPOL-Logoff Attack     18-23
  Denial of Service Attack: FATA-Jack Tool     18-23
  Denial of Service Attack: Premature EAP-Failure     18-25
  Denial of Service Attack: Premature EAP-Success     18-25
  Denial of Service Attack: Probe Reponse Flood     18-26

Intrusion Detection—Security Penetration     18-27
  ASLEAP Tool Detected     18-28
  AirDrop Session Detected     18-29
  AirPwn     18-30
  Airsnarf Attack     18-30
  Bad EAP-TLS Frames     18-32
  Beacon Fuzzed Frame Detected     18-32
Brute Force Hidden SSID 18-32
DHCP Starvation Attack Detected 18-33
Chopchop Attack 18-33
Day-0 Attack by WLAN Performance Anomaly 18-35
Day-0 Attack by WLAN Security Anomaly 18-36
Day-0 Attack by Device Performance Anomaly 18-37
Day-0 Attack by Device Security Anomaly 18-39
Device Broadcasting XSS SSID 18-40
Device Probing for APs 18-40
Dictionary Attack on EAP Methods 18-42
EAP Attack Against 802.1x Authentication 18-43
Fake Access Points Detected 18-43
Fake DHCP Server Detected 18-44
Fast WEP Crack Tool Detected 18-44
Fragmentation Attack 18-45
HT_Intolerant Degradation of Service 18-47
Identical Send and Receive Address 18-47
Improper Broadcast Frames 18-47
Karma Tool Detected 18-48
Hot-Spotter Tool Detected 18-48
Malformed 802.11 Packets Detected 18-50
Man-in-the-Middle Attack 18-50
Monitored Device Detected 18-51
NetStumbler Detected 18-52
NetStumbler Victim Detected 18-53
Publicly Secure Packet Forwarding (PSPF) Violation Detected 18-54
Probe Request Fuzzed Frame Detected 18-55
Probe Response Fuzzed Frame Detected 18-56
Honey Pot AP Detected 18-56
Soft AP or Host AP Detected 18-57
Spoofed MAC Address Detected 18-57
Suspicious After-Hours Traffic Detected 18-58
Unauthorized Association by Vendor List 18-58
Unauthorized Association Detected 18-59
Wellenreiter Detected 18-60
WiFi Protected Setup Pin Brute Force 18-61
WiFiTap Tool Detected 18-62

Troubleshooting and Best Practices A-1
Troubleshooting Cisco-compatible Extensions Version 5 Client Devices A-1
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagnostic Channel</td>
<td>A-1</td>
</tr>
<tr>
<td>Configuring the Diagnostic Channel</td>
<td>A-2</td>
</tr>
<tr>
<td>Web Auth Security on WLANs</td>
<td>A-2</td>
</tr>
<tr>
<td>Debug Commands</td>
<td>A-3</td>
</tr>
<tr>
<td>Debug Strategy</td>
<td>A-3</td>
</tr>
<tr>
<td>RF Heatmap Analysis</td>
<td>A-8</td>
</tr>
<tr>
<td>Best Practices</td>
<td>A-8</td>
</tr>
<tr>
<td>Troubleshooting RAID Card Configuration</td>
<td>A-8</td>
</tr>
<tr>
<td>Applying for a Cisco.com Account with Cryptographic Access</td>
<td>A-9</td>
</tr>
<tr>
<td>Performing Disk Cleanup</td>
<td>A-9</td>
</tr>
<tr>
<td>Checking on System Disk Usage</td>
<td>A-10</td>
</tr>
<tr>
<td>Replacing an Old Controller Model with a New Model</td>
<td>A-10</td>
</tr>
</tbody>
</table>

**Cisco Prime Infrastructure Server Hardening** B-1

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prime Infrastructure Password Handling</td>
<td>B-1</td>
</tr>
<tr>
<td>Setting Up SSL Certification</td>
<td>B-1</td>
</tr>
<tr>
<td>Setting Up SSL Client Certification</td>
<td>B-2</td>
</tr>
<tr>
<td>Setting Up SSL Server Certification</td>
<td>B-3</td>
</tr>
</tbody>
</table>

**Certificate Signing Request (CSR) Generation for a Third-Party Certificate on Cisco Prime Infrastructure** C-1

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>C-1</td>
</tr>
<tr>
<td>Certificate Signing Request (CSR)</td>
<td>C-2</td>
</tr>
<tr>
<td>Generating a Certificate Signing Request (CSR) File</td>
<td>C-2</td>
</tr>
<tr>
<td>Get a Signed Certificate for CSR from Microsoft Certificate Authority (CA)</td>
<td>C-3</td>
</tr>
<tr>
<td>Importing a Certificate Authority (CA) Certificate and Key</td>
<td>C-4</td>
</tr>
<tr>
<td>Viewing the list of Certificates</td>
<td>C-4</td>
</tr>
<tr>
<td>Deleting Certificates</td>
<td>C-5</td>
</tr>
<tr>
<td>Related Publications</td>
<td>C-5</td>
</tr>
</tbody>
</table>
Cisco Prime Infrastructure Overview

Cisco Prime Infrastructure is a network management tool that supports lifecycle management of your entire network infrastructure from one graphical interface. Prime Infrastructure provides network administrators with a single solution for provisioning, monitoring, optimizing, and troubleshooting both wired and wireless devices. Robust graphical interfaces make device deployments and operations simple and cost-effective.

Prime Infrastructure provides two different graphical user interfaces (from which you can switch back and forth by clicking the downward arrow next to your login name):

- Lifecycle view, which is organized according to home, design, deploy, operate, report and administer menus.
- Classic view, which closely corresponds to the graphical user interface in the Cisco Prime Network Control System 1.1 or Cisco Wireless Control System (WCS).

The Cisco Prime Infrastructure enables you to configure and monitor one or more controllers, switches and associated access points. Prime Infrastructure includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points.

On Linux, the Prime Infrastructure runs as a service, which runs continuously and resumes running after a reboot.

Prime Infrastructure simplifies controller configuration and monitoring and reduces data entry errors. Prime Infrastructure uses the industry-standard SNMP protocol to communicate with the controllers. Prime Infrastructure also includes the Floor Plan editor, which allows you to do the following:

- Access vectorized bitmap campus, floor plan, and outdoor area maps.
- Add and change wall types.
- Import the vector wall format maps into the database.

The vector files allow the Cisco Prime Infrastructure RF Prediction Tool to make better RF predictions based on more accurate wall and window RF attenuation values.

For information on browser requirement, see the Cisco Prime Infrastructure 2.2 Quick Start Guide at the following URL:


This chapter describes the different components in Cisco Unified Network and contains the following sections:

- Cisco Unified Network Components, page 1-2
- Access Point Communication Protocols, page 1-4
Cisco Unified Network Components

The Cisco Unified Wireless Network (CUWN) solution is based on Cisco wireless LAN controllers running Airespace Operating System. The wireless LAN controller models include 2100, 2500, 4400, WiSM/WiSM2 (6500 service module), 5500, 7500, 8500. In this solution, access points tunnel the wireless traffic to the controllers through CAPWAP.

The Cisco Unified Access (UA) Wireless Solution is new architecture that provides a converged model where you can manage your wired and wireless network configurations in the same place. This solution includes the Catalyst 3850 series switch with integrated wireless support. The solution also includes the 5760 series wireless controller, which can act as an aggregation point for many Catalyst 3850 switches. This platform is based on Cisco IOS-XE, so the command structure is similar to other Cisco IOS products. In this solution, the wireless traffic can terminate directly on the Catalyst 3850 switch, so that it can be treated in a similar mode to a wired connection on the switch. This section describes the different components in the Cisco Unified Network.

- Cisco Wireless LAN Controller, page 1-2
- Virtual LAN Controllers, page 1-2
- Access Points, page 1-3

Cisco Wireless LAN Controller

The Cisco wireless LAN controllers are highly scalable and flexible platforms that enable system wide services for mission-critical wireless in medium to large-sized enterprises and campus environments. Designed for 802.11n performance and maximum scalability, the Cisco WLAN controllers offer enhanced uptime with the ability to simultaneously manage from 5000 access points to 250 access points; superior performance for reliable streaming video and toll quality voice; and improved fault recovery for a consistent mobility experience in the most demanding environments.

Prime Infrastructure supports the Cisco wireless LAN controllers that help reduce the overall operational expense of Cisco Unified Networks by simplifying network deployment, operations, and management. See the Release Notes for Cisco Prime Infrastructure, Release 2.2 for a list of Cisco wireless LAN controllers supported by Prime Infrastructure.

Virtual LAN Controllers

The virtual wireless LAN controller is a software that can run on a hardware that is compliant with an industry standard virtualization infrastructure. Virtual Wireless LAN Controllers provide flexibility for users to select the hardware based on their requirement.

When you view or configure the properties of a virtual wireless LAN controller using the controller configuration page, the Prime Infrastructure displays the value of the Device Type as VWLC (Configure > Controllers > IP address > Properties > Settings).

Features Not Supported by Virtual LAN Controllers

The following is a list of features that are not supported by VLAN controllers:
Access Points

Prime Infrastructure supports the industry-leading performance access points for highly secure and reliable wireless connections for both indoor and outdoor environments. Prime Infrastructure supports a broad portfolio of access points targeted to the specific needs of all industries, business types, and topologies.

See the Release Notes for Cisco Prime Infrastructure, Release 2.2 for a list of access points supported by Prime Infrastructure.

Embedded Access Points

Prime Infrastructure supports the AP801, which is the integrated access point on the Cisco 800 Series Integrated Services Routers (ISRs). This access point uses a Cisco IOS software image that is separate from the router Cisco IOS software image. It can operate as an autonomous access point that is configured and managed locally, or it can operate as a centrally managed access point using CAPWAP or LWAPP protocol. The AP801 is preloaded with both an autonomous Cisco IOS software release and a recovery image for the unified mode.

When you want to use the AP801 with a controller, you must enable the recovery image for the unified mode on the access point by entering the service-module wlan-ap 0 bootimage unified command on the router in privileged EXEC mode.

If the service-module wlan-ap 0 bootimage unified command does not work, make sure that the software license is current.

After enabling the recovery image, enter the service-module wlan-ap 0 reload command on the router to shut down and reboot the access point. After the access point reboots, it discovers the controller, downloads the full CAPWAP or LWAPP software release from the controller, and acts as a lightweight access point.
Access Point Communication Protocols

In controller software Release 5.2 or later, Cisco lightweight access points use the IETF standard Control and Provisioning of Wireless Access Points (CAPWAP) protocol to communicate between the controller and other lightweight access points on the network. Controller software releases prior to 5.2 use the Lightweight Access Point Protocol (LWAPP) for these communications.

CAPWAP, which is based on LWAPP, is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points. CAPWAP is being implemented in controller software Release 5.2 for the following reasons:
To provide an upgrade path from Cisco products that use LWAPP to next-generation Cisco products that use CAPWAP

To manage RFID readers and similar devices

To enable controllers to interoperate with third-party access points in the future

LWAPP-enabled access points are compatible with CAPWAP, and conversion to a CAPWAP controller is seamless. For example, the controller discovery process and the firmware downloading process when using CAPWAP are the same as when using LWAPP. The one exception is for Layer 2 deployments, which are not supported by CAPWAP.

Deployments can combine CAPWAP and LWAPP software on the controllers. The CAPWAP-enabled software allows access points to join either a controller running CAPWAP or LWAPP. The only exception is the Cisco Aironet 1140 Series Access Point, which supports only CAPWAP and therefore joins only controllers running CAPWAP.

**Note**

The Cisco Aironet 1140 series and 3500 series access points associate only with CAPWAP controllers that run Cisco WLC versions 7.0 or later.

- Guidelines and Restrictions for Using CAPWAP, page 1-5
- WLAN Controller Autodiscovery, page 1-5
- The Controller Discovery Process, page 1-6

**Guidelines and Restrictions for Using CAPWAP**

- CAPWAP and LWAPP controllers cannot be used in the same mobility group. Therefore, client mobility between CAPWAP and LWAPP controllers is not supported.
- If your firewall is currently configured to allow traffic only from access points using LWAPP, you must change the rules of the firewall to allow traffic from access points using CAPWAP.
- Make sure that the CAPWAP ports are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.
- Any access control lists (ACLs) in your network might need to be modified if CAPWAP uses different ports than LWAPP.

**WLAN Controller Autodiscovery**

Controller Autodiscovery is limited to the Cisco WLAN Solution mobility group subnets defined by the operator.

The Cisco Wireless LAN Controller Autodiscovery:

- Allows operators to search for a single controller by IP address.
- Finds the controller on the network within the specified IP address range.
- Automatically enters the controller information into the Cisco Prime Infrastructure database.

**Note**

Controller Autodiscovery can take a long time in a Class C address range. Because of the large number of addresses in a Class B or Class A range, we recommend that you do not attempt Autodiscovery across Class B or Class A ranges.
As access points associate with a controller, the controller immediately transmits the access point information to Cisco Prime Infrastructure, which automatically adds the access point to the database. Once the access point information is added to the Cisco Prime Infrastructure database, operators can add the access point to the appropriate spot on a Cisco Prime Infrastructure user interface map.

The Controller Discovery Process

In a CAPWAP environment, a lightweight access point discovers a controller by using CAPWAP discovery mechanisms and then sends it a CAPWAP join request. The controller sends the access point a CAPWAP join response allowing the access point to join the controller. When the access point joins the controller, the controller manages its configuration, firmware, control transactions, and data transactions.

Lightweight access points must be discovered by a controller before they can become an active part of the network. The lightweight access points support the following controller discovery processes:

- **Layer 3 CAPWAP or LWAPP discovery**—Can occur on different subnets from the access point and uses IP addresses and UDP packets rather than the MAC addresses used by Layer 2 discovery.
- **Over-the-air provisioning (OTAP)**—This feature is supported by Cisco 4400 series controllers. If this feature is enabled on the controller (in the controller General page), all associated access points transmit wireless CAPWAP or LWAPP neighbor messages, and new access points receive the controller IP address from these messages. This feature is disabled by default and should remain disabled when all access points are installed.
- **Locally stored controller IP address discovery**—If the access point was previously associated to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the non-volatile memory of an access point. This process of storing controller IP addresses on access points for later deployment is called **priming the access point**.
- **DHCP server discovery**—This feature uses DHCP option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability.
- **DNS discovery**—The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-CAPWAP-CONTROLLER.localdomain or CISCO-LWAPP-CONTROLLER.localdomain, where localdomain is the access point domain name. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.localdomain or CISCO-LWAPP-CONTROLLER.localdomain. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.

Prime Infrastructure Services

The IT departments within organizations are tasked with meeting increased bandwidth and performance demands, managing a proliferation of new mobile devices, while guaranteeing network access, availability, and regulatory compliance.

Cisco and its partners can work with IT staff to assist with migration to the Cisco Unified Network, making it easier to manage a secure, high-performance, and integrated wired and wireless network that incorporates rich media and diverse mobile devices, including Wi-Fi-enabled phones and tablets.
This section describes the services provided by the Prime Infrastructure and contains the following topics:

- Cisco Context-Aware Service Solution, page 1-7
- Cisco Identity Service Engine Solution, page 1-7
- Cisco Adaptive Wireless Intrusion Prevention Service, page 1-8

**Cisco Context-Aware Service Solution**

Context-Aware Service (CAS) provides the capability for a Wi-Fi 802.11a/b/g/n network to determine the location of a person or object with an active Wi-Fi device, such as a wireless client or active RFID tag and/or associated data that can be passed by the end point through the wireless infrastructure to an upstream client.

Context-Aware Service (CAS) allows a mobility services engine (MSE) to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as location and availability from Cisco access points.

The collected contextual information can be viewed in GUI format in the Prime Infrastructure User Interface, the centralized WLAN management platform. Prime Infrastructure is the management system that interfaces with the MSE and serves the user interface (UI) for the services that the MSE provides.

After the MSE installation and initial configurations are complete, the MSE can communicate with multiple Cisco wireless LAN controllers to collect operator-defined contextual information. You can then use the associated Prime Infrastructure to communicate with each MSE to transfer and display selected data.

You can configure the MSE to collect data for clients, switches, rogue access points, rogue clients, mobile stations, and active RFID asset tags.

With Context-Aware Location Services, administrators can determine the location of any 802.11-based device, as well as the specific type or status of each device. Clients (associated, probing, and so on.), rogue access points, rogue clients, and active tags can all be identified and located by the system. See the Context-Aware Mobility Solution Deployment Guide for more information.

**Note**

One MSE can be managed by only one Prime Infrastructure, that is, a single MSE cannot be managed by more than one Prime Infrastructure, but a single Prime Infrastructure can manage multiple MSEs. When the number of devices to be managed exceeds the capacity of a single MSE, you need to deploy multiple, independent MSEs.

**Cisco Identity Service Engine Solution**

The Cisco Identity Services Engine (ISE) is a next-generation identity and policy-based network access platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations.

The Cisco ISE provides a single console where authentication, authorization, posture, guest, and profiling policies can be created and managed. In addition, policy elements can now be reused across all services, reducing the number of tasks and overhead and bringing consistency to the enterprise.
The Cisco ISE gathers information from devices, the infrastructure, and services to enable organizations to build richer contextual policies that can be enforced centrally across the network. The ISE tracks all clients and devices connected to the network, acting as a single source of information for connected user and device identity and location, as well as the health of the endpoint.

The ability to discover, identify, and monitor all IP-enabled endpoint devices gives IT teams complete visibility of both users and “headless” devices on the corporate network.

The Cisco ISE combines AAA, posture, profiling, and guest management capabilities in a single appliance to enforce dynamic access control. The Identity Services Engine can be deployed across the enterprise infrastructure, supporting 802.1x wired, wireless, and VPN networks.

Prime Infrastructure manages the wired and the wireless clients in the network. When Cisco ISE is used as a RADIUS server to authenticate clients, the Prime Infrastructure collects additional information about these clients from Cisco ISE and provides all client relevant information to the Prime Infrastructure to be visible in a single console.

When posture profiling is enforced in the network, the Prime Infrastructure talks to Cisco ISE to get the posture data for the clients and displays it along with other client attributes. When Cisco ISE is used to profile the clients or an endpoint in the network, the Prime Infrastructure collects the profiled data to determine what type of client it is, whether it is an iPhone, iPad, an Android device, or any other device.

Cisco ISE is assisting the Prime Infrastructure to monitor and troubleshoot client information, and displays all the relevant information for a client in a single console.

**Cisco Adaptive Wireless Intrusion Prevention Service**

Maintain a constant awareness of your RF environment to minimize legal liability, protect your brand reputation, and assure regulatory compliance.

Cisco Adaptive Wireless Intrusion Prevention System (IPS) offers advanced network security for dedicated monitoring and detection of wireless network anomalies, unauthorized access, and RF attacks. Fully integrated with the Cisco Unified Network, this solution delivers integrated visibility and control across the network, without the need for an overlay solution.

Cisco Adaptive Wireless Intrusion Prevention Service (wIPS) performs rogue access point, rogue client, and ad-hoc connection detection and mitigation, over-the-air wireless hacking and threat detection, security vulnerability monitoring, performance monitoring and self-optimization, network hardening for proactive prevention of threats and complete wireless security management and reporting.

Cisco wIPS is made up of the following components that work together to provide a unified security monitoring solution:

- Mobility services engine (MSE) running wIPS software—Serves as the central point of alarm aggregation for all controllers and their respective wIPS monitor mode access points. Alarm information and forensic files are stored on the mobility services engine for archival purposes.
- A wIPS monitor mode access point—Provides constant channel scanning with attack detection and forensics (packet capture) capabilities.
- Local mode access point—Provides wireless service to clients in addition to time-sliced rogue scanning.
- Wireless LAN Controller—Forwards attack information received from wIPS monitor mode access points to the mobility services engine and distributes configuration parameters to access points.
Prime Infrastructure—Provides a centralized management platform for the administrator to configure the wIPS Service on the mobility services engine, push wIPS configurations to the controller, and configure access points in wIPS monitor mode. Prime Infrastructure is also used to view wIPS alarms, forensics, reporting, and to access the attack encyclopedia.
Getting Started

Cisco Prime Infrastructure is an application used to configure, manage, and monitor the wired and wireless networks. The Prime Infrastructure home page, is the landing page, displaying real-time monitoring and troubleshooting data. The navigation tabs and menus at the top of the page provide point-and-click access to all other administration features. The Prime Infrastructure home page allows you to:

- Create and configure Cisco Unified Network Solution coverage area layouts, configure system operating parameters, monitor real-time Cisco Unified Network Solution operations, and perform troubleshooting tasks using an HTTPS web browser page.
- Create, modify, and delete user accounts; change passwords; assign permissions; and schedule periodic maintenance tasks. The administrator creates new usernames and passwords and assigns them to predefined permissions groups.
- Perform all necessary network administration tasks from one page.

Prime Infrastructure user interface provides an integrated network administration console from which you can manage various devices and services. These include wired and wireless devices, and clients. The services might include authentication, authorization, profiler, location and mobility services, monitoring, troubleshooting, and reporting. All of these devices and services can be managed from a single console called the Prime Infrastructure home page.

This section describes the Prime Infrastructure user interface page and contains the following topics:

- Menu Bar, page 2-1
- Global Toolbar, page 2-2

Menu Bar

The primary form of navigation used in the Prime Infrastructure is the menu located at the top of the Prime Infrastructure page. Administrators can monitor and perform various tasks from this menu. This menu is an easy-access, pop-up menu that provides quick access to the submenus that are associated with the primary menu. Hover your mouse cursor over any menu title to access the associated menu. Clicking the menu title takes you directly to the feature page.

The following table describes the high-level task areas or menus available in Prime Infrastructure.
Global Toolbar

The Global toolbar is always available at the bottom of the Prime Infrastructure page, providing instantaneous access to the tools, Prime Infrastructure online Help system, and a summary of alarm notifications. Hover your mouse cursor over the Help icon to access the available online Help (see Figure 2-1).

Hover your mouse cursor over the Alarms Browser to display the summarized Alarms page, with a list of recent system alarms and the ability to filter for alarms of a specific nature. You can also drill down for detailed information on individual alarms. For more information on Alarms, see the “Alarm Summary” section on page 2-3.

Figure 2-1 Global Toolbar

- Tools, page 2-2
- Help, page 2-3
- Alarm Summary, page 2-3

Tools

The Tools menu provides access to the Voice Audit, Location Accuracy Tools, Configuration Audit, Migration Analysis, and TAC Case Attachment features of the Prime Infrastructure.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
<th>Used By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home</td>
<td>View dashboards, which give you a quick view of devices, performance information, and various incidents. See dashboards and Dashlets for more information.</td>
<td>Network Engineers</td>
</tr>
<tr>
<td>Monitor</td>
<td>Monitor your network on a daily basis and perform other day-to-day or ad hoc operations related to network devices (controllers, switches, access points, clients, tags, chokepoints, Wi-Fi TDOA receivers) and configuration management. You can also monitor maps, Google Earth maps, RRM, alarms, and events.</td>
<td>Network Engineers, NOC Operators, and Service Operators</td>
</tr>
<tr>
<td>Configure</td>
<td>Configure templates, controllers, access points, switches, chokepoints, Wi-Fi TDOA receivers, config groups, auto provisioning, scheduled configuration tasks, profiles, ACS view servers, and TFTP servers on your network.</td>
<td>Network Engineers, Designers, and Architects</td>
</tr>
<tr>
<td>Services</td>
<td>Manage mobility services including mobility services engines and identity service engines.</td>
<td>Service Operators</td>
</tr>
<tr>
<td>Reports</td>
<td>Create reports, view saved report templates, and run scheduled reports.</td>
<td>Network Engineers, NOC Operators, and Service Operators</td>
</tr>
<tr>
<td>Administration</td>
<td>Specify system configuration settings and data collection settings, and manage access control. You can view and approve jobs, specify health rules, and manage licenses.</td>
<td>Network Engineers</td>
</tr>
</tbody>
</table>
Help

The Help menu allows you to access online help, learning modules, submit feedback, and to verify the current version of the Prime Infrastructure. The Help icon is located in the bottom left corner of the Global Toolbar in the Prime Infrastructure page. The Help provides quick access to the comprehensive online Help for the Prime Infrastructure.

The following submenu options are available from the Help drop-down menu:

- Online Help—Enables you to view online Help. The online Help is context sensitive and opens documentation for the Prime Infrastructure window that you currently have open.
- Learning Modules—Allows you to access short video clips of certain Prime Infrastructure features. To learn more about the Cisco Prime Infrastructure features and functionality, go to Cisco.com to watch multimedia presentations about the Prime Infrastructure configuration workflow, monitoring, troubleshooting, and more. Over future releases, more overview and technical presentations will be added to enhance your learning.
- MSE Installation Guide—Provides links to the MSE installation section.
- Submit Feedback— Allows you to access a page where you can enter feedback about the Prime Infrastructure.
- Help Us Improve Cisco Products— Allows you to enable and provide permission to automatic collect data about how you and your organization use your Cisco wireless products, this data is useful to improve product performance and usability. The data is automatically collected and sent to Cisco in encrypted form. The data might contain information about your organization and it is not be shared or used outside of Cisco.

Note

To get the automated feedback enabled, you must configure your Mail Server Configuration by choosing Administration > Settings > Mail Server Configuration.

- About Cisco Prime Infrastructure—Allows you to verify the version of the Prime Infrastructure that you are running. It provides the version number, hostname, feature, AP limit, and license type.

Alarm Summary

The Alarm Summary launches the alarm summary window that displays all alarms and indicates the number of critical, major, and minor alarms.

For information on other Prime Infrastructure user interface components such as, dashboards and dashlets, filters, data entry features, 360° view, and search methods, see the Prime Infrastructure User Interface Reference appendix in the Cisco Prime Infrastructure 2.2 User Guide.

For information on system requirements, licenses, setting up and starting Prime Infrastructure, see Cisco Prime Infrastructure 2.2 Quick Start Guide.
CHAPTER 3

Configuring Security Solutions

This chapter describes the security solutions for wireless LANs. It contains the following sections:

- Cisco Unified Wireless Network Solution Security, page 3-1
- Interpreting the Security Dashboard, page 3-4
- Rogue Access Points, Ad hoc Events, and Clients, page 3-9
- Rogue Access Point Location, Tagging, and Containment, page 3-12
- Security Overview, page 3-19
- Switch Port Tracing, page 3-27
- Using Prime Infrastructure to Convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 Mode, page 3-28
- Configuring a Firewall for Prime Infrastructure, page 3-29
- Access Point Authorization, page 3-29
- Management Frame Protection (MFP), page 3-30
- Configuring Intrusion Detection Systems (IDS), page 3-32
- Configuring IDS Signatures, page 3-32
- Enabling Web Login, page 3-37
- Certificate Signing Request (CSR) Generation, page 3-40

Cisco Unified Wireless Network Solution Security

The Cisco Unified Wireless Network Solution bundles potentially complicated Layer 1, Layer 2, and Layer 3 802.11 access point security components into a simple policy manager that customizes system-wide security policies on a per wireless LAN basis. It provides simple, unified, and systematic security management tools.

One of the challenges to wireless LAN deployment in the enterprise is Wired Equivalent Privacy (WEP) encryption, which is a weak standalone encryption method. A more recent problem is the availability of low-cost access points that can be connected to the enterprise network and used to mount man-in-the-middle and denial of service attacks. Also, the complexity of add-on security solutions has prevented many IT managers from embracing the benefits of the latest advances in wireless LAN security.

- Layer 1 Solutions, page 3-2
Layer 1 Solutions

The Cisco Unified Wireless Network Solution operating system security solution ensures that all clients gain access within an operator-set number of attempts. Should a client fail to gain access within that limit, it is automatically excluded (blocked from access) until the operator-set timer expires. The operating system can also disable SSID broadcasts on a per wireless LAN basis.

Layer 2 Solutions

If a higher level of security and encryption is required, the network administrator can also implement industry-standard security solutions such as 802.1X dynamic keys with Extensible Authentication Protocol (EAP) or Wi-Fi Protected Access (WPA) dynamic keys. The Cisco Unified Wireless Network Solution WPA implementation includes Advanced Encryption Standard (AES), Temporal Key Integrity Protocol + message integrity code checksum (TKIP + Michael MIC) dynamic keys, or static WEP keys. Disabling is also used to automatically block Layer 2 access after an operator-set number of failed authentication attempts.

Regardless of the wireless security solution selected, all Layer 2 wired communications between controllers and access points are secured by passing data through Lightweight Access Point Protocol (LWAPP) tunnels.

Layer 3 Solutions

The WEP problem can be further solved using industry-standard Layer 3 security solutions such as Virtual Private Networks (VPNs).

The Cisco Unified Wireless Network Solution supports local and RADIUS Media Access Control (MAC) filtering. This filtering is best suited to smaller client groups with a known list of 802.11 access card MAC addresses. The Cisco Unified Wireless Network Solution also supports local and RADIUS user/password authentication. This authentication is best suited to small to medium client groups.

Single Point of Configuration Policy Manager Solutions

When the Cisco Unified Wireless Network Solution is equipped with the Cisco Prime Infrastructure, you can configure system-wide security policies on a per wireless LAN basis. Small office, home office (SOHO) access points force you to individually configure security policies on each access point or use a third-party appliance to configure security policies across multiple access points. Because the Cisco Unified Wireless Network Solution security policies can be applied across the whole system from the Prime Infrastructure, errors can be eliminated, and the overall effort is greatly reduced.
Rogue Access Point Solutions

This section describes security solutions for rogue access points and contains the following topics:

- Rogue Access Point Challenges, page 3-3
- Tagging and Containing Rogue Access Points, page 3-3
- Securing Your Network Against Rogue Access Points, page 3-3

Rogue Access Point Challenges

Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain text, 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 passwords and usernames. The hacker can then transmit a series of clear-to-send (CTS) frames, which mimics an access point informing a particular wireless LAN client adapter to transmit and instructing all others to wait. This scenario results in legitimate clients being unable to access the wireless LAN resources. Thus, wireless LAN service providers have a strong interest in banning rogue access points from the air space.

The operating system security solution uses the Radio Resource Management (RRM) function to continuously monitor all nearby access points, automatically discover rogue access points, and locate them as described in the “Tagging and Containing Rogue Access Points” section on page 3-3.

Tagging and Containing Rogue Access Points

When the Cisco Unified Wireless Network Solution is monitored using the Prime Infrastructure, the Prime Infrastructure generates the flags as rogue access point traps and displays the known rogue access points by MAC address. The operator can then display a map showing the location of the access points closest to each rogue access point. The next step is to mark them as Known or Acknowledged rogue access points (no further action), Alert rogue access points (watch for and notify when active), or Contained rogue access points (have between one and four access points discourage rogue access point clients by sending the clients deauthenticate and disassociate messages whenever they associate with the rogue access point).

Securing Your Network Against Rogue Access Points

You can secure your network against any rogue access points and disallow access point attacks for those access points not defined in the MAC filter list.

To set up MAC filtering, follow these steps:

1. Choose Configure > Controllers.
2. Click the IP address for which you want to enter MAC filters.
3. Choose Security > AAA > MAC Filtering from the left sidebar menu. The MAC Filtering page appears. The RADIUS compatibility mode, MAC delimiter, MAC address, profile name, interface, and description appears.
4. If you want to set the same configuration across multiple devices, you can choose Add MAC Filter from the Select a command drop-down list, and click Go. If a template exists, you can apply it. If you need to create a template, you can click the URL to get redirected to the template creation page.
Interpreting the Security Dashboard

Because unauthorized rogue access points are inexpensive and readily available, employees sometimes plug them into existing LANs and build ad hoc wireless networks without IT department 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. Even more alarming, wireless users frequently publish insecure access point locations, increasing the odds of having the enterprise security breached.

Rather than having a person with a scanner manually detect rogue access points, the Cisco Unified Wireless Network Solution automatically collects information on rogue access points detected by its managed access points (by MAC and IP address) and allows the system operator to locate, tag, and contain them. It can also be used to discourage rogue access point clients by sending them deauthenticate and disassociate messages from one to four access points.

For a summary of existing events and the security state of the network, click the Security dashboard from the Prime Infrastructure home page.

This section describes the Security dashboard, dashlets and contains the following topics:

- Security Index, page 3-4
- Malicious Rogue Access Points, page 3-5
- Adhoc Rogues, page 3-6
- CleanAir Security, page 3-6
- Unclassified Rogue Access Points, page 3-7
- Friendly Rogue Access Points, page 3-7
- Access Point Threats or Attacks, page 3-8
- MFP Attacks, page 3-8
- Attacks Detected, page 3-8

You can customize the order of information you want the Security dashboard to display. You can move the dashlets to change the order. Use the Edit Dashlet icon to customize the information displayed in the dashlet. You can change the dashlet title, enable refresh, and set the refresh time interval using the Edit Dashlet icons.

Security Index

The Security Index dashlet indicates the security of the Prime Infrastructure managed network, and it is calculated as part of daily background tasks. It is calculated by assigning weight to the various security configurations and displaying it in visual form. The combined weighting can vary from 0 to 100 where...
0 signifies the least secured and 100 is the maximum secured. The weighting comes from the lowest scoring controller and the lowest scoring Location Server/Mobility Service Engine related security configurations that are maintained within the Prime Infrastructure itself. The Security Index of the Prime Infrastructure managed network is equal to the lowest scoring controller plus the lowest scoring Location Service/Mobility Service Engine.

The security thermometer color range is represented as follows:

- Above or equal to 80 - Green
- Below 80 but greater than or equal to 60 - Yellow
- Below 60 - Red

Note: The security index calculation includes the WLANs that is configured with only Layer 3 security.

The security index of the latest release is the benchmark for the required security configurations. For example, if AES encryption was not present in an earlier version of code, the index is reduced by the number associated with the AES encryption security configuration. Likewise, if new security configurations are introduced, the weighting would be altered.

Note: The configurations stored in the Prime Infrastructure might not be the latest with the ones in the controllers unless the Refresh from Controller command is run from the Prime Infrastructure. You can run Security Index calculations from the Configuration Sync task to get the latest configuration data from all the controllers.

### Malicious Rogue Access Points

This dashlet provides information on rogue access points that are classified as Malicious. Table 3-1 describes the various parameters. For each of these parameters, a value is provided for last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a page with further information appears.

Note: Malicious access points are detected as untrusted or unknown access points with a malicious intent within the system. They also refer to access points that fit the user-defined malicious rules or have been manually moved from the friendly access point classification.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>Indicates the number of rogues in an alert state.</td>
</tr>
<tr>
<td></td>
<td>Note: An access point is moved to Alert if it is not on the neighbor list or part of the user-configured Friendly AP list.</td>
</tr>
<tr>
<td>Contained</td>
<td>Indicates the number of contained rogues.</td>
</tr>
</tbody>
</table>
Interpreting the Security Dashboard

Table 3-1 Malicious Rogue AP Details (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat</td>
<td>Indicates the number of threat rogues.</td>
</tr>
<tr>
<td>Contained Pending</td>
<td>Indicates the number of contained rogues pending.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Contained Pending indicates that the containment action is delayed due to unavailable resources.</td>
</tr>
</tbody>
</table>

Adhoc Rogues

The Adhoc Rogues dashlet displays the rogues that have occurred in the last hour, last 24 hours, and the total active. Table 3-2 describes the various parameters. If you click the number in any of these columns, a page with further information appears.

Note The Adhoc Rogue state is displayed as Alert when first scanned by the controller or as Pending when operating system identification is underway.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>Indicates the number of ad hoc rogues in an alert state.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> An access point is moved to Alert if it is not on the neighbor list or part of the user-configured Friendly AP list.</td>
</tr>
<tr>
<td>Contained</td>
<td>Indicates the number of contained rogues.</td>
</tr>
<tr>
<td>Threat</td>
<td>Indicates the number of threat rogues.</td>
</tr>
<tr>
<td>Contained Pending</td>
<td>Indicates the number of contained rogues pending.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Contained pending indicates that the containment action is delayed due to unavailable resources.</td>
</tr>
</tbody>
</table>

CleanAir Security

This dashlet provides information on CleanAir security and provides information about the security-risk devices active during the last hour, 24 hours, and Total Active security-risk devices on the wireless network.

The following information is displayed:

- Severity
- Failure Source
- Owner
- Date/Time
- Message
- Acknowledged

To learn more about the security-risk interferers, see the “Monitoring CleanAir Security Alarms” section on page 5-136.
Unclassified Rogue Access Points

Table 3-3 describes the unclassified rogue access point parameters. For each of these parameters, a value is provided for last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a page with further information appears.

**Note**
An unclassified rogue access point refers to a rogue access point that is not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>Number of unclassified rogues in alert state. Rogue access point radios appear as Alert when first scanned by the controller or as Pending when operating system identification is underway.</td>
</tr>
<tr>
<td>Contained</td>
<td>Number of contained unclassified rogues.</td>
</tr>
<tr>
<td>Contained Pending</td>
<td>Number of contained unclassified rogues pending.</td>
</tr>
</tbody>
</table>

Friendly Rogue Access Points

This dashlet provides information on rogue access points that are classified as friendly. Table 3-4 describes the various parameters. For each of these parameters, a value is provided for last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a page with further information appears.

**Note**
Friendly rogue access points are known, acknowledged, or trusted access points. They also refer to access points that fit the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>Indicates the number of rogues in an alert state.</td>
</tr>
<tr>
<td>Note</td>
<td>An access point is moved to Alert if it is not on the neighbor list or part of the user-configured Friendly AP list.</td>
</tr>
<tr>
<td>Internal</td>
<td>Indicates the number of internal access points.</td>
</tr>
<tr>
<td>Note</td>
<td>Internal indicates that the detected access point is inside the network and has been manually configured as Friendly - Internal.</td>
</tr>
<tr>
<td>External</td>
<td>Indicates the number of external access points.</td>
</tr>
<tr>
<td>Note</td>
<td>External indicates that the detected access point is outside of the network and has been manually configured as Friendly - External.</td>
</tr>
</tbody>
</table>
Interpreting the Security Dashboard

**Access Point Threats or Attacks**

Table 3-5 describes the AP Threats or Attacks parameters. For each of these parameters, a value is provided for last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a page with further information appears.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fake Attacks</td>
<td>Number of fake attacks.</td>
</tr>
<tr>
<td>AP Missing</td>
<td>Number of missing access points.</td>
</tr>
<tr>
<td>AP Impersonation</td>
<td>Number of access point impersonations.</td>
</tr>
<tr>
<td>AP Invalid SSID</td>
<td>Number of invalid access point SSIDs.</td>
</tr>
<tr>
<td>AP Invalid Preamble</td>
<td>Number of invalid access point preambles.</td>
</tr>
<tr>
<td>AP Invalid Encryption</td>
<td>Number of invalid access point encryption.</td>
</tr>
<tr>
<td>AP Invalid Radio Policy</td>
<td>Number of invalid access point radio policies.</td>
</tr>
<tr>
<td>Denial of Service (NAV related)</td>
<td>Number of Denial of Service (NAV related) request.</td>
</tr>
<tr>
<td>AP Detected Duplicate IP</td>
<td>Number of detected duplicate access point IPs.</td>
</tr>
</tbody>
</table>

**MFP Attacks**

A value is provided for Infrastructure and client MFP attacks in the last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a page with further information appears.

**Attacks Detected**

A value is provided for wIPS Denial of Service and wIPS Security Penetration attacks and custom signature attacks for the past hour, past 24 hours, and total active. If you click an underline number in any of the time period categories, a page with further information appears.

**Recent Rogue AP Alarms**

A value is provided for the five most recent rogue alarms. Click the number in parentheses to access the Alarms page. Then click an item under MAC address to view alarm details.

**Recent Adhoc Rogue Alarm**

Displays the five most recent ad hoc rogue alarms. Click the number in parentheses to access the Alarms page. Click an item under MAC address to view ad hoc details.

**Most Recent Security Alarms**

Displays the five most recent security alarms. Click the number in parentheses to access the Alarms page.
Rogue Access Points, Ad hoc Events, and Clients

This section describes security solutions for rogue devices. A rogue device is an unknown access point or client that is detected by managed access points in your network.

Controllers continuously monitor all nearby access points and automatically discover and collect information on rogue access points and clients. When a controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) to determine if the rogue is attached to your network.

Note
Prime Infrastructure consolidates all of the rogue access point data of the controller.

You can configure controllers to use RLDP on all access points or only on access points configured for monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded RF space, allowing monitoring without creating unnecessary interference and without affecting regular data access point functionality. If you configure a controller to use RLDP on all access points, the 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 either manually or automatically contain the detected rogue.

- Classifying Rogue Access Points, page 3-9
- Rogue Access Point Classification Types, page 3-10
- Adhoc Rogue, page 3-12

Classifying Rogue Access Points

Classification and reporting of rogue access points occurs through the use of rogue states and user-defined classification rules that enable rogues to automatically move between states. You can create rules that enable the controller to organize and display rogue access points as Friendly, Malicious, or Unclassified.

Note
Prime Infrastructure consolidates all of the rogue access point data of the controller.

By default, none of the classification rules are enabled. Therefore, all unknown access points are categorized as Unclassified. When you create a rule, configure conditions for it, and enable the rule, the unclassified access points are reclassified. Whenever you change a rule, it is applied to all access points (friendly, malicious, and unclassified) in the Alert state only.

Note
Rule-based rogue classification does not apply to ad hoc rogues and rogue clients.

Note
The 5500 series controllers support up to 2000 rogues (including acknowledged rogues); the 4400 series controllers, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch support up to 625 rogues; and the 2100 series controllers and Controller Network Module for Integrated Services Routers support up to 125 rogues. Each controller limits the number of rogue containments to three per radio (or six per radio for access points in monitor mode).
When the controller receives a rogue report from one of its managed access points, it responds as follows:

1. The controller verifies that the unknown access point is in the friendly MAC address list. If it is, the controller classifies the access point as Friendly.

2. If the unknown access point is not in the friendly MAC address list, the controller starts applying rogue classification rules.

3. If the rogue is already classified as Malicious, Alert or Friendly, Internal or External, the controller does not reclassify it automatically. If the rogue is classified differently, the controller reclassifies it automatically only if the rogue is in the Alert state.

4. The controller applies the first rule based on priority. If the rogue access point matches the criteria specified by the rule, the controller classifies the rogue according to the classification type configured for the rule.

5. If the rogue access point does not match any of the configured rules, the controller classifies the rogue as Unclassified.

6. The controller repeats the previous steps for all rogue access points.

7. If RLDP determines that the rogue access point is on the network, the controller marks the rogue state as Threat and classifies it as Malicious automatically, even if no rules are configured. You can then manually contain the rogue (unless you have configured RLDP to automatically contain the rogue), which would change the rogue state to Contained. If the rogue access point is not on the network, the controller marks the rogue state as Alert, and you can manually contain the rogue.

8. If desired, you can manually move the access point to a different classification type and rogue state.

As mentioned previously, the controller can automatically change the classification type and rogue state of an unknown access point based on user-defined rules, or you can manually move the unknown access point to a different classification type and rogue state. Table 3-6 shows the allowable classification types and rogue states from and to which an unknown access point can be configured.

### Table 3-6 Allowable Classification Type and Rogue State Transitions

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friendly (Internal, External, Alert)</td>
<td>Malicious (Alert)</td>
</tr>
<tr>
<td>Friendly (Internal, External, Alert)</td>
<td>Unclassified (Alert)</td>
</tr>
<tr>
<td>Friendly (Alert)</td>
<td>Friendly (Internal, External)</td>
</tr>
<tr>
<td>Malicious (Alert, Threat)</td>
<td>Friendly (Internal, External)</td>
</tr>
<tr>
<td>Malicious (Contained, Contained Pending)</td>
<td>Malicious (Alert)</td>
</tr>
<tr>
<td>Unclassified (Alert, Threat)</td>
<td>Friendly (Internal, External)</td>
</tr>
<tr>
<td>Unclassified (Contained, Contained Pending)</td>
<td>Unclassified (Alert)</td>
</tr>
<tr>
<td>Unclassified (Alert)</td>
<td>Malicious (Alert)</td>
</tr>
</tbody>
</table>

If the rogue state is Contained, you have to uncontain the rogue access point before you can change the classification type. If you want to move a rogue access point from Malicious to Unclassified, you must delete the access point and allow the controller to reclassify it.

### Rogue Access Point Classification Types

Rogue access points classification types include the following:
Malicious—Detected but untrusted or unknown access points with a malicious intent within the system. They also refer to access points that fit the user-defined malicious rules or have been manually moved from the friendly access point classification. See the “Malicious Rogue Access Points” section on page 3-5 for more information.

Friendly—Known, acknowledged, or trusted access points. They also refer to access points that fit the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained. See the “Friendly Rogue APs” section on page 3-11 for more information. For more information on configuring friendly access point rules, see the “Configuring a Friendly Access Point Template” section on page 11-76.

Unclassified—Rogue access point that are not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list. See the “Unclassified Rogue APs” section on page 3-12 for more information.

Malicious Rogue APs

Malicious rogue access points are detected but untrusted or unknown access points with a malicious intent within the system. They also refer to access points that fit the user-defined malicious rules or have been manually moved from the friendly access point classification.

The Security dashboard of the Prime Infrastructure home page displays the number of malicious rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active malicious rogue access points.

Malicious rogue access point states include the following:

- Alert—Indicates that the access point is not on the neighbor list or part of the user-configured Friendly AP list.
- Contained—The unknown access point is contained.
- Threat—The unknown access point is found to be on the network and poses a threat to WLAN security.
- Contained Pending—Indicates that the containment action is delayed due to unavailable resources.
- Removed—This unknown access point was seen earlier but is not seen now.

Click an underlined number in any of the time period categories for detailed information regarding the malicious rogue access points. See the “Monitoring Rogue Access Points” section on page 5-89 for more information.

Friendly Rogue APs

Friendly rogue access points are known, acknowledged or trusted access points. They also refer to access points that fit the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained.

The Security dashboard of the Prime Infrastructure home page displays the number of friendly rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active friendly rogue access points.

Friendly rogue access point states include the following:

- Internal—If the unknown access point is inside the network and poses no threat to WLAN security, you would manually configure it as Friendly, Internal. For example, the access points in your lab network.
- External—If the unknown access point is outside the network and poses no threat to WLAN security, you would manually configure it as Friendly, External. For example, the access points belonging to a neighboring coffee shop.
Rogue Access Point Location, Tagging, and Containment

- Alert—The unknown access point is not on the neighbor list or part of the user-configured Friendly AP list.

Click an underlined number in any of the time period categories for detailed information regarding the friendly rogue access points. See the “Monitoring Rogue Access Points” section on page 5-89 for more information.

Unclassified Rogue APs

An unclassified rogue access point refers to a rogue access point that is not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list.

The Security dashboard of the Prime Infrastructure home page displays the number of unclassified rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active unclassified rogue access points.

Unclassified rogue access point states include the following:

- Pending—On first detection, the unknown access point is put in the Pending state for 3 minutes. During this time, the managed access points determine if the unknown access point is a neighbor access point.
- Alert—The unknown access point is not on the neighbor list or part of the user-configured Friendly AP list.
- Contained—The unknown access point is contained.
- Contained Pending—The unknown access point is marked Contained, but the action is delayed due to unavailable resources.

Click an underlined number in any of the time period categories for further information. See the “Monitoring Rogue Access Points” section on page 5-89.

Adhoc Rogue

If the MAC address of a mobile client operating in an ad hoc network is not in the authorized MAC address list, then it is identified as an ad hoc rogue.

Rogue Access Point Location, Tagging, and Containment

When the Cisco Unified Wireless Network Solution is monitored using the Prime Infrastructure, the Prime Infrastructure generates the flags as rogue access point traps and displays the known rogue access points by MAC address. The operator can then display a map showing the location of the access points closest to each rogue access point. The next step is to mark them as Known or Acknowledged rogue access points (no further action), Alert rogue access points (watch for and notify when active), or Contained rogue access points (have between one and four access points discourage rogue access point clients by sending the clients deauthenticate and disassociate messages whenever they associate with the rogue access point).

This built-in detection, tagging, monitoring, and containment capability enables system administrators to take the appropriate action:

- Locate rogue access points.
- Receive new rogue access point notifications, eliminating hallway scans.
- Monitor unknown rogue access points until they are eliminated or acknowledged.
Chapter 3 Configuring Security Solutions

Rogue Access Point Location, Tagging, and Containment

- Determine the closest authorized access point, making directed scans faster and more effective.
- Contain rogue access points by sending their clients deauthenticate and disassociate messages from one to four access points. This containment can be done for individual rogue access points by MAC address or can be mandated for all rogue access points connected to the enterprise subnet.
- Tag rogue access points:
  - Acknowledge rogue access points when they are outside of the LAN and do not compromise the LAN or wireless LAN security.
  - Accept rogue access points when they do not compromise the LAN or wireless LAN security.
  - Tag rogue access points as unknown until they are eliminated or acknowledged.
  - Tag rogue access points as contained and discourage clients from associating with the rogue access points by having between one and four access points transmit deauthenticate and disassociate messages to all rogue access point clients. This function applies to all active channels on the same rogue access point.

- Detecting Access Points on a Network, page 3-13
- Viewing Rogue Access Points by Controller, page 3-14

Detecting Access Points on a Network

Use the Detecting Access Points feature to view information about the Cisco lightweight access points that are detecting a rogue access point.

To access the Rogue AP Alarms details page, follow these steps:

**Step 1** To display the Rogue AP Alarms page, do one of the following:

- Perform a search for rogue APs.
- In the Prime Infrastructure home page, click the **Security** dashboard. This page displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.
- Click the **Malicious AP** number link in the dashlet.

**Step 2** In the Rogue AP Alarms page, click the Rogue MAC Address for the applicable rogue access point. The Rogue AP Alarms details page displays.

**Step 3** From the Select a command drop-down list, choose **View Detecting AP on Network**.

**Step 4** Click **Go**.

Click a list item to display data about that item:
- AP Name
- Radio
- Detecting AP Location
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Channel Number—The channel on which the rogue access point is broadcasting.
- WEP—Enabled or disabled.
- WPA—Enabled or disabled.
- Pre-Amble—Long or short.
- RSSI—Received signal strength indicator in dBm.
- SNR—Signal-to-noise ratio.
- Containment Type—Type of containment applied from this access point.
- Containment Channels—Channels that this access point is currently containing.

### Viewing Rogue Access Points by Controller

Use the Detecting Access Points feature to view information about the rogue access points by controller.

To access the Rogue AP Alarms details page, follow these steps:

**Step 1**
To display the Rogue AP Alarms page, do one of the following:
- Perform a search for rogue APs.
- In the Prime Infrastructure home page, click the **Security** dashboard. This page displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.
- Click the **Malicious AP** number link in the dashlet.

**Step 2**
In the Rogue AP Alarms page, click the Rogue MAC Address for the applicable rogue access point. The Rogue AP Alarms details page displays.

**Step 3**
From the Select a command drop-down list, choose **View AP Details by Controller**.

**Step 4**
Click **Go**.

Click a list item to display data about that item:
- Controller IP Address
- Detecting AP Name
- Radio
- Detecting AP Location
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Channel Number—The channel on which the rogue access point is broadcasting.
- RSSI—Received Signal Strength Indicator in dBm.
- Classification—Indicates if the rogue AP classification.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point. See the “Rogue Access Point Classification Types” section on page 3-10 for additional information.
- On Network—Whether it belongs to this network “Yes” or “No”.
- Containment Level—Indicates the containment level of the rogue access point or Unassigned (not contained).
- Last Updated Time
Working with Alarms

You can view, assign, and clear alarms and events on access points and mobility services engine using the Prime Infrastructure.

Details on how to have e-mail notifications of alarms sent to you is also described.

- Assigning and Unassigning Alarms, page 3-15
- Deleting and Clearing Alarms, page 3-15
- Acknowledging Alarms, page 3-16

Assigning and Unassigning Alarms

To assign and unassign an alarm to yourself, follow these steps:

**Step 1** Perform an advanced search for access point alarms.

**Step 2** Select the alarms that you want to assign to yourself by selecting their corresponding check boxes.

*Note* To unassign an alarm assigned to you, unselect the box next to the appropriate alarm. You cannot unassign alarms assigned to others.

**Step 3** From the Select a command drop-down list, choose **Assign to Me** (or **Unassign**), and click **Go**.

If you choose **Assign to Me**, your username appears in the Owner column. If you choose **Unassign**, the username column becomes empty.

Deleting and Clearing Alarms

To delete or clear an alarm from a mobility services engine, follow these steps:

**Step 1** In the Monitor > Alarms page, select the alarms that you want to delete or clear by selecting their corresponding check boxes.

*Note* If you delete an alarm, the Prime Infrastructure removes it from its database. If you clear an alarm, it remains in the Prime Infrastructure database, but in the Clear state. You clear an alarm when the condition that caused it no longer exists.

**Step 2** From the Select a command drop-down list, choose **Delete** or **Clear**, and click **Go**.

*Note* To set up cleanup of old alarms and cleared alarms, choose **Administration > Settings > Alarms**.
Acknowledging Alarms

You might want certain alarms to be removed from the Alarms List. For example, if you are continuously receiving an interference alarm from a certain access point on the 802.11g interface, you might want to stop that access point from being counted as an active alarm on the page or any alarms list. In this scenario, you can find the alarm for the 802.11g interface in the Alarms list, select the check box, and choose Acknowledge from the Select a command drop-down list.

Now if the access point generates a new violation on the same interface, the Prime Infrastructure does not create a new alarm, and the page shows no new alarms. However, if the interference violation is created on another interface, such as 802.11a, a new alarm is created.

Any alarms, once acknowledged, do not show up on either the page or any alarm list page. Also, no e-mails are generated for these alarms after you have marked them as acknowledged. By default, acknowledged alarms are not included for any search criteria. To change this default, choose Administration > Settings > Alarms page and disable the Hide Acknowledged Alarms preference.

Note When you acknowledge an alarm, a warning displays as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled. Use the Administration > User Preferences page to disable this warning message.

You can also search for all previously acknowledged alarms to reveal the alarms that were acknowledged during the last seven days. Prime Infrastructure automatically deletes cleared alerts that are more than seven days old so your results can only show activity for the last seven days. Until an existing alarm is deleted, a new alarm cannot be generated for any managed entity for which the Prime Infrastructure has already generated an alarm.

Monitoring Rogue Alarm Events

The Events page enables you to review information about rogue alarm events. Prime Infrastructure generates an event when a rogue access point is detected or if you make manual changes to a rogue access point (such as changing its state). The Rogue AP Events list page displays all rogue access point events.

To access the Rogue AP Events list page, follow these steps:

Step 1 Do one of the following:
- Perform a search for rogue access point events using the Advanced Search feature of the Prime Infrastructure.
- In the Rogue AP Alarms details page, choose Event History from the Select a command drop-down list.

Step 2 The Rogue AP Events list page displays the following event information.
- Severity—Indicates the severity of the alarm.
- Rogue MAC Address—Click the rogue MAC address to view the Rogue AP Event Details page. See the “Viewing Rogue AP Event Details” section on page 3-17 for more information.
- Vendor—Rogue access point vendor name or Unknown.
- Classification Type—Malicious, Friendly, or Unclassified. See the “Rogue Access Point Classification Types” section on page 3-10 for more information.
- On Network—Indicates how the rogue detection occurred.
Viewing Rogue AP Event Details

To view rogue access point event details, follow these steps:

**Step 1**  In the Rogue AP Events list page, click the Rogue MAC Address link.

**Step 2**  The Rogue AP Events Details page displays the following information:

- Rogue MAC Address
- Vendor—Rogue access point vendor name or Unknown.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Classification Type—Malicious, Friendly, or Unclassified. See the “Rogue Access Point Classification Types” section on page 3-10 for more information.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point. See the “Rogue Access Point Classification Types” section on page 3-10 for additional information.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Channel Number—The channel on which the rogue access point is broadcasting.
- Containment Level—Indicates the containment level of the rogue access point or Unassigned.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Created—The date and time that the event was generated.
- Generated By—The method by which the event was generated (such as Controller).
- Device IP Address
- Severity—Indicates the severity of the alarm.
- Message—Provides details of the current event.
Monitoring Adhoc Rogue Events

The Events page enables you to review information about ad hoc rogue events. Prime Infrastructure generates an event when an ad hoc rogue is detected or if you make manual changes to an ad hoc rogue (such as changing its state). The Adhoc Rogue Events list page displays all ad hoc rogue events.

To access the Rogue AP Events list page, follow these steps:

**Step 1**
- Do one of the following:
  - Perform a search for ad hoc rogue events using the Advanced Search feature of the Prime Infrastructure.
  - In the Adhoc Rogue Alarms details page, choose Event History from the Select a command drop-down list.

**Step 2**
The Rogue AP Events list page displays the following event information:
- Severity—Indicates the severity of the alarm.
- Rogue MAC Address—Click the rogue MAC address to view the Rogue AP Event Details page. See the “Viewing Adhoc Rogue Event Details” section on page 3-18 for more information.
- Vendor—Rogue access point vendor name or Unknown.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Date/Time—The date and time that the event was generated.
- State—Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

Viewing Adhoc Rogue Event Details

To view rogue access point event details, follow these steps:

**Step 1**
In the Rogue AP Events list page, click the Rogue MAC Address link.

**Step 2**
The Rogue AP Events Details page displays the following information:
- Rogue MAC Address
- Vendor—Rogue access point vendor name or Unknown.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
• State—Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
• SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
• Channel Number—The channel on which the rogue access point is broadcasting.
• Containment Level—Indicates the containment level of the rogue access point or Unassigned.
• Radio Type—Lists all radio types applicable to this rogue access point.
• Created—The date and time that the event was generated.
• Generated By—The method by which the event was generated (such as Controller).
• Device IP Address
• Severity—Indicates the severity of the alarm.
• Message—Provides details of the current event.

Security Overview

Prime Infrastructure provides a foundation that allows IT managers to design, control, secure, and monitor enterprise wireless networks from a centralized location.

Prime Infrastructure provides the following tools for managing and enforcing wireless security configurations and policies within the Cisco wireless network infrastructure:

• Network security policy creation and enforcement, such as user authentication, encryption, and access control.
• Wireless infrastructure security configuration.
• Rogue detection, location, and containment.
• wireless Intrusion Prevention System (wIPS).
• Wireless IPS signature tuning and management.
• Management Frame Protection (MFP).
• Collaboration with Cisco wired Network IPS for monitoring and mitigating unauthorized or malicious wireless user activity.
• Comprehensive security event management and reporting.

Security Vulnerability Assessment

In Cisco Unified Wireless Network Version 5.1, an automated security vulnerability assessment is available to facilitate analysis for the overall wireless security posture of an enterprise, as well as to provide WLAN operators with real-time benchmarking of their security services configurations against industry best practices. The automated security vulnerability assessment provides the following:

• Proactive vulnerability monitoring of the entire wireless network.
• Comprehensive information on security vulnerabilities that could lead to loss of data, network intrusion, or malicious attack.
Chapter 3      Configuring Security Solutions

Security Overview

- Reduction in the time and expertise required to analyze and remedy weaknesses in wireless security posture.

The automated wireless vulnerability assessment audits the security posture of the entire wireless network for vulnerabilities. These vulnerabilities can result in:

- Unauthorized management access or using management protocols to compromise or adversely impact the network.
- Unauthorized network access, data leakage, man-in-the-middle, or replay attacks.
- Compromised or adverse impacts to the network through manipulation of network protocols and services, for example through denial of service (DoS) attacks.

Prime Infrastructure automatically scans the entire network and compares settings against Cisco recommended and industry best practices for wireless security configurations. The automated wireless security assessment functions within the Prime Infrastructure scan wireless LAN controllers, access points, and network management interfaces for vulnerabilities in configuration settings, encryption, user authentication, infrastructure authentication network management, and access control.

Status of the wireless network security is graphically displayed to provide wireless network administrators with an easy-to-read dashboard of security events. Prime Infrastructure displays the vulnerability assessment results through a Security Index on the Prime Infrastructure security dashboard. The Security Index summarizes the network security posture with a composite security score and prioritized summary of vulnerabilities. See the “Security Index” section on page 3-20 for more information.

Administrators can drill down to the Security Index Detailed Report if an event in the Security Summary warrants further investigation. The Security Index Detailed Report provides in-depth analysis of the vulnerabilities across the network. It also identifies optimal security settings and recommends changes that remedy the vulnerabilities. Any changes the administrator makes are reflected in an updated Security Index score. See the “Security Index Detailed Report” section on page 3-21 for more information.

Security Index

The Security Index gives an indication of the security of the Prime Infrastructure managed network. The security index is calculated by assigning weight to the various security configurations and displaying it in visual form. The combined weightages can vary from 0 to 100, where 0 signifies least secured and 100 maximum secured.

The weighting comes from the lowest scoring controller and the lowest scoring Location Server/Mobility Service Engine related security configurations that are maintained within the Prime Infrastructure itself. For example, the security index of the Prime Infrastructure managed network is equal to the lowest scoring controller plus the lowest scoring Location Server/Mobility Service Engine.

The following color scheme applies for the security index:

- Above or equal to 80—Green
- Below 80 but above or equal to 60—Yellow
- Below 60—Red

Note

Guest WLANs are excluded from the WLANs. A WLAN which has web authentication or web passthrough enabled is identified as a guest WLAN.
The security index of the latest release is the benchmark for the required security configurations. For example, if AES encryption was not present in an earlier version of code, the index is reduced by the number associated with the AES encryption security configuration. Likewise, if new security configurations are introduced, the weighting would be altered.

The configurations stored in the Prime Infrastructure might not be up-to-date with the ones in the controllers unless the Refresh from Controller command is run from the Prime Infrastructure. You can run Security Index calculations from the Configuration Sync task to get the latest config data from all the controllers.

**Top Security Issues**

The Top Security Issues section displays the five top security issues. The View All and Devices links sort relevant columns and show a report of security issues occurring across all controllers. Click View All to open the Security Index Detailed Report. Click Devices to view the Security Index Controller Report.

- Security Index Detailed Report, page 3-21
- Security Index Controller Report, page 3-21
- Potential Security Issues, page 3-22

**Security Index Detailed Report**

The Security Index Detailed Report displays all security issues found across all controllers, location servers, and mobility service engines. It details problems found in a particular security configuration retrieved from the device. If a particular issue has been acknowledged (just like alarms), it is ignored when the next Configuration Sync task runs (if Security Index Calculation is enabled).

In some cases when an issue is acknowledged and it is ignored the next time the Configuration Sync task runs, the final security index score does not change. Some possible reasons for this might include the following:

- The acknowledged issue is on a controller which is not directly affecting the security index score (for instance, it is not the controller with the lowest score).
- The acknowledged issue is on a WLAN that is not directly affecting the security index score. Only the lowest scoring WLAN of the lowest scoring controller affects the security index score.

When SSH and Telnet are enabled on a controller and are both flagged as issues, the Telnet issue has a higher precedence than SSH. Even if SSH is acknowledged on the controller with the lowest score, no change would occur for the security index.

From the Select a command drop-down list, choose Show All to view all security issues (both acknowledged and unacknowledged). Choose Show Unacknowledged to only view unacknowledged security issues. This is the default view when View All is selected from the Security Summary page. Choose Show Acknowledged to only view acknowledged security issues.

**Note** For a user to acknowledge or unacknowledge security issues, the user must have “Ack and Unack Security Index Issues permission enabled”.

**Security Index Controller Report**

This page shows the security violation report as a summary for each controller. By row, each controller shows the number of security issues that occurred on that controller and provides a link to all security issues.
If you click the number in the Security Issues Count column, the Security Index Detailed Report appears.

**Potential Security Issues**

Table 3-7 and Table 3-8 describe the potential security issues.

**Table 3-7 Potential Security Issues**

<table>
<thead>
<tr>
<th>Controller Security Issue</th>
<th>Why is this an Issue?</th>
<th>What is the Solution?</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN SSID on the controller has a weak authentication method.</td>
<td>Weak authentication method for a WLAN which can be broken by using tools available online if WLAN packets are sniffed.</td>
<td>Use the most secured authentication method and one that is WPA+WPA2.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has a weak authentication method (CKIP) configured.</td>
<td>Weak authentication method for a WLAN.</td>
<td>Use the most secured authentication method and one that is WPA+WPA2.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has no user authentication configured.</td>
<td>No authentication method is a clear security risk for a WLAN.</td>
<td>Configure strong authentication methods such as WPA+WPA2.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has a weak encryption method (CKIP WEP 40 bits) configured.</td>
<td>Weak encryption method for a WLAN.</td>
<td>Configure strong authentication and encryption methods such as WPA+WPA2 with AES.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has a weak encryption method (CKIP WEP 40 bits with Key Permutation) configured.</td>
<td>Weak encryption method for a WLAN.</td>
<td>Configure strong authentication and encryption methods such as WPA+WPA2 with AES.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has a weak encryption method (CKIP WEP 104 bits) configured.</td>
<td>Weak encryption method for a WLAN.</td>
<td>Configure strong authentication and encryption methods such as WPA+WPA2 with AES.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has a weak encryption method (CKIP WEP 104 bits with MMH and Key Permutation) configured.</td>
<td>Weak encryption method for a WLAN.</td>
<td>Configure strong authentication and encryption methods such as WPA+WPA2 with AES.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has a weak encryption method (WEP 104 bits) configured.</td>
<td>Weak encryption method for a WLAN.</td>
<td>Configure strong authentication and encryption methods such as WPA+WPA2 with AES.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has a weak encryption method (CKIP WEP 104 bits) configured.</td>
<td>Weak encryption method for a WLAN.</td>
<td>Configure strong authentication and encryption methods such as WPA+WPA2 with AES.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has a weak encryption method (CKIP WEP 104 bits with MMH) configured.</td>
<td>Weak encryption method for a WLAN.</td>
<td>Configure strong authentication and encryption methods such as WPA+WPA2 with AES.</td>
</tr>
<tr>
<td>Controller Security Issue</td>
<td>Why is this an Issue?</td>
<td>What is the Solution?</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>WLAN SSID on the controller has a weak encryption method (CKIP WEP 104 bits with Key Permutation) configured.</td>
<td>Weak encryption method for a WLAN.</td>
<td>Configure strong authentication and encryption methods such as WPA+WPA2 with AES.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has a weak encryption method (CKIP WEP 104 bits with MMH and Key Permutation) configured.</td>
<td>Weak encryption method for a WLAN.</td>
<td>Configure strong authentication and encryption methods such as WPA+WPA2 with AES.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has a weak encryption method (WEP 40 bits) configured.</td>
<td>Weak encryption method for a WLAN.</td>
<td>Configure strong authentication and encryption methods such as WPA+WPA2 with AES.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has a weak encryption method (WEP 128 bits) configured.</td>
<td>Weak encryption method for a WLAN.</td>
<td>Configure strong authentication and encryption methods such as WPA+WPA2 with AES.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has a weak encryption method (TKIP) configured.</td>
<td>Weak encryption method for a WLAN.</td>
<td>Configure strong authentication and encryption methods such as WPA+WPA2 with AES.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has no encryption configured.</td>
<td>No encryption method is a clear security risk for a WLAN.</td>
<td>Configure strong authentication and encryption methods such as WPA+WPA2 with AES.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has a weak encryption method (WEP 104 bits) configured.</td>
<td>Weak encryption method for WLAN.</td>
<td>Configure strong authentication and encryption methods such as WPA+WPA2 with AES.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has no key management methods configured (applicable only for WPA+WPA2).</td>
<td>A key management method enhances the security of keys; without one, WLAN is less secure.</td>
<td>Configure at least one key management methods such as CCKM.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has MFP Client Protection set to “Optional”.</td>
<td>With MFP Client Protection set to optional for a WLAN, authenticated clients might not be shielded from spoofed frames.</td>
<td>Set MFP Client Protection to “Required” to protect against clients connecting to a rogue access point.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has MFP Client Protection set to “Disabled”.</td>
<td>With MFP Client Protection set to disabled for a WLAN, authenticated clients might not be shielded from spoofed frames.</td>
<td>Set MFP Client Protection to “Required” to protect against clients connecting to a rogue access point.</td>
</tr>
<tr>
<td>WLAN SSID interface is set to “management” on the controller.</td>
<td>As recommended from SAFE, user traffic should be separated from management traffic.</td>
<td>WLAN interface should not be set to “management” on the controller.</td>
</tr>
<tr>
<td>Interface set to one which is VLAN for a WLAN.</td>
<td>As recommended from SAFE, user traffic should be separated from VLAN traffic.</td>
<td>WLAN needs its interface to be set to one which is neither management nor one which has a VLAN.</td>
</tr>
</tbody>
</table>
### Table 3-7 Potential Security Issues (continued)

<table>
<thead>
<tr>
<th>Controller Security Issue</th>
<th>Why is this an Issue?</th>
<th>What is the Solution?</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN SSID on the controller has “Client Exclusion” disabled.</td>
<td>With Client Exclusion policies disabled, an attacker is able to continuously try to access the WLAN network.</td>
<td>Enable “Client Exclusion” to secure against malicious WLAN client behavior.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has “Broadcast SSID” enabled.</td>
<td></td>
<td>Disable “Broadcast SSID” to secure your wireless network.</td>
</tr>
<tr>
<td>WLAN SSID on the controller has “MAC Filtering” disabled.</td>
<td></td>
<td>Enable “MAC Filtering” to secure your wireless network.</td>
</tr>
<tr>
<td>Protection Type is set to “AP Authentication” on the controller.</td>
<td>When AP Authentication is set, an access point checks beacon/probe response frames in neighboring access points to see if they contain an authenticated information element (IE) that matches that of the RF group. This provides some security but does not cover all management frames and is open to alteration by rogue access points.</td>
<td>Set Protection Type to “Management Frame Protection (MFP)” on the controller.</td>
</tr>
<tr>
<td>Protection Type is set to “None” of the controller.</td>
<td>No security for 802.11 management messages passed between access points and clients.</td>
<td>Set Protection Type to “Management Frame Protection (MFP)” on the controller.</td>
</tr>
<tr>
<td>Radio type is configured to detect rogues only on DCA channels.</td>
<td>Rogue detection, if done only on a subset of country/all channels, is less secure than one that is done on country/all channels.</td>
<td>Configure radio types 802.11a/n and 802.11b/g/n to detect rogues on country channels or all channels.</td>
</tr>
<tr>
<td>Radio type is configured to detect rogues on neither country channels nor DCA channels.</td>
<td>Rogue detection, if not configured on country nor DCA channels, is less secure than when done on country/all channels.</td>
<td>Configure radio types 802.11a/n and 802.11b/g/n to detect rogues on country channels or all channels.</td>
</tr>
<tr>
<td>The rogue policy to detect and report ad hoc networks is disabled on the controller.</td>
<td>With detection and reporting of ad hoc networks turned off, ad hoc rogues go undetected.</td>
<td>Enable the rogue policy to detect and report ad hoc networks.</td>
</tr>
<tr>
<td>“Check for all Standard and Custom Signatures” is disabled on the controller.</td>
<td>If check for all Standard and Custom Signatures is disabled, various types of attacks in incoming 802.11 packets would go undetected. various types of attacks in incoming 802.11 packets would go undetected.</td>
<td>Check for all Standard and Custom Signatures needs to be turned on to identify various types of attacks in incoming 802.11 packets.</td>
</tr>
<tr>
<td>Some of the Standard Signatures are disabled on the controller.</td>
<td>If only some of the Standard Signatures are disabled,</td>
<td>Enable all Standard Signatures on the controller.</td>
</tr>
</tbody>
</table>
### Table 3-7 Potential Security Issues (continued)

<table>
<thead>
<tr>
<th>Controller Security Issue</th>
<th>Why is this an Issue?</th>
<th>What is the Solution?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The “Excessive 802.11 Association Failures” Client Exclusion Policy is disabled on the controller.</td>
<td>Excessive failed association attempts can consume system resources and launch potential a denial of service attack to the infrastructure.</td>
<td>Enable the “Excessive 802.11 Association Failures” Client Exclusion Policy on the controller.</td>
</tr>
<tr>
<td>The “Excessive 802.11 Authentication Failures” Client Exclusion Policy is disabled on the controller.</td>
<td>Excessive failed authentication attempts can consume system resources and launch potential Denial of Service attack to the infrastructure.</td>
<td>Enable the “Excessive 802.11 Authentication Failures” Client Exclusion Policy on the controller.</td>
</tr>
<tr>
<td>The “Excessive 802.1X Authentication Failures” Client Exclusion Policy is disabled on the controller.</td>
<td>Excessive 802.1X failed authentication attempts can consume system resources and launch potential denial of service attack to the infrastructure.</td>
<td>Excessive 802.1X Authentication Failures Client Exclusion Policy must be enabled to prevent denial of service attack to the infrastructure.</td>
</tr>
<tr>
<td>The “Excessive 802.11 Web Authentication Failures” Client Exclusion Policy is disabled on the controller.</td>
<td>If Excessive 802.11 Web failed web authentication attempts can consume system resources and launch potential denial of service attack to the infrastructure.</td>
<td>Enable the “Excessive 802.11 Web Authentication Failures” Client Exclusion Policy on the controller.</td>
</tr>
<tr>
<td>The “IP Theft or IP Reuse” Client Exclusion Policy is disabled on the controller.</td>
<td>If IP Theft or Reuse Client Exclusion Policy is disabled, then an attacker masquerading as another client would not be disallowed.</td>
<td>Enable the “IP Theft or IP Reuse” Client Exclusion Policy on the controller.</td>
</tr>
<tr>
<td>No CIDS Sensor configured on the controller.</td>
<td>If no enabled IDS Sensor is configured, then IP-level attacks would not be detected.</td>
<td>Configure at least one CIDS Sensor on the controller.</td>
</tr>
<tr>
<td>Controller is configured with default community strings for SNMP v1/v2.</td>
<td>If SNMP V1 or V2 with default Community is configured then it is open to easy attacks because default communities are well known.</td>
<td>Use SNMPv3 with Auth and Privacy Types.</td>
</tr>
<tr>
<td>Controller is configured with non-default community strings for SNMP v1/v2.</td>
<td>SNMP V1 or V2 with non-default Community is slightly more secure than default Community but still less secure than SNMP V3.</td>
<td>Use SNMPv3 with Auth and Privacy types.</td>
</tr>
<tr>
<td>SNMPv3 is configured with a default user on the controller.</td>
<td>Using a default user makes SNMP V3 connections less secure.</td>
<td>Use a non-default username for SNMPv3 with Auth and Privacy Types.</td>
</tr>
<tr>
<td>SNMPv3 is configured with either no Auth or Privacy Type on the controller.</td>
<td>SNMP V3 with either Auth or Privacy Type set to none reduces the security of SNMP V3 connection.</td>
<td>Use SNMPv3 with Auth and Privacy Types to secure your wireless network.</td>
</tr>
</tbody>
</table>
Table 3-7 Potential Security Issues (continued)

<table>
<thead>
<tr>
<th>Controller Security Issue</th>
<th>Why is this an Issue?</th>
<th>What is the Solution?</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP (Web Mode enabled but Secure Web Mode disabled) is enabled on the controller.</td>
<td>HTTP is less secure than HTTPS.</td>
<td>Enable HTTPS (both Web Mode and Secure Web Mode) on the controller.</td>
</tr>
<tr>
<td>Telnet is enabled on the controller.</td>
<td>If telnet is enabled, then the controller is at risk of being hacked into.</td>
<td>Disable telnet on the controller.</td>
</tr>
<tr>
<td>SSH is disabled and timeout value is set to zero on the controller.</td>
<td>If SSH is enabled and timeout is zero then the controller has risk of being hacked into.</td>
<td>Enable SSH with non-zero timeout value on the controller.</td>
</tr>
<tr>
<td>Telnet is enabled on the AP.</td>
<td>If telnet is enabled, then the access point is at risk of being hacked into.</td>
<td>Disable Telnet on all access points.</td>
</tr>
<tr>
<td>SSH is enabled on the AP.</td>
<td></td>
<td>Disable SSH on all the access points.</td>
</tr>
<tr>
<td>At least one of the APs is configured with default username or password.</td>
<td>If default password is configured, then access points are more susceptible to connections from outside the network.</td>
<td>Configure a non-default username and strong password for all access points associated to the controller.</td>
</tr>
</tbody>
</table>

Table 3-8 Potential Security Issues

<table>
<thead>
<tr>
<th>Location Server/ Mobility Server Engine Security Issue</th>
<th>Why is this an Issue?</th>
<th>What is the Solution?</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP is enabled on the location server.</td>
<td>HTTP is less secure than HTTPS.</td>
<td>Enable HTTPS on the location server.</td>
</tr>
<tr>
<td>A location server user has a default password configured.</td>
<td>If default password is configured, then Location Server/ Mobility Server Engine is more susceptible to connections from outside the network.</td>
<td>Configure a strong password for the location server users.</td>
</tr>
<tr>
<td>HTTP is enabled on the mobility services engine.</td>
<td>HTTP is less secure than HTTPS.</td>
<td>Enable HTTPS on the mobility services engine.</td>
</tr>
<tr>
<td>A mobility services engine user has default password configured.</td>
<td>If default password is configured, then Location Server/ Mobility Server Engine is more susceptible to connections from outside the network.</td>
<td>Configure a strong password for the users on the mobility services engine.</td>
</tr>
<tr>
<td>wIPS Service is not enabled on the mobility services engine.</td>
<td>Your network is vulnerable to advanced security threats.</td>
<td>Deploy wIPS Service to protect your network from advanced security threats.</td>
</tr>
</tbody>
</table>
Switch Port Tracing

Currently, the Prime Infrastructure provides rogue access point detection by retrieving information from the controller. The rogue access point table is populated with any detected BSSID addresses from any frames that are not present in the neighbor list. At the end of a specified interval, the contents of the rogue table are sent to the controller in a CAPWAP Rogue AP Report message. With this method, the Prime Infrastructure would simply gather the information received from the controllers; but with software Release 5.1, you can incorporate switch port tracing of Wired Rogue Access Point Switch Ports. This enhancement allows you to react to found wired rogue access points and prevent future attacks. The trace information is available only in the Prime Infrastructure log and only for rogue access points, not rogue clients.

Rogue Client connected to the Rogue Access point information is used to track the switch port to which the Rogue Access point is connected in the network.

If you try to set tracing for a friendly or deleted rogue, a warning message appears.

---

**Note**

Auto Switch Port Tracing depends on wired client polling to run. The wired clients polling requires full Lifecycle license.

**Note**

For Switch Port Tracing to successfully trace the switch ports using SNMP v3, all of the OIDs should be included in the SNMP v3 view and VLAN content should be created for each VLAN in the SNMP v3 group.

**Establishing Switch Port Tracing**

To establish switch port tracing, follow these steps:

**Step 1**  
In the Prime Infrastructure home page, click the **Security** dashboard.

**Step 2**  
In the Rogue APs and Adhoc Rogues dashlet, click the number URL which specifies the number of rogues in the last hour, last 24 hours, or total active.

The Alarms window opens.

**Step 3**  
Choose the rogue you are setting switch port tracking by checking the checkbox.

**Step 4**  
From the **Troubleshoot** drop-down list, choose **Traceroute**. The Traceroute window opens, and the Prime Infrastructure runs a switch port trace.

When one or more searchable MAC addresses are available, the Prime Infrastructure uses CDP to discover any switches connected up to two hops away from the detecting access point. The MIBs of each CDP discovered switch is examined to see if it contains any of the target MAC addresses. If any of the MAC addresses are found, the corresponding port number is returned and reported as the switch port of a rogue.

---

**Integrated Security Solutions**

The Cisco Unified Wireless Network Solution also provides these integrated security solutions:
Cisco Unified Wireless Network Solution operating system security is built around a robust 802.1X authorization, authentication, and accounting (AAA) engine, which enables operators to rapidly configure and enforce a variety of security policies across the Cisco Unified Wireless Network Solution.

The controllers and access points are equipped with system-wide authentication and authorization protocols across all ports and interfaces, maximizing system security.

Operating system security policies are assigned to individual wireless LANs, and access points simultaneously broadcast all (up to 16) configured wireless LANs. These policies can eliminate the need for additional access points, which can increase interference and degrade system throughput.

Operating system security uses the RRM function to continually monitor the air space for interference and security breaches and notify the operator when they are detected.

Operating system security works with industry-standard AAA servers, making system integration simple and easy.

The Cisco Intrusion Detection System/Intrusion Protection System (IDS/IPS) instructs controllers to block certain clients from accessing the wireless network when attacks involving these clients are detected.

The operating system security solution offers comprehensive Layer 2 and Layer 3 encryption algorithms, which typically require a large amount of processing power. Rather than assigning the encryption tasks to yet another server, the controller can be equipped with a VPN/enhanced security module that provides extra hardware required for the most demanding security configurations.

### Using Prime Infrastructure to Convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 Mode

To convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 LWAPP transport mode using the Prime Infrastructure user interface, follow these steps:

**Note**
Cisco-based lightweight access points do not support Layer 2 LWAPP mode. These access points can only be run with Layer 3.

**Note**
This procedure causes your access points to go offline until the controller reboots and the associated access points reassociate to the controller.

**Step 1**
Make sure that all controllers and access points are on the same subnet.

**Note**
You must configure the controllers and associated access points to operate in Layer 2 mode before completing the conversion.

**Step 2**
Log into the Prime Infrastructure user interface. Then follow these steps to change the LWAPP transport mode from Layer 3 to Layer 2:

- Choose **Configure > Controllers** to navigate to the All Controllers page.
- Click the desired IP address of a controller to display the **IP Address > Controller Properties** page.
c. From the left sidebar menu, click **System > General** to display the **IP Address > General** page.

d. Change LWAPP transport mode to **Layer2**, and click **Save**.

e. If the Prime Infrastructure displays the following message, click **OK**:

   Please reboot the system for the LWAPP Mode change to take effect.

**Step 3**

To restart your Cisco Unified Wireless Network Solution, follow these steps:

a. Return to the **IP Address > Controller Properties** page.

b. Click **System > Commands** to display the **IP Address > Controller Commands** page.

c. Under Administrative Commands, choose **Save Config To Flash**, and click **Go** to save the changed configuration to the controller.

d. Click **OK** to continue.

e. Under Administrative Commands, choose **Reboot**, and click **Go** to reboot the controller.

f. Click **OK** to confirm the save and reboot.

**Step 4**

After the controller reboots, follow these steps to verify that the LWAPP transport mode is now Layer 2:

a. Click **Monitor > Controllers** to navigate to the Controllers > Search Results page.

b. Click the desired IP address of a controller to display the Controllers > **IP Address > Summary** page.

c. Under General, verify that the current LWAPP transport mode is Layer2.

You have completed the LWAPP transport mode conversion from Layer 3 to Layer 2. The operating system software now controls all communications between controllers and access points on the same subnet.

---

**Configuring a Firewall for Prime Infrastructure**

When the Prime Infrastructure server and the Prime Infrastructure user interface are on different sides of a firewall, they cannot communicate unless the following ports on the firewall are open to two-way traffic:

- 80 (for initial http)
- 69 (tftp)
- 162 (trap port)
- 443 (https)
- 1522 (for HA configuration between the primary and secondary Prime Infrastructure)

Open these ports to configure your firewall to allow communications between the Prime Infrastructure server and the Prime Infrastructure user interface.

**Access Point Authorization**

To view a list of authorized access points along with the type of certificate that an access point uses for authorization, follow these steps:
Chapter 3  Configuring Security Solutions

Management Frame Protection (MFP)

Management Frame Protection (MFP) provides security for the otherwise unprotected and unencrypted 802.11 management messages passed between access points and clients. MFP provides both infrastructure and client support.

- **Infrastructure MFP**—Protects management frames by detecting adversaries who are invoking denial of service attacks, flooding the network with associations and probes, interjecting as rogue access points, and affecting network performance by attacking the QoS and radio measurement frames. It also provides a quick and effective means to detect and report phishing incidents.

  Specifically, infrastructure MFP protects 802.11 session management functions by adding message integrity check information elements (MIC IEs) to the management frame emitted by access points (and not those emitted by clients), which are then validated by other access points in the network. Infrastructure MFP is passive. It can detect and report intrusions but has no means to stop them.

- **Client MFP**—Shields authenticated clients from spoofed frames, preventing many of the common attacks against wireless LANs from becoming effective. Most attacks, such as deauthentication attacks, revert to simply degrading performance by contending with valid clients.

  Specifically, client MFP encrypts management frames sent between access points and Cisco-compatible Extension clients so that both access points and clients can take preventive action by dropping spoofed class 3 management frames (that is, management frames passed between an access point and a client that is authenticated and associated). Client MFP leverages the security mechanisms defined by IEEE 802.11i to protect the following types of class 3 unicast management frames: disassociation, deauthentication, and QoS (WMM) action. Client MFP is active. It can protect a client-access point session from the most common type of denial of service attack. It protects class 3 management frames by using the same encryption method used for the data frames of the session. If a frame received by the access point or client fails decryption, it is dropped, and the event is reported to the controller.
To use client MFP, clients must support Cisco-compatible Extensions (Version 5) MFP and must negotiate WPA2 using either TKIP or AES-CCMP. EAP or PSK might be used to obtain the PMK. CCKM and controller mobility management are used to distribute session keys between access points or Layer 2 and Layer 3 fast roaming.

To prevent attacks against broadcast frames, access points supporting Cisco-compatible Extensions (version 5) do not emit any broadcast class 3 management frames (such as disassociation, deauthentication, or action). Compatible extensions clients (Version 5) and access points must discard broadcast class 3 management frames.

Client MFP supplements infrastructure MFP rather than replacing it because infrastructure MFP continues to detect and report invalid unicast frames sent to clients that are not client-MFP capable, as well as invalid class 1 and 2 management frames. Infrastructure MFP is applied only to management frames that are not protected by client MFP.

Infrastructure MFP consists of three main components:

- Management frame protection—The access point protects the management frames it transmits by adding a MIC IE to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing any receiving access point configured to detect MFP frames to report the discrepancy.

- Management frame validation—in infrastructure MFP, the access point validates every management frame it receives from other access points in the network. It ensures that the MIC IE is present (when the originator is configured to transmit MFP frames) and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE from a BSSID belonging to an access point that is configured to transmit MFP frames, it reports the discrepancy to the network management system. For the timestamps to operate properly, all controllers must be Network Transfer Protocol (NTP) synchronized.

- Event reporting—The access point notifies the controller when it detects an anomaly, and the controller aggregates the received anomaly events and reports the results through SNMP traps to the network management system.

**Note**

Client MFP uses the same event reporting mechanisms as infrastructure MFP.

Infrastructure MFP is enabled by default and can be disabled globally. When you upgrade from a previous software release, infrastructure MFP is disabled globally if access point authentication is enabled because the two features are mutually exclusive. After infrastructure MFP is enabled globally, signature generation (adding MICs to outbound frames) can be disabled for selected WLANs, and validation can be disabled for selected access points.

You set MFP in the WLAN template. See the “Configuring WLAN Templates” section on page 11-19.

### Guidelines for Using MFP

Follow these guidelines for using MFP:

- MFP is supported for use with Cisco Aironet lightweight access points, except for the 1500 series mesh access points.

- Lightweight access points support infrastructure MFP in local and monitor modes and in REAP and FlexConnect modes when the access point is connected to a controller. They support client MFP in local, FlexConnect, and bridge modes.

- Client MFP is supported for use only with Cisco-compatible Extensions (Version 5) clients using WPA2 with TKIP or AES-CCMP.
Non-Cisco-compatible Extensions (Version 5) clients might associate to a WLAN if client MFP is disabled or optional.

## Configuring Intrusion Detection Systems (IDS)

The Cisco Intrusion Detection System/Intrusion Prevention System (IDS/IPS) instructs controllers to block certain clients from accessing the wireless network when attacks involving these clients are detected. This system offers significant network protection by helping to detect, classify, and stop threats including worms, spyware/adware, network viruses, and application abuse. Two methods are available to detect IDS attacks:

- IDS sensors (for Layer 3)
- IDS signatures (for Layer 2)

### Viewing IDS Sensors

When the sensors identify an attack, they alert the controller to shun the offending client. When you add a new IDS sensor, you register the controller with that IDS sensor so that the sensor can send shunned client reports to the controller. The controller also polls the sensor periodically.

To view IDS sensors, follow these steps:

1. **Step 1** Choose Configure > Controllers.
2. **Step 2** Choose a controller by clicking an IP address.
3. **Step 3** From the left sidebar menu, choose Security > IDS Sensor Lists. The IDS Sensor page appears. This page lists all of the IDS sensors that have been configured for this controller.

### Configuring IDS Signatures

You can configure **IDS signatures**, or bit-pattern matching rules used to identify various types of attacks in incoming 802.11 packets, on the controller. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller. If an attack is detected, an appropriate mitigation action is initiated.

Cisco supports 17 standard signatures on the controller as shown on the Standard Signatures and Custom Signatures page. To open this page, choose Configure > Controllers, select a controller IP address, and then choose Security > Wireless Protection Policies > Standard Signatures from the left sidebar menu.

These signatures are divided into six main groups. The first four groups contain management signatures, and the last two groups contain data signatures:

- **Broadcast deauthentication frame signatures**—During a broadcast deauthentication frame attack, a hacker sends an 802.11 deauthentication frame to the broadcast MAC destination address of another client. This attack causes the destination client to disassociate from the access point and lose its connection. If this action is repeated, the client experiences a denial of service. When the broadcast deauthentication frame signature (precedence 1) is used to detect such an attack, the access point
listens for clients transmitting broadcast deauthentication frames that match the characteristics of the signature. If the access point detects such an attack, it alerts the controller. Depending on how your system is configured, the offending device is contained so that its signals no longer interfere with authorized clients, or the controller forwards an immediate alert to the system administrator for further action, or both.

- **NULL probe response signatures**—During a NULL probe response attack, a hacker sends a NULL probe response to a wireless client adapter. As a result, the client adapter locks up. When a NULL probe response signature is used to detect such an attack, the access point identifies the wireless client and alerts the controller. The NULL probe response signatures include the following:
  - NULL probe resp 1 (precedence 2)
  - NULL probe resp 2 (precedence 3)

- **Management frame flood signatures**—During a management frame flood attack, a hacker floods an access point with 802.11 management frames. The result is a denial of service to all clients associated or attempting to associate to the access point. This attack can be implemented with different types of management frames: association requests, authentication requests, reassociation requests, probe requests, disassociation requests, deauthentication requests, and reserved management subtypes.

  When a management frame flood signature is used to detect such an attack, the access point identifies management frames matching the entire characteristics of the signature. If the frequency of these frames is greater than the value of the frequency set in the signature, an access point that hears these frames triggers an alarm. The controller generates a trap and forwards it to the Prime Infrastructure.

  The management frame flood signatures include the following:
  - Assoc flood (precedence 4)
  - Auth flood (precedence 5)
  - Reassoc flood (precedence 6)
  - Broadcast probe flood (precedence 7)
  - Disassoc flood (precedence 8)
  - Deauth flood (precedence 9)
  - Reserved mgmt 7 (precedence 10)
  - Reserved mgmt F (precedence 11)

  The reserved management frame signatures 7 and F are reserved for future use.

- **EAPOL flood signature**—During an EAPOL flood attack, a hacker floods the air with EAPOL frames containing 802.1X authentication requests. As a result, the 802.1X authentication server cannot respond to all of the requests and fails to send successful authentication responses to valid clients. The result is a denial of service to all affected clients. When the EAPOL flood signature (precedence 12) is used to detect such an attack, the access point waits until the maximum number of allowed EAPOL packets is exceeded. It then alerts the controller and proceeds with the appropriate mitigation.

- **NetStumbler signatures**—NetStumbler is a wireless LAN scanning utility that reports access point broadcast information (such as operating channel, RSSI information, adapter manufacturer name, SSID, WEP status, and the latitude and longitude of the device running NetStumbler when a GPS is attached). If NetStumbler succeeds in authenticating and associating to an access point, it sends a data frame with the following strings, depending on the NetStumbler version listed in Table 3-9.
Table 3-9  NetStumbler Versions

<table>
<thead>
<tr>
<th>Version</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.0</td>
<td>“Flurble gronk bloopit, bnip Frundletrune”</td>
</tr>
<tr>
<td>3.2.3</td>
<td>“All your 802.11b are belong to us”</td>
</tr>
<tr>
<td>3.3.0</td>
<td>Sends white spaces</td>
</tr>
</tbody>
</table>

When a NetStumbler signature is used to detect such an attack, the access point identifies the offending device and alerts the controller. The NetStumbler signatures include the following:

- NetStumbler 3.2.0 (precedence 13)
- NetStumbler 3.2.3 (precedence 14)
- NetStumbler 3.3.0 (precedence 15)
- NetStumbler generic (precedence 16)

- Wellenreiter signature—Wellenreiter is a wireless LAN scanning and discovery utility that can reveal access point and client information. When the Wellenreiter signature (precedence 17) is used to detect such an attack, the access point identifies the offending device and alerts the controller.

This section provides the instructions to configure signatures and contains the following topics:

- Uploading IDS Signatures, page 3-34
- Downloading IDS Signatures, page 3-35
- Enabling or Disabling IDS Signatures, page 3-36

Uploader DS Signatures

To upload IDS signatures from the controller, follow these steps:

Step 1  Obtain a signature file from Cisco (hereafter called a standard signature file). You can also create your own signature file (hereafter called a custom signature file) by following the “Downloading IDS Signatures” section on page 3-35.

Step 2  You can configure a TFTP server for the signature download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable. However, if you want to put the TFTP server on a different network while the management port is down, add a static route if the subnet where the service port resides has a gateway (config route add IP address of TFTP server).

- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.

- A third-party TFTP server cannot run on the same computer as Prime Infrastructure because built-in TFTP server of the Prime Infrastructure and third-party TFTP server use the same communication port.

Step 3  Choose Configure > Controllers.

Step 4  Choose a controller by clicking an IP address.
Step 5  From the left sidebar menu, choose **Security** and then choose **Standard Signatures** or **Custom Signatures**.

Step 6  From the Select a command drop-down list, choose **Upload Signature Files from Controller**.

Step 7  Specify the TFTP server name being used for the transfer.

Step 8  If the TFTP server is new, enter the TFTP IP address at the Server IP Address text box.

Step 9  Choose **Signature Files** from the File Type drop-down list.

Step 10  The signature files are uploaded to the root directory which was configured for use by the TFTP server. You can change to a different directory at the Upload to File field (this field only shows if the Server Name is the default server). The controller uses this local file name as a base name and then adds _std.sig as a suffix for standard signature files and _custom.sig as a suffix for custom signature files.

Step 11  Click **OK**.

---

**Downloading IDS Signatures**

If the standard signature file is already on the controller but you want to download customized signatures to it, follow these steps:

---

Step 1  Choose **Configure > Controllers**.

Step 2  Choose a controller by clicking an IP address.

Step 3  Choose **System > Commands**.

Step 4  From the Upload/Download Commands drop-down list, choose **Download IDS Signatures**, and click **Go**.

Step 5  Copy the signature file (*.sig) to the default directory on your TFTP server.

Step 6  Choose **local machine** from the File is Located On field. If you know the filename and path relative to the root directory of the server, you can also choose TFTP server.

Step 7  Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries field.

Step 8  Enter the maximum amount of time, in seconds, before the controller times out while attempting to download the signature file in the Timeout field.

Step 9  The signature files are uploaded to the c:\tftp directory. Specify the local file name in that directory or use the Browse button to navigate to it. A “revision” line in the signature file specifies whether the file is a Cisco-provided standard signature file or a site-tailored custom signature file (custom signature files must always have revision=custom).

Step 10  If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On field, and the Server File Name is populated for you and retried. The local machine option initiates a two-step operation. First, the local file is copied from the workstation of the administrator to the built-in TFTP server of the Prime Infrastructure. Then the controller retrieves that file. For later operations, the file is already in the TFTP directory of the Prime Infrastructure server, and the download web page now automatically populates the filename.

Step 11  Click **OK**.
Enabling or Disabling IDS Signatures

To enable or disable IDS signature, follow these steps:

**Step 1** Choose Configure > Controllers.

**Step 2** Choose a controller by clicking an IP address.

**Step 3** From the left sidebar menu, choose Security and then choose Standard Signatures or Custom Signatures.

**Step 4** To enable or disable an individual signature, click in the Name column for the type of attack you want to enable or disable.

The Standard Signature Parameters page shows the list of Cisco-supplied signatures that are currently on the controller. The Custom Signatures page shows the list of customer-supplied signatures that are currently on the controller. The following information is displayed either in the signature page or the detailed signature page:

- **Precedence**—The order, or precedence, in which the controller performs the signature checks.
- **Name**—The type of attack the signature is trying to detect.
- **Description**—A more detailed description of the type of attack that the signature is trying to detect.
- **Frame Type**—Management or data frame type on which the signature is looking for a security attack.
- **Action**—What the controller is directed to do when the signature detects an attack. One possibility is None, where no action is taken, and another is Report, to report the detection.
- **Frequency**—The signature frequency, or the number of matching packets per interval that must be identified at the detecting access point level before an attack is detected. The range is 1 to 32,000 packets per interval, and the default value is 50 packets per interval.
- **Quiet Time**—The length of time (in seconds) after which no attacks have been detected at the individual access point level, and the alarm can stop. This time appears only if the MAC information is all or both. The range is 60 to 32,000 seconds, and the default value is 300 seconds.
- **MAC Information**—Whether the signature is to be tracked per network or per MAC address or both at the detecting access point level.
- **MAC Frequency**—The signature MAC frequency, or the number of matching packets per interval that must be identified at the controller level before an attack is detected. The range is 1 to 32,000 packets per interval, and the default value is 30 packets per interval.
- **Interval**—Enter the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval. The range is 1 to 3600 seconds, and the default value is 1 second.
- **Enable**—Select this to enable this signature to detect security attacks or unselect it to disable this signature.
- **Signature Patterns**—The pattern that is being used to detect a security attack.

**Step 5** From the Enabled yes or no drop-down list, choose yes. Because you are downloading a customized signature, you should enable the files named with the _custom.sgi and disable the standard signature with the same name but differing suffix. (For example, if you are customizing broadcast probe flood, you want to disable broadcast probe flood in the standard signatures but enable it in custom signatures.)

**Step 6** To enable all standard and custom signatures currently on the controller, choose Edit Signature Parameters from the Select a command drop-down list, and choose Go. The Edit Signature Parameters page appears.
Step 7 Select the Check for All Standard and Custom Signatures field, Enable check box. This enables all signatures that were individually selected as enabled in Step 5. If this check box remains unselected, all files are disabled, even those that were previously enabled in Step 5. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller.

Step 8 Click Save.

Enabling Web Login

With web authentication, guests are automatically redirected to web authentication pages when they launch their browsers. Guests gain access to the WLAN through this web portal. Wireless LAN administrators using this authentication mechanism should have the option of providing unencrypted or encrypted guest access. Guest users can then log into the wireless network using a valid username and password, which is encrypted with SSL. Web authentication accounts might be created locally or managed by a RADIUS server. The Cisco Wireless LAN controllers can be configured to support a web authentication client. See the “Configuring a Web Authentication Template” section on page 11-61 to create a template that replaces the Web authentication page provided on the controller.

Step 1 Choose Configure > Controllers.

Step 2 Choose the controller on which to enable web authentication by clicking an IP address URL in the IP Address column.

Step 3 From the left sidebar menu, choose Security > AAA > Web Auth Configuration.

Step 4 Choose the appropriate web authentication type from the drop-down list. The choices are default internal, customized web authentication, or external.

- If you choose default internal, you can still alter the page title, message, and redirect URL, as well as choose whether the logo appears. Continue to Step 5.
- If you choose customized web authentication, skip to the “Downloading Customized Web Authentication” section on page 3-38.
- If you choose external, you need to enter the URL you want to redirect to after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user is directed to the company home page.

Step 5 Select the Logo Display check box if you want your company logo to display.

Step 6 Enter the title you want displayed on the Web authentication page.

Step 7 Enter the message you want displayed on the Web authentication page.

Step 8 In the Customer Redirect URL field, provide the URL where the user is redirected after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user is directed to the company home page.

Step 9 Click Save.
Downloading Customized Web Authentication

You can download a customized Web authentication page to the controller. A customized web page is created to establish a username and password for user web access.

When downloading customized web authentication, these strict guidelines must be followed:

- A username must be provided.
- A password must be provided.
- A redirect URL must be retained as a hidden input item after extracting from the original URL.
- The action URL must be extracted and set from the original URL.
- Scripts to decode the return status code must be included.
- All paths used in the main page should be of relative type.

Before downloading, if you chose the customized web authentication option in Step 4 of the previous section, follow these steps:

**Step 1**
Click the preview image to download the sample login.html bundle file from the server. See Figure 3-1 for an example of the login.html file. The downloaded bundle is a .TAR file.

![Login.html](image)

**Step 2**
Open and edit the login.html file and save it as a .tar or .zip file.

**Note**
You can edit the text of the Submit button with any text or HTML editor to read “Accept terms and conditions and Submit.”

**Step 3**
Make sure you have a Trivial File Transfer Protocol (TFTP) server available for the download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable.
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as Prime Infrastructure because the built-in TFTP server of the Prime Infrastructure and third-party TFTP server use the same communication port.
Step 4  Click here in the “After editing the HTML you might click here to redirect to the Download Web Auth Page” link to download the .tar or .zip file to the controller(s). The Download Customized Web Auth Bundle to Controller page appears.

| Note | The IP address of the controller to receive the bundle and the current status are displayed. |

Step 5  Choose local machine from the File is Located On field. If you know the filename and path relative to the root directory of the server, you can also choose TFTP server.

| Note | For a local machine download, either .zip or .tar file options exists, but the Prime Infrastructure does the conversion of .zip to .tar automatically. If you chose a TFTP server download, only .tar files are specified. |

Step 6  Enter the maximum amount of time in seconds before the controller times out while attempting to download the file in the Timeout field.

Step 7  The Prime Infrastructure Server Files In field specifies where the Prime Infrastructure server files are located. Specify the local file name in that directory or use the Browse button to navigate to it. A “revision” line in the signature file specifies whether the file is a Cisco-provided standard signature file or a site-tailored custom signature file (custom signature files must always have revision=custom).

Step 8  If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On field, and the Server File Name is populated. The local machine option initiates a two-step operation. First, the local file is copied from the workstation of the administrator to the built-in TFTP server of the Prime Infrastructure. Then the controller retrieves that file. For later operations, the file is already in the TFTP directory of the Prime Infrastructure server, and the download web page now automatically populates the filename.

Step 9  Click OK.

If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On field, and the Server File Name is populated for you.

Step 10  After completing the download, you are directed to the new page and able to authenticate.

---

**Connecting to the Guest WLAN**

To connect to the guest central WLAN to complete the web authentication process, follow these steps: See the “Creating Guest User Accounts” section on page 7-8 for more explanation of a guest user account.

Step 1  When you are set for open authentication and are connected, browse to the virtual interface IP address (such as /209.165.200.225/login.html).

Step 2  When the Prime Infrastructure user interface displays the Login page, enter your username and password.

| Note | All entries are case sensitive. |
The lobby ambassador has access to the templates only to add guest users.

## Certificate Signing Request (CSR) Generation

To generate a Certificate Signing Request (CSR) for a third-party certificate using the Prime Infrastructure, see the Appendix C, “Certificate Signing Request (CSR) Generation for a Third-Party Certificate on Cisco Prime Infrastructure.”
Performing Maintenance Operations

You can perform the actions at the system level, such as updating system softwares or downloading certificates that can be used with many items.

This chapter describes the system level tasks to perform with Cisco Prime Infrastructure. It contains the following sections:

- Information About Maintenance Operations, page 4-1
- Performing System Tasks, page 4-1
- Performing Prime Infrastructure Operations, page 4-6

Information About Maintenance Operations

A system-level task is a collection of tasks that relate to operations that apply to the Prime Infrastructure database as a whole. System tasks also include restoring the Prime Infrastructure database. For more information, see the “Restoring the Prime Infrastructure Database” section on page 4-8.

Performing System Tasks

This sections describes how to use the Prime Infrastructure to perform system-level tasks.

- Adding a Controller to the Prime Infrastructure Database, page 4-1
- Using Prime Infrastructure to Update System Software, page 4-2
- Downloading Vendor Device Certificates, page 4-3
- Downloading Vendor CA Certificates, page 4-4
- Using Prime Infrastructure to Enable Long Preambles for SpectraLink NetLink Phones, page 4-5
- Creating an RF Calibration Model, page 4-5

Adding a Controller to the Prime Infrastructure Database

To add a controller to the Prime Infrastructure database, follow these steps:
Performing System Tasks

Note
We recommend that you manage controllers through the controller dedicated service port for improved security. However, when you manage controllers that do not have a service port (such as 2000 series controllers) or for which the service port is disabled, you must manage those controllers through the controller management interface.

Step 1 Log into the Prime Infrastructure user interface.
Step 2 Choose Configure > Controllers to display the All Controllers page.
Step 3 From the Select a command drop-down list, choose Add Controller, and click Go.
Step 4 In the Add Controller page, enter the controller IP address, network mask, and required SNMP settings.
Step 5 Click OK. Prime Infrastructure displays a Please Wait dialog box while it contacts the controller and adds the current controller configuration to the Prime Infrastructure database. It then returns you to the Add Controller page.
Step 6 If the Prime Infrastructure does not find a controller at the IP address that you entered for the controller, the Discovery Status dialog displays this message:
No response from device, check SNMP.
Check these settings to correct the problem:
- The controller service port IP address might be set incorrectly. Check the service port setting on the controller.
- Prime Infrastructure might not have been able to contact the controller. Make sure that you can ping the controller from the Prime Infrastructure server.
- The SNMP settings on the controller might not match the SNMP settings that you entered in the Prime Infrastructure. Make sure that the SNMP settings configured on the controller match the settings that you entered in the Prime Infrastructure.
Step 7 Add additional controllers if desired.

Using Prime Infrastructure to Update System Software

To update controller (and access point) software using the Prime Infrastructure, follow these steps:

Step 1 Enter the ping ip-address command to be sure that the Prime Infrastructure server can contact the controller. If you use an external TFTP server, enter the ping ip-address command to be sure that the Prime Infrastructure server can contact the TFTP server.

Note
When you are downloading through a controller distribution system (DS) network port, the TFTP server can be on the same or a different subnet because the DS port is routable.

Step 2 Choose Configure > Controllers to navigate to the All Controllers page.
Step 3 Select the check box of the desired controller, choose Download Software (TFTP or FTP) from the Select a command drop-down list, and click Go. Prime Infrastructure displays the Download Software to Controller page.
Step 4  If you use the built-in Prime Infrastructure TFTP server, choose Default Server from the Server Name drop-down list box. If you use an external TFTP server, choose New from the Server Name drop-down list box and add the external TFTP server IP address.

Step 5  Enter the file path and server file name in their respective text boxes (for example, AS_2000_release.aes for 2000 series controllers). The files are uploaded to the root directory which was configured for use by the TFTP server. You can change to a different directory.

Note  Be sure that you have the correct software file for your controller.

Step 6  Click Download. Prime Infrastructure downloads the software to the controller, and the controller writes the code to flash RAM. As Prime Infrastructure performs this function, it displays its progress in the Status field.

### Downloading Vendor Device Certificates

Each wireless device (controller, access point, and client) has its own device certificates. For example, the controller is shipped with a Cisco-installed device certificate. This certificate is used by EAP-TLS and EAP-FAST (when not using PACs) to authenticate wireless clients during local EAP authentication. However, if you want to use your own vendor-specific device certificate, it must be downloaded to the controller.

To download a vendor-specific device certificate to the controller, follow these steps:

Step 1  Choose Configure > Controllers.

Step 2  You can download the certificates in one of two ways:
   a. Select the check box of the controller you choose.
   b. Choose Download Vendor Device Certificate from the Select a command drop-down list, and click Go.

   or

   a. Click the URL of the desired controller in the IP Address column.
   b. Choose System > Commands from the left sidebar menu.
   c. Choose TFTP or FTP in the Upload/Download Command section.
   d. Choose Download Vendor Device Certificate from the Upload/Download Commands drop-down list, and click Go.

Step 3  In the Certificate Password text box, enter the password which was used to protect the certificate.

Step 4  Specify if the certificate to download is on the TFTP server or on the local machine. If it is on the TFTP server, the name must be supplied in the Server File Name field. If the certificate is on the local machine, you must specify the file path in the Local File Name field using the Choose File button.

Step 5  Enter the TFTP server name in the Server Name field. The default is for the Prime Infrastructure server to act as the TFTP server.

Step 6  Enter the server IP address.

Step 7  In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.
Step 8 In the Timeout text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 9 In the Local File Name text box, enter the directory path of the certificate.

Step 10 Click OK.

---

**Downloading Vendor CA Certificates**

Controllers and access points have a certificate authority (CA) certificate that is used to sign and validate device certificates. The controller is shipped with a Cisco-installed CA certificate. This certificate might be used by EAP-TLS and EAP-FAST (when not using PACs) to authenticate wireless clients during local EAP authentication. However, if you want to use your own vendor-specific CA certificate, it must be downloaded to the controller. To download vendor CA certificate to the controller, follow the instructions:

Step 1 Choose Configure > Controllers.

Step 2 You can download the certificates in one of two ways:
   a. Select the check box of the controller you choose.
   b. Choose Download Vendor CA Certificate from the Select a command drop-down list, and click Go.

   or

   a. Click the URL of the desired controller in the IP Address column.
   b. Choose System > Commands from the left sidebar menu.
   c. Choose Download Vendor CA Certificate from the Upload/Download Commands drop-down list, and click Go.

Step 3 Specify if the certificate to download is on the TFTP server or on the local machine. If it is on the TFTP server, the name must be supplied in the Server File Name field in Step 9. If the certificate is on the local machine, you must specify the file path in the Local File Name field in Step 8 using the Browse button.

Step 4 Enter the TFTP server name in the Server Name field. The default is for the Prime Infrastructure server to act as the TFTP server.

Step 5 Enter the server IP address.

Step 6 In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 7 In the Timeout text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 8 In the Local File Name text box, enter the directory path of the certificate.

Step 9 Click OK.
Using Prime Infrastructure to Enable Long Preambles for SpectraLink NetLink Phones

A radio preamble (sometimes called a header) is a section of data at the head of a packet. It contains information that wireless devices need when sending and receiving packets. Short preambles improve throughput performance, so they are enabled by default. However, some wireless devices, such as SpectraLink NetLink phones, require long preambles.

To optimize the operation of SpectraLink NetLink phones on your wireless LAN, to use the Prime Infrastructure to enable long preambles, follow these steps:

1. Log into the Prime Infrastructure user interface.
2. Choose Configure > Controllers to navigate to the All Controllers page.
3. Click the IP address of the desired controller.
4. From the left sidebar menu, choose 802.11b/g/n > Parameters.
5. If the IP Address > 802.11b/g/n Parameters page shows that short preambles are enabled, continue to the next step. However, if short preambles are disabled, which means that long preambles are enabled, the controller is already optimized for SpectraLink NetLink phones, and you do not need to continue this procedure.
6. Enable long preambles by unselecting the Short Preamble check box.
7. Click Save to update the controller configuration.
8. To save the controller configuration, choose System > Commands from the left sidebar menu, choose Save Config To Flash from the Administrative Commands drop-down list, and click Go.
9. To reboot the controller, choose Reboot from the Administrative Commands drop-down list and click Go.
10. Click OK when the following message appears.

Please save configuration by clicking “Save Config to flash”. Do you want to continue rebooting anyways?

The controller reboots. This process might take some time, during which the Prime Infrastructure loses its connection to the controller.

Note You can view the controller reboot process with a command-line interface session.

Creating an RF Calibration Model

If you would like to further refine the Prime Infrastructure Location tracking of client and rogue access points across one or more floors of a building, you have the option of creating an RF calibration model that uses physically collected RF measurements to fine-tune the location algorithm. When you have multiple floors in a building with the same physical layout as the calibrated floor, you can save time calibrating the remaining floors by using the same RF calibration model for the remaining floors.
The calibration models are used as RF overlays with measured RF signal characteristics that can be applied to different floor areas. This allows the Cisco Unified Wireless Network Solution installation team to lay out one floor in a multi-floor area, use the RF calibration tool to measure and save the RF characteristics of that floor as a new calibration model, and apply that calibration model to all the other floors with the same physical layout.

Performing Prime Infrastructure Operations

- Verifying the Status of Prime Infrastructure, page 4-6
- Stopping Prime Infrastructure, page 4-6
- Backing Up the Prime Infrastructure Database, page 4-7
- Restoring the Prime Infrastructure Database, page 4-8
- Restoring the Prime Infrastructure Database in a High Availability Environment, page 4-9
- Upgrading WCS to Prime Infrastructure, page 4-9
- Upgrading the Network, page 4-10
- Reinitializing the Database, page 4-10
- Recovering the Prime Infrastructure Password, page 4-11
- Performing Disk Cleanup, page 4-11

Verifying the Status of Prime Infrastructure

This section provides instructions for checking the status of the Prime Infrastructure. To check the status of the Prime Infrastructure, you can check the status at any time, follow these steps:

Step 1 Log into the system as admin.
Step 2 Using the CARS command-line interface, enter `ncs status` command.

The command-line interface displays messages indicating the status of the Prime Infrastructure.

Stopping Prime Infrastructure

This section provides instructions for stopping the Prime Infrastructure. You can stop the Prime Infrastructure at any time. To stop the Prime Infrastructure, follow these steps:

Note If any users are logged in when you stop the Prime Infrastructure, their Prime Infrastructure sessions stop functioning.

Step 1 Log into the system as admin.
Performing Prime Infrastructure Operations

To see which version of the Prime Infrastructure you currently have installed, enter `show application version ncs`.

### Step 2
Using the CARS command-line interface, enter `ncs stop` command.
The command-line interface displays messages indicating that the Prime Infrastructure is stopping.

### Backing Up the Prime Infrastructure Database

This section provides instructions for backing up the Prime Infrastructure database. You can schedule regular backups through the Prime Infrastructure user interface or manually initiate a backup. The following files are backed up using both the Prime Infrastructure user interface and command-line interface:

- Oracle database
- Maps
- Report files
- Accuracy files used for generating reports
- USERMGT file

The device configurations are obtained from the devices in the backup files.

**Note**
Machine specific settings (such as FTP enable and disable, FTP port, FTP root directory, TFTP enable and disable, TFTP port, TFTP root directory, HTTP forward enable and disable, HTTP port, HTTPS port, report repository directory, and all high availability settings) are not included in the back up and restore function if the back up is restored to a different device.

- Scheduling Automatic Backups, page 4-7
- Performing a Manual Backup, page 4-8

### Scheduling Automatic Backups

To schedule automatic backups of the Prime Infrastructure database, follow these steps:

1. Log into the Prime Infrastructure user interface.
2. Choose **Administration > Background Tasks** to display the Scheduled Tasks page.
3. Click **NCS Server Backup** task.
4. Select the **Enabled** check box.
5. At the Backup Repository field, choose an existing backup repository, or click **Create** to create a new repository.
6. If you are backing up in remote location, select the **FTP Repository** check box. You need to enter the FTP location, username, and password of the remote machine.
Performing Prime Infrastructure Operations

Chapter 4 Performing Maintenance Operations

Step 7 In the Interval (Days) text box, enter a number representing the number of days between each backup. For example, 1 = a daily backup, 2 = a backup every other day, 7 = a weekly backup, and so on.

Range: 1 to 360
Default: 7

Step 8 In the Time of Day text box, enter the time when you want the backup to start. It must be in this format: hh:mm AM/PM (for example: 03:00 AM).

Note Backing up a large database affects the performance of the Prime Infrastructure server. Therefore, we recommend that you schedule backups to run when the Prime Infrastructure server is idle (for example, in the middle of the night).

Step 9 Click Submit to save your settings. The backup file is saved as a .zip file in the ftp-install-dir/ftp-server/admin/NCSBackup directory using this format: dd-mmm-yyyy_hh-mm-ss.zip (for example, 11-Nov-05_10-30-00.zip).

Performing a Manual Backup

To back up the Prime Infrastructure database, follow these steps:

Note We recommend that you do a backup using the User Interface when the system is running. To do this, choose Administration > Background Tasks, select the NCS Server Backup task, and then select Execute Now.

Step 1 Log into the system as admin.

Step 2 You can perform a backup using the command-line interface.

Step 3 Back up the application data to the repository (local or remote) by entering the following command:

```
backup testbackup repository backup_repo application NCS
```

Restoring the Prime Infrastructure Database

If you are restoring the Prime Infrastructure database in a high availability environment, see the “Restoring the Prime Infrastructure Database in a High Availability Environment” section on page 4-9.

To restore the Prime Infrastructure database from a backup file, follow these steps:

Step 1 To view all local repository backups, enter the following command:

```
show repository backup_repo
```

Note If possible, stop all the Prime Infrastructure user interfaces to stabilize the database.

Step 2 Manually shut down the platform using the ncs stop command.
Step 3  Restore the application back up by entering the following command:

```
restore backup gpg file repository repository name application NCS
```

Step 4  Click Yes if a message appears indicating that the Prime Infrastructure is running and needs to be shut down.

The command-line interface displays messages indicating that the Prime Infrastructure database is being restored.

### Restoring the Prime Infrastructure Database in a High Availability Environment

During installation, you were prompted to determine if a secondary Prime Infrastructure server would be used for high availability support to the primary Prime Infrastructure server. If you opted for this high availability environment and enabled it in the Administration > High Availability page, the status appears as HA enabled. Before restoring a database, you must convert the status to HA not configured.

**Caution**

You should not upgrade the system while the system is in HA enabled mode. If you attempt to restore the database while the status is set to HA enabled, unexpected results might occur.

To change the status from HA enabled to HA not configured, do the following

- Choose Administration > High Availability.
- Click Remove in the HA Configuration page.

The primary server is now in HA Not Configured mode, and you can safely restore the data from the back up.

Once the data is successfully restored and the system is operational, reestablish the HA between the primary and the secondary systems.

### Upgrading WCS to Prime Infrastructure

A direct upgrade from a WCS release to the Prime Infrastructure 1.2 is not supported. You must first upgrade to an NCS 1.1 release, and then upgrade to the Prime Infrastructure 1.2.

Prime Infrastructure supports data migration in the NCS Releases 1.0.2.29, 1.1.0.58, and 1.1.1.24. Before you migrate from an NCS release to Prime Infrastructure 1.2, you must perform the following:

- Install the ‘disk space management’ patch to the existing system.
- Ensure that you perform a back up before attempting to upgrade.
- Use a console connection when you upgrade, to avoid Telnet/SSH terminal timeouts.
- Remove high availability before performing the upgrade.

For detailed information about the application upgrade, see the following URL:


If you are upgrading to the Prime Infrastructure in a high availability environment, see the “Upgrading Prime Infrastructure in a High Availability Environment” section on page 4-10.
### Upgrading Prime Infrastructure in a High Availability Environment

If you have a primary and secondary Prime Infrastructure, follow these steps for a successful upgrade:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Step 1** | You must first remove the HA configuration with the following steps:  
   a. Log in to the primary Prime Infrastructure server.  
   b. Choose Administration > High Availability, and choose HA Configuration from the left sidebar menu.  
   c. Click Remove to remove the HA configuration.  
   
   **Note** | It might take a few minutes for the remove to complete. |
| **Step 2** | You must first upgrade the secondary Prime Infrastructure with the following steps:  
   a. Shut down the secondary Prime Infrastructure. See the “Stopping Prime Infrastructure” section on page 4-6 for more information.  
   b. Perform an upgrade on the secondary Prime Infrastructure.  
   c. Start the secondary Prime Infrastructure.  
   
   **Note** | You can use ncs stop for a graceful shut down. |
| **Step 3** | Upgrade the primary Prime Infrastructure.  
   a. Shut down the primary Prime Infrastructure. See the “Stopping Prime Infrastructure” section on page 4-6 for more information.  
   b. Perform an upgrade on the primary Prime Infrastructure.  
   c. Start the primary Prime Infrastructure. |
| **Step 4** | Enable HA again on the primary Prime Infrastructure.  
   a. Login to the primary Prime Infrastructure server.  
   b. Choose Administration > High Availability and select HA Configuration from the left sidebar menu.  
   c. Enter the HA configuration settings and click Save to enable high availability. |

### Upgrading the Network

Network upgrades must follow a recommended procedure so that databases can remain synchronized with each other. For example, You cannot upgrade the controller portion of the network to a newer release but maintain the current Prime Infrastructure version and not upgrade it. The supported order of upgrade is Prime Infrastructure first, followed by the controller, and then any additional devices.

### Reinitializing the Database

If you need to reset the database because of a synchronization problem or a corruption of some type, enter ncs db reinitdb to reinitialize the database.
Recovering the Prime Infrastructure Password

You can change the Prime Infrastructure application root user or FTP user password. This option provides a safeguard if you lose the root password. An executable was added to the installer /bin directory (passwd.bat for Windows and passwd.sh for Linux). To recover the passwords and regain access, follow these steps:

Note
If you are a Linux user, you must be the root user to run the command.

Note
In Linux, use the **passwd.sh** to change the Prime Infrastructure password. The **passwd** is a built-in Linux command to change the OS password.

Step 1
Log in to the Prime Infrastructure command-line interface as an admin user.

Step 2
Run the following command:

```
ncs password root password
```

Where **password** is the root user login password. You can enter a password not exceeding 80 characters.

Example of the command usage:

```
ncs-appliance/admin# ncs password root password ?
<WORD> Type in root user login password (Max Size - 80)
```

You should now be able to login to the Prime Infrastructure web interface with the new root password.

Performing Disk Cleanup

When the Prime Infrastructure is running low on disk space, an alarm is raised in the system. Also, the following error appears as a pop-up dialog box.

The system is running low on disk space, please refer to online help to perform disk cleanup.

To resolve this issue, use the following CLI command:

```
ncs cleanup
```

You can use this command to free up and reclaim disk space.

For more information, see the “Performing Disk Cleanup” section on page A-9.
Monitoring Devices

Information About Monitoring

This chapter describes how to use the Cisco Prime Infrastructure to monitor Cisco WLAN Solution device configurations. This chapter contains the following sections:

- Monitoring Controllers, page 5-1
- Monitoring Third Party Controllers, page 5-33
- Monitoring Switches, page 5-34
- Monitoring Access Points, page 5-43
- Monitoring RFID Tags, page 5-112
- Monitoring Chokepoints, page 5-115
- Monitoring Interferers, page 5-116
- Monitoring Spectrum Experts, page 5-119
- Monitoring WiFi TDOA Receivers, page 5-121
- Monitoring Media Streams, page 5-122
- Monitoring Radio Resource Management (RRM), page 5-123
- Monitoring Clients and Users, page 5-126
- Monitoring Alarms, page 5-126
- Monitoring Events, page 5-141
- Monitoring Site Maps, page 5-149
- Monitoring Google Earth Maps, page 5-149

Monitoring Controllers

Choose Monitor > Controllers to access the controller list page. Click a controller IP address to view its details.

- Searching Controllers, page 5-2
- Viewing a List of Controllers, page 5-2
- Monitoring System Parameters, page 5-3
- Monitoring Ports, page 5-9
Searching Controllers

Use the Prime Infrastructure Search feature to find specific controllers or to create and save custom searches.

For a controller search, you can search using the following fields:

<table>
<thead>
<tr>
<th>Table 5-1</th>
<th>Search Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fields</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| Search for controller by | Choose All Controllers, IP Address, Controller Name, or Network.  
  Note: Search fields might change depending on the selected category. When applicable, enter the additional field or filter information to help identify the Search By category. |
| Enter Controller IP Address | This field only appears if you select IP Address from the Search for controller by field. |
| Enter Controller Name | This field only appears if you select Controller Name from the Search for controller by field. |
| Audit Status | Choose one of the following from the drop-down list:  
  - All Status  
  - Mismatch—Configuration differences were found between Prime Infrastructure and controller during the last audit.  
  - Identical—No configuration differences were found during the last audit.  
  - Not Available—Audit status is unavailable. |

Viewing a List of Controllers

Choose Monitor > Controllers or perform a controller search to access the controller list page.

Note: For more information on performing an advanced search, see the Search Methods section in the Cisco Prime Infrastructure 2.0 User Guide.
The data area of this page contains a table with the following columns.

**Table 5-2  Controller List Details**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Local network IP address of the controller management interface. Click an IP address in the list to display the controller details.</td>
</tr>
<tr>
<td>Controller Name</td>
<td>Name of the controller.</td>
</tr>
<tr>
<td>Location</td>
<td>The geographical location (such as a campus or building).</td>
</tr>
<tr>
<td>Mobility Group Name</td>
<td>Name of the controller mobility or WPS group.</td>
</tr>
<tr>
<td>Reachability Status</td>
<td>Reachable or Unreachable. Click the title to toggle from ascending to descending order.</td>
</tr>
</tbody>
</table>

Click the title to toggle from ascending to descending order. To add, remove, or reorder columns in the table, click the **Edit View** link to go to the Edit View page.

**Configuring the Controller List Display**

The **Edit View** page allows you to add, remove, or reorder columns in the Controllers table.

To edit the available columns in the Controllers table, follow these steps:

1. **Step 1** Choose **Monitor > Controllers**.
2. **Step 2** Click the **Edit View** link.
3. **Step 3** To add an additional column to the controllers table, click to highlight the column heading in the left list. Click **Show** to move the heading to the right list. All items in the right list are displayed in the Controllers table.
4. **Step 4** To remove a column from the Controllers table, click to highlight the list heading in the right list. Click **Hide** to move the heading to the left list. All items in the left list are not displayed in the Controllers table.
5. **Step 5** Use the buttons to specify the order in which the information appears in the table. Highlight the desired list heading and click **Up** or **Down** to move it higher or lower in the current list.
6. **Step 6** Click **Reset** to restore the default view.
7. **Step 7** Click **Submit** to confirm the changes.

**Monitoring System Parameters**

This section provides the detailed information regarding monitoring controller system parameters and contains the following topics:

- **Monitoring System Summary**, page 5-4
- **Monitoring Spanning Tree Protocol**, page 5-5
- **Monitoring CLI Sessions**, page 5-7
- **Monitoring DHCP Statistics**, page 5-8
 Monitoring System Summary

This page displays a summary of the controller parameters with a graphic displaying the status of the controller. The graphic of the front of the controller shows front-panel ports (click a port to go to Monitor Controllers > IPaddr > Ports > General for information about that port). You can find the links to alarms, events and access points details related to the controller.

You can access this page in the following ways:

- Choose **Monitor > Controllers** and click the applicable IP address.
- Choose **Monitor > Access Points**, click a list item under AP Name, then click **Registered Controller**.
- Choose **Configure > Access Points**, choose a list item under AP Name, then click **Registered Controller**.

Click **Controllers** in the page title to view a list of all the controllers. See the “Viewing a List of Controllers” section on page 5-2.

**Table 5-3** lists the Monitoring System Summary page fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Local network IP address of the controller management interface.</td>
</tr>
<tr>
<td>Name</td>
<td>User-defined name of the controller.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Type of controller.</td>
</tr>
<tr>
<td>UP Time</td>
<td>Time in days, hours and minutes since the last reboot.</td>
</tr>
<tr>
<td>System Time</td>
<td>Time used by the controller.</td>
</tr>
<tr>
<td>Internal Temperature</td>
<td>The temperature of the controller.</td>
</tr>
<tr>
<td>Location</td>
<td>User-defined physical location of the controller.</td>
</tr>
<tr>
<td>Contact</td>
<td>Contact person or the owner of the controller.</td>
</tr>
<tr>
<td>Total Client Count</td>
<td>Total number of clients currently associated with the controller.</td>
</tr>
<tr>
<td>Current CAPWAP Transport Mode</td>
<td>Control and Provisioning of Wireless Access Points (CAPWAP) protocol transport mode. Communications between controllers and access points. Choose <strong>Layer 2</strong> or <strong>Layer 3</strong>.</td>
</tr>
<tr>
<td>Power Supply One</td>
<td>If the power supply is available and operation. This is only for 4400 series controller.</td>
</tr>
<tr>
<td>Power Supply Two</td>
<td>If the power supply is available and operation. This is only for 4400 series controller.</td>
</tr>
<tr>
<td>Inventory</td>
<td></td>
</tr>
<tr>
<td>Software Version</td>
<td>The operating system release version number currently running on the controller.</td>
</tr>
<tr>
<td>Emergency Image Version</td>
<td>An image version of the controller.</td>
</tr>
</tbody>
</table>
Chapter 5 Monitoring Devices

Monitoring Controllers

The Spanning Tree Protocol (STP) is a link management protocol. Cisco WLAN Solution implements the IEEE 802.1D standard for media access control bridges.

### Table 5-3 Monitoring System Summary Page Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Description of the inventory item.</td>
</tr>
<tr>
<td>Model No</td>
<td>Specifies the machine model as defined by the Vital Product Data.</td>
</tr>
<tr>
<td>Serial No</td>
<td>Unique serial number for this controller.</td>
</tr>
<tr>
<td>Burned-in MAC Address</td>
<td>The burned-in MAC address for this controller.</td>
</tr>
<tr>
<td>Number of APs Supported</td>
<td>The maximum number of access points supported by the controller.</td>
</tr>
<tr>
<td>Gig Ethernet/Fiber Card</td>
<td>Displays the presence or absence of the optional 1000BASE-T/1000BASE-SX GigE card.</td>
</tr>
<tr>
<td>Crypto Card One</td>
<td>Displays the presence or absence of an enhanced security module which enables IPsec security and provides enhanced processing power.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> By default, the enhanced security module is not installed on a controller.</td>
</tr>
<tr>
<td></td>
<td>Maximum number of crypto cards that can be installed on a Cisco Wireless LAN controller:</td>
</tr>
<tr>
<td></td>
<td>- Cisco 2000 Series—None</td>
</tr>
<tr>
<td></td>
<td>- Cisco 4100 Series—One</td>
</tr>
<tr>
<td></td>
<td>- Cisco 4400 Series—Two</td>
</tr>
<tr>
<td>Crypto Card Two</td>
<td>Displays the presence or absence of a second enhanced security module.</td>
</tr>
<tr>
<td>GIGE Port(s) Status</td>
<td>Up or Down. Click to review the status of the port.</td>
</tr>
<tr>
<td>Unique Device Identifier (UDI)</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Product type. Chassis for controller and Cisco AP for access points.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of controller and might include number of access points.</td>
</tr>
<tr>
<td>Product ID</td>
<td>Orderable product identifier.</td>
</tr>
<tr>
<td>Version ID</td>
<td>Version of product identifier.</td>
</tr>
<tr>
<td>Serial No</td>
<td>Unique product serial number.</td>
</tr>
<tr>
<td>Utilization</td>
<td></td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>Displays a graph of the maximum, average, and minimum CPU utilization over the specified amount of time.</td>
</tr>
<tr>
<td>Memory Utilization</td>
<td>Displays a graph of the maximum, average, and minimum memory utilization over the specified amount of time.</td>
</tr>
</tbody>
</table>
Spanning tree algorithm provides redundancy while preventing undesirable loops in a network that are created by multiple active paths between stations. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail.

You can access this page in the following ways:

- Choose Monitor > Controllers, select an IP address, and choose System > Spanning Tree Protocol from the left sidebar menu.
- Choose Monitor > Clients, click a list item under AP Name, click Registered Controller, then choose System > Spanning Tree Protocol from the left sidebar menu.

**Note**

The controllers that do not support Spanning Tree Protocol are WISM, 2500, 5500, 7500 and SMWLC.

Table 5-4 lists the Spanning Tree Protocol page fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Spanning Tree Specification</td>
<td>An indication of what version of the Spanning Tree Protocol is being run. IEEE 802.1D implementations return 'IEEE 802.1D'. If future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version, a new value is defined.</td>
</tr>
<tr>
<td>Spanning Tree Algorithm</td>
<td>Specifies if this controller participates in the Spanning Tree Protocol. Might be enabled or disabled by choosing the corresponding line in the drop-down list. The factory default is disabled.</td>
</tr>
<tr>
<td>Priority</td>
<td>The value of the writable portion of the Bridge ID, that is, the first two octets of the (8 octet long) Bridge ID. The other (last) 6 octets of the Bridge ID are given by the value of Bridge MAC Address. The value might be specified as a number between 0 and 65535. The factory default is 32768.</td>
</tr>
<tr>
<td><strong>STP Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Topology Change Count</td>
<td>The total number of topology changes detected by this bridge since the management entity was last reset or initialized.</td>
</tr>
<tr>
<td>Time Since Topology Changed</td>
<td>Time (in days, hours, minutes, and seconds) since a topology change was detected by the bridge.</td>
</tr>
<tr>
<td>Designated Root</td>
<td>The bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol as executed by this node. This value is used as the Root Identifier parameter in all Configuration Bridge PDUs originated by this node.</td>
</tr>
<tr>
<td>Root Cost</td>
<td>The cost of the path to the root as seen from this bridge.</td>
</tr>
<tr>
<td>Root Port</td>
<td>The port number of the port which offers the lowest cost path from this bridge to the root bridge.</td>
</tr>
</tbody>
</table>
Monitor > Controllers, click the applicable IP address, then choose System > CLI Sessions from the left sidebar menu. 
- Choose Monitor > Clients, click a list item under AP Name, click Registered Controller, then choose System > CLI Sessions from the left sidebar menu.

Table 5-5 lists CLI Sessions page fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Index</td>
<td>Session identification.</td>
</tr>
<tr>
<td>Username</td>
<td>Login username.</td>
</tr>
<tr>
<td>Connection Type</td>
<td>Telnet or serial session.</td>
</tr>
<tr>
<td>Connection From</td>
<td>IP address of the client computer system.</td>
</tr>
<tr>
<td>Session Time</td>
<td>Elapsed active session time.</td>
</tr>
<tr>
<td>Idle Time</td>
<td>Elapsed inactive session time.</td>
</tr>
</tbody>
</table>
Monitoring DHCP Statistics

Prime Infrastructure provides DHCP server statistics for Version 5.0.6.0 controllers or later. These statistics include information on the packets sent and received, DHCP server response information, and the last request time stamp.

To access this page, choose Monitor > Controllers, click the applicable IP address, then choose System > DHCP Statistics from the left sidebar menu.

Table 5-6 lists the The DHCP Statistics page fields.

Table 5-6    DHCP Statistics Page Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server IP</td>
<td>Identifies the IP address of the server.</td>
</tr>
<tr>
<td>Is Proxy</td>
<td>Identifies whether or not this server is proxy.</td>
</tr>
<tr>
<td>Discover Packets Sent</td>
<td>Identifies the total number of packets sent intended to locate available servers.</td>
</tr>
<tr>
<td>Request Packets Sent</td>
<td>Identifies the total number of packets sent from the client requesting parameters from the server or confirming the correctness of an address.</td>
</tr>
<tr>
<td>Decline Packets</td>
<td>Identifies the number of packets indicating that the network address is already in use.</td>
</tr>
<tr>
<td>Inform Packets</td>
<td>Identifies the number of client requests to the DHCP server for local configuration parameters because the client already has an externally configured network address.</td>
</tr>
<tr>
<td>Release Packets</td>
<td>Identifies the number of packets that release the network address and cancel the remaining lease.</td>
</tr>
<tr>
<td>Reply Packets</td>
<td>Identifies the number of reply packets.</td>
</tr>
<tr>
<td>Offer Packets</td>
<td>Identifies the number of packets that respond to the discover packets with an offer of configuration parameters.</td>
</tr>
<tr>
<td>Ack Packets</td>
<td>Identifies the number of packets that acknowledge successful transmission.</td>
</tr>
<tr>
<td>Nak Packets</td>
<td>Identifies the number of packets that indicate that the transmission occurred with errors.</td>
</tr>
<tr>
<td>Tx Failures</td>
<td>Identifies the number of transfer failures that occurred.</td>
</tr>
<tr>
<td>Last Response Received</td>
<td>Provides a timestamp of the last response received.</td>
</tr>
<tr>
<td>Last Request Sent</td>
<td>Provides a timestamp of the last request sent.</td>
</tr>
</tbody>
</table>
Monitoring WLANs

Choose Monitor > Controllers click a controller IP address, and choose WLANs from the left sidebar menu. This page enables you to view a summary of the wireless local access networks (WLANs) that you have configured on this controller.

Table 5-7 lists the WLAN Details page fields.

Table 5-7 WLAN Page Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN ID</td>
<td>Identification number of the WLAN.</td>
</tr>
<tr>
<td>Profile Name</td>
<td>User-defined profile name specified when initially creating the WLAN. Profile Name is the WLAN name.</td>
</tr>
<tr>
<td>SSID</td>
<td>User-defined SSID name.</td>
</tr>
<tr>
<td>Security Policies</td>
<td>Security policies enabled on the WLAN.</td>
</tr>
<tr>
<td>No of Mobility Anchors</td>
<td>Mobility anchors are a subset of a mobility group specified as the anchor controllers for a WLAN.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Status of the WLAN is either enabled or disabled.</td>
</tr>
<tr>
<td>No. of Clients</td>
<td>Current number of clients currently associated with this WLAN.</td>
</tr>
</tbody>
</table>

Monitoring Ports

This section provides the detailed information regarding monitoring controller port parameters and contains the following topics:

- Monitoring General Ports, page 5-9
- Monitoring CDP Interface Neighbors, page 5-14

Monitoring General Ports

The Ports > General page provides information regarding physical ports on the selected controller. Click a port number to view details for that port. See the “Port Details” section on page 5-10 for more information.
Table 5-8 lists the General page fields.

**Table 5-8 General Page Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Click the port number to view port details. See the “Port Details” section on page 5-10 for more information.</td>
</tr>
<tr>
<td>Physical Mode</td>
<td>Displays the physical mode of all ports. The choices include the following:</td>
</tr>
<tr>
<td></td>
<td>- 100 Mbps Full Duplex</td>
</tr>
<tr>
<td></td>
<td>- 100 Mbps Half Duplex</td>
</tr>
<tr>
<td></td>
<td>- 10 Mbps Full Duplex</td>
</tr>
<tr>
<td></td>
<td>- 10 Mbps Half Duplex</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Displays the port state as either Enable or Disable.</td>
</tr>
<tr>
<td>STP State</td>
<td>Displays the STP state of the port as either Forwarding or Disabled.</td>
</tr>
<tr>
<td>Physical Status</td>
<td>Displays the actual port physical interface:</td>
</tr>
<tr>
<td></td>
<td>- Auto Negotiate</td>
</tr>
<tr>
<td></td>
<td>- Half Duplex 10 Mbps</td>
</tr>
<tr>
<td></td>
<td>- Full Duplex 10 Mbps</td>
</tr>
<tr>
<td></td>
<td>- Half Duplex 100 Mbps</td>
</tr>
<tr>
<td></td>
<td>- Full Duplex 100 Mbps</td>
</tr>
<tr>
<td></td>
<td>- Full Duplex 1 Gbps</td>
</tr>
<tr>
<td>Link Status</td>
<td>Red (down/failure), Yellow (alarm), Green (up/normal).</td>
</tr>
</tbody>
</table>

To access the Monitor > Ports > General page, do one of the following:

- Choose **Configure > Controllers**, click the applicable IP address. From the left sidebar menu, choose **General** under Ports.
- Choose **Monitor > Controllers**, click the applicable, and click a port to access this page.
- Choose **Monitor > Access Points** and click a list item under AP Name, click **Registered Controller**, then click a port to access this page.
- Choose **Monitor > Clients** and click a list item under AP Name, then click **Registered Controller**, then click a port to access this page.

**Port Details**

**Note**

Click **Alarms** to open the Monitor Alarms page. See the “Monitoring Alarms” section on page 5-126 for more information.

Click **Events** to open the Monitor Events page. See the “Monitoring Events” section on page 5-141 for more information.
Table 5-9 lists the Port Detail page fields.

**Table 5-9 Port Details Page Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Displays the operational status of the controller: The options are UP or DOWN.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>The number of packets of unknown type which were received from this server on this port.</td>
</tr>
<tr>
<td>Unknown Protocol Packets</td>
<td>The number of packets of unknown type which were received from this server on this port.</td>
</tr>
<tr>
<td>Traffic (Received and Transmitted)</td>
<td></td>
</tr>
<tr>
<td>Total Bytes</td>
<td>The total number of packets received.</td>
</tr>
<tr>
<td>Packets</td>
<td>The total number of packets (including bad packets) received that were within the indicated octet range in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets Discarded</td>
<td>Packets Discarded (Received/Transmitted): The number of inbound/outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.</td>
</tr>
<tr>
<td>Unicast Packets</td>
<td>The number of subnetwork-unicast packets delivered/sent to a higher-layer protocol.</td>
</tr>
<tr>
<td>Broadcast Packets</td>
<td>The total number of packets received/sent that were directed to the broadcast address.</td>
</tr>
<tr>
<td>Errors in Packets</td>
<td>The total number of packets received with errors.</td>
</tr>
<tr>
<td>Received packets with MAC errors</td>
<td></td>
</tr>
</tbody>
</table>
Table 5-9  Port Details Page Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jabbers</td>
<td>The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Note</td>
<td>This definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10Base-5) and section 10.3.1.4 (10Base-2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 and 150 ms.</td>
</tr>
<tr>
<td>Fragments/Undersize</td>
<td>The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Alignment Errors</td>
<td>The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.</td>
</tr>
<tr>
<td>FCS Errors</td>
<td>The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.</td>
</tr>
<tr>
<td>Transmit discards</td>
<td></td>
</tr>
<tr>
<td>Single Collision Frames</td>
<td>A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.</td>
</tr>
<tr>
<td>Multiple Collision Frames</td>
<td>A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.</td>
</tr>
<tr>
<td>Deferred Transmissions</td>
<td>A count of frames for which transmission on a particular interface fails due to deferred transmissions.</td>
</tr>
<tr>
<td>Late Collisions</td>
<td>A count of frames for which transmission on a particular interface fails due to late collisions.</td>
</tr>
<tr>
<td>Excessive Collisions</td>
<td>A count of frames for which transmission on a particular interface fails due to excessive collisions.</td>
</tr>
<tr>
<td>Ether Stats</td>
<td></td>
</tr>
</tbody>
</table>
### Table 5-9 Port Details Page Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRC Align Errors</td>
<td>The number of incoming packets with the Checksum (FCS) alignment error. This represents a count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. Received frames for which multiple error conditions obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</td>
</tr>
<tr>
<td>Undersize Packets</td>
<td>The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Oversize Packets</td>
<td>The total number of frames that exceeded the maximum permitted frame size. This counter has a maximum increment rate of 815 counts per second at 10 Mbps.</td>
</tr>
<tr>
<td>Ether Stats Collisions</td>
<td>The number of packets with collision errors.</td>
</tr>
<tr>
<td>SQE Test Errors</td>
<td>Signal Quality Error Test errors (that is, Heartbeat) during transmission. This tests the important collision detection electronics of the transceiver, and lets the Ethernet interface in the computer know that the collision detection circuits and signal paths are working correctly. The errors indicate a count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.</td>
</tr>
<tr>
<td>Internal MAC Receive Errors</td>
<td>A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLong property, the AlignmentErrors property, or the FCSErrors property. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object might represent a count of receive errors on a particular interface that are not otherwise counted.</td>
</tr>
</tbody>
</table>
To access the Monitor CDP Interface Neighbors page, follow these steps:

**Step 1**  Choose Monitor > Controllers.

**Step 2**  Click the IP address of the applicable controller.

**Step 3**  From the left sidebar menu, choose CDP Interface Neighbors (under the Port heading).

---

### Table 5-9  Port Details Page Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal MAC Transmit Errors</td>
<td>A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions property, the ExcessiveCollisions property, or the CarrierSenseErrors property. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object might represent a count of transmission errors on a particular interface that are not otherwise counted.</td>
</tr>
<tr>
<td>Carrier Sense Errors</td>
<td>The Carrier Sense detects the presence of a carrier. The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface.</td>
</tr>
<tr>
<td>Too Long Frames</td>
<td>A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the FrameTooLong status is returned by the MAC layer to the LLC (or other MAC user). Received frames for which multiple error conditions obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</td>
</tr>
</tbody>
</table>
Step 4 Table 5-10 lists the CDP Interface Neighbors page fields.

**Table 5-10**  CDP Interface Neighbors Page Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Interface</td>
<td>Local Port information.</td>
</tr>
<tr>
<td>Neighbor Name</td>
<td>The name of each CDP neighbor.</td>
</tr>
<tr>
<td>Neighbor Address</td>
<td>The IP address of each CDP neighbor.</td>
</tr>
<tr>
<td>Neighbor Port</td>
<td>The port used by each CDP neighbor for transmitting CDP packets.</td>
</tr>
<tr>
<td>Capability</td>
<td>The functional capability of each CDP neighbor.</td>
</tr>
<tr>
<td>Platform</td>
<td>The hardware platform of each CDP neighbor device.</td>
</tr>
<tr>
<td>Duplex</td>
<td>Indicates Full Duplex or Half Duplex.</td>
</tr>
<tr>
<td>Software Version</td>
<td>The software running on the CDP neighbor.</td>
</tr>
</tbody>
</table>

**Monitoring Controller Security**

This section provides the detailed information regarding monitoring controller security and contains the following topics:

- Monitoring RADIUS Authentication, page 5-15
- Monitoring RADIUS Accounting, page 5-17
- Monitoring Management Frame Protection, page 5-19
- Monitoring Rogue AP Rules, page 5-20
- Monitoring Guest Users, page 5-22

**Monitoring RADIUS Authentication**

The RADIUS Authentication page displays RADIUS authentication server information and enables you to add or delete a RADIUS authentication server.

To access this page, do one of the following:

- Choose Monitor > Controllers, click the applicable IP address, then choose Security > Radius Authentication from the left sidebar menu.
- Choose Monitor > Access Points, click a list item under AP Name, click Registered Controller, then choose Security > Radius Authentication from the left sidebar menu.
- Choose Monitor > Clients, click a list item under AP Name, click Registered Controller, then choose Security > Radius Authentication from the left sidebar menu.
Table 5-11 lists the RADIUS Authentication page fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RADIUS Authentication Servers</strong></td>
<td></td>
</tr>
<tr>
<td>Server Index</td>
<td>Access priority number for RADIUS servers. Up to four servers can be configured, and controller polling of the servers starts with Index 1, Index 2 second, and so forth. The index number is based on when the RADIUS server is added to the controller.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the RADIUS server.</td>
</tr>
<tr>
<td>Ping</td>
<td>Click the icon to ping the RADIUS server from the controller to verify the link.</td>
</tr>
<tr>
<td>Port</td>
<td>Controller port number for the interface protocols.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Indicates whether the server is enabled or disabled.</td>
</tr>
<tr>
<td><strong>Authentication Server Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Msg Round Trip Time</td>
<td>The time interval (in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.</td>
</tr>
<tr>
<td>First Requests</td>
<td>The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.</td>
</tr>
<tr>
<td>Retry Requests</td>
<td>The number of RADIUS Authentication-Request packets retransmitted to this RADIUS authentication server.</td>
</tr>
<tr>
<td>Accept Responses</td>
<td>The number of RADIUS Access-Accept packets (valid or invalid) received from this server.</td>
</tr>
<tr>
<td>Reject Responses</td>
<td>The number of RADIUS Access-Reject packets (valid or invalid) received from this server.</td>
</tr>
<tr>
<td>Challenge Responses</td>
<td>The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.</td>
</tr>
<tr>
<td>Malformed Msgs</td>
<td>The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or unknown types are not included as malformed access responses.</td>
</tr>
</tbody>
</table>
Table 5-11  RADIUS Authentication Page Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending Requests</td>
<td>The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout, or retransmission.</td>
</tr>
<tr>
<td>Bad Authentication Msgs</td>
<td>The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.</td>
</tr>
<tr>
<td>Timeouts Requests</td>
<td>The number of authentication timeouts to this server. After a timeout the client might retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.</td>
</tr>
<tr>
<td>Unknown Type Msgs</td>
<td>The number of RADIUS packets of unknown type which were received from this server on the authentication port.</td>
</tr>
<tr>
<td>Other Drops</td>
<td>The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.</td>
</tr>
</tbody>
</table>

Monitoring RADIUS Accounting

You can access this page by any of the following ways:

- Choose Monitor > Controllers and click the applicable IP address, then choose Security > Radius Accounting from the left sidebar menu.
- Choose Monitor > Clients and click a list item under AP Name, click Registered Controller, then choose Security > Radius Accounting from the left sidebar menu.
- Choose Monitor > Maps, click an item in the Name column, click an access point icon, click Controller, then choose Security > Radius Accounting from the left sidebar menu.
- Choose Configure > Access Points and select a list item under AP Name, click Registered Controller, then choose Security > Radius Accounting from the left sidebar menu.
Table 5-12 lists the RADIUS Accounting page fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RADIUS Accounting Server</strong></td>
<td></td>
</tr>
<tr>
<td>Server Index</td>
<td>Access priority number for RADIUS servers. Up to four servers can be configured, and controller polling of the servers starts with Index 1, Index 2 second, and so forth. Index number is based on when the RADIUS server is added to the controller.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the RADIUS server.</td>
</tr>
<tr>
<td>Ping</td>
<td>Click the icon to ping the RADIUS Server from the controller to verify the link.</td>
</tr>
<tr>
<td>Port</td>
<td>The port of the RADIUS server.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Indicates whether the server is enabled or disabled.</td>
</tr>
<tr>
<td><strong>Accounting Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Msg Round Trip Time</td>
<td>The time interval (in milliseconds) between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.</td>
</tr>
<tr>
<td>First Requests</td>
<td>The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.</td>
</tr>
<tr>
<td>Retry Requests</td>
<td>The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.</td>
</tr>
<tr>
<td>Accounting Responses</td>
<td>The number of RADIUS packets received on the accounting port from this server.</td>
</tr>
<tr>
<td>Malformed Msgs</td>
<td>The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.</td>
</tr>
<tr>
<td>Bad AuthenticationMsgs</td>
<td>The number of RADIUS Accounting-Response packets which contained invalid authenticators received from this server.</td>
</tr>
</tbody>
</table>
Monitoring Controllers

### Monitoring Management Frame Protection

This page displays the Management Frame Protection (MFP) summary information. MFP provides the authentication of 802.11 management frames. Management frames can be protected to detect adversaries who are invoking denial of service attacks, flooding the network with probes, interjecting as rogue access points, and affecting the network performance by attacking the QoS and radio measurement frames.

If one or more of the WLANs for the controller has MFP enabled, the controller sends each registered access point a unique key for each BSSID the access point uses for those WLANs. Management frames sent by the access point over the MFP enabled WLANs is signed with a Frame Protection Information Element (IE). Any attempt to alter the frame invalidates the message causing the receiving access point configured to detect MFP frames to report the discrepancy to the WLAN controller.

Access this page in one of the following ways:

- Choose **Monitor > Controllers**. From the Controllers > Search Results page, click the applicable IP address, then choose **Security > Management Frame Protection** from the left sidebar menu.
- Choose **Monitor > Access Points**, click a list item under AP Name, click **Registered Controller**, then choose **Security > Management Frame Protection** from the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **Security > Management Frame Protection** from the left sidebar menu.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending Requests</td>
<td>The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.</td>
</tr>
<tr>
<td>Timeouts Requests</td>
<td>The number of accounting timeouts to this server. After a timeout the client might retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.</td>
</tr>
<tr>
<td>Unknown Type Msgs</td>
<td>The number of RADIUS packets of unknown type which were received from this server on the accounting port.</td>
</tr>
<tr>
<td>Other Drops</td>
<td>The number of RADIUS packets which were received from this server on the accounting port and dropped for some other reason.</td>
</tr>
</tbody>
</table>
Table 5-13 lists the MFP page fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
</tr>
<tr>
<td>Management Frame Protection</td>
<td>Indicates if the infrastructure MFP is enabled globally for the controller.</td>
</tr>
<tr>
<td>Controller Time Source Valid</td>
<td>The Controller Time Source Valid field indicates whether the controller time is set locally (by manually entering the time) or through an external source (such as NTP server). If the time is set by an external source, the value of this field is “True.” If the time is set locally, the value is “False.” The time source is used for validating the timestamp on management frames between access points of different controllers within a mobility group.</td>
</tr>
</tbody>
</table>

WLAN Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN ID</td>
<td>The WLAN ID, 1 through 17.</td>
</tr>
<tr>
<td>WLAN Name</td>
<td>User-defined profile name when initially creating the WLAN. Both the SSID name and profile name are user-defined. The WLAN name is same as the profile name.</td>
</tr>
<tr>
<td>MFP Protection</td>
<td>Management Frame Protection is either enabled or disabled.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the WLAN is either enabled or disabled.</td>
</tr>
</tbody>
</table>

AP Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Name</td>
<td>Operator-defined name of access point.</td>
</tr>
<tr>
<td>MFP Validation</td>
<td>Management Frame Protection is enabled or disabled.</td>
</tr>
<tr>
<td>Radio</td>
<td>802.11a or 802.11b/g.</td>
</tr>
<tr>
<td>Operation Status</td>
<td>Displays the operational status: either UP or DOWN.</td>
</tr>
<tr>
<td>Protection</td>
<td>Full (All Frames).</td>
</tr>
<tr>
<td>Validation</td>
<td>Full (All Frames).</td>
</tr>
</tbody>
</table>

Monitroing Rogue AP Rules

Rogue AP rules automatically classify rogue access points based on criteria such as authentication type, matching configured SSIDs, client count, and RSSI values. Prime Infrastructure applies the rogue access point classification rules to the controllers and respective access points.

These rules can limit a rogue appearance on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time).

Rogue AP Rules also help reduce false alarms.
Rogue classes include the following types:
Malicious Rogue—A detected access point that matches the user-defined malicious rules or has been manually moved from the Friendly AP category.
Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined friendly rules.
Unclassified Rogue—A detected access point that does not match the malicious or friendly rules.

Choose Monitor > Controllers. From the Controllers > Search Results page, click the applicable IP address, then choose Security > Rogue AP Rules from the left sidebar menu.

The Rogue AP Rules page provides a list of all rogue access point rules currently applied to this controller.

The following information is displayed for rogue access point rules:
• Rogue AP Rule name—Click the link to view Rogue AP Rule details.
• Rule Type—Malicious or Friendly.
  – Malicious Rogue—A detected access point that matches the user-defined Malicious rules or has been manually moved from the Friendly AP category.
  – Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined Friendly rules.
• Priority—Indicates the priority level for this rogue AP rule.

See the “Configuring a Rogue AP Rules Template” section on page 11-73 for more information on Rogue AP Rules.

### Rogue AP Rules

Table 5-14 lists the Rogue AP Rules page fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Name of the rule.</td>
</tr>
<tr>
<td>Rule Type</td>
<td>Malicious or Friendly</td>
</tr>
<tr>
<td></td>
<td>– Malicious Rogue—A detected access point that matches the user-defined Malicious rules or has been manually moved from the Friendly AP category.</td>
</tr>
<tr>
<td></td>
<td>– Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined Friendly rules.</td>
</tr>
</tbody>
</table>
Chapter 5  Monitoring Devices

Monitoring Controllers

Table 5-14  Rogue AP Rule Page Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match Type</td>
<td>Match any or match all conditions.</td>
</tr>
<tr>
<td>Enabled Rule Conditions</td>
<td>Indicates all enabled rule conditions including:</td>
</tr>
<tr>
<td></td>
<td>- Open Authentication</td>
</tr>
<tr>
<td></td>
<td>- Match Managed AP SSID</td>
</tr>
<tr>
<td></td>
<td>- Match User Configured SSID</td>
</tr>
<tr>
<td></td>
<td>- Minimum RSSI</td>
</tr>
<tr>
<td></td>
<td>- Time Duration</td>
</tr>
<tr>
<td></td>
<td>- Minimum Number Rogue Clients</td>
</tr>
</tbody>
</table>

Note

See the “Configuring a Rogue AP Rules Template” section on page 11-73 for more information on Rogue AP Rules.

Monitoring Guest Users

Choose Monitor > Controllers. From the Controllers > Search Results page, click the applicable IP Address, then choose Security > Guest Users from the left sidebar menu.

Prime Infrastructure allows you to monitor guest users from the Guest Users page as well as from the Prime Infrastructure home page.

The Guest Users page provides a summary of the guest access deployment and network use.

The following information is displayed for guest users currently associates on the network. Table 5-15 lists the Guest Users page fields.

Table 5-15  Guest Users Page Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest User Name</td>
<td>Indicates the guest user login name.</td>
</tr>
<tr>
<td>Profile</td>
<td>Indicates the profile to which the guest user is connected.</td>
</tr>
<tr>
<td>Lifetime</td>
<td>Indicates the length of time that the guest user account is active. Length of time appears in days, hours, and minutes or as Never Expires.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Indicates when the guest user account was activated.</td>
</tr>
<tr>
<td>Remaining Lifetime</td>
<td>Indicates the remaining time for the guest user account.</td>
</tr>
<tr>
<td>Role</td>
<td>Indicates the designated user role.</td>
</tr>
<tr>
<td>First Logged in at</td>
<td>Indicates the date and time of the user first login.</td>
</tr>
</tbody>
</table>
### Monitoring Controller Mobility

#### Monitoring Mobility Stats

The Mobility Stats page displays the statistics for mobility group events.

Access this page in one of the following ways:

- Choose **Monitor > Controllers** and click the applicable IP address, then choose **Mobility > Mobility Stats** from the left sidebar menu.
- Choose **Monitor > Access Points**, click a list item under AP Name, click **Registered Controller**, then choose **Mobility > Mobility Stats** from the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **Mobility > Mobility Stats** from the left sidebar menu.

Table 5-16 lists the Mobility Stats page fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of logins</td>
<td>Indicates the total number of logins for this guest user.</td>
</tr>
<tr>
<td>Description</td>
<td>User-defined description of the guest user account for identification purposes.</td>
</tr>
</tbody>
</table>

### Table 5-15 Guest Users Page Fields (continued)

Table 5-16 Mobility Stats Page Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global Mobility Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Rx Errors</td>
<td>Generic protocol packet receive errors, such as packet too short or format incorrect.</td>
</tr>
<tr>
<td>Tx Errors</td>
<td>Generic protocol packet transmit errors, such as packet transmission fail.</td>
</tr>
<tr>
<td>Responses Retransmitted</td>
<td>The Mobility protocol uses UDP and it resends requests several times if it does not receive a response. Because of network or processing delays, the responder might receive one or more retry requests after it initially responds to a request. This is a count of the response resends.</td>
</tr>
<tr>
<td>Handoff Requests Received</td>
<td>Total number of handoff requests received, ignored or responded to.</td>
</tr>
<tr>
<td>Handoff End Requests</td>
<td>Total number of handoff end requests received. These are sent by the Anchor or the Foreign to notify the other about the close of a client session.</td>
</tr>
<tr>
<td>State Transitions Disallowed</td>
<td>PEM (policy enforcement module) has denied a client state transition, usually resulting in the handoff being aborted.</td>
</tr>
</tbody>
</table>
### Table 5-16  Mobility Stats Page Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Unavailable</td>
<td>A necessary resource, such as a buffer, was unavailable, resulting in the handoff being aborted.</td>
</tr>
<tr>
<td><strong>Mobility Responder Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Handoff Requests Ignored</td>
<td>Number of handoff requests/client announces that were ignored. The controller simply had no knowledge of that client.</td>
</tr>
<tr>
<td>Ping Pong Handoff Requests Dropped</td>
<td>Number of handoff requests that were denied because the handoff period was too short (3 sec).</td>
</tr>
<tr>
<td>Handoff Requests Dropped</td>
<td>Number of handoff requests that were dropped due to an incomplete knowledge of the client or a problem with the packet.</td>
</tr>
<tr>
<td>Handoff Requests Denied</td>
<td>Number of handoff requests that were actively denied.</td>
</tr>
<tr>
<td>Client Handoff as Local</td>
<td>Number of handoffs responses sent while in the local role.</td>
</tr>
<tr>
<td>Client Handoff as Foreign</td>
<td>Number of handoffs responses sent while in the foreign role.</td>
</tr>
<tr>
<td>Anchor Requests Received</td>
<td>Number of anchor requests received.</td>
</tr>
<tr>
<td>Anchor Requests Denied</td>
<td>Number of anchor requests denied.</td>
</tr>
<tr>
<td>Anchor Requests Granted</td>
<td>Number of anchor requests granted.</td>
</tr>
<tr>
<td>Anchor Transferred</td>
<td>Number of anchors transferred because the client has moved from a foreign controller to controller on the same subnet as the current anchor.</td>
</tr>
<tr>
<td><strong>Mobility Initiator Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Handoff Requests Sent</td>
<td>Number of clients that have associated with controller and have been announced to the mobility group.</td>
</tr>
<tr>
<td>Handoff Replies Received</td>
<td>Number of handoff replies that have been received in response to the requests sent.</td>
</tr>
<tr>
<td>Handoff as Local Received</td>
<td>Number of handoffs in which the entire client session has been transferred.</td>
</tr>
<tr>
<td>Handoff as Foreign Received</td>
<td>Number of handoffs in which the client session was anchored elsewhere.</td>
</tr>
<tr>
<td>Handoff Denies Received</td>
<td>Number of handoffs that were denied.</td>
</tr>
<tr>
<td>Anchor Request Sent</td>
<td>Number of anchor requests that were sent for a three-party (foreign to foreign) handoff. Handoff was received from another foreign and the new controller is requesting the anchor to move the client.</td>
</tr>
<tr>
<td>Anchor Deny Received</td>
<td>Number of anchor requests that were denied by the current anchor.</td>
</tr>
</tbody>
</table>
Table 5-16  Mobility Stats Page Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anchor Grant Received</td>
<td>Number of anchor requests that were approved by</td>
</tr>
<tr>
<td></td>
<td>the current anchor.</td>
</tr>
<tr>
<td>Anchor Transfer Received</td>
<td>Number of anchor transfers that were received by</td>
</tr>
<tr>
<td></td>
<td>the current anchor.</td>
</tr>
</tbody>
</table>

Monitoring Controller 802.11a/n

This section provides detailed information regarding monitoring 802.11a/n parameters and contains the following topics:

- Monitoring 802.11a/n Parameters, page 5-25
- Monitoring 802.11a/n RRM Groups, page 5-27

Monitoring 802.11a/n Parameters

Access the 802.11a/n Parameters page in one of the following ways:

- Choose Monitor > Controllers and click the applicable IP address, then choose Parameters from the 802.11a/n section of the left sidebar menu.
- Choose Monitor > Access Points, click a list item under AP Name, click Registered Controller, then choose Parameters from the 802.11a/n section of the left sidebar menu.
- Choose Monitor > Clients, click a list item under AP Name, click Registered Controller, then choose Parameters from the 802.11a/n section of the left sidebar menu.

Table 5-17 lists the 802.11a/n Parameters page fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Operation Parameters</td>
<td></td>
</tr>
<tr>
<td>RTS Threshold</td>
<td>Indicates the number of octets in an MPDU, below</td>
</tr>
<tr>
<td></td>
<td>which an RTS/CTS handshake is not performed.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> An RTS/CTS handshake is performed at</td>
</tr>
<tr>
<td></td>
<td>the beginning of any frame exchange sequence</td>
</tr>
<tr>
<td></td>
<td>where the MPDU is a data or management type, the</td>
</tr>
<tr>
<td></td>
<td>MPDU has an individual address in the Address1</td>
</tr>
<tr>
<td></td>
<td>field, and the length of the MPDU is greater</td>
</tr>
<tr>
<td></td>
<td>than this threshold. Setting this attribute</td>
</tr>
<tr>
<td></td>
<td>higher than the maximum MSDU size turns off the</td>
</tr>
<tr>
<td></td>
<td>RTS/CTS handshake for data or management type</td>
</tr>
<tr>
<td></td>
<td>frames transmitted by this STA. Setting this</td>
</tr>
<tr>
<td></td>
<td>attribute to zero turns on the RTS/CTS handshake</td>
</tr>
<tr>
<td></td>
<td>for all transmitted data or management type</td>
</tr>
<tr>
<td></td>
<td>frames.</td>
</tr>
</tbody>
</table>
### Table 5-17  802.11 a/n Parameters Page Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Retry Limit</td>
<td>The maximum number of transmission attempts of a frame (less than or equal to dot11RTSThreshold) made before a failure condition is indicated. The default value is 7.</td>
</tr>
<tr>
<td>Long Retry Limit</td>
<td>The maximum number of transmission attempts of a frame (greater than dot11RTSThreshold) made before a failure condition is indicated. The default value is 4.</td>
</tr>
<tr>
<td>Max Tx MSDU Lifetime</td>
<td>The elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU are terminated. The default value is 512.</td>
</tr>
<tr>
<td>Max Rx Lifetime</td>
<td>The elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU, after which further attempts to reassemble the MMPDU or MSDU are terminated. The default value is 512.</td>
</tr>
<tr>
<td><strong>Physical Channel Fields</strong></td>
<td></td>
</tr>
<tr>
<td>TI Threshold</td>
<td>The threshold being used to detect a busy medium (frequency). CCA shall report a busy medium upon detecting the RSSI above this threshold.</td>
</tr>
<tr>
<td>Channel Agility Enabled</td>
<td>Physical channel agility functionality is or is not implemented.</td>
</tr>
<tr>
<td><strong>Station Configuration Fields</strong></td>
<td></td>
</tr>
<tr>
<td>Medium Occupancy Limit</td>
<td>Indicates the maximum amount of time, in TU, that a point coordinator might control the usage of the wireless medium without relinquishing control for long enough to allow at least one instance of DCF access to the medium. The default value is 100, and the maximum value is 1000.</td>
</tr>
<tr>
<td>CFP Period</td>
<td>The number of DTIM intervals between the start of CFPs. It is modified by MLME-START.request primitive.</td>
</tr>
<tr>
<td>CFP Max Duration</td>
<td>The maximum duration of the CFP in TU that might be generated by the PCF. It is modified by MLME-START.request primitive.</td>
</tr>
<tr>
<td>CF Pollable</td>
<td>When this attribute is implemented, it indicates that the client is able to respond to a CF-Poll with a data frame within a SIFS time. This attribute is not implemented if the STA is not able to respond to a CF-Poll with a data frame within a SIFS time.</td>
</tr>
</tbody>
</table>
Monitoring 802.11a/n RRM Groups

Access the RRM Grouping page in one of the following ways:

- Choose Monitor > Controllers and click the applicable IP address, then choose Grouping or WPS Grouping from the 802.11a/n section of the left sidebar menu.
- Choose Monitor > Access Points, click a list item under AP Name, click Registered Controller, then choose RRM Grouping or WPS Grouping from the 802.11a/n section of the left sidebar menu.
- Choose Monitor > Clients, click a list item under AP Name, click Registered Controller, then choose RRM Grouping or WPS Grouping from the 802.11a/n section of the left sidebar menu.

Table 5-18 lists the 802.11a/n RRM Grouping page fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a Grouping Control</td>
<td>Dynamic grouping has two modes: on and off. When the grouping is off, no dynamic grouping occurs. Each controller optimizes only its own parameters of the access point. When grouping is on, the controller forms groups and elects leaders to perform better dynamic parameter optimization.</td>
</tr>
</tbody>
</table>
There are five grouping roles:

- None—This grouping role appears when the RF Group Mode is configured as Off.
- Auto-Leader—This grouping role appears when the RF Group Mode is configured as Automatic and the controller is elected as a leader by the automatic grouping algorithm.
- Auto-Member—This grouping role appears when the RF Group Mode is configured as Automatic and the controller is selected as a member by the automatic grouping algorithm.
- Static-Leader—This grouping role appears when the RF Group Mode is configured as Leader.
- Static-member—This grouping role appears when the RF Group Mode is configured as automatic and the controller joins the leader as a result of the join request from the leader.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grouping Role</td>
<td>There are five grouping roles:</td>
</tr>
<tr>
<td></td>
<td>- None—This grouping role appears when the RF Group Mode is configured as Off.</td>
</tr>
<tr>
<td></td>
<td>- Auto-Leader—This grouping role appears when the RF Group Mode is configured as Automatic and the controller is elected as a leader by the automatic grouping algorithm.</td>
</tr>
<tr>
<td></td>
<td>- Auto-Member—This grouping role appears when the RF Group Mode is configured as Automatic and the controller is selected as a member by the automatic grouping algorithm.</td>
</tr>
<tr>
<td></td>
<td>- Static-Leader—This grouping role appears when the RF Group Mode is configured as Leader.</td>
</tr>
<tr>
<td></td>
<td>- Static-member—This grouping role appears when the RF Group Mode is configured as automatic and the controller joins the leader as a result of the join request from the leader.</td>
</tr>
<tr>
<td>Group Leader IP Address</td>
<td>This is the IP address of the group leader.</td>
</tr>
<tr>
<td>Group Leader MAC Address</td>
<td>This is the MAC address of the group leader for the group containing this controller.</td>
</tr>
<tr>
<td>Is 802.11a Group Leader</td>
<td>Yes, if this controller is the group leader or No if the controller is not the group leader.</td>
</tr>
<tr>
<td>Last Update Time (secs)</td>
<td>The elapsed time since the last group update in seconds. This is only valid if this controller is a group leader.</td>
</tr>
<tr>
<td>Group Update Interval (secs)</td>
<td>When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. Grouping algorithm also runs when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. Default value is 3600 seconds.</td>
</tr>
<tr>
<td>Group Members</td>
<td></td>
</tr>
<tr>
<td>Group Member Name</td>
<td>Name of group member(s).</td>
</tr>
<tr>
<td>Group Member IP Address</td>
<td>IP address of group member(s).</td>
</tr>
<tr>
<td>Member Join Reason</td>
<td>Current state of the member(s).</td>
</tr>
</tbody>
</table>
Monitoring Controllers 802.11b/g/n

This section provides the detailed information regarding monitoring 802.11b/g/n parameters and contains the following topics:

- Monitoring 802.11b/g/n Parameters, page 5-29
- Monitoring 802.11b/g/n RRM Groups, page 5-30

Monitoring 802.11b/g/n Parameters

Access the 802.11b/g/n Parameters page in one of the following ways:

- Choose Monitor > Controllers and click the applicable IP Address, then choose Parameters from the 802.11b/g/n section of the left sidebar menu.
- Choose Monitor > Access Points, click a list item under AP Name, click Registered Controller, then choose Parameters from the 802.11b/g/n section of the left sidebar menu.
- Choose Monitor > Clients, click a list item under AP Name, click Registered Controller, then choose Parameters from the 802.11b/g/n section of the left sidebar menu.

Table 5-19 lists the 802.11b/g Parameters page fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Operation Parameters</td>
<td></td>
</tr>
<tr>
<td>RTS Threshold</td>
<td>Indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>An RTS/CTS handshake is performed at the beginning of any frame exchange sequence where the MPDU is a data or management type, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute higher than the maximum MSDU size turns off the RTS/CTS handshake for data or management type frames transmitted by this STA. Setting this attribute to zero turns on the RTS/CTS handshake for all transmitted data or management type frames.</td>
</tr>
<tr>
<td>Short Retry Limit</td>
<td>The maximum number of transmission attempts of a frame (less than or equal to dot11RTSThreshold) made before a failure condition is indicated. The default value is 7.</td>
</tr>
<tr>
<td>Long Retry Limit</td>
<td>The maximum number of transmission attempts of a frame (greater than dot11RTSThreshold) made before a failure condition is indicated. The default value is 4.</td>
</tr>
</tbody>
</table>
### Monitoring Controllers

**Chapter 5  Monitoring Devices**

#### 802.11 b/g/n Parameters Page Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Tx MSDU Lifetime</td>
<td>The elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU are terminated. The default value is 512.</td>
</tr>
<tr>
<td>Max Rx Lifetime</td>
<td>The elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU, after which further attempts to reassemble the MMPDU or MSDU are terminated. The default value is 512.</td>
</tr>
<tr>
<td>Physical Channel Fields</td>
<td></td>
</tr>
<tr>
<td>TI Threshold</td>
<td>The threshold being used to detect a busy medium (frequency). CCA shall report a busy medium upon detecting the RSSI above this threshold.</td>
</tr>
<tr>
<td>Channel Agility Enabled</td>
<td>Physical channel agility functionality is or is not implemented.</td>
</tr>
<tr>
<td>Station Configuration Fields</td>
<td></td>
</tr>
<tr>
<td>Medium Occupancy Limit</td>
<td>Indicates the maximum amount of time, in TU, that a point coordinator might control the usage of the wireless medium without relinquishing control for long enough to allow at least one instance of DCF access to the medium. The default value is 100, and the maximum value is 1000.</td>
</tr>
<tr>
<td>CFP Period</td>
<td>The number of DTIM intervals between the start of CFPs. It is modified by MLME-START.request primitive.</td>
</tr>
<tr>
<td>CFP Max Duration</td>
<td>The maximum duration of the CFP in TU that might be generated by the PCF. It is modified by MLME-START.request primitive.</td>
</tr>
<tr>
<td>CF Pollable</td>
<td>When this attribute is implemented, it indicates that the client is able to respond to a CF-Poll with a data frame within a SIFS time. This attribute is not implemented if the STA is not able to respond to a CF-Poll with a data frame within a SIFS time.</td>
</tr>
<tr>
<td>CF Poll Request</td>
<td>Specifies whether CFP is requested by the client.</td>
</tr>
<tr>
<td>DTTIM Period</td>
<td>The number of beacon intervals that elapse between transmission of Beacon frames containing a TIM element whose DTIM Count field is 0. This value is transmitted in the DTIM Period field of Beacon frames.</td>
</tr>
</tbody>
</table>

### Monitoring 802.11b/g/n RRM Groups

Access the 802.11b/g/n RRM Grouping page in one of the following ways:

- Choose **Monitor > Controllers** and click the applicable IP address, then choose **RRM Grouping** or **WPS Grouping** from the 802.11b/g/n section of the left sidebar menu.
• Choose Monitor > Access Points, click a list item under AP Name, click Registered Controller, then choose RRM Grouping or WPS Grouping from the 802.11b/g/n section of the left sidebar menu.

• Choose Monitor > Clients, click a list item under AP Name, click Registered Controller, then choose RRM Grouping or WPS Grouping from the 802.11b/g/n section of the left sidebar menu.

Table 5-20 lists the 802.11b/g/n RRM grouping page fields.

Table 5-20  802.11 b/g/n RRM Grouping Page Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11 b/g/n Grouping Control</td>
<td>Dynamic grouping has two modes: on and off. When the grouping is off, no</td>
</tr>
<tr>
<td></td>
<td>dynamic grouping occurs. Each controller optimizes only its own parameters</td>
</tr>
<tr>
<td></td>
<td>of the access point. When grouping is on, the controller forms groups and</td>
</tr>
<tr>
<td></td>
<td>elects leaders to perform better dynamic parameter optimization.</td>
</tr>
<tr>
<td>Grouping Mode</td>
<td></td>
</tr>
<tr>
<td>Grouping Role</td>
<td>There are five grouping roles:</td>
</tr>
<tr>
<td></td>
<td>– None—This grouping role appears when the RF Group Mode is configured as</td>
</tr>
<tr>
<td></td>
<td>Off.</td>
</tr>
<tr>
<td></td>
<td>– Auto-Leader—This grouping role appears when the RF Group Mode is</td>
</tr>
<tr>
<td></td>
<td>configured as Automatic and the controller is elected as a leader by the</td>
</tr>
<tr>
<td></td>
<td>automatic grouping algorithm.</td>
</tr>
<tr>
<td></td>
<td>– Auto-Member—This grouping role appears when the RF Group Mode is</td>
</tr>
<tr>
<td></td>
<td>configured as Automatic and the controller is selected as a member by the</td>
</tr>
<tr>
<td></td>
<td>automatic grouping algorithm.</td>
</tr>
<tr>
<td>Group Leader IP Address</td>
<td>This is the IP address of the group leader.</td>
</tr>
<tr>
<td>Group Leader MAC Address</td>
<td>This is the MAC address of the group leader for the group containing this</td>
</tr>
<tr>
<td>Is 802.11a Group Leader</td>
<td>Yes, if this controller is the group leader or No if the controller is not</td>
</tr>
<tr>
<td>Last Update Time (secs)</td>
<td>The elapsed time since the last group update in seconds. This is only valid</td>
</tr>
</tbody>
</table>

Cisco Prime Infrastructure Classic View Configuration Guide for Wireless Devices
Table 5-20 802.11 b/g/n RRM Grouping Page Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Update Interval (secs)</td>
<td>When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. Grouping algorithm also runs when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. Default value is 3600 seconds.</td>
</tr>
</tbody>
</table>

**Group Members**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Member Name</td>
<td>Name of group member(s).</td>
</tr>
<tr>
<td>Group Member IP Address</td>
<td>IP address of group member(s).</td>
</tr>
<tr>
<td>Member Join Reason</td>
<td>Current state of the member(s).</td>
</tr>
</tbody>
</table>

### Monitoring Controllers IPv6

#### Monitoring Neighbor Bind Counter Statistics

Access the Neighbor Bind Counter Statistics page in one of the following ways:

- Choose **Monitor > Controllers**, select an IP Address, and choose **IPv6 > Neighbor Bind Counters** from the left sidebar menu.
- Choose **Monitor > Access Points**, click a list item under AP Name, click **Registered Controller**, then choose **IPv6 > Neighbor Bind Counters** from the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **IPv6 > Neighbor Bind Counters** from the left sidebar menu.

Table 5-21 lists the Neighbor Bind Counter Stats page fields.

Table 5-21 Neighbor Bind Counter Stats Page Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor Bind Counters</td>
<td>Provides the statistics of the number of messages exchanged between the host or client and the router to generate and acquire IPv6 addresses, link, MTU, and so on.</td>
</tr>
<tr>
<td>Received Messages</td>
<td>The number of Advertisement, Solicitation and other messages received for NDP and DHCPv6.</td>
</tr>
<tr>
<td>Bridged Messages</td>
<td>The number of Advertisement, Solicitation and other messages bridged for NDP and DHCPv6.</td>
</tr>
<tr>
<td>Total Snooping Dropped Messages</td>
<td>The number of Advertisement, Solicitation and other messages bridged for NDP and DHCPv6 along with the reason for the drop.</td>
</tr>
</tbody>
</table>
Monitoring Third Party Controllers

Choose Monitor > Third Party Controllers to view the detailed information about the third party (non-Cisco) controllers that are managed by Prime Infrastructure.

### Table 5-21 Neighbor Bind Counter Stats Page Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor Discovery Suppress Drop Counter</td>
<td>The total number of neighbor discovery messages dropped.</td>
</tr>
<tr>
<td>Total Suppress Dropped Messages</td>
<td>The reason for the neighbor discovery messages drop.</td>
</tr>
</tbody>
</table>

**Note** Hover your mouse cursor over the values in the Total Snooping/Suppress Drop Messages column to see the reasons due to which the corresponding messages were dropped.

### Monitoring mDNS Service Provider Information

This page enables you to view the list of mDNS services and service provider information.

**Table 5-22** Service Provider Information Page Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>Name of the mDNS Service.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address of the service provider.</td>
</tr>
<tr>
<td>Service Provider Name</td>
<td>Name of the service provider. You can have a maximum of 100 service providers associated with the controller.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>VLAN ID of the service provider.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the interface on which the service is available. For example wired, wireless, and wired-guest.</td>
</tr>
<tr>
<td>TTL (seconds)</td>
<td>Time to Live (TTL) value in seconds that determines the validity of the service offered by the service provider. The service provider is removed from the controller when the TTL expires.</td>
</tr>
<tr>
<td>Time Left (seconds)</td>
<td>Time left in seconds before the service provider is removed from the controller.</td>
</tr>
</tbody>
</table>
Monitoring Switches

Choose Monitor > Switches to view the detailed information about the switches. This section provides more detailed information regarding monitoring switches and includes the following topics:

- Searching Switches, page 5-34
- Viewing the Switches, page 5-34
- Monitoring Switch System Parameters, page 5-35
- Monitoring Switch Interfaces, page 5-41
- Monitoring Switch Clients, page 5-43

Searching Switches

Use the Prime Infrastructure search feature to find specific switches or to create and save custom searches.

You can configure the following fields when performing an advanced search for switches (see Table 5-23).

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search for Switches by</td>
<td>Choose All Switches, IP Address, or Switch Name. You can use wildcards (*)</td>
</tr>
<tr>
<td></td>
<td>For example, if you select IP Address and enter 172*, the Prime Infrastructure returns all switches that begin with IP address 172.</td>
</tr>
<tr>
<td>Items per page</td>
<td>Select the number of switches to return per page.</td>
</tr>
</tbody>
</table>

Viewing the Switches

Choose Monitor > Switches to view a list of the switches. From this page you can view a summary of the switches including the default information shown in Table 5-24.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address assigned to the switch. Click a list item to view access point details.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the switch.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Type of switch.</td>
</tr>
<tr>
<td>Reachability Status</td>
<td>Indicates OK if the switch is reachable or Unreachable if the switch is not reachable.</td>
</tr>
<tr>
<td>Endpoint Count</td>
<td>Number of endpoints on the switch.</td>
</tr>
</tbody>
</table>

Configuring the Switch List Page

The Edit View page allows you to add, remove, or reorder columns in the Switches table.
To edit the available columns in the table, follow these steps:

**Step 1** Choose Monitor > Switches.

**Step 2** Click the Edit View link.

**Step 3** To add an additional column to the table, click to highlight the column heading in the left column. Click Show to move the heading to the right column. All items in the right column are displayed in the table.

**Step 4** To remove a column from the table, click to highlight the column heading in the right column. Click Hide to move the heading to the left column. All items in the left column are not displayed in the table.

**Step 5** Use the Up/Down buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click Up or Down to move it higher or lower in the current list.

**Step 6** Click Reset to restore the default view.

**Step 7** Click Submit to confirm the changes.

## Monitoring Switch System Parameters

Choose Monitor > Switches, then click an IP address in the IP Address column to view details about the switch. This section provides the detailed information regarding each switch details page and contains the following topics:

- Viewing Switch Summary Information, page 5-35
- Viewing Switch Memory Information, page 5-36
- Viewing Switch Environment Information, page 5-37
- Viewing Switch Module Information, page 5-37
- Viewing Switch VLAN Information, page 5-38
- Viewing Switch VTP Information, page 5-38
- Viewing Switch Physical Ports Information, page 5-38
- Viewing Switch Sensor Information, page 5-39
- Viewing Switch Spanning Tree Information, page 5-39
- Viewing Switch Stacks Information, page 5-40
- Viewing Switch NMSP and Location Information, page 5-40

### Viewing Switch Summary Information

Choose Monitor > Switches, then click an IP address in the IP Address column to view details about the switch. Table 5-25 describes the summary information that is displayed.

<table>
<thead>
<tr>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Device Name</td>
</tr>
<tr>
<td>Device Type</td>
</tr>
</tbody>
</table>

| Table 5-25 Viewing Switches Summary Information |
**Table 5-25  Viewing Switches Summary Information (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up Time</td>
<td>Time since last reboot.</td>
</tr>
<tr>
<td>System Time</td>
<td>Time on the switch.</td>
</tr>
<tr>
<td>Reachability Status</td>
<td>which can be the following:</td>
</tr>
<tr>
<td></td>
<td>• Reachable</td>
</tr>
<tr>
<td></td>
<td>• Unreachable</td>
</tr>
<tr>
<td>Location</td>
<td>Location of the switch.</td>
</tr>
<tr>
<td>Contact</td>
<td>Contact name for the switch.</td>
</tr>
<tr>
<td>Cisco Identity Capable</td>
<td>Specifies if the switch is identity-capable.</td>
</tr>
<tr>
<td>Location Capable</td>
<td>Specifies if the switch is capable of storing the location information.</td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>Displays a graph of the maximum, average, and minimum CPU utilization over the specified amount of time.</td>
</tr>
</tbody>
</table>

**Unique Device Identifier (UDI)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Product type.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of UDI.</td>
</tr>
<tr>
<td>Product ID</td>
<td>Orderable product identifier.</td>
</tr>
<tr>
<td>Version ID</td>
<td>Version of product identifier.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Unique product serial number.</td>
</tr>
</tbody>
</table>

**Inventory**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Version</td>
<td>Version of software currently running on the switch.</td>
</tr>
<tr>
<td>Model No.</td>
<td>Model number of the switch.</td>
</tr>
</tbody>
</table>

**Port Summary**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Ports Up</td>
<td>Number of ports up on the switch.</td>
</tr>
<tr>
<td>Number of Ports Down</td>
<td>Number of ports down on the switch.</td>
</tr>
</tbody>
</table>

**Memory Utilization**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays a graph of the maximum, average, and minimum memory utilization over the specified amount of time.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topic**

- **Monitoring Switch Interfaces, page 5-41**

**Viewing Switch Memory Information**

Choose **Monitor > Switches**, then click an IP address in the IP Address column to view details about the switch. From the System menu, choose **Memory**. **Table 5-26** describes the memory information that is displayed.

**Table 5-26  Viewing Switches Memory Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Pool</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Type of memory.</td>
</tr>
<tr>
<td>Name</td>
<td>Name assigned to the memory pool.</td>
</tr>
</tbody>
</table>
Chapter 5  Monitoring Devices

Monitoring Switches

Table 5-26  Viewing Switches Memory Information (continued)

<table>
<thead>
<tr>
<th>Used (MB)</th>
<th>Amount of memory (in MB) used.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free (MB)</td>
<td>Amount of memory (in MB) available.</td>
</tr>
</tbody>
</table>

Viewing Switch Environment Information

Choose Monitor > Switches, then click an IP address in the IP Address column to view details about the switch. From the System menu, choose Environment. Table 5-27 describes the environment information that is displayed.

Table 5-27  Viewing Switches Environment Information

<table>
<thead>
<tr>
<th>Power Supply</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Name</td>
<td>Model name of the power supply.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the power supply.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Status of the associated power supply:</td>
</tr>
<tr>
<td></td>
<td>• Green—Power supply is operational.</td>
</tr>
<tr>
<td></td>
<td>• Red—Power supply is inoperable.</td>
</tr>
<tr>
<td>Manufacturer Name</td>
<td>Name of the power supply manufacturer.</td>
</tr>
<tr>
<td>Free</td>
<td>Free power supply slots.</td>
</tr>
<tr>
<td>Vendor Equipment Type</td>
<td>Description of vendor equipment type.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fans</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of fan.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of fan.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Status of the fan:</td>
</tr>
<tr>
<td></td>
<td>• Green—Fan is operational.</td>
</tr>
<tr>
<td></td>
<td>• Red—Fan is inoperable.</td>
</tr>
<tr>
<td>Vendor Equipment Type</td>
<td>Description of vendor equipment type.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Serial number of the fan.</td>
</tr>
</tbody>
</table>

Viewing Switch Module Information

Choose Monitor > Switches, then click an IP address in the IP Address column to view details about the switch. From the System menu, choose Modules. Table 5-28 describes the module information that is displayed.

Table 5-28  Viewing Switches Modules Information

<table>
<thead>
<tr>
<th>Modules</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Name</td>
<td>Name of the module.</td>
</tr>
<tr>
<td>Physical Location</td>
<td>Location where the module is contained.</td>
</tr>
<tr>
<td>Number of Ports</td>
<td>Number of ports supported by the module.</td>
</tr>
<tr>
<td>Operational State</td>
<td>Operational status of the module.</td>
</tr>
</tbody>
</table>
Chapter 5      Monitoring Devices

Viewing Switch VLAN Information

Choose Monitor > Switches, then click an IP address under the IP Address column to view details about the switch. From the System menu, choose VLANs. Table 5-29 describes the VLAN information that is displayed.

<table>
<thead>
<tr>
<th>Table 5-29 Viewing Switches VLANs Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLANs</td>
</tr>
<tr>
<td>VLAN ID</td>
</tr>
<tr>
<td>VLAN Name</td>
</tr>
<tr>
<td>VLAN Type</td>
</tr>
</tbody>
</table>

Viewing Switch VTP Information

Choose Monitor > Switches, then click an IP address in the IP Address column to view details about the switch. From the System menu, choose VTP. Table 5-30 describes the VTP information that is displayed.

<table>
<thead>
<tr>
<th>Table 5-30 Viewing Switches VTP Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTP</td>
</tr>
<tr>
<td>VTP Domain Name</td>
</tr>
<tr>
<td>VTP Version</td>
</tr>
<tr>
<td>VTP Mode</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Pruning Enabled</td>
</tr>
</tbody>
</table>

Viewing Switch Physical Ports Information

Choose Monitor > Switches, then click an IP address in the IP Address column to view details about the switch. From the System menu, choose Physical Ports. Table 5-31 describes the physical ports information that is displayed.
Table 5-31  Viewing Switches Physical Ports Information

<table>
<thead>
<tr>
<th>Physical Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Name</td>
</tr>
<tr>
<td>Port Description</td>
</tr>
<tr>
<td>Residing Module</td>
</tr>
<tr>
<td>Vendor Equipment Type</td>
</tr>
</tbody>
</table>

Viewing Switch Sensor Information

Choose Monitor > Switches, then click an IP address under the IP Address column to view details about the switch. From the System menu, choose Sensors. Table 5-32 describes the sensor information that is displayed.

Table 5-32  Viewing Switches Sensors Information

<table>
<thead>
<tr>
<th>Sensors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor Name</td>
</tr>
<tr>
<td>Sensor Description</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Vendor Sensor Type</td>
</tr>
<tr>
<td>Equipment Name</td>
</tr>
<tr>
<td>Precision</td>
</tr>
<tr>
<td>Status</td>
</tr>
</tbody>
</table>

Viewing Switch Spanning Tree Information

Choose Monitor > Switches, then click an IP address in the IP Address column to view details about the switch. From the System menu, choose Spanning Tree. Table 5-33 describes the spanning tree information that is displayed.

Table 5-33  Viewing Switches Spanning Tree Information

<table>
<thead>
<tr>
<th>Spanning Tree</th>
</tr>
</thead>
<tbody>
<tr>
<td>STP Instance ID</td>
</tr>
<tr>
<td>VLAN ID</td>
</tr>
<tr>
<td>Root Path Cost</td>
</tr>
<tr>
<td>Designated Root</td>
</tr>
<tr>
<td>Bridge Priority</td>
</tr>
<tr>
<td>Root Bridge Priority</td>
</tr>
</tbody>
</table>
**Chapter 5      Monitoring Devices**

**Monitoring Switches**

**Viewing Spanning Tree Details**

Choose Monitor > Switches, then click an IP address in the IP Address column to view details about the switch. From the System menu, choose Spanning Tree, then click an STP instance ID to see the spanning tree details as described in Table 5-34.

**Table 5-34 Viewing Spanning Tree Details**

<table>
<thead>
<tr>
<th>Spanning Tree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the STP port.</td>
</tr>
<tr>
<td>Role of the port.</td>
</tr>
<tr>
<td>Priority number of the port.</td>
</tr>
<tr>
<td>Cost of the path.</td>
</tr>
<tr>
<td>State of the port.</td>
</tr>
<tr>
<td>Type of port.</td>
</tr>
</tbody>
</table>

**Viewing Switch Stacks Information**

Choose Monitor > Switches, then click an IP address in the IP Address column to view details about the switch. From the System menu, choose Stacks. Table 5-35 describes the spanning tree information that is displayed.

**Table 5-35 Viewing Switches Stacks Information**

<table>
<thead>
<tr>
<th>Stacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC address of the stack.</td>
</tr>
<tr>
<td>Role:</td>
</tr>
<tr>
<td>Master—Stack master</td>
</tr>
<tr>
<td>Member—Active member of the stack</td>
</tr>
<tr>
<td>Not Member—Non-active stack member</td>
</tr>
<tr>
<td>Priority number of the switch.</td>
</tr>
<tr>
<td>Current state of the stack.</td>
</tr>
<tr>
<td>Software image running on the switch.</td>
</tr>
</tbody>
</table>

**Viewing Switch NMSP and Location Information**

You can view the NMSP and Location information for a switch using the System left sidebar menu. To view the NMSP and Location information for a switch, choose Monitor > Switches, then click an IP address in the IP Address column. Choose System > NMSP and Location.

The NMSP and Location page appears.
You can view the NMSP Status in the NMSP Status group box and Location information in the Location group box.

For more information on NMSP and Location, see the Configuring Switch NMSP and Location.

**Monitoring Switch Interfaces**

Choose Monitor > Switches, then click an IP address in the IP Address column. From the System menu, choose Interfaces, then select one of the following interfaces described in this section.

- Monitoring Switch Ethernet Interfaces, page 5-41
- Monitoring Switch IP Interfaces, page 5-42
- Monitoring Switch VLAN Interfaces, page 5-42
- Monitoring Switch EtherChannel Interfaces, page 5-43

**Monitoring Switch Ethernet Interfaces**

Choose Monitor > Switches, then click an IP address in the IP Address column. From the System menu, choose Interfaces > Ethernet Interfaces. Table 5-36 describes the Ethernet interface information that is displayed.

*Table 5-36 Viewing Switch Ethernet Interfaces*

<table>
<thead>
<tr>
<th>Name</th>
<th>Name of the Ethernet interface. Click an Ethernet interface name to see details as described in “Monitoring Switch Ethernet Interface Details” section on page 5-41.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>MAC address of the Ethernet interface.</td>
</tr>
<tr>
<td>Speed (Mbps)</td>
<td>Estimate of the current bandwidth of the Ethernet interface in bits per second.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Current operational state of the Ethernet interface.</td>
</tr>
<tr>
<td>MTU</td>
<td>Size of the largest packet that can be sent/received on the interface.</td>
</tr>
<tr>
<td>Desired VLAN Mode</td>
<td>VLAN mode.</td>
</tr>
<tr>
<td>Access VLAN</td>
<td>VLAN on which the port is configured.</td>
</tr>
</tbody>
</table>

**Monitoring Switch Ethernet Interface Details**

Choose Monitor > Switches, then click an IP address in the IP Address column. From the System menu, choose Interfaces > Ethernet Interfaces, then click an Ethernet interface name in the Name column. Table 5-37 describes the Ethernet interface detail information that is displayed.

*Table 5-37 Viewing Switch Ethernet Interface Details*

<table>
<thead>
<tr>
<th>Ethernet Interfaces</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Ethernet interface.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Administration status of the interface.</td>
</tr>
<tr>
<td>Duplex Mode</td>
<td>Duplex mode configured on the interface.</td>
</tr>
</tbody>
</table>

**VLAN Switch Port**
Chapter 5  Monitoring Devices

Monitoring Switches

Table 5-37  Viewing Switch Ethernet Interface Details

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational VLAN Mode</td>
<td>Specifies the operational mode of the VLAN switch port, which can be either an access port or a trunk port.</td>
</tr>
<tr>
<td>Desired VLAN Mode</td>
<td>VLAN mode, which can be truck, access, dynamic, or desirable.</td>
</tr>
<tr>
<td>Access VLAN</td>
<td>VLAN on which the port is configured.</td>
</tr>
<tr>
<td>Operational Truck Encapsulation</td>
<td>Trunk encapsulation, which can be 802.1Q or none.</td>
</tr>
</tbody>
</table>

**VLAN Trunk**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Native VLAN</td>
<td>Untagged VLAN on the trunk switch port.</td>
</tr>
<tr>
<td>Prune Eligible</td>
<td>Specifies whether VLANs on the trunk port can be pruned.</td>
</tr>
<tr>
<td>Allows VLANs</td>
<td>List of allowed VLANs on the trunk port.</td>
</tr>
<tr>
<td>Desired Trunking Encapsulation</td>
<td>Trunk encapsulation.</td>
</tr>
<tr>
<td>Trunking Encapsulation Negotiation</td>
<td>Specifies that the interface negotiate with the neighboring interface to become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring interface.</td>
</tr>
</tbody>
</table>

Monitoring Switch IP Interfaces

Choose **Monitor > Switches**, then click an IP address in the IP Address column. From the System menu, choose **Interfaces > IP Interfaces**. Table 5-38 describes the IP interface information that is displayed.

Table 5-38  Viewing Switch IP Interfaces

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of the interface.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the interface.</td>
</tr>
<tr>
<td>Address Type</td>
<td>Type of address (IPv4 or IPv6).</td>
</tr>
</tbody>
</table>

Monitoring Switch VLAN Interfaces

Choose **Monitor > Switches**, then click an IP address in the IP Address column. From the System menu, choose **Interfaces > VLAN Interfaces**. Table 5-39 describes the VLAN interface information that is displayed.

Table 5-39  Viewing Switch VLAN Interfaces

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Name</td>
<td>Name of the VLAN port.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>ID of the VLAN port.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Current operational state of the VLAN interface.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Current administrative state of the VLAN interface.</td>
</tr>
<tr>
<td>Port Type</td>
<td>Type of VLAN port.</td>
</tr>
<tr>
<td>Maximum Speed (Mbps)</td>
<td>Maximum supported speed for the VLAN interface.</td>
</tr>
<tr>
<td>MTU</td>
<td>Size of the largest packet that can be sent/received on the VLAN interface.</td>
</tr>
</tbody>
</table>
Monitoring Switch EtherChannel Interfaces

Choose **Monitor > Switches**, then click an IP address in the IP Address column. From the System menu, choose **Interfaces > EtherChannel Interfaces**. Table 5-40 describes the EtherChannel interface information that is displayed.

**Table 5-40 Viewing Switch EtherChannel Interfaces**

<table>
<thead>
<tr>
<th>Name</th>
<th>Name of the EtherChannel interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel Group ID</td>
<td>Numeric identifier for the EtherChannel.</td>
</tr>
<tr>
<td>Control Method</td>
<td>Protocol for managing the EtherChannel either LACP or TAgP.</td>
</tr>
<tr>
<td>Actor Admin Key</td>
<td>Channel Identifier.</td>
</tr>
<tr>
<td>Number of (LAG) Members</td>
<td>Number of ports configured.</td>
</tr>
</tbody>
</table>

Monitoring Switch Clients

Choose **Monitor > Switches**, then click an IP address in the IP Address column. From the System menu, choose **Clients**. Table 5-40 describes the EtherChannel interface information that is displayed.

**Table 5-41 Viewing Current Associated Client**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>IP address of the client.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>MAC address of the client.</td>
</tr>
<tr>
<td>User Name</td>
<td>Username of the client.</td>
</tr>
<tr>
<td>Vendor Name</td>
<td>Vendor Name of the client.</td>
</tr>
<tr>
<td>Map Location</td>
<td>Location of the client.</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN on which the client is configured.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface on which the client is configured.</td>
</tr>
<tr>
<td>Association Time</td>
<td>Timestamp of the client association.</td>
</tr>
<tr>
<td>Authorization Profile Name</td>
<td>Authorization Profile Name stored.</td>
</tr>
</tbody>
</table>

Monitoring Access Points

This section describes access to the controller access points summary details. Use the main date area to access the respective access point details.

Choose **Monitor > Access Points** to access this page. This section provides more detailed information regarding monitoring access points and contains the following topics:

- **Searching Access Points**, page 5-44
- **Viewing a List of Access Points**, page 5-44
- **Generating a Report for Access Points**, page 5-48
- **Monitoring Access Points Details**, page 5-58
- **Monitoring Access Point Radio Details**, page 5-69
- **Monitoring Mesh Access Points**, page 5-80
• Retrieving the Unique Device Identifier on Controllers and Access Points, page 5-86
• Monitoring Coverage Holes, page 5-86
• Monitoring Rogue Access Points, page 5-89
• Monitoring Ad hoc Rogues, page 5-103
• Searching Rogue Clients Using Advanced Search, page 5-107
• Monitoring Rogue Access Point Location, Tagging, and Containment, page 5-107

Searching Access Points

Use the Prime Infrastructure Search feature to find specific access points or to create and save custom searches. See the Search Methods section in the Cisco Prime Infrastructure 2.0 User Guide for additional information.

Note

Users working in Converged View of Prime Infrastructure, can not find Monitoring AP options in Search bar.

Viewing a List of Access Points

Choose Monitor > Access Points or perform an access point search to access this page.

This page enables you to view a summary of access points including the default information listed in Table 5-42.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Name Ethernet MAC</td>
<td>The name assigned to the access point. Click a list item to view access point details. See the “Monitoring Access Points Details” section on page 5-58 for more information.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Local IP address of the access point.</td>
</tr>
<tr>
<td>Radio</td>
<td>Protocol of the rogue access point is 802.11a, 802.11b or 802.11g. Click a list item to view access point radio details. See the “Monitoring Access Point Radio Details” section on page 5-69 for more information.</td>
</tr>
<tr>
<td>Map Location</td>
<td>Click a list item to go to the location indicated on the list.</td>
</tr>
<tr>
<td>Controller</td>
<td>Click a list item to display a graphic and information about the controller. See the “Monitoring System Summary” section on page 5-4 for more information.</td>
</tr>
<tr>
<td>Client Count</td>
<td>Displays the total number of clients currently associated with the controller.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Displays the administration state of the access point as either enabled or disabled.</td>
</tr>
</tbody>
</table>
### Table 5-42 Access Point Search Results

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Mode</td>
<td>Displays the operational mode of the access point.</td>
</tr>
<tr>
<td>Oper Status</td>
<td>Displays the operational status of the Cisco WLAN Solution device, either Up or Down. If the admin status is disabled, the operation status is labeled as down and there are no alarms.</td>
</tr>
</tbody>
</table>
| Alarm Status      | Alarms are color coded as follows:  
  - Clear—No Alarm  
  - Red—Critical Alarm  
  - Orange—Major Alarm  
  - Yellow—Minor Alarm  
  
  **Note** This status is radio alarm status ONLY and does not include the admin status in the operation status. |

### Configuring the Access Point List Display

To add, remove, or reorder columns in the table, click the **Edit View** link to go to the Edit View page. **Table 5-43** lists the optional access point parameters available for the search results.

### Table 5-43 Edit View Search Results

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Type</td>
<td>Indicates the type of access point (unified or autonomous).</td>
</tr>
<tr>
<td>Antenna Azim. Angle</td>
<td>Indicates the horizontal angle of the antenna.</td>
</tr>
<tr>
<td>Antenna Diversity</td>
<td>Indicates if antenna diversity is enabled or disabled. Antenna diversity refers to the access point sampling the radio signal from two integrated antenna ports to choose the preferred antenna.</td>
</tr>
<tr>
<td>Antenna Elev. Angle</td>
<td>Indicates the elevation angle of the antenna.</td>
</tr>
<tr>
<td>Antenna Gain</td>
<td>The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means 4 x 0.5 = 2 dBm of gain.</td>
</tr>
<tr>
<td>Antenna Mode</td>
<td>Indicates the antenna mode such as omni, directional, or non-applicable.</td>
</tr>
<tr>
<td>Antenna Name</td>
<td>Indicates the antenna name or type.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Audit Status</td>
<td>Indicates one of the following audit statuses:</td>
</tr>
<tr>
<td></td>
<td>- Mismatch—Configuration differences were found between Prime Infrastructure and controller during the last audit.</td>
</tr>
<tr>
<td></td>
<td>- Identical—No configuration differences were found during the last audit.</td>
</tr>
<tr>
<td></td>
<td>- Not Available—Audit status is unavailable.</td>
</tr>
<tr>
<td>Base Radio MAC</td>
<td>Indicates the MAC address of the base radio.</td>
</tr>
<tr>
<td>Bridge Group Name</td>
<td>Indicates the name of the bridge group used to group the access points, if applicable.</td>
</tr>
<tr>
<td>CDP Neighbors</td>
<td>Indicates all directly connected Cisco devices.</td>
</tr>
<tr>
<td>Channel Control</td>
<td>Indicates whether the channel control is automatic or custom.</td>
</tr>
<tr>
<td>Channel Number</td>
<td>Indicates the channel on which the Cisco Radio is broadcasting.</td>
</tr>
<tr>
<td>Channel Width</td>
<td>Indicates the channel bandwidth for this radio. The Channel Width field is supported only for 11n APs. Displays “N/A” for other APs.</td>
</tr>
<tr>
<td>Controller Port</td>
<td>Indicates the number of controller ports.</td>
</tr>
<tr>
<td>Google Earth Location</td>
<td>Indicates whether or not a Google Earth location is assigned and indicates the location.</td>
</tr>
<tr>
<td>Location</td>
<td>Indicates the physical location of the access point.</td>
</tr>
<tr>
<td>Node Hops</td>
<td>Indicates the number of hops between access points.</td>
</tr>
<tr>
<td>OfficeExtend AP</td>
<td>Specifies whether or not OfficeExtend access is enabled. If it is disabled, the access point is remotely deployed which increases the security risk.</td>
</tr>
</tbody>
</table>
**Chapter 5  Monitoring Devices**

**Monitoring Access Points**

---

**Table 5-43  Edit View Search Results (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PoE Status</td>
<td>Indicates the power over Ethernet status of the access point. The possible values include the following:</td>
</tr>
<tr>
<td></td>
<td>- Low—The access point draws low power from the Ethernet.</td>
</tr>
<tr>
<td></td>
<td>- Lower than 15.4 volts—The access point draws lower than 15.4 volts from the Ethernet.</td>
</tr>
<tr>
<td></td>
<td>- Lower than 16.8 volts—The access point draws lower than 16.8 volts from the Ethernet.</td>
</tr>
<tr>
<td></td>
<td>- Normal—The power is high enough for the operation of the access point.</td>
</tr>
<tr>
<td></td>
<td>- Not Applicable—The power source is not from the Ethernet.</td>
</tr>
<tr>
<td>Primary Controller</td>
<td>Indicates the name of the primary controller for this access point.</td>
</tr>
<tr>
<td>Radio MAC</td>
<td>Indicates the radio MAC address.</td>
</tr>
<tr>
<td>Reg. Domain Supported</td>
<td>Indicates whether or not the regulatory domain is supported.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Indicates the access point serial number.</td>
</tr>
<tr>
<td>Slot</td>
<td>Indicates the slot number.</td>
</tr>
<tr>
<td>Tx Power Control</td>
<td>Indicates whether the transmission power control is automatic or custom.</td>
</tr>
<tr>
<td>Tx Power Level</td>
<td>Indicates the transmission power level.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Indicates how long the access point has been up in days, hours, minutes and seconds.</td>
</tr>
<tr>
<td>WLAN Override Names</td>
<td>Indicates the WLAN override profile names.</td>
</tr>
<tr>
<td>WLAN Override</td>
<td>Indicates whether WLAN Override is enabled or disabled.</td>
</tr>
</tbody>
</table>

---

**Configuring the List of Access Points Display**

The Edit View page allows you to add, remove, or reorder columns in the Access Points table.

To edit the available columns in the alarms table, follow these steps:

**Step 1** Choose Monitor > Access Points.

**Step 2** Click the Edit View link.

**Step 3** To add an additional column to the access points table, click to highlight the column heading in the left column. Click **Show** to move the heading to the right column. All items in the right column are displayed in the table.
Step 4 To remove a column from the access points table, click to highlight the column heading in the right column. Click Hide to move the heading to the left column. All items in the left column are not displayed in the table.

Step 5 Use the Up/Down buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click Up or Down to move it higher or lower in the current list.

Step 6 Click Reset to restore the default view.

Step 7 Click Submit to confirm the changes.

Note See the “Viewing a List of Access Points” section on page 5-44 for additional access point fields than can be added through Edit View.

---

Generating a Report for Access Points

Note You cannot customize any report that you create in the Access Points list (Monitor > Access Points).

To generate a report for access points, follow these steps:

Step 1 Choose Monitor > Access Points.

Step 2 Click to select the access point(s) for which you want to run a report.

Step 3 Choose the applicable report from the Select a report drop-down list.

Step 4 Click Go.

Table 5-44 lists the available reports.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load</td>
<td>Generates a report with load information.</td>
<td>See the “Monitoring Traffic Load” section on page 5-50 for more information.</td>
</tr>
<tr>
<td>Dynamic Power Control</td>
<td>Generates a report with Dynamic Power Control information.</td>
<td>See the “Monitoring Dynamic Power Control” section on page 5-51 for more information.</td>
</tr>
<tr>
<td>Noise</td>
<td>Generates a report with Noise information.</td>
<td>See the “Monitoring Access Points Noise” section on page 5-52 for more information.</td>
</tr>
<tr>
<td>Interference</td>
<td>Generates a report with Interference information.</td>
<td>See the “Monitoring Access Points Interference” section on page 5-52 for more information.</td>
</tr>
<tr>
<td>Coverage (RSSI)</td>
<td>Generates a report with Coverage (RSSI) information.</td>
<td>See the “Monitoring Access Points Coverage (RSSI)” section on page 5-53 for more information.</td>
</tr>
</tbody>
</table>
### Table 5-44  Access Point Reports (continued)

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coverage (SNR)</td>
<td>Generates a report with Coverage (SNR) information.</td>
<td>See the “Monitoring Access Points Coverage (SNR)” section on page 5-53 for more information.</td>
</tr>
<tr>
<td>Up/Down Statistics</td>
<td>Time in days, hours and minutes since the last reboot. Generates a report with Up Time information.</td>
<td>See the “Monitoring Access Points Up/Down Statistics” section on page 5-53 for more information.</td>
</tr>
<tr>
<td>Voice Statistics</td>
<td>Generates a report for selected access points showing radio utilization by voice traffic.</td>
<td>See the “Monitoring the Access Points Voice Statistics” section on page 5-54 for more information.</td>
</tr>
<tr>
<td>Voice TSM Table</td>
<td>Generates a report for selected access points and radio, organized by client device showing QoS status, PLR, and latency of its voice traffic stream.</td>
<td>See the “Monitoring the Access Points Voice TSM Table” section on page 5-54 for more information.</td>
</tr>
<tr>
<td>Voice TSM Reports</td>
<td>Graphical representation of the TSM table except that metrics from the clients are averaged together on the graphs.</td>
<td>See the “Monitoring the Access Points Voice TSM Reports” section on page 5-56 for more information.</td>
</tr>
<tr>
<td>802.11 Counters</td>
<td>Displays counters for access points at the MAC layer. Statistics such as error frames, fragment counts, RTS/CTS frame count, and retransmitted frames are generated based on the filtering criteria and can help interpret performance (and problems, if any) at the MAC layer.</td>
<td>See the “Monitoring Access Points 802.11 Counters” section on page 5-56 for more information.</td>
</tr>
<tr>
<td>AP Profile Status</td>
<td>Displays access point load, noise, interference, and coverage profile status.</td>
<td>See the “Monitoring Access Points AP Profile Status” section on page 5-57 for more information.</td>
</tr>
<tr>
<td>Air Quality vs. Time</td>
<td>Displays the air quality index of the wireless network during the configured time duration.</td>
<td>See the “Monitoring Air Quality” section on page 5-58 for more information.</td>
</tr>
<tr>
<td>Traffic Stream Metrics</td>
<td>Useful in determining the current and historical quality of service (QoS) for given clients at the radio level. It also displays uplink and downlink statistics such as packet loss rate, average queuing delay, distribution of delayed packets, and roaming delays.</td>
<td>See the “Monitoring Access Points Traffic Stream Metrics” section on page 5-57 for more information.</td>
</tr>
<tr>
<td>Tx Power and Channel</td>
<td>Displays the channel plan assignment and transmit power level trends of devices based on the filtering criteria used when the report was generated. It could help identify unexpected behavior or issues with network performance.</td>
<td>See the “Monitoring Access Points Tx Power and Channel” section on page 5-57 for more information.</td>
</tr>
</tbody>
</table>
Monitoring Traffic Load

Traffic Load is the total amount of bandwidth used for transmitting and receiving traffic. This enables WLAN managers to track network growth and plan network growth ahead of client demand.

To access the access point load report, follow these steps:

**Step 1** Choose Monitor > Access Points.

**Step 2** Select the check box(es) of the applicable access point(s).

**Step 3** From the Generate a report for selected APs drop-down list, choose Load.

**Step 4** Click Go. The Load report displays for the selected access points.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIP Calls Table</td>
<td>Provides the same information as the VoIP Calls Graph report but in table form.</td>
<td>See the “Monitoring VoIP Calls” section on page 5-58 for more information.</td>
</tr>
<tr>
<td>Voice Statistics</td>
<td>Helps analyze wireless network usage from a voice perspective by providing details such as percentage of bandwidth used by voice clients, voice calls, roaming calls, and rejected calls (per radio) on the network. To be able to gather useful data from this report, make sure call admission control (CAC) is supported on voice clients.</td>
<td>See the “Monitoring Voice Statistics” section on page 5-58 for more information.</td>
</tr>
<tr>
<td>Worst Air Quality APs</td>
<td>Provides a high-level, easy-to-understand metric to facilitate an &quot;at a glance&quot; understanding of where interference problems are impacting the network. Air Quality (AQ) is reported at a channel, floor, and system level and it supports AQ alerts, so that you can be automatically notified when AQ falls below a desired threshold.</td>
<td>See the “Monitoring Air Quality” section on page 5-58 for more information.</td>
</tr>
</tbody>
</table>
Chapter 5 Monitoring Devices

Monitoring Access Points

Table 5-45 lists the fields displayed on this page.

**Table 5-45 Traffic Load**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Name</td>
<td>Click the access point name to view access point details. See the “Monitoring Access Points Details” section on page 5-58 for more information.</td>
</tr>
<tr>
<td>Radio</td>
<td>Protocol of the rogue access point is either 802.11a, 802.11b or 802.11g. Click the radio to view On-Demand Statistics for this access point. See the “Monitoring Access Point Radio Details” section on page 5-69 for more information.</td>
</tr>
<tr>
<td>Attached Client Count</td>
<td>Number of clients attached (Actual and Threshold.)</td>
</tr>
<tr>
<td>Channel Utilization</td>
<td>802.11a RF utilization threshold between 0 and 100 percent (Actual and Threshold).</td>
</tr>
<tr>
<td>Receive Utilization</td>
<td>802.11a or 802.11b/g RF receive utilization threshold between 0 and 100 percent.</td>
</tr>
<tr>
<td>Transmit Utilization</td>
<td>802.11a or 802.11b/g RF transmit utilization threshold between 0 and 100 percent.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the client connection.</td>
</tr>
</tbody>
</table>

**Monitoring Dynamic Power Control**

To access the access point Load report, follow these steps:

1. **Step 1**: Choose Monitor > Access Points.
2. **Step 2**: Select the check box(es) of the applicable access point(s).
3. **Step 3**: From the Generate a report for selected APs drop-down list, choose Dynamic Power Control.
4. **Step 4**: Click Go. The Dynamic Power Control report displays the selected access points.

Table 5-46 lists the dynamic control fields for access points displayed on this page.

**Table 5-46 Dynamic Power Control Page Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Name</td>
<td>This is the name assigned to the access point. Click an access point name in the list to access its fields. See the “Monitoring Access Points Details” section on page 5-58 for more information.</td>
</tr>
<tr>
<td>Radio</td>
<td>Protocol of the rogue access point is either 802.11a, or 802.11b/g. Click a Cisco Radio in the list to access its fields. See the “Monitoring Access Point Radio Details” section on page 5-69 for more information.</td>
</tr>
</tbody>
</table>
To access the access point Noise report, follow these steps:

**Step 1** Choose Monitor > Access Points.

**Step 2** Select the check box(es) of the applicable access point(s).

**Note** If multiple access points are selected, they must have the same radio type.

**Step 3** From the Generate a report selected APs drop-down list, choose Noise.

**Step 4** Click Go. The Noise report displays the selected access points.

This page displays a bar graph of noise (RSSI in dBm) for each channel.

**Monitoring Access Points Interference**

To access the access point Interference report, follow these steps:

**Step 1** Choose Monitor > Access Points.

**Step 2** Select the check box(es) of the applicable access point(s).
Note: If multiple access points are selected, they must have the same radio type.

**Step 3**  
From the Generate a report for selected APs drop-down list, choose **Interference**.

**Step 4**  
Click **Go**. The Interference report displays the selected access points.

This page displays a bar graph of interference (RSSI in dBm) for each channel:
- High interference -40 to 0 dBm.
- Marginal interference -100 to -40 dBm.
- Low interference -110 to -100 dBm.

---

**Monitoring Access Points Coverage (RSSI)**

To access the access point Coverage (RSSI) report, follow these steps:

**Step 1**  
Choose **Monitor > Access Points**.

**Step 2**  
Select the check box(es) of the applicable access point(s).

**Step 3**  
From the Generate a report for selected APs drop-down list, choose **Coverage (RSSI)**.

**Step 4**  
Click **Go**. The Coverage (RSSI) report displays the selected access points.

This page displays a bar graph of client distribution by received signal strength showing the number of clients versus RSSI in dBm.

---

**Monitoring Access Points Coverage (SNR)**

To access the access point Coverage (SNR) report, follow these steps:

**Step 1**  
Choose **Monitor > Access Points**.

**Step 2**  
Select the check box(es) of the applicable access point(s).

**Step 3**  
From the Generate a report for selected APs drop-down list, choose **Coverage (SNR)**.

**Step 4**  
Click **Go**. The Coverage (SNR) report displays the selected access points.

This page displays a bar graph of client distribution by signal-to-noise ratio showing the number of clients versus SNR.

---

**Monitoring Access Points Up/Down Statistics**

To access the access point Up/Down Statistics report, follow these steps:

**Step 1**  
Choose **Monitor > Access Points**.

**Step 2**  
Select the check box of the applicable access point.
Step 3 From the Generate a report for selected APs drop-down list, choose **Up/Down Statistics**. Click **Go**. The Up/Down Statistics report displays the selected access points.

**Note** Up Time is time in days, hours, and minutes since the last reboot.

This page displays a line graph of access point up time graphed against time. If you select more than one access point, the following message appears:

Please select only one AP for the Up Time Report.

---

### Monitoring the Access Points Voice Statistics

This generates a report for selected access points showing radio utilization by voice traffic. The report includes the number of current calls.

**Note** Voice Statistics reports are only applicable for CAC/WMM clients.

To access the access point Voice Statistics report, follow these steps:

1. Choose **Monitor > Access Points**.
2. Select the check box(es) of the applicable access point(s).
3. From the Generate a report for selected APs drop-down list, choose **Voice Statistics**. Click **Go**. The Voice Statistics report displays for the selected access points.

The page displays the following access point voice statistics:

- **AP Name**—Select an item under AP Name. For more information, see the “Monitoring Access Points Details” section on page 5-58.
- **Radio**—Select an item under Radio. For more information, see the “Monitoring Access Point Radio Details” section on page 5-69.
- **Calls in Progress**—Number of calls in progress.
- **Roaming Calls in Progress**—Number of roaming calls in progress.
- **Bandwidth in Use**—Percentage of bandwidth in use.

---

### Monitoring the Access Points Voice TSM Table

This generates a report for selected access points and radio, organized by client device showing QoS status, PLR, and latency of its voice traffic stream.

To access the access point Voice TSM Table report, follow these steps:

1. Choose **Monitor > Access Points**.
2. Select the check box of the applicable access point.
**Step 3**  From the Generate a report for selected APs drop-down list, choose **Voice TSM Table**.

**Step 4**  Click **Go**. The Voice Traffic Stream Metrics Table report displays the selected access point.

Table 5-47 lists the Voice Traffic Stream Metrics Table page fields.

**Table 5-47 Voice Traffic Stream Metrics Table Page Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time that the statistics were gathered from the access point(s).</td>
</tr>
<tr>
<td>Client MAC</td>
<td>MAC address of the client. This shows a list of the clients evaluated during the most recent 90 second interval. The client could be a VoIP phone, laptop, PDA and refers to any client attached to the access point collecting measurements.</td>
</tr>
<tr>
<td>QoS</td>
<td>QoS values (packet latency, packet jitter, packet loss, roaming time) which can affect the WLAN are monitored. Access points and clients measure the metrics, access points collect the measurements and send them to the controller. The access points update the controller with traffic stream metric information every 90 seconds and 10 minutes of data is stored at one time.</td>
</tr>
<tr>
<td>% PLR (Downlink)</td>
<td>Percentage of packets lost on the downlink (access point to client) during the 90 second interval.</td>
</tr>
<tr>
<td>% PLR (Uplink)</td>
<td>Percentage of packets lost on the uplink (client to access point) during the 90 second interval.</td>
</tr>
<tr>
<td>Avg Queuing Delay (ms) (Downlink)</td>
<td>Average queuing delay in milliseconds for the downlink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.</td>
</tr>
<tr>
<td>Avg Queuing Delay (ms) (Uplink)</td>
<td>Average queuing delay in milliseconds for the uplink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.</td>
</tr>
<tr>
<td>% Packets &gt; 40 ms Queuing Delay</td>
<td>Percentage of queuing delay packets greater than 40 ms.</td>
</tr>
<tr>
<td>% Packets &gt; 20 ms Queuing Delay</td>
<td>Percentage of queuing delay packets greater than 20 ms.</td>
</tr>
<tr>
<td>Roaming Delay</td>
<td>Roaming delay in milliseconds. Roaming delay, which is measured by clients, is measured beginning when the last packet is received from the old access point and ending when the first packet is received from the new access point after a successful roam.</td>
</tr>
</tbody>
</table>
Monitoring the Access Points Voice TSM Reports

This report provides a graphical representation of the Voice Traffic Stream Metrics Table except that metrics from the clients are averaged together on the graphs.

To access the access point Voice Traffic Stream Metrics Table report, follow these steps:

**Step 1** Choose Monitor > Access Points.

**Step 2** Select the check box of the applicable access point.

**Step 3** From the Generate a report for selected APs drop-down list, choose Voice TSM Reports.

Click Go. The Voice Traffic Stream Metrics Table report displays for the selected access point.

This page displays line graphs of the following downlink and uplink metric information, including times and dates (see Table 5-48).

**Table 5-48 Voice Traffic Stream Metrics Table Reports Page Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Queuing Delay (ms)</td>
<td>Average queuing delay in milliseconds. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.</td>
</tr>
<tr>
<td>% Packet with less than 10 ms delay</td>
<td>Percentage of packets with less than 10 milliseconds delay.</td>
</tr>
<tr>
<td>% Packet with more than 10 &lt; 20 ms delay</td>
<td>Percentage of packets with more than 10 milliseconds delay but less than 20 milliseconds delay.</td>
</tr>
<tr>
<td>% Packet with more than 20 &lt; 40 ms delay</td>
<td>Percentage of packets with more than 20 milliseconds delay but less than 40 milliseconds delay.</td>
</tr>
<tr>
<td>% Packet with more than 40 ms delay</td>
<td>Percentage of packets with more than 40 milliseconds delay.</td>
</tr>
<tr>
<td>Packet Loss Ratio</td>
<td>Ratio of lost packets.</td>
</tr>
<tr>
<td>Total Packet Count</td>
<td>Number of total packets.</td>
</tr>
<tr>
<td>Roaming Count</td>
<td>Number of packets exchanged for roaming negotiations in this 90 seconds metrics page.</td>
</tr>
<tr>
<td>Roaming Delay</td>
<td>Roaming delay in milliseconds.</td>
</tr>
</tbody>
</table>

Monitoring Access Points 802.11 Counters

Displays counters for access points at the MAC layer. Statistics such as error frames, fragment counts, RTS/CTS frame count, and retried frames are generated based on the filtering criteria and can help interpret performance (and problems, if any) at the MAC layer.

See the “Reports” section on page 14-1 for more information on 802.11 Counters reports.
Chapter 5  Monitoring Devices

Monitoring Access Points AP Profile Status

Displays access point load, noise, interference, and coverage profile status.

See the “Reports” section on page 14-1 for more information on AP Profile Status reports.

Monitoring Access Points Radio Utilization

See the “Reports” section on page 14-1 for more information on Radio Utilization reports.

Monitoring Access Points Traffic Stream Metrics

Useful in determining the current and historical quality of service (QoS) for given clients at the radio level. It also displays uplink and downlink statistics such as packet loss rate, average queuing delay, distribution of delayed packets, and roaming delays.

See the “Reports” section on page 14-1 for more information on Traffic Stream Metrics reports.

Monitoring Access Points Tx Power and Channel

See the “Reports” section on page 14-1 for more information on Tx Power and Channel reports.

The Current Tx Power Level setting controls the maximum conducted transmit power. The maximum available transmit power varies according to the configured channel, individual country regulation, and access point capability. See the Product Guide or data sheet at www.cisco.com for each specific model to determine the access point capability.

The Current Tx Power Level setting of 1 represents the maximum conducted power setting for the access point. Each subsequent power level (for example. 2, 3, 4, and so on.) represents approximately a 50% (or 3dBm) reduction in transmit power from the previous power level.

Note

The actual power reduction might vary slightly for different models of access points.

Based on the configured antenna gain, the configured channel, and the configured power level, the actual transmit power at the access point can be reduced so that the specific country regulations are not exceeded.

Note

Irrespective of whether you choose Global or Custom assignment method, the actual conducted transmit power at the access point is verified such that country specific regulations are not exceeded.

Command Buttons

- Save—Save the current settings.
- Audit—Discover the present status of this access point.
Monitoring VoIP Calls

VoIP calls reports helps analyze wireless network usage from a voice perspective by providing details such as the number and duration of VoIP calls (per radio) on the network over time. To be able to gather useful data from this report, VoIP snooping must be enabled on the WLAN. This report displays information in a graph.

Click VoIP Calls Graph from the Report Launch Pad to open the VoIP Calls Graph Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the “Reports” section on page 14-1 for more information.

Monitoring Voice Statistics

Voice Statistics report helps analyze wireless network usage from a voice perspective by providing details such as percentage of bandwidth used by voice clients, voice calls, roaming calls, and rejected calls (per radio) on the network. To be able to gather useful data from this report, make sure Call Admission Control (CAC) is supported on voice clients. See the “Reports” section on page 14-1 for more information.

Monitoring Air Quality

To facilitate an "at a glance" understanding of where interference problems are impacting the network, the Prime Infrastructure rolls up the detailed information into a high-level, easy-to-understand metric referred to as Air Quality (AQ). AQ is reported at a channel, floor, and system level and it supports AQ alerts, so that you can be automatically notified when AQ falls below a desired threshold. See the “Monitoring CleanAir Air Quality Events” section on page 5-146 for more information.

Monitoring Access Points Details

The Access Points Details page enables you to view access point information for a single AP.

Choose Monitor > Access Points and click an item in the AP Name column to access this page. Depending on the type of access point, the following tabs might be displayed. This section provides the detailed information regarding each Access Points Details page tab and contains the following topics:

- General Tab, page 5-58
- Interfaces Tab, page 5-65
- Mesh Statistics Tab, page 5-81
- Mesh Links Tab, page 5-85
- CDP Neighbors Tab, page 5-67
- Current Associated Clients Tab, page 5-67
- SSID Tab, page 5-68
- Clients Over Time Tab, page 5-69

General Tab

**Note**

The General tab fields differ between lightweight and autonomous access points.
### General—Lightweight Access Points

Table 5-49 lists the General (for Lightweight Access Points) Tab fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>AP Name</td>
<td>Operator defined name of access point.</td>
</tr>
<tr>
<td>AP IP address, Ethernet</td>
<td>IP address, Ethernet MAC address and Radio MAC address.</td>
</tr>
<tr>
<td>MAC address, and Base Radio</td>
<td></td>
</tr>
<tr>
<td>MAC address</td>
<td></td>
</tr>
<tr>
<td>Country Code</td>
<td>The codes of the supported countries. Up to 20 countries can be supported per controller.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Access points might not operate properly if they are not designed for use in your country of operation. For a complete list of country codes supported per product, see the following URL: <a href="http://www.cisco.com/en/US/docs/wireless/wcs/4.0/configuration/guide/wscod.html">http://www.cisco.com/en/US/docs/wireless/wcs/4.0/configuration/guide/wscod.html</a>.</td>
</tr>
<tr>
<td>Link Latency Settings</td>
<td>You can configure link latency on the controller to measure the link between an access point and the controller. See the “Configuring Link Latency Settings for Access Points” section on page 9-218 for more information.</td>
</tr>
<tr>
<td>Current Link Latency (in msec)</td>
<td>The current round-trip time (in milliseconds) of heartbeat packets from the access point to the controller and back.</td>
</tr>
<tr>
<td>Minimum Link Latency (in msec)</td>
<td>Because link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of heartbeat packets from the access point to the controller and back.</td>
</tr>
<tr>
<td>Maximum Link Latency (in msec)</td>
<td>Because link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of heartbeat packets from the access point to the controller and back.</td>
</tr>
<tr>
<td>LWAPP/CAPWAP Uptime</td>
<td>Displays how long the LWAPP/CAPWAP connection has been active.</td>
</tr>
<tr>
<td>LWAPP/CAPWAP Join Taken Time</td>
<td>Displays how long the LWAPP/CAPWAP connection has been joined.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>The administration state of the access point as either enabled or disabled.</td>
</tr>
<tr>
<td><strong>AP Mode</strong></td>
<td></td>
</tr>
</tbody>
</table>
Monitoring Access Points

Chapter 5  Monitoring Devices

Table 5-49  General (for Lightweight Access Points) Tab Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Local         | Default mode. Data clients are serviced while configured channels are scanned for noise and rogues. The access point goes off-channel for 50 ms and listens for rogues. It cycles through each channel for the period specified under the Auto RF configuration.  
**Note** To configure Local or FlexConnect access points for the Cisco Adaptive wIPS feature, choose Local or FlexConnect and select the **Enhanced wIPS Engine Enabled** check box. |
| Monitor       | Radio receive only mode. The access point scans all configured channels every 12 seconds. Only deauthenticated packets are sent in the air with an access point configured this way. A monitor mode access point can connect as a client to a rogue access point.  
**Note** To configure access points for Cisco Adaptive wIPS feature, select Monitor. Select the **Enhanced wIPS Engine Enabled** check box and choose wIPS from the Monitor Mode Optimization drop-down list. Before you can enable an access point to be in wIPS mode, you must disable the access point radios. If you do not disable the access point radio, an error message appears.  
**Note** Once you have enabled the access point for wIPS, reenable the radios. |
| Rogue Detector| The access point radio is turned off and the access point listens to wired traffic only. The controllers that operate in this mode monitor the rogue access points. The controller sends all the rogue access point and client MAC address lists to the rogue detector, and the rogue detector forwards this information to the WLC. The MAC address list is compared to what the WLC access points heard over the network. If the MAC addresses match, you can determine which rogue access points are connected on the wired network. |
| Sniffer       | The access point captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek. These packets contain information such as timestamp, signal strength, packet size, and so on. This feature can only be enabled if you run AiroPeek, which is a third-party network analyzer software that supports the decoding of data packets. |
| FlexConnect   | Enables FlexConnect for up to six access points. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost.  
**Note** FlexConnect must be selected to configure an OfficeExtend access point. When the AP mode is FlexConnect, FlexConnect configuration options display including the option to enable OfficeExtend AP and to enable Least Latency Controller Join. |
### Table 5-49  General (for Lightweight Access Points) Tab Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge</td>
<td>This is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The bridge and its wired clients are listed as client in the Prime Infrastructure if the AP mode is set to Bridge, and the access point is bridge capable.</td>
</tr>
<tr>
<td>Spectrum Expert</td>
<td>This mode allows a CleanAir-enabled access point to be used extensively for interference detection on all monitored channels. All other functions such as IDS scanning and Wi-Fi are suspended.</td>
</tr>
<tr>
<td>Enhanced wIPS Engine</td>
<td>Enabled or Disabled, to enable the monitoring of the security attacks using Cisco Adaptive wIPS feature.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Registered or Not Registered, as determined by the controller.</td>
</tr>
<tr>
<td>Registered Controller</td>
<td>The controller to which the access point is registered. Click to display the registered controller details. See the “Monitoring System Summary” section on page 5-4 for more information.</td>
</tr>
<tr>
<td>Primary Controller</td>
<td>The name of the primary controller for this access point.</td>
</tr>
<tr>
<td>Port Number</td>
<td>The SNMP name of the access point primary controller. The access point attempts to associate with this controller first for all network operations and in the event of a hardware reset.</td>
</tr>
<tr>
<td>AP Uptime</td>
<td>Displays how long the access point has been active to receive and transmit.</td>
</tr>
<tr>
<td>Map Location</td>
<td>Customer-definable location name for the access point. Click to look at the actual location on a map. Choose Monitor &gt; Access Points &gt; name &gt; Map Location for more information.</td>
</tr>
<tr>
<td>Google Earth Location</td>
<td>Indicates whether a Google Earth location is assigned.</td>
</tr>
<tr>
<td>Location</td>
<td>The physical location where the access point is placed (or Unassigned).</td>
</tr>
<tr>
<td>Statistics Timer</td>
<td>This counter sets the time in seconds that the access point sends its DOT11 statistics to the controller.</td>
</tr>
<tr>
<td>PoE Status</td>
<td>The power over ethernet status of the access point. The possible values include the following:</td>
</tr>
<tr>
<td></td>
<td>- Low—The access point draws low power from the Ethernet.</td>
</tr>
<tr>
<td></td>
<td>- Lower than 15.4 volts—The access point draws lower than 15.4 volts from the Ethernet.</td>
</tr>
<tr>
<td></td>
<td>- Lower than 16.8 volts—The access point draws lower than 16.8 volts from the Ethernet.</td>
</tr>
<tr>
<td></td>
<td>- Normal—The power is high enough for the operation of the access point.</td>
</tr>
<tr>
<td></td>
<td>- Not Applicable—The power source is not from the Ethernet.</td>
</tr>
</tbody>
</table>
### Rogue Detection
Indicates whether or not Rogue Detection is enabled.

**Note** Rogue detection is disabled automatically for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. For more information regarding OfficeExtend access points, see the *Cisco Wireless LAN Controller Configuration Guide*.

### OfficeExtend AP
Indicates whether or not the access point is enabled as an OfficeExtend access point. The default is Enabled.

### Encryption
Indicates whether or not encryption is enabled.

**Note** Enabling or disabling encryption functionality causes the access point to reboot which then causes a loss of connectivity for clients.

**Note** DTLS data encryption is enabled automatically for OfficeExtend access points to maintain security. Encryption is only available if the access point is connected to a 5500 series controller with a Plus license.

### Least Latency Join
The access point switches from a priority order search (primary, secondary, and then tertiary controller) to a search for the controller with the best latency measurement (least latency). The controller with the least latency provides the best performance.

### Telnet Access
Indicates whether or not Telnet Access is enabled.

### SSH Access
Indicates whether or not SSH is enabled.

**Note** An OfficeExtend access point might be connected directly to the WAN which could allow external access if the default password is used by the access point. Because of this, Telnet and SSH access are disabled automatically for OfficeExtend access points.

### Software Version
The operating system release.version.dot.maintenance number of the code currently running on the controller.

### Boot Version
The operating system bootloader version number.

### Inventory Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Type</td>
<td>Type of Access Point</td>
</tr>
<tr>
<td>AP Model</td>
<td>Access point model number.</td>
</tr>
<tr>
<td>Cisco IOS Version</td>
<td>The Cisco IOS Release details.</td>
</tr>
<tr>
<td>AP Certificate Type</td>
<td>Either Self Signed or Manufacture Installed.</td>
</tr>
<tr>
<td>FlexConnect Mode</td>
<td>Indicates if FlexConnect mode is supported or not.</td>
</tr>
</tbody>
</table>

### Table 5-49 General (for Lightweight Access Points) Tab Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wIPS Profile (when applicable)</td>
<td>Click the user-assigned profile name to view wIPS profile details.</td>
</tr>
</tbody>
</table>
### Table 5-49  General (for Lightweight Access Points) Tab Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Version</td>
<td></td>
</tr>
<tr>
<td><strong>Unique Device Identifier (UDI)</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name of the Cisco AP for access points.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the access point.</td>
</tr>
<tr>
<td>Product ID</td>
<td>Orderable product identifier.</td>
</tr>
<tr>
<td>Version ID</td>
<td>Version of product identifier.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Unique product serial number.</td>
</tr>
<tr>
<td>Run Ping Test Link</td>
<td>Click to ping the access point. The results are displayed in a pop-up dialog box.</td>
</tr>
<tr>
<td>Alarms Link</td>
<td>Click to display alarms associated with this access point.</td>
</tr>
<tr>
<td>Events Link</td>
<td>Click to display events associated with this access point.</td>
</tr>
</tbody>
</table>

### General—Autonomous

**Note**
For autonomous clients, the Prime Infrastructure *only* collects client counts. The client counts in the Monitor page and reports have autonomous clients included. Client search, client traffic graphs, or other client reports (such as Unique Clients, Busiest Clients, Client Association) do *not* include clients from autonomous access points.

Table 5-50 lists the General (for Autonomous Access Points) tab fields.

### Table 5-50  General (for Autonomous Access Points) Tab Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Name</td>
<td>Operator defined name of access point.</td>
</tr>
<tr>
<td>AP IP address and Ethernet MAC address</td>
<td>IP address, Ethernet MAC address of the access point.</td>
</tr>
<tr>
<td>AP UpTime</td>
<td>Indicates how long the access point has been up in number of days, hours, minutes, and seconds.</td>
</tr>
<tr>
<td>Map Location</td>
<td>Customer-definable location name for the access point. Click to look at the actual location on a map. See the “Monitoring Maps” section on page 6-1 for more information.</td>
</tr>
<tr>
<td>WGB Mode</td>
<td>Indicates whether or not the access point is in work group bridge mode.</td>
</tr>
<tr>
<td>SNMP Info</td>
<td></td>
</tr>
</tbody>
</table>
### Table 5-50  General (for Autonomous Access Points) Tab Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SysObjectId</td>
<td>System Object ID.</td>
</tr>
<tr>
<td>SysDescription</td>
<td>The system device type and current version of firmware.</td>
</tr>
<tr>
<td>SysLocation</td>
<td>The physical location of the device, such as a building name or room in which it is installed.</td>
</tr>
<tr>
<td>SysContact</td>
<td>The name of the system administrator responsible for the device.</td>
</tr>
</tbody>
</table>

### Versions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Version</td>
<td>The operating system release, version, dot, maintenance number of the code currently running on the controller.</td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>Displays the maximum, average, and minimum CPU utilization over the specified amount of time.</td>
</tr>
<tr>
<td>Memory Utilization</td>
<td>Displays the maximum, average, and minimum memory utilization over the specified amount of time.</td>
</tr>
</tbody>
</table>

### Inventory Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Type</td>
<td>Autonomous or lightweight.</td>
</tr>
<tr>
<td>AP Model</td>
<td>The Access Point model number.</td>
</tr>
<tr>
<td>AP Serial Number</td>
<td>Unique serial number for this access point.</td>
</tr>
<tr>
<td>FlexConnect Mode Supported</td>
<td>If FlexConnect mode is supported or not.</td>
</tr>
</tbody>
</table>

### Unique Device Identifier (UDI)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of Cisco AP for access points.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of access point.</td>
</tr>
<tr>
<td>Product ID</td>
<td>Orderable product identifier.</td>
</tr>
<tr>
<td>Version ID</td>
<td>Version of product identifier.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Unique product serial number.</td>
</tr>
</tbody>
</table>

---

**Note**

Memory and CPU utilization charts are displayed.

**Note**

Click **Alarms** to display the alarms associated with the access point. Click **Events** to display events associated with the access point.
Interfaces Tab

Table 5-51 lists the Interfaces tab fields.

**Table 5-51  Interfaces Tab Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td></td>
</tr>
<tr>
<td>Admin Status</td>
<td>Indicates whether the Ethernet interface is enabled.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Indicates whether the Ethernet interface is operational.</td>
</tr>
<tr>
<td>Rx Unicast Packets</td>
<td>Indicates the number of unicast packets received.</td>
</tr>
<tr>
<td>Tx Unicast Packets</td>
<td>Indicates the number of unicast packets sent.</td>
</tr>
<tr>
<td>Rx Non-Unicast Packets</td>
<td>Indicates the number of non-unicast packets received.</td>
</tr>
<tr>
<td>Tx Non-Unicast Packets</td>
<td>Indicates the number of non-unicast packets sent.</td>
</tr>
<tr>
<td>Radio Interface</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>802.11a/n or 802.11b/g/n.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Indicates whether the access point is enabled or disabled.</td>
</tr>
<tr>
<td>CleanAir Capable</td>
<td>Indicates whether the access point is able to use CleanAir.</td>
</tr>
<tr>
<td>CleanAir Status</td>
<td>Indicates the status of CleanAir.</td>
</tr>
<tr>
<td>Channel Number</td>
<td>Indicates the channel on which the Cisco Radio is broadcasting.</td>
</tr>
<tr>
<td>Extension Channel</td>
<td>Indicates the secondary channel on which Cisco radio is broadcasting.</td>
</tr>
<tr>
<td>Power Level</td>
<td>Access Point transmit power level: 1 = Maximum power allowed per</td>
</tr>
<tr>
<td></td>
<td>Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to</td>
</tr>
<tr>
<td></td>
<td>12.5% power, and 5 = 0.195 to 6.25% power.</td>
</tr>
<tr>
<td>Channel Width</td>
<td>Indicates the channel bandwidth for this radio interface. See the</td>
</tr>
<tr>
<td></td>
<td>“Configuring 802.11a/n RRM Dynamic Channel Allocation” section on page 9-131</td>
</tr>
<tr>
<td></td>
<td>for more information on configuring channel bandwidth.</td>
</tr>
<tr>
<td></td>
<td>Minimum (default) setting is 20 MHz. Maximum setting is the</td>
</tr>
<tr>
<td></td>
<td>maximum channel width supported by this radio.</td>
</tr>
<tr>
<td>Antenna Name</td>
<td>Identifies the type of antenna.</td>
</tr>
</tbody>
</table>

Click an interface name to view its properties (see Table 5-52).

**Table 5-52  Interface Properties**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Name</td>
<td>Name of the Access Point.</td>
</tr>
<tr>
<td>Link speed</td>
<td>Indicates the speed of the interface in Mbps.</td>
</tr>
<tr>
<td>RX Bytes</td>
<td>Indicates the total number of bytes in the error-free packets received on</td>
</tr>
<tr>
<td></td>
<td>the interface.</td>
</tr>
<tr>
<td>RX Unicast Packets</td>
<td>Indicates the total number of unicast packets received on the interface.</td>
</tr>
<tr>
<td>RX Non-Unicast Packets</td>
<td>Indicates the total number of non-unicast or multicast packets received</td>
</tr>
<tr>
<td></td>
<td>on the interface.</td>
</tr>
</tbody>
</table>
### Table 5-52 Interface Properties (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input CRC</td>
<td>Indicates the total number of CRC error in packets received on the interface.</td>
</tr>
<tr>
<td>Input Errors</td>
<td>Indicates the sum of all errors in the packets while receiving on the interface.</td>
</tr>
<tr>
<td>Input Overrun</td>
<td>Indicates the number of times the receiver hardware was incapable of handling received data to a hardware buffer because the input rate exceeded the receiver capability to handle the data.</td>
</tr>
<tr>
<td>Input Resource</td>
<td>Indicates the total number of resource errors in packets received on the interface.</td>
</tr>
<tr>
<td>Runts</td>
<td>Indicates the number of packets that are discarded because they are smaller than the medium minimum packet size.</td>
</tr>
<tr>
<td>Throttle</td>
<td>Indicates the total number of times the interface advised a sending NIC that it was overwhelmed by packets being sent and to slow the pace of delivery.</td>
</tr>
<tr>
<td>Output Collision</td>
<td>Indicates the total number of packet retransmitted due to an Ethernet collision.</td>
</tr>
<tr>
<td>Output Resource</td>
<td>Indicates the total number of resource errors in packets transmitted on the interface.</td>
</tr>
<tr>
<td>Output Errors</td>
<td>Indicates the sum of all errors that prevented the final transmission of packets out of the interface.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Indicates the operational state of the physical Ethernet interface on the AP.</td>
</tr>
<tr>
<td>Duplex</td>
<td>Indicates the duplex mode of an interface.</td>
</tr>
<tr>
<td>TX Bytes</td>
<td>Indicates the total number of bytes in the error-free packets transmitted on the interface.</td>
</tr>
<tr>
<td>TX Unicast Packets</td>
<td>Indicates the total number of unicast packets transmitted on the interface.</td>
</tr>
<tr>
<td>TX Non-Unicast Packets</td>
<td>Indicates the total number of non-unicast or multicast packets transmitted on the interface.</td>
</tr>
<tr>
<td>Input Aborts</td>
<td>Indicates the total number of packet aborted while receiving on the interface.</td>
</tr>
<tr>
<td>Input Frames</td>
<td>Indicates the total number of packet received incorrectly having a CRC error and a non-integer number of octets on the interface.</td>
</tr>
<tr>
<td>Input Drops</td>
<td>Indicates the total number of packets dropped while receiving on the interface because the queue was full.</td>
</tr>
<tr>
<td>Unknown Protocol</td>
<td>Indicates the total number of packet discarded on the interface due to an unknown protocol.</td>
</tr>
<tr>
<td>Giants</td>
<td>Indicates the number of packets that are discarded because they exceed the maximum packet size of the medium.</td>
</tr>
<tr>
<td>Interface Resets</td>
<td>Indicates the number of times that an interface has been completely reset.</td>
</tr>
</tbody>
</table>
### CDP Neighbors Tab

Table 5-53 lists the CDP Neighbors tab fields.

**Note**  
This tab is visible only when the CDP is enabled.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Name</td>
<td>The name assigned to the access point.</td>
</tr>
<tr>
<td>AP IP Address</td>
<td>IP address of the access point.</td>
</tr>
<tr>
<td>Port No</td>
<td>Port number connected or assigned to the access point.</td>
</tr>
<tr>
<td>Local Interface</td>
<td>Identifies the local interface.</td>
</tr>
<tr>
<td>Neighbor Name</td>
<td>Name of the neighboring Cisco device.</td>
</tr>
<tr>
<td>Neighbor Address</td>
<td>Network address of the neighboring Cisco device.</td>
</tr>
<tr>
<td>Neighbor Port</td>
<td>Port of the neighboring Cisco device.</td>
</tr>
<tr>
<td>Duplex</td>
<td>Indicates Full Duplex or Half Duplex.</td>
</tr>
<tr>
<td>Interface Speed</td>
<td>Speed at which the interface operates.</td>
</tr>
</tbody>
</table>

### Current Associated Clients Tab

Table 5-54 lists the Current Associated Clients tab fields.

**Note**  
This tab is visible only when there are clients associated to the AP (CAPWAP or Autonomous AP).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Click the username to view the Monitor Client Details page for this client. See the “Monitoring Clients and Users” section on page 10-9 for more information.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the associated client.</td>
</tr>
</tbody>
</table>
**Table 5-54  Current Associated Clients Tab Fields (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client MAC Address</td>
<td>Click the client MAC address to view the Monitor Client Details page for this client. See the “Monitoring Clients and Users” section on page 10-9 for more information.</td>
</tr>
<tr>
<td>Association Time</td>
<td>Date and time of the association.</td>
</tr>
<tr>
<td>UpTime</td>
<td>Time duration of the association.</td>
</tr>
<tr>
<td>SSID</td>
<td>User-defined SSID name.</td>
</tr>
<tr>
<td>SNR (dB)</td>
<td>Signal to Noise Ratio in dB of the associated client.</td>
</tr>
<tr>
<td>RSSI</td>
<td>Received Signal Strength Indicator in dBm.</td>
</tr>
<tr>
<td>Bytes Tx</td>
<td>This indicates the total amount of data that has passed through the Ethernet interface either way.</td>
</tr>
<tr>
<td>Bytes Rx</td>
<td>This indicate the total amount of data that has been received through the Ethernet interface either way.</td>
</tr>
</tbody>
</table>

When the access point is not associated with the controller, then the database is used to retrieve the data (rather than the controller itself). If the access point is not associated, the following fields appear.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Username of the client.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Local IP Address</td>
</tr>
<tr>
<td>Client MAC Address</td>
<td>Client MAC Address</td>
</tr>
<tr>
<td>Association Time</td>
<td>Timestamp of the client association.</td>
</tr>
<tr>
<td>Session Length</td>
<td>Time length of the session</td>
</tr>
<tr>
<td>SSID</td>
<td>User-defined SSID name.</td>
</tr>
<tr>
<td>Protocol</td>
<td></td>
</tr>
<tr>
<td>Avg. Session Throughput</td>
<td>Traffic (MB) as before</td>
</tr>
</tbody>
</table>

**Note**

Click the **Edit View** link to add, remove or reorder columns in the Current Associated Clients table. See the “Configuring the List of Access Points Display” section on page 5-47 for adding a new field using the Edit View.

**SSID Tab**

Table 5-55 lists the SSID tab fields.
**Chapter 5 Monitoring Devices**

**Monitoring Access Points**

This tab is visible only when the access point is Autonomous AP and there are SSIDs configured on the AP.

**Table 5-55 SSID Tab**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>Service Set Identifier being broadcast by the access point radio.</td>
</tr>
<tr>
<td>SSID Vlan</td>
<td>SSID on an access point is configured to recognize a specific VLAN ID or name.</td>
</tr>
<tr>
<td>SSID Vlan Name</td>
<td>SSID on an access point is configured to recognize a specific VLAN ID or name.</td>
</tr>
<tr>
<td>MB SSID Broadcast</td>
<td>SSID broadcast disabled essentially makes your Access Point invisible unless a wireless client already knows the SSID, or is using tools that monitor or 'sniff' traffic from an AP's associated clients.</td>
</tr>
<tr>
<td>MB SSID Time Period</td>
<td>Within this specified time period, internal communication within the SSID continues to work.</td>
</tr>
</tbody>
</table>

**Clients Over Time Tab**

This tab displays the following charts:

- Client Count on AP—Displays the total number of clients currently associated with an access point over time.
- Client Traffic on AP—Displays the traffic generated by the client connected in the AP distribution over time.

The information that appears in the above charts is presented in a time-based graph. For graphs that are time-based, there is a link bar at the top of the graph page that displays 6h, 1d, 1w, 2w, 4w, 3m, 6m, 1y, and Custom. When selected, the data for that time frame is retrieved and the corresponding graph is displayed. See the “Time-Based Graphs” section on page 6-71 for more information.

**Monitoring Access Point Radio Details**

Choose **Monitor > Access Points** and click an item in the Radio column to access this page.

Choose **Monitor > Maps** and click an item in the Name column, then click an access point icon to access this page.

Choose **Monitor > Access Points** and click an item in the AP Name column, click **802.11a** or **802.11b** on the AP Interfaces tab to access this page. This page enables you to view access point information for a single 802.11a or 802.11b/g Cisco Radio.
The default is to show On Demand Statistics. Use the View drop-down list to choose a different view:

- Choose On Demand Statistics, and click Go to display On Demand Statistics. See the “Monitoring On Demand Statistics” section on page 5-70 for more information.
- Choose Operational Parameters, and click Go to display Operational Parameters. See the “Monitoring Operational Parameters” section on page 5-74 for more information.
- Choose 802.11 MAC Counters, and click Go to display 802.11 MAC Counters. See the “Monitoring 802.11 MAC Counters” section on page 5-77 for more information.
- Choose View Alarms and, click Go to display View Alarms. See the “Monitoring View Alarms” section on page 5-78 for more information.
- Choose View Events and, click Go to display View Events. See the “Monitor View Events” section on page 5-79 for more information.

**Monitoring On Demand Statistics**

To view On Demand Statistics for an access point, click the Radio of the applicable access point in the Monitor > Access Points page. The Radio Details page defaults to On Demand Statistics. See the “Monitoring Access Point Radio Details” section on page 5-69 for more information on radio details.

---

**Note**

You can also select On Demand Statistics from the View drop-down list located on the Radio Details page.

This page enables you to view the following access point 802.11a or 802.11b Cisco Radio statistics for a single access point.

**General**

- AP Name—Click to view the access point details. See the “Monitoring Access Points Details” section on page 5-58 for more information.
- AP MAC Address
- Radio
- CleanAir Capable—Indicates if the access point is CleanAir Capable.
- AP in SE-Connect Mode—Yes or No. Indicates if the access point is connected in SE-Connect mode.
- CleanAir Enabled—Indicates if CleanAir is enabled on this access point.
- CleanAir Sensor Status—Indicates the operational status of the CleanAir censor (Up or Down).
- Admin Status—Enabled or disabled.
- Operational Status—Displays the operational status of the Cisco Radios (Up or Down).
- Controller—Click to display controller system details. See the “Monitoring System Summary” section on page 5-4 for more information.
- Channel—The channel upon which the Cisco Radio is broadcasting.
- Extension Channel—Indicates the secondary channel on which Cisco radio is broadcasting.
- Channel Width—Indicates the channel bandwidth for this radio interface. See the “Configuring 802.11a/n RRM Dynamic Channel Allocation” section on page 9-131 for more information on configuring channel bandwidth.
• Power Level—Access Point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power. The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis.
• Port—(1 to 24) Port to which the access point is connected.
• Map Location—Click to display the floor map showing the access point location.

Management Frame Protection

• Protection Capability—All Frames
• Validation Capability—All Frames
• MFP Version Supported—Management Frame Protection version supported and configured.

Profile Information

• Noise Profile—Notification sent when Noise Profile state changes between Success and Failure.
• Interference Profile—Notification sent when Interference Profile state changes between Success and Failure.
• Load Profile—Notification sent when Load Profile state changes between Success and Failure.
• Coverage Profile—Notification sent when Coverage Profile state changes between Success and Failure.

Note Click Success or Failure to view associated alarms.

Noise by Channel (dBm)

Graph showing channel and noise.

Interference by Channel (dBm%)

Graph showing the percentage of interference per channel.

Note Channel Utilization is a combination of Receive Power (RX) + Transmit Power (TX) + Interference. Interference—Access points report on the percentage of the medium taken up by interfering 802.11 transmissions (this can be from overlapping signals from foreign APs, as well as non-neighbors).

Note The channel list (as configured from the RRM page) is scanned completely using the “channel scan duration” field under monitor intervals. For example, if scanning all 11 channels in 2.4 GHz, and using the default duration (180 seconds), you get: 180/11 = 16.36 seconds approximately between each channel that is being scanned.

Load Statistics

• RX Utilization—802.11a or 802.11b/g RF receive utilization threshold between 0 and 100 percent.
• TX Utilization—802.11a or 802.11b/g RF transmit utilization threshold between 0 and 100 percent.
• Channel Utilization—802.11a RF utilization threshold between 0 and 100 percent (Subcolumns for Actual and Threshold).
• Attached Client Count—The number of clients attached.

General Tab

This section describes the information that appears on the General tab and contains the following topics:

• “% Client Count by RSSI” section on page 5-72
• “% Client Count by SNR” section on page 5-72
• “Channel Utilization (% Busy)” section on page 5-72
• “Noise by Channel(dBm)” section on page 5-72
• “Rx Neighbors” section on page 5-72
• “Channel Utilization Statistics” section on page 5-72

% Client Count by RSSI

Graph with % and Received Signal Strength Indicator.

% Client Count by SNR

Graph with % and Signal-to-Noise Ratio.

Channel Utilization (% Busy)

Graph displaying the channel number on the x-axis and channel utilization on the y-axis.

Noise by Channel(dBm)

Graph displaying the channel on the x-axis and power in dBm on the y-axis.

Rx Neighbors

• Radio MAC Address
• AP Name—Click to view access point details.
• Map—Click to view the map.
• Mobility Group-Leader IP Address
• Neighbor Channel
• Channel Bandwidth
• RSSI (dBm)

Channel Utilization Statistics

• Time
• Picc—Percentage of time consumed by received frames from co-channel APs and clients.
• Pib—Percentage of time consumed by interference on the channel which cannot be correctly demodulated.
Client Count Over last 24 Hrs

This graph shows the client count specific to the AP radios (in the last 24 hours).

CleanAir Tab

This section describes the information that appears on the CleanAir tab and contains the following topics:

- “Air Quality” section on page 5-73
- “Interference Power” section on page 5-73
- “Non-WiFi Channel Utilization” section on page 5-73
- “Active Interferers” section on page 5-73
- “View Drop-Down List” section on page 5-73

Air Quality

This graph displays the air quality index of the wireless network. A value of 100 indicates the air quality is best and a value of 1 indicates maximum interference.

Interference Power

This graph displays the interference power of the interfering devices on the channel number.

Non-WiFi Channel Utilization

This graph displays the non-WiFi channel utilization of the wireless network.

Active Interferers

This section displays the details of the active interferers on the wireless network. The following details are available:

- Interferer Name—The name of the interfering device.
- Affected Channels—The channel the interfering device is affecting.
- Detected Time—The time at which the interference was detected.
- Severity—The severity index of the interfering device.
- Duty Cycle(%)—The duty cycle (in percentage) of the interfering device.
- RSSI(dBm)—The Received Signal Strength Indicator of the interfering device.

View Drop-Down List

- Choose On Demand Statistics, and click Go to display On Demand Statistics for this access point radio. See the “Monitoring On Demand Statistics” section on page 5-70 for more information.
- Choose **Operational Parameters**, and click **Go** to display Operational parameters for this access point radio. See the “Monitoring Operational Parameters” section on page 5-74 for more information.

- Choose **802.11 MAC Counters**, and click **Go** to display 802.11 MAC Counters for this access point radio. See the “Monitoring 802.11 MAC Counters” section on page 5-77 for more information.

- Choose **View Alarms**, and click **Go** to display alarms for this access point radio. See the “Monitoring View Alarms” section on page 5-78 for more information.

- Choose **View Events**, and click **Go** to display events for this access point radio. See the “Monitor View Events” section on page 5-79 for more information.

### Monitoring Operational Parameters

To view Operational Parameters for an access point radio, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>Monitor &gt; Access Points</strong>, click the radio for the applicable access point.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>From the <strong>View</strong> drop-down list, choose Operational Parameters.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Go</strong>.</td>
</tr>
</tbody>
</table>

This page enables you to view configuration information for a single 802.11a or 802.11b Cisco radio.

### General

- **AP Name**—Click to view the access point details. See the “Monitoring Access Points Details” section on page 5-58 for more information.
- **AP MAC Address**
- **Radio**
- **Admin Status**—Enabled or disabled.
- **Operational Status**—Displays the operational status of the Cisco Radios (Up or Down).
- **Controller**—Click to display controller system details. See the “Monitoring System Summary” section on page 5-4 for more information.
- **Channel**—The channel upon which the Cisco Radio is broadcasting.
- **Extension Channel**—Indicates the secondary channel on which Cisco radio is broadcasting.
- **Channel Width**—Indicates the channel bandwidth for this radio interface. See the “Configuring 802.11a/n RRM Dynamic Channel Allocation” section on page 9-131 for more information on configuring channel bandwidth.
- **Power Level**—Access Point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power. The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis.
- **Port**—(1 to 24) Port to which the access point is connected.
- **Map Location**—Click to display the floor map showing the access point location.
Station Configuration Parameters

- Configuration Type—Automatic or Custom.
- Number of WLANs—1 (one) is the default.
- Medium Occupancy Limit—Indicates the maximum amount of time, in TU, that a point coordinator might control the usage of the wireless medium without relinquishing control for long enough to allow at least one instance of DCF access to the medium. The default value is 100, and the maximum value is 1000.
- CFP Period—The number of DTIM intervals between the start of CFPs.
- CFP Max. Duration—The maximum duration of the CFP in TU that might be generated by the PCF.
- BSSID—MAC address of the access point.
- Beacon Period—The rate at which the SSID is broadcast by the access point, from 100 to 600 milliseconds.
- DTIM Period—The number of beacon intervals that shall elapse between transmission of Beacon frames containing a TIM element whose DTIM Count field is 0. This value is transmitted in the DTIM Period field of Beacon frames.
- Country String—Identifies the country in which the station is operating. The first two octets of this string are the two character country code.

Physical Channel Parameters

- Current Channel—Current operating frequency channel.
- Configuration—Locally customized or globally controlled.
- Current CCA Mode—CCA method in operation. Valid values:
  - Energy detect only (edonly) = 01.
  - Carrier sense only (csonly) = 02.
  - Carrier sense and energy detect (edandcs)= 04.
  - Carrier sense with timer (cswithtimer)= 08.
  - High rate carrier sense and energy detect (hrcsanded)=16.
- ED/TI Threshold—The Energy Detect and Threshold being used to detect a busy medium (frequency). CCA reports a busy medium upon detecting the RSSI above this threshold.

Physical Antenna Parameters

- Antenna Type—Internal or External.
- Diversity—Enabled via the internal antennas or via either Connector A or Connector B. (Enabled or Disabled).

RF Recommendation Parameters

- Channel—802.11a Low Band, Medium Band, and High Band; 802.11b/g.
- Tx Power Level—Zero (0) if Radio Resource Management (RRM) disabled, 1 - 5 if Radio Resource Management (RRM) is enabled.
- RTS/CTS Threshold—Zero (0) if Radio Resource Management (RRM) disabled, 1 - 5 if Radio Resource Management (RRM) is enabled.
• Fragmentation Threshold—Zero (0) if Radio Resource Management (RRM) is disabled.

MAC Operation Parameters

• Configuration Type—Automatic or Custom.
• RTS Threshold—This attribute indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed.

An RTS/CTS handshake is performed at the beginning of any frame exchange sequence where the MPDU is a Data or Management type, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute to be larger than the maximum MSDU size turns off the RTS/CTS handshake for Data or Management type frames transmitted by this STA. Setting this attribute to zero turns on the RTS/CTS handshake for all frames of Data or Management type transmitted by this STA. The default value of this attribute shall be 2347.

• Short Retry Limit—The maximum number of transmission attempts of a frame, the length of which is less than or equal to dot11RTSThreshold, that shall be made before a failure condition is indicated. The default value of this attribute is 7.

• Long Retry Limit—The maximum number of transmission attempts of a frame, the length of which is greater than dot11RTSThreshold, that shall be made before a failure condition is indicated. The default value of this attribute shall be 4.

• Fragmentation Threshold—The current maximum size, in octets, of the MPDU that might be delivered to the PHY. An MSDU shall be broken into fragments if its size exceeds the value of this attribute after adding MAC headers and trailers. An MSDU or MMPDU shall be fragmented when the resulting frame has an individual address in the Address1 field, and the length of the frame is larger than this threshold. The default value for this attribute shall be the lesser of 2346 or the aMPDUMaxLength of the attached PHY and shall never exceed the lesser of 2346 or the aMPDUMaxLength of the attached PHY. The value of this attribute shall never be less than 256.

• Max Tx MSDU Lifetime—The elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU shall be terminated. The default value of this attribute is 512.

• Max Rx Lifetime—The MaxReceiveLifetime shall be the elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU, after which further attempts to reassemble the MMPDU or MSDU shall be terminated. The default value is 512.

Tx Power

• # Supported Power Levels—Five or fewer power levels, depending on operator preference.

• Tx Power Level x—Access point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.

Note

The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis.

• Tx Power Configuration—Globally controlled or customized for this access point (Custom or Global).

• Current Tx Power Level—Displays the operating transmit power level from the transmit power table.
Monitoring 802.11 MAC Counters

To view Operational Parameters for an access point radio, follow these steps:

**Step 1** Choose Monitor > Access Points, click the radio for the applicable access point.

**Step 2** From the View drop-down list, choose 802.11 MAC Counters.

**Step 3** Click Go.

This page enables you to view 802.11 MAC Counter information for a single 802.11a or 802.11b Cisco Radio.

**General**

- AP Name—Click to view the access point details. See the “Monitoring Access Points Details” section on page 5-58 for more information.
- AP MAC Address
- Radio
- Admin Status—Enabled or disabled.
- Operational Status—Displays the operational status of the Cisco Radios (Up or Down).
- Controller—Click to display controller system details. See the “Monitoring System Summary” section on page 5-4 for more information.
- Channel—The channel upon which the Cisco Radio is broadcasting.
- Extension Channel—Indicates the secondary channel on which Cisco radio is broadcasting.
- Channel Width—Indicates the channel band width for this radio interface. See the “Configuring 802.11a/n RRM Dynamic Channel Allocation” section on page 9-131 for more information on configuring channel bandwidth.

**Note** Minimum (default) setting is 20 MHz. Maximum setting is the maximum channel width supported by this radio.

- Power Level—Access Point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power. The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis.
- Port—(1 to 24) Port to which the access point is connected.
- Map Location—Click to display the floor map showing the access point location.

**RF Counters**

- Tx Fragment Count—This counter is incremented for each successfully received MPDU Data or Management type.
Monitoring Access Points

Chapter 5  Monitoring Devices

- Multicast Tx Frame Count—This counter increments only when the multicast bit is set in the destination MAC address of a successfully transmitted MSDU. When operating as a STA in an ESS, where these frames are directed to the access point, this implies having received an acknowledgment to all associated MPDUs.
- Tx Failed Count—This counter increments when an MSDU is not successfully transmitted due to the number of transmit attempts exceeding retry limit.
- Retry Count—This counter increments when an MSDU is successfully transmitted after one or more retransmissions.
- Multiple Retry Count—This counter increments when an MSDU is successfully transmitted after two or more retransmissions.
- Frame Duplicate Count—This counter increments when a frame is received that the Sequence Control field indicates is a duplicate.
- RTS Success Count—This counter increments when a CTS is received in response to an RTS.
- RTS Failure Count—This counter increments when a CTS is not received in response to an RTS.
- ACK Failure Count—This counter increments when an ACK is not received when expected.
- Rx Fragment Count—The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
- Multicast Rx Framed Count—This counter increments when a MSDU is received with the multicast bit set in the destination MAC address.
- FCS Error Count—This counter increments when an FCS error is detected in a received MPDU.
- Tx Frame Count—This counter increments for each successfully transmitted MSDU.
- WEP Undecryptable Count—This counter increments when a frame is received with the WEP subfield of the Frame Control field set to one and the WEP On value for the key mapped to the AT MAC address indicates that the frame should not have been encrypted or that frame is discarded due to the receiving STA not implementing the privacy option.

Monitoring View Alarms

To access the View Alarms page from the Monitor Access Points page, follow these steps:

Step 1  Choose Monitor > Access Points.
Step 2  Select the Radio Type in the Radio Type column of the applicable access point.
Step 3  From the View drop-down list, choose View Alarms.
Step 4  Click Go.
For more information on Viewing Alarms, see the “Monitoring Alarms” section on page 5-126.

Monitor View Events

To access the View Events page from the Monitor Access Points page, follow these steps:

Step 1 Choose Monitor > Access Points.
Step 2 Select the Radio Type in the Radio Type column of the applicable access point.
Step 3 From the View drop-down list, select View Events.
Step 4 Click Go.

For more information on viewing events, see the “Monitoring Events” section on page 5-141.

Monitoring Third-Party Access Points

Prime Infrastructure supports the monitoring of certain third-party access points.

For third-party access points, the following parameters are monitored:

- Current configuration of SSID
- Mode
- Current Channel
- Tx-Power
- RTS Threshold
- Retry Limit
- Preamble
- Beacon Interval
- Power management
- Load balance
- Rates
- DTIM Period
- LMS address
- Encryption
- Status
- Ageout
- MTU
- Location
- Hide SSID
- Deny Broadcast
- BG mode
- Radio Chipset
- Regulatory Domain
- Country Code
- Tx Rates

To view third-party access point details, follow these steps:

Step 1 Choose Monitor > Third Party Access Points.
Step 2 In the Third-Party Access Point page, click the access point’s name. The information appears on the General tab.
Monitoring Mesh Access Points

Mesh Health monitors the overall health of Cisco Aironet 1500 and 1520 series outdoor access points as well as Cisco Aironet 1130 and 1240 series indoor access points when configured as mesh access points, except as noted. Tracking this environmental information is particularly critical for access points that are deployed outdoors. The following factors are monitored:

- **Temperature**: Displays the internal temperature of the access point in Fahrenheit and Celsius (Cisco Aironet 1510 and 1520 outdoor access points only).
- **Heater status**: Displays the heater as on or off (Cisco Aironet 1510 and 1520 outdoor access points only)
- **AP Up time**: Displays how long the access point has been active to receive and transmit.
- **LWAPP Join Taken Time**: Displays how long it took to establish the LWAPP connection (excluding Cisco Aironet 1505 access points).
- **LWAPP Up Time**: Displays how long the LWAPP connection has been active (excluding Cisco Aironet 1505 access points).

Mesh Health information is displayed in the General Properties page for mesh access points.

**Note**
The wIPS mode is not supported in the Cisco Aironet 1500 series mesh access points.

To view the mesh health details for a specific mesh access point, follow these steps:

**Step 1**
Choose **Monitor > Access Points**. A listing of radios belonging to access points appears.

**Note**
The radio status (not an access point status) is displayed when you choose Monitor > Access Points. The given status is updated frequently from traps and wireless status polling and takes several minutes to reflect actual radio status. The overall status of an access point can be found by viewing the access point on a map.

**Note**
You can also use the New Search button to display the mesh access point summary. With the New Search option, you can further define the criteria of the access points that appear. Search criteria include AP Type, AP Mode, Radio Type, and 802.11n Support.

**Step 2**
Click the AP Name link to display details for that mesh access point. The General tab for that mesh access point appears.

**Note**
You can also access the General tab for a mesh access point from an Prime Infrastructure map page. To display the page, double-click the mesh access point label. A tabbed page appears and displays the General tab for the selected access point.

To add, remove, or reorder columns in the table, click the **Edit View** link in the Monitor > Access Points page.
Mesh Statistics Tab

Mesh Statistics are reported when a child mesh access point authenticates or associates with a parent mesh access point.

Security entries are removed and no longer displayed when the child mesh access point disassociates from the controller.

The following mesh security statistics are displayed for mesh access points:

- Bridging
- Queue
- Security

To view the mesh statistics for a specific mesh access point, follow these steps:

**Step 1** Choose Monitor > Access Points. A listing of radios belonging to access points appears.

**Step 2** Click the AP Name link of the target mesh access point.

A tabbed page appears and displays the General Properties page for the selected access point.

**Step 3** Click the Mesh Statistics tab. A three-tabbed Mesh Statistics page appears.

**Note** The Mesh Statistics tab and its subordinate tabs (Bridging, Queue and Security) only appear for mesh access points. The Mesh Link Alarms and Mesh Link Events links are accessible from each of the three tabbed panels. You can click these links to view the relevant alarms and events.

**Note** You can also access the Mesh Securities page for a mesh access point from a Prime Infrastructure map. To display the page, double-click the mesh access point label.

Summaries of the Bridging, Queue and Security Statistics and their definitions are provided in Table 5-56, Table 5-57 and Table 5-58 respectively.
### Table 5-56  Bridging Mesh Statistics

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>The role of the mesh access point. Options are mesh access point (MAP) and root access point (RAP).</td>
</tr>
<tr>
<td>Bridge Group Name</td>
<td>The name of the bridge group to which the MAP or RAP is a member. We recommend assigning membership in a bridge group name. If one is not assigned, a MAP is by default assigned to a default bridge group name.</td>
</tr>
<tr>
<td>Backhaul Interface</td>
<td>The radio backhaul for the mesh access point.</td>
</tr>
<tr>
<td>Routing State</td>
<td>The state of parent selection. Values that display are seek, scan and maint. Maint appears when parent selection is complete.</td>
</tr>
<tr>
<td>Malformed Neighbor Packets</td>
<td>The number of malformed packets received from the neighbor. Examples of malformed packets include malicious floods of traffic such as malformed or short DNS packets and malformed DNS replies.</td>
</tr>
<tr>
<td>Poor Neighbor SNR</td>
<td>The number of times the signal-to-noise ratio falls below 12 dB on the backhaul link.</td>
</tr>
<tr>
<td>Excluded Packets</td>
<td>The number of packets received from excluded neighbor mesh access points.</td>
</tr>
<tr>
<td>Insufficient Memory</td>
<td>The number of insufficient memory conditions.</td>
</tr>
<tr>
<td>RX Neighbor Requests</td>
<td>The number of broadcast and unicast requests received from the neighbor mesh access points.</td>
</tr>
<tr>
<td>RX Neighbor Responses</td>
<td>The number of responses received from the neighbor mesh access points.</td>
</tr>
<tr>
<td>TX Neighbor Requests</td>
<td>The number of unicast and broadcast requests sent to the neighbor mesh access points.</td>
</tr>
<tr>
<td>TX Neighbor Responses</td>
<td>The number of responses sent to the neighbor mesh access points.</td>
</tr>
<tr>
<td>Parent Changes</td>
<td>The number of times a mesh access point (child) moves to another parent.</td>
</tr>
<tr>
<td>Neighbor Timeouts</td>
<td>The number of neighbor timeouts.</td>
</tr>
<tr>
<td>Node Hops</td>
<td>The number of hops between the MAP and the RAP. Click the value link to display a dialog box which enables you to configure details of what is reported, how often the node hop value is updated, and view a graphical representation of the report.</td>
</tr>
</tbody>
</table>
### Chapter 5      Monitoring Devices

#### Monitoring Access Points

**Table 5-57    Queue Mesh Statistics**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silver Queue</td>
<td>The average and peak number of packets waiting in the silver (best effort) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.</td>
</tr>
<tr>
<td>Gold Queue</td>
<td>The average and peak number of packets waiting in the gold (video) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.</td>
</tr>
<tr>
<td>Platinum Queue</td>
<td>The average and peak number of packets waiting in the platinum (voice) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.</td>
</tr>
<tr>
<td>Bronze Queue</td>
<td>The average and peak number of packets waiting in the bronze (background) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.</td>
</tr>
<tr>
<td>Management Queue</td>
<td>The average and peak number of packets waiting in the management queue during the defined statistics time interval. Packets dropped and queue size is also summarized.</td>
</tr>
</tbody>
</table>

**Table 5-58    Security Mesh Statistics**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets Transmitted</td>
<td>Summarizes the total number of packets transmitted during security negotiations by the selected mesh access point.</td>
</tr>
<tr>
<td>Packets Received</td>
<td>Summarizes the total number of packets received during security negotiations by the selected mesh access point.</td>
</tr>
<tr>
<td>Association Request Failures</td>
<td>Summarizes the total number of association request failures that occur between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td>Association Request Timeouts</td>
<td>Summarizes the total number of association request time outs that occur between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td>Association Request Success</td>
<td>Summaries the total number of successful association requests that occur between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td>Authentication Request Failures</td>
<td>Summarizes the total number of failed authentication requests that occur between the selected mesh access point and its parent.</td>
</tr>
</tbody>
</table>
### Table 5-58  Security Mesh Statistics (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Request Timeouts</td>
<td>Summarizes the total number of authentication request timeouts that occur between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td>Authentication Request Success</td>
<td>Summarizes the total number of successful authentication requests between the selected mesh access point and its parent mesh node.</td>
</tr>
<tr>
<td>Reassociation Request Failures</td>
<td>Summarizes the total number of failed reassociation requests between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td>Reassociation Request Timeouts</td>
<td>Summarizes the total number of reassociation request timeouts between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td>Reassociation Request Success</td>
<td>Summarizes the total number of successful reassociation requests between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td>Reauthentication Request Failures</td>
<td>Summarizes the total number of failed reauthentication requests between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td>Reauthentication Request Timeouts</td>
<td>Summarizes the total number of reauthentication request timeouts that occurred between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td>Reauthentication Request Success</td>
<td>Summarizes the total number of successful reauthentication requests that occurred between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td>Invalid Association Request</td>
<td>Summarizes the total number of invalid association requests received by the parent mesh access point from the selected child mesh access point. This state might occur when the selected child is a valid neighbor but is not in a state that allows association.</td>
</tr>
<tr>
<td>Unknown Association Requests</td>
<td>Summarizes the total number of unknown association requests received by the parent mesh access point from its child. The unknown association requests often occur when a child is an unknown neighbor mesh access point.</td>
</tr>
<tr>
<td>Invalid Reassociation Request</td>
<td>Summarizes the total number of invalid reassociation requests received by the parent mesh access point from a child. This might happen when a child is a valid neighbor but is not in a proper state for reassociation.</td>
</tr>
</tbody>
</table>
Table 5-58  Security Mesh Statistics (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown Reassociation Request</td>
<td>Summarizes the total number of unknown reassociation requests received by the parent mesh access point from a child. This might happen when a child mesh access point is an unknown neighbor.</td>
</tr>
<tr>
<td>Invalid Reauthentication Request</td>
<td>Summarizes the total number of invalid reauthentication requests that occurred between the selected mesh access point and its parent. This state might occur when the selected mesh access point is a valid neighbor but is not in a state that allows reauthentication.</td>
</tr>
</tbody>
</table>

Mesh Links Tab

Table 5-59 lists the Mesh Links tab fields.

Note This tab is visible only for mesh access points. You can click the Mesh Link Alarms and Mesh Link Events links to view the relevant alarms and events.

Table 5-59  Mesh Links Tab Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of the access point.</td>
</tr>
<tr>
<td>AP Name</td>
<td>The name assigned to the access point.</td>
</tr>
<tr>
<td>AP MAC Address</td>
<td>The MAC address of the access point.</td>
</tr>
<tr>
<td>PER</td>
<td>The Packet Error Rate measured from the total packets that are transmitted in the link test.</td>
</tr>
<tr>
<td>Link Detail</td>
<td>Click to view the details of the mesh link alarms, mesh link events, and link metrics.</td>
</tr>
<tr>
<td>Link Test</td>
<td>The test used to measure the air link quality between the AP and the neighbor AP.</td>
</tr>
<tr>
<td>Channel</td>
<td>The channel number of the mesh access point.</td>
</tr>
<tr>
<td>Link SNR (dB)</td>
<td>The air link SNR measured between the AP and the neighbor AP.</td>
</tr>
<tr>
<td>SNR Down</td>
<td>The Signal Noise Ratio measured on the air link from the AP to the neighbor AP.</td>
</tr>
<tr>
<td>SNR Up</td>
<td>The Signal Noise Ratio measured on the air link from the neighbor AP to the AP.</td>
</tr>
</tbody>
</table>

Note Click the Edit View link to add, remove or reorder columns in the Mesh Links table. See the “Configuring the List of Access Points Display” section on page 5-47 for adding a new field using the Edit View.
### Retrieving the Unique Device Identifier on Controllers and Access Points

The unique device identifier (UDI) standard uniquely identifies products across all Cisco hardware product families, enabling customers to identify and track Cisco products throughout their business and network operations and to automate their asset management systems. The standard is consistent across all electronic, physical, and standard business communications. The UDI consists of five data elements:

- The orderable product identifier (PID)
- The version of the product identifier (VID)
- The serial number (SN)
- The entity name
- The product description

The UDI is burned into the EEPROM of controllers and lightweight access points at the factory and can be retrieved through the GUI.

To retrieve the UDI on controllers and access points, perform the following steps:

**Step 1** Choose **Monitor > Controllers/Access Points**. The Controllers/Access Points page appears.

**Step 2** Click the IP address of the controller/access point whose UDI information you want to retrieve. Data elements of the controller/access point UDI display. These elements are described in Table 5-60.

### Table 5-60 Maximum Number of Crypto Cards That can be Installed on a Cisco Wireless LAN Controller

<table>
<thead>
<tr>
<th>Type of Controller</th>
<th>Maximum Number of Crypto Cards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 2000 Series</td>
<td>None</td>
</tr>
<tr>
<td>Cisco 4100 Series</td>
<td>One</td>
</tr>
<tr>
<td>Cisco 4400 Series</td>
<td>Two</td>
</tr>
</tbody>
</table>

### Monitoring Coverage Holes

Coverage holes are areas where clients cannot receive a signal from the wireless network. The Cisco Unified Network Solution, radio resource management (RRM) identifies these coverage hole areas and reports them to the Prime Infrastructure, enabling the IT manager to fill holes based on user demand.

Prime Infrastructure is informed about the reliability-detected coverage holes by the controllers. Prime Infrastructure alerts the user about these coverage holes. For more information on finding coverage holes, refer to Cisco Context-Aware Services documentation at this location: [http://www.cisco.com/en/US/docs/wireless/mse/3350/5.2/CAS/configuration/guide/msecg_ch7_CAS.html](http://www.cisco.com/en/US/docs/wireless/mse/3350/5.2/CAS/configuration/guide/msecg_ch7_CAS.html)

**Note** Coverage holes are displayed as alarms. Pre-coverage holes are displayed as events.
Monitoring Pre-Coverage Holes

To view pre-coverage hole events, perform these steps:

**Step 1** Choose **Monitor > Events** to display all current events.

**Step 2** To view pre-coverage hole events only, click the **Advanced Search** link.

**Step 3** In the New Search page, change the Search Category drop-down to **Events**.

**Step 4** From the Event Category drop-down list, choose **Pre Coverage Hole**, and click **Go**.

The Pre-Coverage Hole Events page provides the information described in **Table 5-61**.

*Table 5-61  Pre-Coverage Hole Fields*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Pre-coverage hole events are always considered informational (Info).</td>
</tr>
<tr>
<td>Client MAC Address</td>
<td>MAC address of the client affected by the pre-coverage hole.</td>
</tr>
<tr>
<td>AP MAC Address</td>
<td>MAC address of the applicable access point.</td>
</tr>
<tr>
<td>AP Name</td>
<td>The name of the applicable access point.</td>
</tr>
<tr>
<td>Radio Type</td>
<td>The radio type (802.11b/g or 802.11a) of the applicable access point.</td>
</tr>
<tr>
<td>Power Level</td>
<td>Access point transmit power level: 1 = Maximum power allowed per country code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.</td>
</tr>
</tbody>
</table>
Table 5-61  Pre-Coverage Hole Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Type</td>
<td>Client type can be any of the following:</td>
</tr>
<tr>
<td></td>
<td>laptop(0)</td>
</tr>
<tr>
<td></td>
<td>pc(1)</td>
</tr>
<tr>
<td></td>
<td>pda(2)</td>
</tr>
<tr>
<td></td>
<td>dot11mobilephone(3)</td>
</tr>
<tr>
<td></td>
<td>dualmodephone(4)</td>
</tr>
<tr>
<td></td>
<td>wgb(5)</td>
</tr>
<tr>
<td></td>
<td>scanner(6)</td>
</tr>
<tr>
<td></td>
<td>tabletpc(7)</td>
</tr>
<tr>
<td></td>
<td>printer(8)</td>
</tr>
<tr>
<td></td>
<td>projector(9)</td>
</tr>
<tr>
<td></td>
<td>videoconfsystem(10)</td>
</tr>
<tr>
<td></td>
<td>camera(11)</td>
</tr>
<tr>
<td></td>
<td>gamingsystem(12)</td>
</tr>
<tr>
<td></td>
<td>dot11deskphone(13)</td>
</tr>
<tr>
<td></td>
<td>cashregister(14)</td>
</tr>
<tr>
<td></td>
<td>radiotag(15)</td>
</tr>
<tr>
<td></td>
<td>rfidsensor(16)</td>
</tr>
<tr>
<td></td>
<td>server(17)</td>
</tr>
<tr>
<td>WLAN Coverage Hole Status</td>
<td>Determines if the current coverage hole state is enabled or disabled.</td>
</tr>
<tr>
<td>WLAN</td>
<td>The name for this WLAN.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>The date and time the event occurred. Click the title to toggle between ascending and descending order.</td>
</tr>
</tbody>
</table>

**Step 5**  Choose a Client MAC Address to view pre-coverage hole details.

- General—Provides the following information:
  - Client MAC Address
  - AP MAC Address
  - AP Name
  - Radio Type
  - Power Level
  - Client Type
  - Category
  - Created
  - Generated By
  - Device AP Address
Monitoring Access Points

- Severity
  - Neighbor AP’s—Indicates the MAC addresses of nearby access points, their RSSI values, and their radio types.
  - Message—Describes what device reported the pre-coverage hole and on which controller it was detected.
  - Help—Provides additional information, if available, for handling the event.

Monitoring Rogue Access Points

This section describes security solutions for rogue devices. A rogue device is an unknown access point or client that is detected by managed access points in your network.

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 others to wait, which results in legitimate clients being unable to access network resources. Therefore, 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 IT department knowledge or consent. These rogue access points can be a serious breach of network security as 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. Even more alarming, wireless users frequently publish insecure access point locations, increasing the odds of having enterprise security breached.

Detecting Rogue Devices

The controllers continuously monitor all nearby access points and automatically discover and collect information on rogue access points and clients. When a controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) to determine if the rogue is attached to your network.

Prime Infrastructure consolidates all of the controllers rogue access point data.

You can configure controllers to use RLDP on all access points or only on access points configured for monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded RF space, allowing monitoring without creating unnecessary interference and without affecting regular data access point functionality. If you configure a controller to use RLDP on all access points, the 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 either manually or automatically contain the detected rogue. See the “Configuring Rogue Policies” section on page 9-111 for information on enabling RLDP.
Rogue access point partitions are associated with one of the detecting access points (the one with the latest or strongest RSSI value). If there is detecting access point information, the Prime Infrastructure uses the detecting controller. If the rogue access point is detected by two controllers which are in different partitions, the rogue access point partition might be changed at any time.

- Viewing Rogue AP Alarm Details, page 5-97
- Monitoring Rogue AP Alarms, page 5-93
- Viewing Rogue AP Alarm Details, page 5-97
- Viewing Rogue Client Details, page 5-100
- Viewing Rogue AP History Details, page 5-102
- Viewing Rogue AP Event History Details, page 5-102
- Monitoring Ad hoc Rogue Alarms, page 5-103

Classifying Rogue Access Points

Classification and reporting of rogue access points occurs through the use of rogue states and user-defined classification rules that enable rogues to automatically move between states. You can create rules that enable the controller to organize and display rogue access points as Friendly, Malicious, or Unclassified.

Prime Infrastructure consolidates all of the controllers rogue access point data.

By default, none of the classification rules are enabled. Therefore, all unknown access points are categorized as Unclassified. When you create a rule, configure conditions for it, and enable the rule, the unclassified access points are reclassified. Whenever you change a rule, it is applied to all access points (friendly, malicious, and unclassified) in the Alert state only.

Rule-based rogue classification does not apply to ad-hoc rogues and rogue clients.

The 5500 series controllers support up to 2000 rogues (including acknowledged rogues); the 4400 series controllers, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch support up to 625 rogues; and the 2100 series controllers and Controller Network Module for Integrated Services Routers support up to 125 rogues. Each controller limits the number of rogue containments to three per radio (or six per radio for access points in monitor mode).

When the controller receives a rogue report from one of its managed access points, it responds as follows:

1. The controller verifies that the unknown access point is in the friendly MAC address list. If it is, the controller classifies the access point as Friendly.
2. If the unknown access point is not in the friendly MAC address list, the controller starts applying rogue classification rules.
3. If the rogue is already classified as Malicious, Alert or Friendly, Internal or External, the controller
does not reclassify it automatically. If the rogue is classified differently, the controller reclassifies it
automatically only if the rogue is in the Alert state.

4. The controller applies the first rule based on priority. If the rogue access point matches the criteria
specified by the rule, the controller classifies the rogue according to the classification type
configured for the rule.

5. If the rogue access point does not match any of the configured rules, the controller classifies the
rogue as Unclassified.

6. The controller repeats the previous steps for all rogue access points.

7. If RLDP determines that the rogue access point is on the network, the controller marks the rogue
state as Threat and classifies it as Malicious automatically, even if no rules are configured. You can
then manually contain the rogue (unless you have configured RLDP to automatically contain the
rogue), which would change the rogue state to Contained. If the rogue access point is not on the
network, the controller marks the rogue state as Alert, and you can manually contain the rogue.

8. If desired, you can manually move the access point to a different classification type and rogue state.

As mentioned previously, the controller can automatically change the classification type and rogue state
of an unknown access point based on user-defined rules, or you can manually move the unknown access
point to a different classification type and rogue state. Table 5-62 shows the allowable classification
types and rogue states from and to which an unknown access point can be configured.

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friendly (Internal, External, Alert)</td>
<td>Malicious (Alert)</td>
</tr>
<tr>
<td>Friendly (Internal, External, Alert)</td>
<td>Unclassified (Alert)</td>
</tr>
<tr>
<td>Friendly (Alert)</td>
<td>Friendly (Internal, External)</td>
</tr>
<tr>
<td>Malicious (Alert, Threat)</td>
<td>Friendly (Internal, External)</td>
</tr>
<tr>
<td>Malicious (Contained, Contained Pending)</td>
<td>Malicious (Alert)</td>
</tr>
<tr>
<td>Unclassified (Alert, Threat)</td>
<td>Friendly (Internal, External)</td>
</tr>
<tr>
<td>Unclassified (Contained, Contained Pending)</td>
<td>Unclassified (Alert)</td>
</tr>
<tr>
<td>Unclassified (Alert)</td>
<td>Malicious (Alert)</td>
</tr>
</tbody>
</table>

If the rogue state is Contained, you have to uncontain the rogue access point before you can change the
classification type. If you want to move a rogue access point from Malicious to Unclassified, you must
delete the access point and allow the controller to reclassify it.

Rogue access points classification types include:

- **Malicious**—Detected but untrusted or unknown access points with a malicious intent within the
  system. They also refer to access points that fit the user-defined malicious rules or have been
  manually moved from the friendly access point classification. See the “Malicious Rogue APs”
  section on page 5-92 for more information.

- **Friendly**—Known, acknowledged, or trusted access points. They also refer to access points that fit
  the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained.
  See the “Friendly Rogue APs” section on page 5-92 for more information. For more information on
  configuring friendly access point rules, see the “Configuring a Friendly Access Point Template”
  section on page 11-76.
• Unclassified—Rogue access point that are not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list. See for more information. See the “Unclassified Rogue APs” section on page 5-93 for more information.

Malicious Rogue APs

Malicious rogue access points are detected but untrusted or unknown access points with a malicious intent within the system. They also refer to access points that fit the user-defined malicious rules or have been manually moved from the friendly access point classification.

The Security dashboard of the Prime Infrastructure home page displays the number of malicious rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active malicious rogue access points.

Malicious rogue access point states include:
• Alert—Indicates that the access point is not on the neighbor list or part of the user-configured Friendly AP list.
• Contained—The unknown access point is contained.
• Threat—The unknown access point is found to be on the network and poses a threat to WLAN security.
• Contained Pending—Indicates that the containment action is delayed due to unavailable resources.
• Removed—This unknown access point was seen earlier but is not seen now.

Click an underlined number in any of the time period categories for detailed information regarding the malicious rogue access points. See the “Monitoring Rogue Access Points” section on page 5-89 for more information.

Friendly Rogue APs

Friendly rogue access points are known, acknowledged or trusted access points. They also refer to access points that fit the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained.

Note

Only the Prime Infrastructure users can add a rogue access point MAC address to the Friendly AP list. the Prime Infrastructure does not apply the Friendly AP MAC address to controllers.

The Security dashboard of the Prime Infrastructure home page displays the number of friendly rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active friendly rogue access points.

Friendly rogue access point states include the following:
• Internal—If the unknown access point is inside the network and poses no threat to WLAN security, you would manually configure it as Friendly, Internal. For example, the access points in your lab network.
• External—If the unknown access point is outside the network and poses no threat to WLAN security, you would manually configure it as Friendly, External. For example, the access points belonging to a neighboring coffee shop.
• Alert—The unknown access point is not on the neighbor list or part of the user-configured Friendly AP list.
Chapter 5  Monitoring Devices

Click an underlined number in any of the time period categories for detailed information regarding the friendly rogue access points. See the “Monitoring Rogue Access Points” section on page 5-89 for more information.

To delete a rogue access point from the Friendly AP list, ensure that both the Prime Infrastructure and controller remove the rogue access point from the Friendly AP list. Change the rogue access point from Friendly AP Internal or External to Unclassified or Malicious Alert.

Unclassified Rogue APs

An unclassified rogue access point refers to a rogue access point that is not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list.

The Security dashboard of the Prime Infrastructure home page displays the number of unclassified rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active unclassified rogue access points.

Unclassified rogue access point states include:

- Pending—On first detection, the unknown access point is put in the Pending state for 3 minutes. During this time, the managed access points determine if the unknown access point is a neighbor access point.
- Alert—The unknown access point is not on the neighbor list or part of the user-configured Friendly AP list.
- Contained—The unknown access point is contained.
- Contained Pending—The unknown access point is marked Contained, but the action is delayed due to unavailable resources.

Click an underlined number in any of the time period categories for further information. See the “Monitoring Rogue Access Points” section on page 5-89.

Monitoring Rogue AP Alarms

Rogue access point radios are unauthorized access points detected by one or more Cisco 1000 series lightweight access points. To open the Rogue AP Alarms page, do one of the following:

- Search for rogue APs.
- From the Prime Infrastructure home page, click the Security dashboard. This page displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.
- Click the Malicious AP number link in the Alarm Summary.

**Note**

If there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use it to view additional alarms.

**Note**

Rogue access point partitions are associated with one of the detecting access points (the one with the latest or strongest RSSI value). If there is detecting access point information, the Prime Infrastructure uses the detecting controller. If the rogue access point is detected by two controllers which are in different partitions, the rogue access point partition might be changed at any time.

The Rogue AP Alarms page contains the following fields:
Note: When the Prime Infrastructure polls, some data might change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

- Severity—Indicates the severity of the alarm including the following icons:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔴</td>
<td>Critical</td>
</tr>
<tr>
<td>🔴</td>
<td>Major</td>
</tr>
<tr>
<td>🔴</td>
<td>Minor</td>
</tr>
<tr>
<td>🔴</td>
<td>Warning</td>
</tr>
<tr>
<td>🔴</td>
<td>Info</td>
</tr>
<tr>
<td>🔴</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

Note: When the controller goes down, the controller inventory dashlet shown the controller status as critical. But the radio inventory dashlet, retains the last known status. In Monitor > AP page, the AP alarm status is shown as "Unknown".

- Clear—Appears if the rogue is no longer detected by any access point.

Note: Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent.

Note: Once the severity of a rogue is Clear, the alarm is deleted from the Prime Infrastructure after 30 days.

You can use the Severity Configuration feature to determine the level of severity for the following rogue access point alarm types:
- Rogue detected
- Rogue detected contained
- Rogue detected on network

See the “Alarm and Event Dictionary” section on page 13-1 for more information.

- Rogue MAC Address—Indicates the MAC address of the rogue access points. See the “Viewing Rogue AP Alarm Details” section on page 5-97.

- Vendor—Rogue access point vendor name or Unknown.

- Classification Type—Pending, Malicious, Friendly, or Unclassified.

- Radio Type—Lists all radio types applicable to this rogue access point.
• Strongest AP RSSI—Displays the strongest AP RSSI for this rogue access point across the life of the rogue. The strongest AP RSSI over the life of the rogue displays to indicate the nearest distance that existed between the rogue access point and your building or location. The higher the RSSI, the closer the location.

• No. of Rogue Clients—Indicates the number of rogue clients associated to this rogue access point.

  **Note** This number comes from the Prime Infrastructure database. It is updated every two hours. From the Monitor > Alarms > Alarm Details page, this number is a real-time number. It is updated each time you open the Alarm Details page for this rogue access point.

• Owner—Name of person to which this alarm is assigned, or (blank).

• Last Seen Time—Indicates the date and time that the rogue access point was last seen.

• State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point. See the “Classifying Rogue Access Points” section on page 5-90 for additional information.
  - Malicious rogue states include: Alert, Contained, Threat, Contained Pending, and Removed. See the “Malicious Rogue APs” section on page 5-92 for more information.
  - Friendly rogue states include: Internal, External, and Alert. See the “Friendly Rogue APs” section on page 5-92 for more information.
  - Unclassified rogue states include: Pending, Alert, Contained, and Contained Pending. See the “Unclassified Rogue APs” section on page 5-93 for more information.

• SSID—Indicates the service set identifier being broadcast by the rogue access point radio. It is blank if the SSID is not being broadcast.

• Map Location—Indicates the map location for this rogue access point.

• Acknowledged—Displays whether or not the alarm is acknowledged by the user. You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality. See the “Acknowledging Alarms” section on page 5-134 for more information.

  **Note** The alarm remains in the Prime Infrastructure, and you can search for all Acknowledged alarms using the alarm search functionality.

**Caution** When you choose to contain a rogue device, the following warning appears: “There may be legal issues following this containment. Are you sure you want to continue?” The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another network could have legal consequences.

**Select a command Menu**

Select one or more alarms by selecting their respective check boxes, choose one of the following commands from the Select a command drop-down list, and click Go.

• Assign to me—Assign the selected alarm(s) to the current user.

• Unassign—Unassign the selected alarm(s).
• Delete—Delete the selected alarm(s).
• Clear—Clear the selected alarm(s). Indicates that the alarm is no longer detected by any access point.

**Note** Once the severity is Clear, the alarm is deleted from the Prime Infrastructure after 30 days.

• Acknowledge Alarm—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See the “Acknowledging Alarms” section on page 5-134 for more information.

**Note** The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality.

• Unacknowledge Alarm—Unacknowledge an already acknowledged alarm.
• Email Notification—Takes you to the All Alarms > Email Notification page to view and configure email notifications. See the “Monitoring RFID Tags” section on page 5-112 for more information.
• Severity Configuration—Allows you to change the severity level for newly-generated alarms. See the “Alarm and Event Dictionary” section on page 13-1 for more information.
• Detecting APs—View the Cisco 1000 Series lightweight access points that are currently detecting the rogue access point. See the “Detecting Access Points” section on page 5-108 for more information.
• Map (High Resolution)—Click to display a high-resolution map of the rogue access point location.
• Rogue Clients—Click to view a list of rogue clients associated with this rogue access point. The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the Rogue access point. See the “Viewing Rogue Client Details” section on page 5-100 for more information. This information can also be accessed by using the Prime Infrastructure Search feature.
• Set State to ‘Unclassified - Alert’—Choose this command to tag the rogue access point as the lowest threat, continue monitoring the rogue access point, and to turn off Containment. See the “Unclassified Rogue APs” section on page 5-93 for more information on Unclassified rogues.
• Set State to ‘Malicious - Alert’—Choose this command to tag the rogue access point as ‘Malicious’. See the “Malicious Rogue APs” section on page 5-92 for more information on Malicious rogues.
• Set State to ‘Friendly - Internal’—Choose this command to tag the rogue access point as internal, add it to the Known Rogue APs list, and to turn off Containment. See the “Friendly Rogue APs” section on page 5-92 for more information on Friendly rogues.
• Set State to ‘Friendly - External’—Choose this command to tag the rogue access point as external, add it to the Known Rogue APs list, and to turn off Containment. See the “Friendly Rogue APs” section on page 5-92 for more information on Friendly rogues.
• 1 AP Containment—Target the rogue access point for containment by one access point. (Lowest containment level.)
• 2 AP Containment—Target the rogue access point for containment by two Cisco 1000 Series lightweight access points.
• 3 AP Containment—Target the rogue access point for containment by three Cisco 1000 Series lightweight access points.
• 4 AP Containment—Target the rogue access point for containment by four Cisco 1000 Series lightweight access points. (Highest containment level.)
Chapter 5   Monitoring Devices

Monitoring Access Points

Note

The higher the threat of the rogue access point, the higher the containment required.

Caution

Attempting to contain a rogue access point might lead to legal consequences. When you select any of the AP Containment commands and click Go, a message “Containing a Rogue AP may have legal consequences. Do you want to continue?” appears. Click OK if you are sure or click Cancel if you do not wish to contain any access points.

Viewing Rogue AP Alarm Details

Rogue access point radios are unauthorized access points detected by Cisco 1000 Series lightweight access points. Alarm event details for each rogue access point are available in the Rogue AP Alarms list page.

To view alarm events for a rogue access point radio, click the rogue MAC address for the applicable alarm from the Monitor > Alarms page for rogue access point alarms.

Note

All Alarm Details page fields (except No. of Rogue Clients) are populated through polling and are updated every two hours.

The number of rogue clients is a real-time number and is updated each time you access the Alarm Details page for a rogue access point alarm.

When a controller (version 7.4 or 7.5) sends custom rogue AP alarm, the Prime Infrastructure shows it as unclassified rogue alarm. This is because the Prime Infrastructure does not support custom rogue AP alarm.

Note

When the Prime Infrastructure polls, some data might change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

The Alarm Details page displays the following information:

- General
  - Rogue MAC Address—MAC address of the rogue access points.
  - Vendor—Rogue access point vendor name or Unknown.

Note

When a rogue access point alarm displays for Airlink, the vendor displays as Alpha instead of Airlink.

- Rogue Type—Indicates the rogue type such as AP.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Owner—Indicates the owner or is left blank.

- Acknowledged—Indicates whether or not the alarm is acknowledged by the user.

  You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality. See the "Acknowledging Alarms" section on page 5-134 for more information.

- Classification Type—Malicious, Friendly, or Unclassified.

- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point.

- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

- Channel Number—Indicates the channel of the rogue access point.

- Containment Level—Indicates the containment level of the rogue access point or Unassigned (not contained).

- Radio Type—Lists all radio types applicable to this rogue access point.

- Strongest AP RSSI—Displays the strongest AP RSSI for this rogue access point across the life of the rogue. The strongest AP RSSI over the life of the rogue displays to indicate the nearest distance that existed between the rogue access point and your building or location. The higher the RSSI, the closer the location.

- No. of Rogue Clients—Indicates the number of rogue clients associated to this rogue access point.

  **Note**

  The number of rogue clients is the only real-time field in the Monitor > Alarm > Alarm Details page. It updates each time you open the Alarm Details page for this rogue access point. All other fields on the Alarm Details page are populated through polling and are updated every two hours.

- First Seen Time—Indicates the date and time when the rogue access point was first detected. This information is populated from the controller.

- Last Seen Time—Indicates the date and time when the rogue access point was last detected. This information is populated from the controller.

- Modified—Indicates when the alarm event was modified.

- Generated By—Indicates how the alarm event was generated (either NMS or from a trap).

  NMS (Network Management System - Prime Infrastructure)—Generated through polling. Prime Infrastructure periodically polls the controllers and generates events. Prime Infrastructure generates events when the traps are disabled or when the traps are lost for those events. In this case, “Generated by” is NMS.

  Trap—Generated by the controller. Prime Infrastructure process these traps and raises corresponding events for them. In this case, “Generated by” is Controller.

- Severity—The severity of the alarm. See Table 5-63 for the list of alarm severity indicator icons.

  You can use the Severity Configuration feature to determine the level of severity for rogue access points. See the "Alarm and Event Dictionary" section on page 13-1 for more information.

- Previous Severity—The previous severity of the alarm: Critical, Major, Minor, Clear.
- Event Details—Click the **Event History** link to view the event details.

- Rogue AP History—Click the **Rogue AP History** link to view the Rogue Alarm details.

- Switch Port Trace Status—Indicates the switch port trace status. Switch port trace status might include: Traced, but not found, Traced and found, Not traced, Failed.

- Switch Port Tracing Details—Provides the most recent switch port tracing details. To view additional trace details, click the **Click here for more details** link.

- Rogue Clients—Lists rogue clients for this access point including the client MAC address, the last date and time the client was heard, and the current client status. See the "Viewing Rogue Client Details" section on page 5-100 for more information.

  **Note**
  
  The number of rogue clients is the only real-time field in the **Monitor > Alarm > Alarm Details** page. It updates each time you open the Alarm Details page for this rogue access point. All other fields in the Alarm Details page are populated through polling and are updated every two hours.

- Message—Displays the most recent message regarding this rogue access point. A message is sent for the following: When the rogue access point is first detected, for any trap sent, and for any changed state.

- Annotations—Lists current notes regarding this rogue access point. To add a new note, click **New Annotation**. Type the note and click **Post** to save and display the note or **Cancel** to close the page without saving the note.

- Location Notifications—Displays the number of location notifications logged against the client. Clicking a link displays the notifications.

- Location—Provides location information, if available.

  **Note**
  
  The switch port tracing does not update any of the rogue attributes such as severity, state, and so on. As the rogue attributes are not updated by switch port tracing, alarms would not be triggered if a rogue is discovered to be 'on network' using switch port tracing.

**Select a command Menu**

The Select a command drop-down list located in the Rogue AP Alarm Details page provides the following options. Choose an option from the drop-down list, and click **Go**.

- Assign to me—Assign the selected alarm(s) to the current user.

- Unassign—Unassign the selected alarm(s).

- Delete—Delete the selected alarm(s).

- Clear—Clear the selected alarm(s).

- Acknowledge Alarm—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See the "Acknowledging Alarms" section on page 5-134 for more information.

  **Note**
  
  The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality.

- Unacknowledge—Unacknowledge an already acknowledged alarm.
- Trace Switch Port—Click to run a switch port trace for this rogue access point.
- Event History—Click to view a list of events for this rogue access point. See the “Monitoring Rogue Alarm Events” section on page 5-109 for more information.
- Refresh from Network—Click to sync up the rogue APs from the network.
- View Detecting AP on Network—View the Cisco 1000 Series lightweight access points that are currently detecting the rogue access point. See the “Detecting Access Points” section on page 5-108 for more information.

Note: Detecting AP Name, Radio, SSID information might be empty as the information is not available on controller. Refresh the page after the rogue AP task is completed to see the AP details.

- View Details by Controller—View the classification type and state of the rogue APs reported by the controller.
- Map (High Resolution)—Click to display a high-resolution map of the rogue access point location.
- Rogue Clients—Click to view a list of rogue clients associated with this rogue access point. The Rogue Clients page displays the Client MAC address, when it was last heard, its current status, its controller, and the Rogue access point. See the “Viewing Rogue Client Details” section on page 5-100 for more information. This information can also be accessed by using the Prime Infrastructure Search feature.
- Set State to ‘Unclassified - Alert’—Choose this command to tag the rogue access point as the lowest threat, continue monitoring the rogue access point, and to turn off Containment. See the “Unclassified Rogue APs” section on page 5-93 for more information on Unclassified rogues.
- Set State to ‘Malicious - Alert’—Choose this command to tag the rogue access point as ‘Malicious’. See the “Malicious Rogue APs” section on page 5-92 for more information on Malicious rogues.
- Set State to ‘Friendly - Internal’—Choose this command to tag the rogue access point as internal, add it to the Known Rogue APs list, and to turn off Containment. See the “Friendly Rogue APs” section on page 5-92 for more information on Friendly rogues.
- Set State to ‘Friendly - External’—Choose this command to tag the rogue access point as external, add it to the Known Rogue APs list, and to turn off Containment. See the “Friendly Rogue APs” section on page 5-92 for more information on Friendly rogues.
- 1 AP Containment—Target the rogue access point for containment by one access point. (Lowest containment level.)
- 2 AP Containment—Target the rogue access point for containment by two Cisco 1000 series lightweight access points.
- 3 AP Containment—Target the rogue access point for containment by three Cisco 1000 series lightweight access points.
- 4 AP Containment—Target the rogue access point for containment by four Cisco 1000 series lightweight access points. (Highest containment level.)

Note: The higher the threat of the rogue access point, the higher the containment required.

Viewing Rogue Client Details

You can view a list of rogue clients in several ways:
Perform a search for rogue clients using the Prime Infrastructure Search feature.

View the list of rogue clients for a specific rogue access point from the Alarm Details page for the applicable rogue access point. Click the Rogue MAC address for the applicable rogue client to view the Rogue Client details page.

In the Alarms Details page of a rogue access point, choose Rogue Clients from the Select a command drop-down list.

The Rogue Clients page displays the Client MAC address, when it was last heard, its current status, its controller, and the associated rogue access point.

**Note**
Rogue client statuses include: Contained (the controller contains the offending device so that its signals no longer interfere with authorized clients); Alert (the controller forwards an immediate alert to the system administrator for further action); and Threat (the rogue is a known threat).

Click the Client MAC Address for the rogue client to view the Rogue Client details page. The Rogue Client details page displays the following information:

- **General**—Information includes: client MAC address, number of access points that detected this client, when the client was first and last heard, the rogue access point MAC address, and the client current status.
- **Location Notifications**—Indicates the number of notifications for this rogue client including: absence, containment, distance, and all. Click the notification number to open the applicable Monitor > Alarms page.
- **APs that detected the rogue client**—Provides the following information for all access points that detected this rogue client: base radio MAC address, access point name, channel number, radio type, RSSI, SNR, and the date/time that the rogue client was last heard.
- **Location**—Provides location information, if available.

**Note**
The higher the threat of the rogue access point, the higher the containment required.

**Select a command**

The Select a command drop-down list in the Rogue Client details page includes the following options:

- **Set State to ‘Unknown - Alert’**—Choose this command to tag the rogue client as the lowest threat, continue monitoring the rogue client, and to turn off Containment.
- **1 AP Containment**—Target the rogue client for containment by one access point. (Lowest containment level.)
- **2 AP Containment**—Target the rogue client for containment by two access points.
- **3 AP Containment**—Target the rogue client for containment by three access points.
- **4 AP Containment**—Target the rogue client for containment by four access points. (Highest containment level.)
- **Map (High Resolution)**—Click to display a high-resolution map of the rogue client location.
- **Location History**—Click to display the history of the rogue client location based on RF fingerprinting.
Viewing Rogue AP History Details

To view the history of a rogue AP alarms, click the Rogue AP History link in the Rogue AP Alarm page. The Rogue AP History page displays the following information:

- **Severity**—The severity of the alarm.
- **Rogue MAC Address**—MAC address of the rogue access points.
- **Classification Type**—Malicious, Friendly, or Unclassified.
- **Radio Type**—Lists all radio types applicable to this rogue access point.
- **Strongest AP RSSI**—Displays the strongest AP RSSI for this rogue access point across the life of the rogue. The strongest AP RSSI over the life of the rogue displays to indicate the nearest distance that existed between the rogue access point and your building or location. The higher the RSSI, the closer the location.
- **No. of Rogue Clients**—Indicates the number of rogue clients associated to this rogue access point.

**Note**

The number of rogue clients is the only real-time field in the Monitor > Alarm > Alarm Details page. It updates each time you open the Alarm Details page for this rogue access point. All other fields on the Alarm Details page are populated through polling and are updated every two hours.

- **First Seen Time**—Indicates the date and time when the rogue access point was first detected. This information is populated from the controller.
- **Last Seen Time**—Indicates the date and time when the rogue access point was last detected. This information is populated from the controller.
- **State**—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point.
- **SSID**—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- **Category**—Indicates the category of this alarm such as Security or Prime Infrastructure.
- **On Network**—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- **Channel Number**—Indicates the channel of the ad hoc rogue.
- **Containment Level**—Indicates the containment level of the ad hoc rogue or Unassigned.
- **Switch Port Trace Status**—Indicates the switch port trace status. Switch port trace status might include: Traced, but not found, Traced and found, Not traced, Failed.

Click the Rogue MAC address to view the specific rogue AP history details page. The rogue AP history details page displays the above details and also displays the actual alarm message.

Viewing Rogue AP Event History Details

To view the event details of a rogue AP, click the Event History link in the Rogue AP Alarm page. The Rogue AP Event History page displays the following information:

- **Severity**—The severity of the alarm.
• Rogue MAC Address—MAC address of the rogue access points.
• Vendor—Rogue access point vendor name or Unknown.
• Classification Type—Malicious, Friendly, or Unclassified.
• On Network—Indicates whether the rogue detection occurred. The controller detected the rogue (Yes or No).
• Date/Time—The date and time that the event was generated.
• Radio Type—Lists all radio types applicable to this rogue access point.
• State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point.
• SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

**Monitoring Ad hoc Rogues**

If the MAC address of a mobile client operating in an ad hoc network is not in the authorized MAC address list, then it is identified as an ad hoc rogue.

- Monitoring Ad hoc Rogue Alarms, page 5-103
- Viewing Ad hoc Rogue Alarm Details, page 5-105

**Monitoring Ad hoc Rogue Alarms**

The Adhoc Rogue Alarms page displays alarm events for ad hoc rogues. To access the Adhoc Rogue Alarms page, do one of the following:

- Perform a search for ad hoc rogue alarms.
- From the Prime Infrastructure home page, click the Security dashboard. This page displays all the ad hoc rogues detected in the past hour and the past 24 hours. Click the ad hoc rogue number to view the ad hoc rogue alarms.

If there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

The Adhoc Rogue Alarms page contains the following fields:

| Note | When the Prime Infrastructure polls, some data might change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue. |

- Severity—Indicates the severity of the alarm. See Table 5-63 for a list of severity indicator icons. You can use the Severity Configuration feature to determine the level of severity for the following ad hoc rogue alarm types:
  - Adhoc Rogue auto contained
  - Adhoc Rogue detected
  - Adhoc Rogue detected on network
  - Adhoc Rogue detected on network
Monitoring Access Points

See the “Alarm and Event Dictionary” section on page 13-1 for more information.

- Rogue MAC Address—Indicates the MAC address of the rogue. See the “Viewing Ad hoc Rogue Alarm Details” section on page 5-105 for more information.
- Vendor—Indicates the ad hoc rogue vendor name, or Unknown.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Strongest AP RSSI—Displays the strongest AP RSSI for this rogue across the life of the rogue. The strongest AP RSSI over the life of the rogue displays to indicate the nearest distance that existed between the rogue and your building or location. The higher the RSSI, the closer the location.
- No. of Rogue Clients—Indicates the number of rogue clients associated to this rogue access point.

| Note | The number of rogue clients is the only real-time field in the Monitor > Alarm > Alarm Details page. It updates each time you open the Alarm Details page for this rogue access point. All other fields in the Alarm Details page are populated through polling and are updated every two hours. |

- Owner—Indicates the owner or is left blank.
- Last Seen Time—Indicates the date and time that the alarm was last viewed.
- State—Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
- SSID—The Service Set Identifier that is being broadcast by the rogue ad hoc radio. It is blank if there is no broadcast.
- Map Location—Indicates the map location for this ad hoc rogue.
- Acknowledged—Displays whether or not the alarm is acknowledged by the user.

You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality. See the “Acknowledging Alarms” section on page 5-134 for more information.

Select a command Menu

Select one or more alarms by selecting their respective check boxes, choose one of the following commands from the Select a command drop-down list, and click Go.

- Assign to me—Assign the selected alarm(s) to the current user.
- Unassign—Unassign the selected alarm(s).
- Delete—Delete the selected alarm(s).
- Clear—Clear the selected alarm(s).
- Acknowledge—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See the “Acknowledging Alarms” section on page 5-134 for more information.

| Note | The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality. |

- Unacknowledge—Unacknowledge an already acknowledged alarm.
Email Notification—Takes you to the All Alarms > Email Notification page to view and configure email notifications. See the “Monitoring RFID Tags” section on page 5-112 for more information.

Detecting APs—View the access points that are currently detecting the rogue ad hoc. See the Detecting Access Points, page 108 for more information.

Map (High Resolution)—Click to display a high-resolution map of the ad hoc rogue location.

Rogue Clients—Click to view a list of rogue clients associated with this ad hoc rogue. The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the ad hoc rogue.

Set State to ‘Alert’—Choose this command to tag the ad hoc rogue as the lowest threat, continue monitoring the rogue access point, and to turn off Containment.

Set State to ‘Internal’—Choose this command to tag the ad hoc rogue as internal, add it to the Known Rogue APs list, and to turn off Containment.

Set State to ‘External’—Choose this command to tag the ad hoc rogue as external, add it to the Known Rogue APs list, and to turn off Containment.

1 AP Containment—Target the ad hoc rogue for containment by one access point. (Lowest containment level.)

2 AP Containment—Target the ad hoc rogue for containment by two access points.

3 AP Containment—Target the ad hoc rogue for containment by three access points.

4 AP Containment—Target the ad hoc rogue for containment by four access points. (Highest containment level.)

Caution

Attempting to contain an ad hoc rogue might lead to legal consequences. When you select any of the AP Containment commands and click Go, a message “Containing a Rogue AP may have legal consequences. Do you want to continue?” appears. Click OK if you are sure, or click Cancel if you do not want to contain any access points.

Viewing Ad hoc Rogue Alarm Details

Alarm event details for each ad hoc rogue are available from the Adhoc Rogue Alarms page.

To view alarm events for an ad hoc rogue radio, click the applicable Rogue MAC address in the Adhoc Rogue Alarms page.

This page displays alarm events for a rogue access point radio. Rogue access point radios are unauthorized access points detected by Cisco 1000 Series lightweight access points.

Note

When the Prime Infrastructure polls, some data might change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

General

- Rogue MAC Address—Media Access Control address of the ad hoc rogue.
- Vendor—Ad hoc rogue vendor name or Unknown.
- On Network—Indicates how the rogue detection occurred.
- Controller—The controller detected the rogue (Yes or No).
Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.

- Owner—Indicates the owner or left blank.
- Acknowledged—Indicates whether or not the alarm is acknowledged by the user.
  You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality. See the “Acknowledging Alarms” section on page 5-134 for more information.
- State—Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
- SSID—Service Set Identifier being broadcast by the ad hoc rogue radio. (Blank if SSID is not broadcast.)
- Channel Number—Indicates the channel of the ad hoc rogue.
- Containment Level—Indicates the containment level of the ad hoc rogue or Unassigned.
- Radio Type—Lists all radio types applicable to this ad hoc rogue.
- Strongest AP RSSI—Indicates the strongest received signal strength indicator for this Prime Infrastructure (including all detecting access points for all controllers and across all detection times).
- No. of Rogue Clients—Indicates the number of rogue clients associated to this ad hoc.

**Note**
This number comes from the Prime Infrastructure database. It is updated every two hours. In the Monitor > Alarms > Alarm Details page, this number is a real-time number. It is updated each time you open the Alarm Details page for this rogue access point.

- Created—Indicates when the alarm event was created.
- Modified—Indicates when the alarm event was modified.
- Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
  NMS (Network Management System - Prime Infrastructure)—Generated through polling.
  Prime Infrastructure periodically polls the controllers and generates events. Prime Infrastructure generates events when the traps are disabled or when the traps are lost for those events. In this case, “Generated by” is NMS.
  Trap—Generated by the controller. Prime Infrastructure process these traps and raises corresponding events for them. In this case, “Generated by” is Controller.
- Severity—Indicates the severity of the alarm. See Table 5-63 for a list of severity indicator icons.
- Previous Severity—The previous severity of the alarm: Critical, Major, Minor, Clear. Color coded.

- Annotations—Enter any new notes in this box and click Add to update the alarm.
- Message—Displays descriptive information about the alarm.
- Help—Displays the latest information about the alarm.
- Event History—Click to access the Monitor > Events page. See the “Monitoring Events” section on page 5-141 for more information.
- Annotations—Lists existing notes for this alarm.
Searching Rogue Clients Using Advanced Search

When the access points on your wireless LAN are powered up and associated with controllers, the Prime Infrastructure immediately starts listening for rogue access points. When a controller detects a rogue access point, it immediately notifies the Prime Infrastructure, which creates a rogue access point alarm. To find rogue access point alarms using Advanced Search, follow these steps:

Step 1  Click Advanced Search in the top right-hand corner of the Prime Infrastructure main page.
Step 2  Choose Rogue Client from the Search Category drop-down list.
Step 3  (Optional) You can filter the search even further with the other search criteria if desired.
Step 4  Click Search. The list of rogue clients appears.
Step 5  Choose a rogue client by clicking a client MAC address. The Rogue Client detail page appears.
Step 6  To modify the alarm, choose one of these commands from the Select a command drop-down list, and click Go.

- Set State to ‘Unknown-Alert’—Tags the ad hoc rogue as the lowest threat, continues to monitor the ad hoc rogue, and turns off containment.
- 1 AP Containment through 4 AP Containment—Indicates the number of access points (1-4) in the vicinity of the rogue unit that send dauthenticate and disassociate messages to the client devices that are associated to the rogue unit.
- Map (High Resolution)—Displays the current calculated rogue location in the Maps > Building Name > Floor Name page.
- Location History—Displays the history of the rogue client location based on RF fingerprinting.

Note  The client must be detected by an MSE for the location history to appear.

Monitoring Rogue Access Point Location, Tagging, and Containment

When the Cisco Unified Network Solution is monitored using the Prime Infrastructure, the Prime Infrastructure generates the flags as rogue access point traps and displays the known rogue access points by MAC address. The operator can then display a map showing the location of the access points closest to each rogue access point. The next step is to mark them as Known or Acknowledged rogue access points (no further action), Alert rogue access points (watch for and notify when active), or Contained rogue access points (have between one and four access points discourage rogue access point clients by sending the clients deauthenticate and disassociate messages whenever they associate with the rogue access point).

This built-in detection, tagging, monitoring, and containment capability enables system administrators to take appropriate action:

- Locate rogue access points
- Receive new rogue access point notifications, eliminating hallway scans
- Monitor unknown rogue access points until they are eliminated or acknowledged
- Determine the closest authorized access point, making directed scans faster and more effective
Contain rogue access points by sending their clients deauthenticate and disassociate messages from one to four access points. This containment can be done for individual rogue access points by MAC address or can be mandated for all rogue access points connected to the enterprise subnet.

Tag rogue access points:
- Acknowledge rogue access points when they are outside of the LAN and do not compromise the LAN or wireless LAN security
- Accept rogue access points when they do not compromise the LAN or wireless LAN security
- Tag rogue access points as unknown until they are eliminated or acknowledged

Tag rogue access points as contained and discourage clients from associating with the rogue access points by having between one and four access points transmit deauthenticate and disassociate messages to all rogue access point clients. This function applies to all active channels on the same rogue access point.

Detecting Access Points

Use the Detecting Access Points feature to view information about the Cisco lightweight access points that are detecting a rogue access point.

To access the Rogue AP Alarms details page, follow these steps:

**Step 1**
To display the Rogue AP Alarms page, do one of the following:
- Perform a search for rogue APs.
- In the Prime Infrastructure home page, click the **Security** dashboard. This dashboard displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.
- Click the **Malicious AP** number link in the Alarm Summary box.

**Step 2**
In the Rogue AP Alarms page, click the Rogue MAC Address for the applicable rogue access point. The Rogue AP Alarms details page appears.

**Step 3**
From the Select a command drop-down list, choose **Detecting APs**.

**Step 4**
Click **Go**.

Click a list item to display data about that item:
- AP Name
- Radio
- Map Location
- SSID—Service Set Identifier being broadcast by the rogue access point radio.
- Channel Number—Which channel the rogue access point is broadcasting on.
- WEP—Enabled or disabled.
- WPA—Enabled or disabled.
- Pre-Amble—Long or short.
- RSSI—Received signal strength indicator in dBm.
- SNR—Signal-to-noise ratio.
- Containment Type—Type of containment applied from this access point.
- Containment Channels—Channels that this access point is currently containing.

**Monitoring Rogue Alarm Events**

The Events page enables you to review information about rogue alarm events. The Prime Infrastructure generates an event when a rogue access point is detected or if you make manual changes to a rogue access point (such as changing its state). The Rogue AP Events list page displays all rogue access point events.

To access the Rogue AP Events list page, follow these steps:

**Step 1**
- Do one of the following:
  - Perform a search for rogue access point events using the Advanced Search feature of the Prime Infrastructure.
  - In the Rogue AP Alarms details page, click **Event History** from the Select a command drop-down list. See the “Viewing Rogue AP Alarm Details” section on page 5-97 for more information.

**Step 2**
- The Rogue AP Events list page displays the following event information:
  - **Severity**—Indicates the severity of the alarm. See Table 5-63 for a list of severity indicator icons.
  - **Rogue MAC Address**—Click the rogue MAC address to view the Rogue AP Event Details page. See the “Viewing Rogue AP Event Details” section on page 5-109 for more information.
  - **Vendor**—Rogue access point vendor name or Unknown.
  - **Classification Type**—Malicious, Friendly, or Unclassified.
  - **On Network**—Indicates how the rogue detection occurred.
    - Controller—The controller detected the rogue (Yes or No).
    - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
  - **Radio Type**—Lists all radio types applicable to this rogue access point.
  - **Date/Time**—The date and time that the event was generated.
  - **State**—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point.
  - **SSID**—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

**Viewing Rogue AP Event Details**

To view rogue access point event details, follow these steps:

**Step 1**
- In the Rogue AP Events list page, click the **Rogue MAC Address** link.

**Step 2**
- The Rogue AP Events Details page displays the following information:
  - Rogue MAC address
  - Vendor—Rogue access point vendor name or Unknown.
  - On Network—Indicates how the rogue detection occurred.
Chapter 5  Monitoring Devices

Monitoring Access Points

- Controller—The controller detected the rogue (Yes or No).
- Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Classification Type—Malicious, Friendly, or Unclassified.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Channel Number—The channel on which the rogue access point is broadcasting.
- Containment Level—Indicates the containment level of the rogue access point or Unassigned.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Created—The date and time that the event was generated.
- Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
  - NMS (Network Management System - Prime Infrastructure)—Generated through polling. Prime Infrastructure periodically polls the controllers and generates events. Prime Infrastructure generates events when the traps are disabled or when the traps are lost for those events. In this case, “Generated by” is NMS.
  - Trap—Generated by the controller. Prime Infrastructure process these traps and raises corresponding events for them. In this case, “Generated by” is Controller.
- Device IP Address
- Severity—Indicates the severity of the alarm. See Table 5-63 for a list of severity indicator icons.
- Message—Provides details of the current event.

Monitoring Ad hoc Rogue Events

The Events page enables you to review information about ad hoc rogue events. Prime Infrastructure generates an event when an ad hoc rogue is detected or if you make manual changes to an ad hoc rogue (such as changing its state). The Adhoc Rogue Events list page displays all ad hoc rogue events.

To access the Rogue AP Events list page, follow these steps:

Step 1
Do one of the following:
- Perform a search for ad hoc rogues events using the Advanced Search feature of the Prime Infrastructure.
- In the Adhoc Rogue Alarms details page, click Event History from the Select a command drop-down list. See the “Viewing Ad hoc Rogue Alarm Details” section on page 5-105 for more information.

Step 2
The Rogue AP Events list page displays the following event information.
- Severity—Indicates the severity of the alarm. See Table 5-63 for a list of severity indicator icons.
- Rogue MAC Address—Click the rogue MAC address to view the Rogue AP Event Details page. See the “Viewing Ad hoc Rogue Event Details” section on page 5-111 for more information.
- Vendor—Rogue access point vendor name or Unknown.
• On Network—Indicates how the rogue detection occurred.
  – Controller—The controller detected the rogue (Yes or No).
  – Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the
    following: Traced but not found, Traced and found, Not traced.
• Radio Type—Lists all radio types applicable to this rogue access point.
• Date/Time—The date and time that the event was generated.
• State—Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert,
  Internal, External, Contained, Contained Pending, and Removed.
• SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not
  broadcast.)

Viewing Ad hoc Rogue Event Details

To view rogue access point event details, follow these steps:

**Step 1** In the Rogue AP Events list page, click the **Rogue MAC Address** link.

**Step 2** The Rogue AP Events Details page displays the following information:

• Rogue MAC Address
• Vendor—Rogue access point vendor name or Unknown.
• On Network—Indicates how the rogue detection occurred.
  – Controller—The controller detected the rogue (Yes or No).
  – Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the
    following: Traced but not found, Traced and found, Not traced.
• State—Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert,
  Internal, External, Contained, Contained Pending, and Removed.
• SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not
  broadcast.)
• Channel Number—The channel on which the rogue access point is broadcasting.
• Containment Level—Indicates the containment level of the rogue access point or Unassigned.
• Radio Type—Lists all radio types applicable to this rogue access point.
• Created—The date and time that the event was generated.
• Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
  – NMS (Network Management System - Prime Infrastructure)—Generated through polling. Prime
    Infrastructure periodically polls the controllers and generates events. Prime
    Infrastructure generates events when the traps are disabled or when the traps are lost for those
    events. In this case, “Generated by” is NMS.
  – Trap—Generated by the controller. Prime Infrastructure process these traps and raises
    corresponding events for them. In this case, “Generated by” is Controller.
• Device IP Address
• Severity—Indicates the severity of the alarm. See **Table 5-63** for a list of severity indicator icons.
Monitoring RFID Tags

The Monitor > RFID Tags page allows you to monitor tag status and location on the Prime Infrastructure maps as well as review tag details.
Note
This page is only available in the Location version of the Prime Infrastructure.

This section provides information on the tags detected by the location appliance.
Choose **Monitor > RFID Tags** to access this section. By default, the **Tag Summary** page is displayed.

- **Tag Summary, page 5-113**
- **Searching Tags, page 5-113**
- **Viewing RFID Tag Search Results, page 5-114**
- **Viewing the Tag List, page 5-115**

### Tag Summary

Choose **Monitor > RFID Tags** to access this page.

This page provides information on the number of tags that are detected by MSE. The following fields are displayed in the main data area:

- **Device Name**—Name of the MSE device.
- **Total Tags**—Click the number to view tag details. Clicking the number shows the list of tags located by the MSE. Clicking a MAC address shows the tag details pertaining to that MAC address.

### Searching Tags

Use the Prime Infrastructure Advanced Search feature to find specific or all tags.

To search for tags in the Prime Infrastructure, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Click <strong>Advanced Search</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Choose <strong>Tags</strong> from the Search Category drop-down list.</td>
</tr>
<tr>
<td>3</td>
<td>Identify the applicable tag search fields including:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Search By</strong>—Choose All Tags, Asset Name, Asset Category, Asset Group, MAC Address, Controller, MSE, Floor Area, or Outdoor Area.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Search In</strong>—Choose the applicable category.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Last detected within</strong>—Choose a time increment from 5 minutes to 24 hours. The default is 15 minutes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Tag Vendor</strong>—Select the check box, and choose Aeroscout, G2, PanGo, or WhereNet.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Telemetry Tags only</strong>—Select the Telemetry Tags only check box to search tags accordingly.</td>
</tr>
<tr>
<td>4</td>
<td>Click <strong>Go</strong>.</td>
</tr>
</tbody>
</table>

Note
Search fields might change depending on the selected category. When applicable, enter the additional field or filter information to help identify the Search By category.
Viewing RFID Tag Search Results

Use the Prime Infrastructure Advanced Search feature located in the top right of the Prime Infrastructure page to search for tags by asset type (name, category and group), by MAC address, by system (controller or location appliance), and by area (floor area and outdoor area).

---

**Note**

Search fields might change depending on the selected category. When applicable, enter the additional field or filter information to help identify the Search By category.

You can further refine your search using the Advanced search fields and save the search criteria for future use. Saved search criteria can be retrieved from the Saved Searches located in the navigation bar.

When you click the MAC address of a tag location in a search results page, the following details appear for the tag:

- Tag vendor

  **Note**
  This option does not appear when Asset Name, Asset Category, Asset Group or MAC Address are the search criteria for tags.

- Controller to which the tag is associated

- Telemetry data (CCX v1 compliant tags only)
  - Telemetry data displayed is vendor-specific; however, some commonly reported details are GPS location, battery extended information, pressure, temperature, humidity, motion, status, and emergency code.

  **Note**
  The Telemetry data option only appears when MSE (select for location servers), Floor Area, or Outdoor Area are selected as the Search for tags by option.

  **Note**
  Only those vendor tags that support telemetry appear.

- Asset Information (Name, Category, Group)

- Statistics (bytes and packets received)

- Location (Floor, Last Located, MSE, map)

- Location Notification (Absence, Containment, Distance, All)

  **Note**
  Telemetry data displayed is vendor-specific; however, some commonly reported details are GPS location, battery extended information, pressure, temperature, humidity, motion, status, and emergency code.

- Emergency Data (CCX v1 compliant tags only)
Viewing the Tag List

Click the Total Tags number link to view the Tags List for the applicable device name. The Tag List contains the following information:

- MAC Address
- Asset Name
- Asset Group
- Asset Category
- Vendor Name
- Mobility Services Engine
- Controller
- Battery Status
- Map Location

Monitoring Chokepoints

Chokepoints are installed and configured as recommended by the Chokepoint vendor. After the chokepoint installation is complete and operational, the chokepoint can be added to the Prime Infrastructure and placed on Floor Maps. They are pushed to the Location Server during synchronization.

Choose Monitor > Chokepoints. A page appears displaying a list of found chokepoints. Clicking a link in the Map Location column for a particular chokepoint displays a map that shows the location of the chokepoint.

The following fields are displayed:

- MAC Address—The MAC address of the chokepoint.
- Chokepoint Name—The user-defined name of the chokepoint.
- Entry/Exit Chokepoint—Indicates whether or not the chokepoint is an entry/exit chokepoint.
- Range—The range of the chokepoint in feet.
- Static IP—The static IP address of the chokepoint.
- Map Location—A link to a map showing the location of the chokepoint.

Performing a Chokepoint Search

An advanced search allows you to search for chokepoints.

To perform an advanced search for a chokepoint in the Prime Infrastructure, follow these steps:

1. Click Advanced Search located in the top right corner of the Prime Infrastructure.
2. From the New Search page, choose Chokepoint from the Search Category drop-down list.
3. Choose the method by which you want to search (by MAC address or chokepoint name) from the Search for Chokepoint by drop-down list.
Step 4 Enter the MAC address or chokepoint name, depending on the search method selected.

Step 5 Click Search.

Monitoring Interferers

The Monitor > Interferer page allows you to monitor interference devices detected by the CleanAir-enabled access points.

This section provides information on the interferers detected by the CleanAir-enabled access points. By default, the Monitoring AP Detected Interferers page is displayed.

- Monitoring AP Detected Interferers, page 5-116
- Monitoring AP Detected Interferer Details, page 5-117
- Monitoring AP Detected Interferer Details Location History, page 5-118
- Configuring the Search Results Display, page 5-118

Monitoring AP Detected Interferers

Choose Monitor > Interferers to view all the interfering devices detected by the CleanAir-enabled access points on your wireless network. This page enables you to view a summary of the interfering devices including the following default information:

- Interferer ID—A unique identifier for the interferer. This is a pseudo-randomly generated ID. Though it is similar to a MAC address, it is not a real address, such as the one used by a Bluetooth headset.

- Type—Indicates the category of the interferer. Click to read more about the type of device. A pop-up window appears displaying more details. The categories include the following:
  - Bluetooth link—A Bluetooth link (802.11b/g/n only)
  - Microwave Oven—A microwave oven (802.11b/g/n only)
  - 802.11 FH—An 802.11 frequency-hopping device (802.11b/g/n only)
  - Bluetooth Discovery—A Bluetooth discovery (802.11b/g/n only)
  - TDD Transmitter—A time division duplex (TDD) transmitter
  - Jammer—A jamming device
  - Continuous Transmitter—A continuous transmitter
  - DECT-like Phone—A digital enhanced cordless communication (DECT)-compatible phone
  - Video Camera—A video camera
  - 802.15.4—An 802.15.4 device (802.11b/g/n only)
  - WiFi Inverted—A device using spectrally inverted Wi-Fi signals
  - WiFi Invalid Channel—A device using non-standard Wi-Fi channels
  - SuperAG—An 802.11 SuperAG device
  - Canopy—A Motorola Canopy device
  - Radar—A radar device (802.11a/n only)
- XBox—A Microsoft Xbox (802.11b/g/n only)
- WiMAX Mobile—A WiMAX mobile device (802.11a/n only)
- WiMAX Fixed—A WiMAX fixed device (802.11a/n only)
- WiFi AOCI—A WiFi device with AOCI
- Unclassified

- Status—Indicates the status of the interfering device.
  - Active—Indicates that the interferer is currently being detected by the CleanAir capable access point.
  - Inactive—Indicates that the interferer is no longer being detected by the CleanAir capable access point or no longer reachable by the Prime Infrastructure.

- Severity—Displays the severity ranking of the interfering device.
- Affected Band—Displays the band in which this device is interfering.
- Affected Channels—Displays the affected channels.
- Duty Cycle (%)—The duty cycle of interfering device in percentage.
- Discovered—Displays the time at which it was discovered.
- Last Updated—The last time the interference was detected.
- Floor—The location where the interfering device is present.

**Monitoring AP Detected Interferer Details**

Choose **Monitor > Interferers > Interferer ID** to view this page. This page enables you to view the details of the interfering devices detected by the access points. This page provides the following details about the interfering device.

- Interferer Properties
  - Type—Displays the type of the interfering device detected by the AP.

- Status—The status of the interfering device. Indicates the status of the interfering device.
  - Active—Indicates that the interferer is currently being detected by the CleanAir capable access point.
  - Inactive—Indicates that the interferer is no longer being detected by the CleanAir capable access point or no longer reachable by the Prime Infrastructure.
  - Severity—Displays the severity ranking of the interfering device.
  - Duty Cycle (%)—The duty cycle of interfering device in percentage.
  - Affected Band—Displays the band in which this device is interfering.
  - Affected Channels—Displays the affected channels.
  - Discovered—Displays the time at which it was discovered.
  - Last Updated—The last time the interference was detected.

- Location
  - Floor—The location where this interfering device was detected.
  - Last Located At—The last time where the interfering device was located.
  - On MSE—The mobility server engine on which this interference device was located.
• Clustering Information
  – Clustered By—Displays the IP address of the controller or the MSE that clustered the interferer information from the access point.
  – Detecting APs—Displays the details of the access point that has detected the interfering device. The details include: Access Point Name (Mac), Severity, and Duty Cycle(%)..
• Details—Displays a short description about the interfering type.

Select a command

The Select a command drop-down list provides access to the location history of the interfering device detected by the access point. See the “Monitoring AP Detected Interferer Details Location History” section on page 5-118.

**Monitoring AP Detected Interferer Details Location History**

Choose Monitor > Interferers > Interference Device ID, then choose Location History from the Select a command drop-down list, and click Go to view this page.

• Interferer Information—Displays the basic information about the interfering device.
  – Data Collected At—The time stamp at which the data was collected.
  – Type—The type of the interfering device.
  – Severity—The severity index of the interfering device.
  – Duty Cycle—The duty cycle (in percentage) of the interfering device.
  – Affected Channels—A comma separated list of the channels affected.
• Interferer Location History—Displays the location history of the interfering devices.
  – Time Stamp
  – Floor
• Clustering Information
  – Clustered By
• Detecting APs
  – AP Name—The access point that detected the interfering device.
  – Severity—The severity index of the interfering device.
  – Duty Cycle(%)—The duty cycle (in percentage) of the interfering device.
• Location
  – Location Calculated At—Displays the time stamp at which this information was generated.
  – Floor—Displays location information of the interfering device.
  – A graphical view of the location of the interfering device is displayed in a map. Click the Enlarge link to view an enlarged image.

**Configuring the Search Results Display**

The Edit View page allows you to add, remove, or reorder columns in the AP Detected Interferers Summary page.
To edit the columns in the AP Detected Interferers page, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Monitor &gt; Interferers</strong>. The AP Detected Interferers page appears showing details of the interferers detected by the CleanAir-enabled access points.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the <strong>Edit View</strong> link.</td>
</tr>
<tr>
<td>Step 3</td>
<td>To add an additional column to the access points table, click to highlight the column heading in the left column. Click <strong>Show</strong> to move the heading to the right column. All items in the right column are displayed in the table.</td>
</tr>
<tr>
<td>Step 4</td>
<td>To remove a column from the access points table, click to highlight the column heading in the right column. Click <strong>Hide</strong> to move the heading to the left column. All items in the left column are not displayed in the table.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Use the <strong>Up/Down</strong> buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click <strong>Up</strong> or <strong>Down</strong> to move it higher or lower in the current list.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>Reset</strong> to restore the default view.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Click <strong>Submit</strong> to confirm the changes.</td>
</tr>
</tbody>
</table>

**Monitoring Spectrum Experts**

A Spectrum Expert client acts as a remote interference sensor and sends dynamic interference data to the Prime Infrastructure. This feature allows the Prime Infrastructure to collect and archive and monitor detailed interferer and air quality data from Spectrum Experts in the network.

To access the Monitor Spectrum Experts page, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>Monitor &gt; Spectrum Experts</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>From the left sidebar menu, you can access the <strong>Spectrum Experts Summary</strong> page and the <strong>Interferers Summary</strong> page.</td>
</tr>
</tbody>
</table>

**Spectrum Experts Summary**

The Spectrum Experts > Summary page is the default page and provides a table of the Spectrum Experts added to the system. The table provides the following Spectrum Expert information:

- **Hostname**—Displays the hostname or IP Address depending on how it was added. Click the hostname to access the **Spectrum Experts Details** page.
- **Active Interferers**—Indicates the current number of interferes being detected by the Spectrum Experts.
- **Affected APs**—The number of access points seen by the Spectrum Expert that are potentially affected by detected interferers.
- **Alarms**—The number of active interference traps sent by the Spectrum Expert. Click to access the Alarm page that is filtered to the active alarms for this Spectrum Expert.
Interferers Summary

The Interferers > Summary page displays a list of all the Interferers detected over a 30 day interval. The table provides the following Interferers information:

- **Interferer ID**—An identifier that is unique across different spectrum experts. This is a pseudo-randomly generated ID. Though it is similar to a MAC address, it is not a real address, which you can use to find the interfering device.
- **Category**—Indicates the category of the interferer. Categories include: Bluetooth, Cordless Phones, Microwave Ovens, 802.11 FH, Generic - Fixed-Frequency, Jammers, Generic - Frequency-Hopped, Generic - Continuous.
- **Type**—Indicates the type of Interferer. Click to access a pop-up description of the type.
- **Status**—Indicates Active or Inactive.
  - **Active**—Indicates that the interferer is currently being detected by a spectrum expert.
  - **Inactive**—Indicates that the interferer is no longer detected by a spectrum expert or the spectrum expert that saw the interferer is no longer reachable by the Prime Infrastructure.
- **Discover Time**—Indicates the time of discovery.
- **Affected Channels**—Identifies affected channels.
- **Number of APs Affected**—An access point is listed as Affected if the following conditions are met:
  - The access point is managed by the Prime Infrastructure.
  - The spectrum expert detects the access point.
  - The spectrum expert detects an interferer on the serving channel of the access point.
- **Power**—Indicated in dBm.
- **Duty Cycle**—Indicated in percentage.

<table>
<thead>
<tr>
<th>Note</th>
<th>100% indicates the worst value.</th>
</tr>
</thead>
</table>

- **Severity**—Indicates the severity ranking of the Interferer.

<table>
<thead>
<tr>
<th>Note</th>
<th>100% indicates the worst value where 0 indicates no interference.</th>
</tr>
</thead>
</table>

Interferers Search

Use the Prime Infrastructure Search feature to find specific Interferers or to create and save custom searches. See the Search Methods section in the Cisco Prime Infrastructure 2.0 User Guide for additional information.
Spectrum Experts Details

The Spectrum Expert Details page provides all interference details from a single Spectrum Expert. This page updates every 20 seconds providing a real-time look at what is happening on the remote Spectrum Expert and includes the following items:

- **Total Interferer Count**—As seen by the specific Spectrum Expert.
- **Active Interferers Count Chart**—Displays a pie chart that groups interferes by category.
- **Active Interferer Count Per Channel**—Displays the number of interferes grouped by category on different channels.
- **AP List**—Provides a list of access points detected by the Spectrum Expert that are on channels that have active interferers detected by the Spectrum Expert on those channels.
- **Affected Clients List**—Provides a list of clients that are currently authenticated/associated to the radio of one of the access points listed in the access point list.

Monitoring WiFi TDOA Receivers

To monitor Wi-Fi TDOA receivers, follow these steps:

**Step 1** Choose Monitor > WiFi TDOA Receivers. The WiFi TDOA Receiver summary page appears showing all mapped WiFi TDOA receivers.

**Step 2** To refine the search criteria when an extensive lists appears, you can search by MAC address or location sensor name.

- **a.** To initiate a search for a TDOA receiver by its MAC address, click the Advanced Search link in the Prime Infrastructure. Choose WiFi TDOA Receiver from the Search Category drop-down list and MAC Address from the Search by drop-down list. Enter the MAC address of the TDOA receiver in the available text box, and click Search.

- **b.** To initiate a search for a TDOA receiver by its name, click the Advanced Search link in the Prime Infrastructure. Choose WiFi TDOA Receiver from the Search Category drop-down list and WiFi TDOA Receivers from the Search by drop-down list. Enter the name of the TDOA receiver in the available text box, and click Search.

If no match exists, then a message indicating that appears in the page. Otherwise the search result displays.

The WiFi TDOA Receivers page displays the following information:

- **MAC Address**
- **WiFi TDOA Receiver Name**
- **Static IP**—Static IP address of the WiFi TDOA receiver.
- **Oper Status**—Up or down.
- **Map Location**—Click the Map Location link to view the floor map for this WiFi TDOA receiver. See “Monitoring Floor Area” for more information on the Prime Infrastructure floor maps.
Monitoring Media Streams

To monitor the media streams configurations, follow these steps:

Step 1  Choose **Monitor > Media Streams**. The Media Streams page appears showing the list of media streams configured across controllers.

The Media Streams page contains a table with the following columns:

- **Stream Name**—Media Stream name.
- **Start IP**—Starting IP address of the media stream for which the multicast direct feature is enabled.
- **End IP**—Ending IP address of the media stream for which the multicast direct feature is enabled.
- **State**—Operational state of the media stream.
- **Max Bandwidth**—Indicates the maximum bandwidth that is assigned to the media stream.
- **Priority**—Indicates the priority bit set in the media stream. The priority can be any number from 1 to 8. A lower value indicates a higher priority. For example, a priority of 1 is highest and a value of 8 is the lowest.
- **Violation**—Indicates the action to performed in case of a violation. The possible values are as follows:
  - Drop—Indicates that a stream is dropped on periodic revaluation.
  - Best Effort—Indicates that a stream is demoted to best-effort class on periodic reevaluations.
- **Policy**—Indicates the media stream policy. The possible values are Admit or Deny.
- **Controllers**—Indicates the number of controllers that use the specified media stream.
- **Clients**—Indicates the number of clients that use the specified media stream.

Step 2  To view the media stream details, click a media stream name in the Stream column. The Media Streams page appears.

The Media Streams page displays the following group boxes:

- **Media Stream Details**—Displays the media stream configuration information. This includes the Name, Start Address, End Address, Maximum Bandwidth, Operational Status, Average Packet Size, RRC Updates, Priority, and Violation.
- **Statistics**—Displays the number of controllers and number of clients that use the selected media stream. Click the controller count to access the list of controllers that use the selected media stream.
- **Error**—Displays the error, Worst AP, and corresponding floor map for that AP.
- **Client Counts**—Displays the number of clients for each period.
- **Failed Client Counts**—Displays the number of clients that failed for each period.
The client information is presented in a time-based graph. For graphs that are time-based, there is a link bar at the top of the graph page that displays 6h, 1d, 1w, 2w, 4w, 3m, 6m, 1y, and Custom. When selected, the data for that time frame is retrieved and the corresponding graph is displayed.

### Monitoring Radio Resource Management (RRM)

The operating system security solution uses the Radio Resource Management (RRM) function to continuously monitor all nearby access points, automatically discover rogue access points. Radio Resource Management (RRM), built into the Cisco Unified Wireless Network, monitors and dynamically corrects performance issues found in the RF environment.

Prime Infrastructure would receive traps whenever a change in the transmit power of the access point or channel occurred. These trap events or similar events such as RF regrouping were logged into the Prime Infrastructure events as informational and were maintained by the event dispatcher. The reason behind the transmit power or channel changes (such as signals from neighboring access points, interference, noise, load, and the like) were not evident. You could not view these events and statistics to then perform troubleshooting practices.

Radio Resource Management (RRM) statistics helps to identify trouble spots and provides possible reasons for channel or power level changes. The dashboard provides network-wide RRM performance statistics and predicts reasons for channel changes based on grouping the events together (worst performing access points, configuration mismatch between controllers in the same RF group, coverage holes that were detected by access points based on threshold, pre-coverage holes that were detected by controllers, ratios of access points operating at maximum power, and so on).

---

### Channel Change Notifications

Notifications are sent to the Prime Infrastructure RRM dashboard when a channel change occurs. Channel changes depend on the Dynamic Channel Assignment (DCA) configuration where the mode can be set to auto or on demand. When the mode is auto, channel assignment is periodically updated for all lightweight access points which permit this operation. When the mode is set to on demand, channel assignments are updated based on request. If the DCA is static, no dynamic channel assignments occur, and values are set to their global default.

When a channel change trap is received and a channel change had occurred earlier, the event is marked as Channel Revised; otherwise, the event is marked as Channel Changed. Each event for channel change can be caused by multiple reasons. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur. For example, suppose a channel change is caused by signal,
interference, or noise. When the reason code is received in the notification, the reason code is refactored across the reasons. If three reasons caused the event to occur, the reason code is refactored to 1/3 or 0.33 per reason. If ten channel change events are received with the same reason code, all of the three reasons are equally factored to determine the cause of the channel change.

**Transmission Power Change Notifications**

Notifications are sent to the Prime Infrastructure RRM dashboard when transmission power changes occur. Each event for transmit power changes is caused by multiple reasons. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur.

**RF Grouping Notifications**

When RRM is run on the controller, dynamic grouping is done, and a new group leader is chosen. Dynamic grouping has three modes: Automatic, Off and Leader. When the grouping is Off, no dynamic grouping occurs, and each switch optimizes only its own lightweight access point parameters. When the grouping is Automatic, switches form groups and elect leaders to perform better dynamic parameter optimization. With grouping automatic, configured intervals (in seconds) represent the period with which the grouping algorithm is run. (Grouping algorithms also run when the group contents change and automatic grouping is enabled.)

**Viewing the RRM Dashboard**

Choose **Monitor > Radio Resource Management** to access the RRM dashboard.

The dashboard is made up of the following parts:

- The RRM RF Group Summary shows the number of different RF groups.

  **Note** To get the latest number of RF Groups, you have to run the configuration sync background task.

- The RRM Statistics portion shows network-wide statistics
- The Channel Change Reason portion shows why channels changed for all 802.11a/b/g/n radios.
  - Signal—The channel changed because it improved the channel quality for some other neighbor radio(s). Improving the channel quality for some other neighbor radio(s) improved the channel plan of the system as evaluated by the algorithm.
  - Wifi Interference
  - Load
  - Radar
  - Noise
  - Persistent Non-Wifi Interference
  - Major Air Quality Event
  - Other
- The Channel Change shows all events complete with causes and reasons.
- The Configuration Mismatch portion shows comparisons between leaders and members.
Chapter 5  Monitoring Devices

Monitoring Radio Resource Management (RRM)

- The Coverage Hole portion rates how severe the coverage holes are and gives their location.
- The Percent Time at Maximum Power shows what percent of time the access points were at maximum power and gives the location of those access points.

The following statistics are displayed:

- Total Channel Changes—The sum total of channel changes across 802.11a/b/g/n radios, irrespective of whether the channel was updated or revised. The count is split over a 24-hour and 7-day period. If you click the percentages link or the link under the 24-hour column, a page with details for that access point only appears.
- Total Configuration Mismatches—The total number of configuration mismatches detected over a 24-hour period.
- Total Coverage Hole Events—The total number of coverage hole events over a 24-hour and 7-day period.
- Number of RF Groups—The total number of RF groups (derived from all the controllers which are currently managed by the Prime Infrastructure).
- Configuration Mismatch—The configuration mismatch over a 24-hour period by RF group with details on the group leader.
- APs at MAX Power—The percentage of access points with 802.11a/n radios as a total percentage across all access points which are at maximum power. The maximum power levels are preset and are derived with reference to the preset value.

Note Maximum power is shown in three areas of the RRM dashboard. This maximum power portion shows the current value and is poll driven.

- Channel Change Causes—A graphical bar chart for 802.11a/n radios. The chart is factored based on the reason for channel change. The chart is divided into two parts, each depicting the percentage of weighted reasons causing the event to occur over a 24-hour and 7-day period. Each event for channel change can be caused by multiple reasons, and the weight is equally divided across these reasons. The net reason code is factored and equated to one irrespective of the number of reasons for the event to occur.
- Channel Change - APs with channel changes—Each event for channel change includes the MAC address of the lightweight access point. For each reason code, you are given the most channel changes that occurred for the 802.11a/n access point based on the weighted reason for channel events. This count is split over a 24-hour and 7-day period.
- Coverage Hole - APs reporting coverage holes—The top five access points filtered by IF Type 11 a/n which triggered a coverage hole event (threshold based) are displayed.
- Aggregated Percent Max Power APs—A graphical progressive chart of the total percentage of 802.11a/n lightweight access points which are operating at maximum power to accommodate coverage holes events. The count is split over a 24-hour and 7-day period.

Note This maximum power portion shows the values from the last 24 hours and is poll driven. This occurs every 15 minutes or as configured for radio performance.

- Percent Time at Maximum Power—A list of the top five 802.11a/n lightweight access points which have been operating at maximum power.
Monitoring Clients and Users

The Monitor Clients and Users information assists in identifying, diagnosing, and resolving client issues. Using the Monitor Clients and Users feature, you can view a client association history and statistical information. You can also troubleshoot client historical issues. These tools are useful when users complain of network performance as they move throughout a building with their laptop computers. The information might help you assess what areas experience inconsistent coverage and which areas have the potential to drop coverage. See the “Managing Clients” section on page 10-1 for more information.

Monitoring Alarms

- Alarms and Events Overview, page 5-126
- Viewing List of Alarms, page 5-127
- Filtering Alarms, page 5-128
- Viewing Alarm Details, page 5-129
- Viewing Events Related to Alarms, page 5-130
- Modifying Alarms, page 5-130
- Modifying the Alarm Browser, page 5-131
- Viewing the Alarm Summary, page 5-131
- Modifying Alarm Settings, page 5-132
- Working with Alarms, page 5-133
- Monitoring Access Point Alarms, page 5-135
- Monitoring Air Quality Alarms, page 5-135
- Monitoring CleanAir Security Alarms, page 5-136
- Monitoring Email Notifications, page 5-137
- Monitoring Severity Configurations, page 5-137
- Monitoring Cisco Adaptive wIPS Alarms, page 5-138
- Monitoring Cisco Adaptive wIPS Alarm Details, page 5-139

Alarms and Events Overview

An event is an occurrence or detection of some condition in and around the network. For example, it can be a report about radio interference crossing a threshold, the detection of a new rogue access point, or a controller rebooting.
Events are not generated by a controller for each and every occurrence of a pattern match. Some pattern matches must occur a certain number of times per reporting interval before they are considered a potential attack. The threshold of these pattern matches is set in the signature file. Events can then generate alarms which further can generate e-mail notifications if configured as such.

An alarm is a Prime Infrastructure response to one or more related events. If an event is considered of high enough severity (critical, major, minor, or warning), the Prime Infrastructure raises an alarm until the resulting condition no longer occurs. For example, an alarm might be raised while a rogue access point is detected, but the alarm terminates after the rogue has not been detected for several hours.

One or more events can result in a single alarm being raised. The mapping of events to alarms is their correlation function. For example, some IDS events are considered to be network wide so all events of that type (regardless of which access point the event is reported from) map to a single alarm. On the other hand, other IDS events are client-specific. For these, all events of that type for a specific client MAC address map to an alarm which is also specific for that client MAC address, regardless of whether multiple access points report the same IDS violation. If the same kind of IDS violation takes place for a different client, then a different alarm is raised.

A Prime Infrastructure administrator currently has no control over which events generate alarms or when they time out. On the controller, individual types of events can be enabled or disabled (such as management, SNMP, trap controls, and so on).

**Viewing List of Alarms**

Choose **Monitor > Alarms** to access the Alarm Browser page which provides a list of alarms. You can also hover your mouse cursor over **Alarm Browser** on the toolbar at the bottom of the Prime Infrastructure page to view the Alarm Browser page.

The Alarm Browser lists the following information for each alarm:

- **Severity**—Severity of the alarm which can be:
  - Critical
  - Major
  - Minor
  - Warning
  - Informational
- **Status**—Status of the alarm.
- **Timestamp**—Date and time that the alarm occurred.
- **Category**—Category assigned to the alarm such as rogue AP, controller, switch, and security.
- **Condition**—Condition that caused the alarm.
- **Owner**—Name of the person to whom this alarm is assigned, if one was entered.
- **Message**—Messages about the alarm.
- **Failure Source**—Indicates the source of the event (including name and/or MAC address).

---

**Note**

By default, acknowledged alarms are not shown in the Alarm Browser page. To change this, choose **Administration > Settings > Alarms**, then unselect the *Hide Acknowledged Alarms* check box. You must unselect the preference of hiding acknowledged alarms if you want acknowledged alarms to show in the Prime Infrastructure Alarm Summary and alarms lists page.
Use the check box to select one or more alarms. To select all alarms displayed in the Alarm Browser, click the topmost box. See the “Modifying Alarms” section on page 5-130 for more information.

**Filtering Alarms**

In the Monitor > Alarms page, you can filter the alarms that are displayed in the Alarm Browser. Choose Monitor > Alarms, then from the Show drop-down list, select one of the following filters:

- **Quick Filter**—Enter text in any of the boxes to display alarms that contain the text you enter. For example, if you enter AP in the Category field, AP and Rogue AP alarms are displayed. It provides an optional filtered view of alarms for wired and wireless alarms.

- **Advance Filter**—This filter provides an advanced alarm search capability. It provides ability to search on specific fields with various conditions like contains, does not contain, starts with, ends with and so on. Additionally advanced filters allows nesting of AND/OR conditions. Select the category and operator, enter criteria in the text field to compare against, then do the following:
  - Click + to add an additional filter or - to remove a filter you specified.
  - Click Go to apply your filter.
  - Click Clear Filter to clear the entries you entered.
  - Click the disc icon to save your filter. Enter a name for the filter you want to save, then click Save.

**Note**  When you select a preset filter and click the filter button, the filter criteria is dimmed. You can only see the filter criteria but you can not change it. When All is selected to view all the entries, clicking the filter button shows the Quick Filter options, where you can filter the data using the filterable fields. You can also use the free-form box to enter text to filter the table.

- All—Displays all alarms.
- Manage Preset Filter—Displays any previously saved filters and allows you to edit and delete previously saved filters.
- Assigned to Me—Displays all alarms assigned to you.
- Unassigned Alarms—Displays all unassigned alarms.
- Alarms in Last 5 Minutes
- Alarms in Last 15 Minutes
- Alarms in Last 30 Minutes
- Alarms in the last hour
- Alarms in the last 8 hours
- Alarms in the last 24 hours
- Alarms in last 7 days
- All wired alarms—Displays all alarms for wired devices.
- All wireless alarms—Displays all alarms for wireless devices.
Viewing Alarm Details

You can view alarm details in the Monitor > Alarms page by clicking the expand icon to the far left of the Monitor > Alarms page for the alarm for which you want to see details. The details that are displayed depend on the alarm type you selected (see Table 5-64).

Table 5-64 Viewing Alarm Details

<table>
<thead>
<tr>
<th>Section</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Info</td>
<td>Failure Source</td>
<td>Indicates the source of the event (including name and/or MAC address).</td>
</tr>
<tr>
<td></td>
<td>Owner</td>
<td>Name of person to which this alarm is assigned, or blank.</td>
</tr>
<tr>
<td></td>
<td>Acknowledged</td>
<td>Displays whether or not the alarm is acknowledged by the user.</td>
</tr>
<tr>
<td></td>
<td>Category</td>
<td>The category of the alarm (for example, AP, Rogue AP, or Security).</td>
</tr>
<tr>
<td></td>
<td>Created</td>
<td>Month, day, year, hour, minute, second, AM or PM alarm created.</td>
</tr>
<tr>
<td></td>
<td>Modified</td>
<td>Month, day, year, hour, minute, second, AM or PM alarm last modified.</td>
</tr>
<tr>
<td></td>
<td>Generated By</td>
<td>Device that generated the alarm.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Level of security: Critical, Major, Minor, Warning, Clear, Info.</td>
</tr>
<tr>
<td></td>
<td>Previous Severity</td>
<td>The severity of the alarm the after the most recent polling cycle.</td>
</tr>
<tr>
<td>Device Info</td>
<td>Device Name</td>
<td>Name of the device.</td>
</tr>
<tr>
<td></td>
<td>Device Address</td>
<td>IP address of the device.</td>
</tr>
<tr>
<td></td>
<td>Device Contact</td>
<td>Contact information for the device.</td>
</tr>
<tr>
<td></td>
<td>Device Location</td>
<td>Location of the device.</td>
</tr>
<tr>
<td></td>
<td>Device Status</td>
<td>Status of the device.</td>
</tr>
<tr>
<td>Messages</td>
<td></td>
<td>Device information retrieved from log messages.</td>
</tr>
<tr>
<td>Annotation</td>
<td></td>
<td>Lists current notes regarding this rogue access point. To add a new note,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>click New Annotation. Type the note and click Post to save and display the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>note or Cancel to close the page without saving the note.</td>
</tr>
</tbody>
</table>

1. The General information might vary depending on the type of alarm. For example, some alarm details might include location and switch port tracing information.

In the Alarms list page, you can also view the events for the alarm you selected as explained in the “Viewing Events Related to Alarms” section on page 5-130.
Viewing Events Related to Alarms

When you select Monitor > Alarms page, you can view alarm summary information by hovering your mouse cursor over an alarm severity in the Severity column and clicking the icon that appears.

A dialog appears displaying the top 5 events related to the alarm you selected.

Click **Events** to display all events associated with the selected alarm.

Modifying Alarms

In the Monitor > Alarms page, you can modify the alarms by selecting the check box next to an alarm and then clicking one of the tasks at the top of the Alarm Browser page:

**Note**

The alarms that appear in the Monitor > Alarms page depend on the settings you specify on the Administration > Settings page. See the “Modifying Alarm Settings” section on page 5-132 for more information.

- **Change Status**—Change the alarm status to one of the following:
  - **Acknowledge**—You can acknowledge the alarm. By default, acknowledged alarms are not displayed in the Alarm Browser page. Acknowledged alarms remain in the Prime Infrastructure and you can search for all acknowledged alarms using the alarm search functionality. See the “Acknowledging Alarms” section on page 5-134 for more information.
  - **Unacknowledge**—You can choose to unacknowledge an already acknowledged alarm.
  - **Clear**—Clear the selected alarm(s). The alarm is removed from the Alarm Browser. Cleared alarms remain in the Prime Infrastructure and you can search for all cleared alarms using the alarm search functionality.

- **Assign**—For the selected alarm, you can do the following:
  - **Assign to me**—Assigns the alarm to the specified user.
  - **Unassign**—Removes the specified owner from the alarm.

- **Annotation**—Enter an annotation for the selected alarm, then click **Post**. The annotation you entered appears when you view the alarm details.

- **Delete**—Delete the selected alarm(s). Indicates that the alarm is no longer detected by any device.

Specifying Email Notifications for Alarms

In the Monitor > Alarms page, you can set up e-mail notifications for alarms based on the alarm category and severity level.

**Step 1** Choose **Monitor > Alarms**, then click **Email Notification**.
Step 2  Select the **Enable** check box next to the alarm category for which you want to set up e-mail notifications, then click **Save**.

Prime Infrastructure sends e-mail notifications when alarms for the categories you specified occur.

---

### Modifying the Alarm Browser

Choose **Monitor > Alarms** to view a list of alarms. You can also click **Alarm Browser** on the toolbar at the bottom of the Prime Infrastructure home page. You can modify the following information displayed in the Alarm Browser:

- To reorder the columns, drag and drop the column headings into any position.
- Click a column heading to sort the information by that column. By default, the column is sorted in descending order. Click the column heading again to change the sort the column in ascending order.

**Note**  Not every column is sortable. Hover your mouse cursor over a column heading, and the Prime Infrastructure displays whether the column is sortable.

- To customize which columns are displayed, click the **Settings** icon, then click **Columns**. Select the check box next to columns you want to appear, and unselect the boxes for the columns you do not want to appear in the Alarm Browser page.

### Viewing the Alarm Summary

When the Prime Infrastructure receives an alarm message from a controller, switch, or Prime Infrastructure, it displays an alarm indicator in the Alarm Summary. The Alarm Summary is at the bottom of the Prime Infrastructure home page and displays the total count of critical, major, and minor alarms currently detected by the Prime Infrastructure. Hover your mouse cursor over the Alarm Summary, and the alarm details are displayed.

**Note**  The alarms that appear in the Alarm Summary and Monitor > Alarms pages depend on the settings you specify in the Administration > Settings page. By default, acknowledged alarms are not shown. See the “Modifying Alarm Settings” section on page 5-132 for more information.

Alarms are color coded as follows:

- Red—Critical Alarm
- Orange—Major Alarm
- Yellow—Minor Alarm

Alarms indicate the current fault or state of an element, and alarms are usually generated by one or more events. The alarm can be cleared but the event remains. See the “Alarms and Events Overview” section on page 5-126 for more information about alarms.

**Note**  By default, alarm counts refresh every minute. You can modify when alarms are refreshed in the Administration > User Preferences page.
When you hover your mouse cursor over the Alarm Summary, a pop-up page appears listing the number of critical, major, and minor alarms for each of alarm category. You can specify which alarm categories are displayed in the Alarm Summary on the Administration > User Preferences page. By default, all categories are displayed:

- **Alarm Summary**—Displays a summary of the total alarms for all alarm categories.
- **AP**—Displays counts for AP alarms such as AP Disassociated from controller, Thresholds violation for Load, Noise or Interference, AP Contained as Rogue, AP Authorization Failure, AP regulatory domain mismatch, or Radio card Failure.
- **Context Aware Notifications**
- **Controller**—Displays counts for controller alarms, such as reachability problems from the Prime Infrastructure and other controller failures (fan failure, POE controller failure, AP license expired, link down, temperature sensor failure, and low temperature sensed).
- **Coverage Hole**—Displays counts for coverage hole alarms generated for access points whose clients are not having enough coverage set by thresholds. See the “Monitoring Maps” section on page 6-1 for more information.
- **Mesh Links**—Displays counts for mesh link alarms, such as poor SNR, console login, excessive parent change, authorization failure, or excessive association failure.
- **Mobility Services**—Displays counts for location alarms such as reachability problems from the Prime Infrastructure and location notifications (In/Out Area, Movement from Marker, or Battery Level).
- **Prime Infrastructure**—Displays counts for the Prime Infrastructure alarms.
- **Performance**—Displays counts for performance alarms.
- **Rogue AP**—Displays counts for malicious rogue access points alarms.
- **Rogue Adhoc**—Displays counts for unclassified rogue access point alarms.
- **Security**—Displays counts for security alarms such as Signature Attacks, AP Threats/Attacks, and Client Security Events.
- **Switch**—Displays counts for switch alarms such as authentication errors.

### Modifying Alarm Settings

You can modify the following settings for alarms:

- **Alarm count refresh rate**—See the “Modifying Alarm Count Refresh Rate” section on page 5-132.
- **Alarm severity levels**—See the “Configuring Alarm Severity Levels” section on page 5-132.

### Modifying Alarm Count Refresh Rate

By default, alarm counts refresh every minute. You can modify the refresh rate by selecting **Administration > User Preferences**, and then choosing a new value for the Refresh Alarm Count from the Alarm Summary Every menu.

### Configuring Alarm Severity Levels

The Administration > Settings > Severity Configuration page allows you to change the severity level for newly generated alarms.
Note

Existing alarms remain unchanged.

To reconfigure the severity level for a newly generated alarm, follow these steps:

Step 1 Choose Administration > Settings.
Step 2 From the left sidebar menu, choose Severity Configuration.
Step 3 Select the check box of the alarm condition whose severity level you want to change.
Step 4 From the Configure Security Level drop-down list, choose from the following severity levels:
   - Critical
   - Major
   - Minor
   - Warning
   - Informational
   - Reset to Default
Step 5 Click Go.
Step 6 Click OK to confirm the change or Cancel to leave the security level unchanged.

Working with Alarms

You can view, assign, and clear alarms and events on access points and mobility services engine using the Prime Infrastructure.

This section also describes how to have e-mail notifications of alarms sent to you and contains the following topics:

- Assigning and Unassigning Alarms, page 5-133
- Deleting and Clearing Alarms, page 5-134
- Acknowledging Alarms, page 5-134

Assigning and Unassigning Alarms

To assign and unassign an alarm to yourself, follow these steps:

Step 1 Perform an advanced search for access point alarms.
Step 2 Select the alarms that you want to assign to yourself by selecting their corresponding check boxes.

Note To unassign an alarm assigned to you, Unselect the check box next to the appropriate alarm. You cannot unassign alarms assigned to others.

Step 3 From the Select a command drop-down list, choose Assign to Me (or Unassign), and click Go.
If you choose Assign to Me, your username appears in the Owner column. If you choose Unassign, the username column is empty.

**Deleting and Clearing Alarms**

To delete or clear an alarm from a mobility services engine, follow these steps:

**Step 1**
In the Monitor > Alarms page, select the alarms that you want to delete or clear by selecting their corresponding check boxes.

_Note_
If you delete an alarm, the Prime Infrastructure removes it from its database. If you clear an alarm, it remains in the Prime Infrastructure database, but in the Clear state. You clear an alarm when the condition that caused it no longer exists.

**Step 2**
From the Select a command drop-down list, choose Delete or Clear, and click Go.

_Note_
To set up cleanup of old alarms and cleared alarms, choose Administration > Settings > Alarms. See the “Alarm and Event Dictionary” section on page 13-1 for more information.

**Acknowledging Alarms**

You might want certain alarms to be removed from the Alarms List. For example, if you are continuously receiving an interference alarm from a certain access point on the 802.11g interface, you might want to stop that access point from being counted as an active alarm on the Alarm Summary page or any alarms list. In this scenario, you can find the alarm for the 802.11g interface in the Alarms list, select the check box, and choose Acknowledge from the Select a command drop-down list.

Now if the access point generates a new violation on the same interface, the Prime Infrastructure does not create a new alarm, and the Alarm Summary page shows no new alarms. However, if the interference violation is created on another interface, such as 802.11a, a new alarm is created.

By default, acknowledged alarms are not displayed in either the Alarm Summary page or any alarm list page. Also, no e-mail messages generated for these alarms after you have marked them as acknowledged. By default, acknowledged alarms are not included for any search criteria. To change this default, choose to the Administration > Settings > Alarms page and unselect the Hide Acknowledged Alarms check box.

When you acknowledge an alarm, the following warning appears as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled.

_Note_
When you acknowledge an alarm, a warning displays as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled. Choose Administration > User Preferences page to disable this warning message.
You can also search for all previously acknowledged alarms to reveal the alarms that were acknowledged during the last seven days. Prime Infrastructure automatically deletes cleared alerts that are more than seven days old so your results can only show activity for the last seven days. Until an existing alarm is deleted, a new alarm cannot be generated for any managed entity for which the Prime Infrastructure has already generated an alarm.

### Monitoring Access Point Alarms

The Access Point Alarms page displays the access point based alarms on your network.

To access the AP alarms page, do one of the following:

- Perform a search for AP alarms.
- Click the Access Point number link in the Alarm Summary box.

The Monitor AP Alarms page contains the following fields:

- **Severity**—Indicates the severity of the alarm. See Table 5-63 for a list of severity indicator icons.
- **Failure Source**—Device that generated the alarm.
- **Owner**—Name of the person to which this alarm is assigned, or blank.
- **Date/Time**—The time at which the alarm was generated.
- **Message**—The associated message displayed in the Prime Infrastructure alarm browser.
- **Category**—Indicates the category assigned to the alarm such as rogue AP, controller, switch, and security.
- **Condition**—Condition that caused the alarm.
- **Acknowledged**—Displays whether or not the alarm is acknowledged by the user. See the “Acknowledging Alarms” section on page 5-134 for more information.

### Monitoring Air Quality Alarms

The Air Quality Alarms page displays air quality alarms on your network.

To access the air quality alarms page, do one of the following:

- Perform a search for Performance alarms.
- Click the Performance number link in the Alarm Summary box.

The Monitor Air Quality Alarms page contains the following fields:

- **Severity**—Indicates the severity of the alarm. See Table 5-63 for a list of severity indicator icons.
- **Failure Source**—Device that generated the alarm.
- **Owner**—Name of the person to which this alarm is assigned, or blank.
- **Date/Time**—The time at which the alarm was generated.
- **Message**—The associated message displayed in the Prime Infrastructure alarm browser.
- **Acknowledged**—Displays whether or not the alarm is acknowledged by the user. See the “Acknowledging Alarms” section on page 5-134 for more information.
Select a command Menu

Select one or more alarms by selecting their respective check boxes, choose one of the following commands from the Select a command drop-down list, and click Go.

- **Assign to me**—Assign the selected alarm(s) to the current user.
- **Unassign**—Unassign the selected alarm(s).
- **Clear**—Clear the selected alarm(s).
- **Delete**—Delete the selected alarm(s).
- **Acknowledge**—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See the “Acknowledging Alarms” section on page 5-134 for more information.

**Note** The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality.

- **Unacknowledge**—Unacknowledge an already acknowledged alarm.
- **Email Notification**—Takes you to the All Alarms > Email Notification page to view and configure e-mail notifications. See the “Monitoring RFID Tags” section on page 5-112 for more information.

### Monitoring CleanAir Security Alarms

The CleanAir Security Alarms page displays security alarms on your network.

To access the security alarms page, do one of the following:

- Perform a search for Security alarms.
- Click the **Security number** link in the Alarm Summary box.

The Monitor CleanAir Security Alarms page contains the following fields:

- **Severity**—Indicates the severity of the alarm. See Table 5-63 for a list of severity indicator icons.
- **Failure Source**—Device that generated the alarm.
- **Owner**—Name of the person to which this alarm is assigned, or blank.
- **Date/Time**—The time at which the alarm was generated.
- **Message**—The associated message displayed in the Prime Infrastructure alarm browser.
- **Acknowledged**—Displays whether or not the alarm is acknowledged by the user. See the “Acknowledging Alarms” section on page 5-134 for more information.

Select a command Menu

Select one or more alarms by selecting their respective check boxes, choose one of the following commands from the Select a command drop-down list, and click Go.

- **Assign to me**—Assign the selected alarm(s) to the current user.
- **Unassign**—Unassign the selected alarm(s).
- **Clear**—Clear the selected alarm(s).
- **Delete**—Delete the selected alarm(s).
**Monitoring Alarms**

- **Acknowledge**—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See the “Acknowledging Alarms” section on page 5-134 for more information.

  **Note** The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality.

- **Unacknowledge**—Unacknowledge an already acknowledged alarm.

- **Email Notification**—Takes you to the All Alarms > Email Notification page to view and configure e-mail notifications. See the “Monitoring RFID Tags” section on page 5-112 for more information.

### Monitoring Email Notifications

Prime Infrastructure includes a built-in e-mail notification function which can notify the network operator when critical alarms occur.

The Email Notification page allows you to add a filter for each alert category. The severity level is set to critical by default when the alert category is enabled, but you can choose a different severity level for different categories. E-mail notifications are generated only for the severity levels that are configured.

To configure e-mail notifications, follow these steps:

1. **Step 1** Choose Monitor > Alarms from Classic View.
2. Choose Operate > Alarms & Events from Life Cycle View.
3. **Step 2** From the Select a command drop-down list, choose Email Notification.
4. **Step 3** Click Go.
5. **Step 4** Click an Alarm Category to edit severity level and e-mail recipients for its e-mail notifications.
6. **Step 5** Select the severity level check box(es) (Critical, Major, Minor, or Warning) for which you want a notification sent.
7. **Step 6** Enter the notification recipient e-mail addresses in the To text box.

  **Note** Separate multiple e-mail addresses with a comma.

8. **Step 7** Click OK.
9. **Step 8** Select the Enabled check box for applicable alarm categories to activate the delivery of e-mail notifications.
10. **Step 9** Click OK.

### Monitoring Severity Configurations

You can change the severity level for newly generated alarms.
Note

Existing alarms remain unchanged.

To change the severity level of newly-generated alarms, follow these steps:

Step 1  Choose Administration > Setting.
Step 2  Choose Severity Configuration from the left sidebar menu.
Step 3  Select the check box of the alarm condition for which you want to change the severity level.
Step 4  From the Configure Severity Level drop-down list, choose the new severity level (Critical, Major, Minor, Warning, Informational, Reset to Default).
Step 5  Click Go.
Step 6  Click OK to confirm the change.

Monitoring Cisco Adaptive wIPS Alarms

Alarms from Cisco Adaptive wIPS DoS (denial of service) and security penetration attacks are classified as security alarms. You can view these wIPS alarms and their details in the Monitor > Alarms page.

To view a list of wIPS DoS and security penetration attack alarms, follow these steps:

Step 1  Perform a search for Security alarms using the Advanced Search feature.
The following information is provided for wIPS alarms:
  • Severity—Severity levels include critical, major, info, warning, and clear.
  • Failure Object—Displays the name and IP or MAC address of the object for which the alarm was generated. Click the Failure Object to view alarm details. See the “Monitoring Cisco Adaptive wIPS Alarm Details” section on page 5-139 for more information on viewing wIPS alarm details.
  • Date/Time—Displays the date and time that the alarm occurred.
  • Message—Displays a message explaining why the alarm occurred (such as the applicable wIPS policy).
  • Acknowledged—Displays whether or not the alarm is acknowledged by the user.
  • Category—Indicates the category of this alarm such as Security.
  • Condition—Displays a description of what caused this alarm to be triggered.

When there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

To add, remove, or reorder columns in the table, click the Edit View link to go to the Edit View page.

Select a command

Using the Select a command drop-down list, you can perform the following actions on the selected alarms:
  • Assign to me—Assign the selected alarm(s) to the current user.
• **Unassign**—Unassign the selected alarm(s).
• **Delete**—Delete the selected alarm(s).
• **Clear**—Clear the selected alarm(s).
• **Acknowledge**—You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality.
• **Unacknowledge**—You can choose to unacknowledge an already acknowledged alarm.
• **Email Notification**—Takes you to the All Alarms > Email Notification page to view and configure e-mail notifications.

To perform an action on the selected alarm, follow these steps:

1. **Step 1** Select an alarm by selecting its check box.
2. **Step 2** From the Select a command drop-down list, select the applicable command.
3. **Step 3** Click **Go**.

### Monitoring Cisco Adaptive wIPS Alarm Details

Choose **Monitor > Alarms > failure object** to view details of the selected Cisco wIPS alarm. The following Alarm details are provided for Cisco Adaptive wIPS alarms:

- **General**
  - Detected By wIPS AP—The access point that detected the alarm.
  - wIPS AP IP Address—The IP address of the wIPS access point.
  - Owner—Name of person to which this alarm is assigned or left blank.
  - Acknowledged—Displays whether or not the alarm is acknowledged by the user.
  - Category—For wIPS, the alarm category is Security.
  - Created—Month, day, year, hour, minute, second, AM or PM that the alarm was created.
  - Modified—Month, day, year, hour, minute, second, AM or PM that the alarm was last modified.
  - Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
    - NMS (Network Management System - Prime Infrastructure)—Generated through polling.
    - Prime Infrastructure periodically polls the controllers and generates events. Prime Infrastructure generates events when the traps are disabled or when the traps are lost for those events. In this case, “Generated by” is NMS.
    - Trap—Generated by the controller. Prime Infrastructure process these traps and raises corresponding events for them. In this case, “Generated by” is Controller.
  - Severity—Level of severity including critical, major, info, warning, and clear.
  - Last Disappeared—The date and time that the potential attack last disappeared.
  - Channel—The channel on which the potential attack occurred.
  - Attacker Client/AP MAC—The MAC address of the client or access point that initiated the attack.
- Attacker Client/AP IP Address—The IP address of the client or access point that initiated the attack.
- Target Client/AP IP Address—The IP address of the client or access point targeted by the attacker.
- Controller IP Address—The IP address of the controller to which the access point is associated.
- MSE—The IP address of the associated mobility services engine.
- Controller MAC address—The MAC address of the controller to which the access point is associated.
- wIPS access point MAC address
- Forensic File
- Event History—Takes you to the “Monitoring Alarms” page to view all events for this alarm.

• Annotations—Enter any new notes in this text box, and click Add to update the alarm. Notes are displayed in the “Annotations” display area.
• Messages—Displays information about the alarm.
• Audit Report—Click to view config audit alarms details. This report is only available for Config Audit alarms. Configuration audit alarms are generated when audit discrepancies are enforced on config groups.

Note
If enforcement fails, a critical alarm is generated on the config group. If enforcement succeeds, a minor alarm is generated on the config group. The alarms have links to the audit report where you can view a list of discrepancies for each controller.

• Rogue Clients—If the failure object is a rogue access point, information about rogue clients is displayed.

Select a command

Select one or more alarms by selecting their respective check boxes, and click Go.

• Assign to me—Assign the selected alarm(s) to the current user.
• Unassign—Unassign the selected alarm(s).
• Delete—Delete the selected alarm(s).
• Clear—Clear the selected alarm(s).
• Acknowledge—You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality.
• Unacknowledge—You can choose to unacknowledge an already acknowledged alarm.
• Email Notification—Takes you to the All Alarms > Email Notification page to view and configure e-mail notifications.
• Event History—Takes you to the Monitor Alarms > Events page to view events for Rogue Alarms.
Monitoring Events

One or more events might generate an abnormal state or alarm. The alarm can be cleared, but the event remains. Choose Monitor > Events to access the Events page, which displays the following information:

- **Description**—Describes the event details.
- **Time**—Indicates the date and time the event was generated.
- **Severity**—Event severities include: Critical, Major, Minor, Warning, Cleared, or Information.
- **Failure Source**—Indicates the source of the event (including name and/or MAC address).
- **Category**—Type of event such as Rogue AP, Security, or AP.

Click any column heading to sort by that column.

Use the quickview icon to disclose more information on the event. The additional information for the event is divided into general information and the message. In the general information, the failure source, the category, severity, generated time and IP address. The message of the event is also displayed.

---

**Note**

Events also has preset, quick and advanced filters similar to alarms. These filters work in same way as the filters in alarms.

When you filter the table using the Search feature, the Events page might display the additional information. The additional information includes the following:

- **Coverage Hole Events**
  - Access Point Name
  - Failed Clients—Number of clients that failed due to the coverage hole.
  - Total Clients—Total number of clients affected by the coverage hole.
  - Radio Type—The radio type (802.11b/g or 802.11a) of the applicable access point.
  - Coverage Threshold

- **Rogue AP Events**
  - Vendor—Rogue access point vendor name or Unknown.
  - Classification Type—Indicates the type of rogue access point including Malicious, Friendly, or Unclassified.
  - On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
  - Radio Type—Lists all radio types applicable to this rogue access point.
  - State—Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
  - SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
Chapter 5  Monitoring Devices

Monitoring Events

Note  See the “Monitoring Rogue Alarm Events” section on page 5-109 or the “Viewing Rogue AP Event Details” section on page 5-109 for more information on rogue access points events.

- Adhoc Rogue Events
  - Vendor—Rogue access point vendor name or Unknown.
  - On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
  - Radio Type—Lists all radio types applicable to this rogue access point.
  - State—Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
  - SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Interference
  - Detected By—IP address of the device that detected the interference.
  - ID—ID of the device that detected the interference.
- Mesh Links
- Context Aware Notification
- Pre Coverage Hole
  - Client MAC Address—MAC address of the client affected by the Pre Coverage Hole.
  - AP MAC Address—MAC address of the applicable access point.
  - Radio Type—The radio type (802.11b/g or 802.11a) of the applicable access point.
  - Power Level—Access Point transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, 5 = 0.195 to 6.25% power).
  - Client Type—Client type can be laptop(0), pda(2), dot11mobilephone(3), dualmodephone(4), wgb(5), scanner(6), tabletpc(7), printer(8), projector(9), videoconfsystem(10), camera(11), gamingsystem(12), dot11deskphone(13), cashregister(14), radiotag(15), rfidsensor(16), server(17)
  - WLAN Coverage Hole Status

If there is more than one page of events, the number of pages is displayed with a scroll arrow on each side. Use this to view additional events.

- Searching Events, page 5-143
- Monitoring Failure Objects, page 5-143
- Monitoring Events for Rogue APs, page 5-143
- Viewing Ad hoc Rogue Event Details, page 5-111
- Monitoring Cisco Adaptive wIPS Events, page 5-145
Searching Events

Use the Prime Infrastructure Search feature to find specific events or to create and save custom searches. See the Search Methods section in the Cisco Prime Infrastructure 2.0 User Guide for additional information.

Monitoring Failure Objects

Note

The event categories Location Servers and Location Notifications appear only in the Cisco NCS Location version.

Choose Monitor > Events, then click the expand icon to the far left of the Monitor > Events page for the event for which you want to see details. Details about the event are displayed. Depending on the type of event you selected, the associated details vary.

- General Info
  - Failure Source—Indicates the source of the event (including name and/or MAC address).
  - Category—Type of alarm such as Security or AP.
  - Generated—Date and time that the event was generated.
  - Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
  
  NMS (Network Management System - Prime Infrastructure)—Generated through polling. Prime Infrastructure periodically polls the controllers and generates events. Prime Infrastructure generates events when the traps are disabled or when the traps are lost for those events. In this case, “Generated by” is NMS.
  
  Trap—Generated by the controller. Prime Infrastructure process these traps and raises corresponding events for them. In this case, “Generated by” is Controller.
  - Device IP Address—IP address of the alarm-generating device.
  - Severity—Level of severity including critical, major, info, warning, and clear.
- Messages—Message explaining why the event occurred.

Monitoring Events for Rogue APs

Choose Monitor > Events. Click an item in the Description column to display the alarm events for a rogue access point radio. Rogue access point radios are unauthorized access points detected by controllers. The following fields appear:

General

- Rogue MAC Address
- Vendor
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
Monitoring Events

- Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.

- Owner—Name of person to which this alarm is assigned, or (blank).

- State—State of this radio relative to the network or Port. Rogue access point radios appear as “Alert” when first scanned by the Port, or as “Pending” when operating system identification is still underway.

- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

- Containment Level—An access point which is being contained is either unable to provide service at all, or provides exceedingly slow service. There is a level associated with the containment activity which indicates how many Cisco 1000 series lightweight access points to use in containing the threat. This service must be initiated and halted by the administrator. Containment Type - Contained if the rogue access point clients have been contained at Level 1 through Level 4 under Update Status, otherwise Unassigned.

- Channel—Indicates the band at which the ad hoc rogue is broadcasting.

- Radio Type—Lists all radio types applicable to this rogue access point.

- Created—Date and time that the event occurred.

- Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
  - NMS (Network Management System - Prime Infrastructure)—Generated through polling. Prime Infrastructure periodically polls the controllers and generates events. Prime Infrastructure generates events when the traps are disabled or when the traps are lost for those events. In this case, “Generated by” is NMS.
  - Trap—Generated by the controller. Prime Infrastructure process these traps and raises corresponding events for them. In this case, “Generated by” is Controller.

- Device IP Address—IP address of the alarm-generating device.


Message—Displays descriptive information about the alarm.
Help—Displays information about the alarm.

Note
Use the Advance Search feature to find specific events. See the Search Methods section in the Cisco Prime Infrastructure 2.0 User Guide for more information.

Monitoring Events for Ad hoc Rogues

Choose Monitor > Events. Click an item in the Description column to display ad hoc rogue event details.

General
- Rogue MAC Address
- Vendor
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
– Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.

• Owner—Name of person to which this alarm is assigned, or (blank).

• State—State of this radio relative to the network or Port. Rogue access point radios appear as “Alert” when first scanned by the Port, or as “Pending” when operating system identification is still underway.

• SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

• Containment Level—An access point which is being contained is either unable to provide service at all, or provides exceedingly slow service. There is a level associated with the containment activity which indicates how many Cisco 1000 series lightweight access points to use in containing the threat. This service must be initiated and halted by the administrator. Containment Type - Contained if the rogue access point clients have been contained at Level 1 through Level 4 under Update Status, otherwise Unassigned.

• Channel—Indicates the band at which the ad hoc rogue is broadcasting.

• Created—Date and time that the event occurred.

• Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
  – NMS (Network Management System - Prime Infrastructure)—Generated through polling. Prime Infrastructure periodically polls the controllers and generates events. Prime Infrastructure generates events when the traps are disabled or when the traps are lost for those events. In this case, “Generated by” is NMS.
  – Trap—Generated by the controller. Prime Infrastructure process these traps and raises corresponding events for them. In this case, “Generated by” is Controller.

• Device IP Address—IP address of the alarm-generating device.


Message—Displays descriptive information about the alarm.

Help—Displays information about the alarm.

**Monitoring Cisco Adaptive wIPS Events**

Choose **Monitor > Events** to view wIPS events. One or more events might generate an abnormal state or alarm. The alarm can be cleared, but the event remains. For more information regarding monitoring events, see the “Monitoring Events” section on page 5-141.

The following sections provide additional information regarding Cisco Adaptive wIPS:

- Configuring wIPS Profiles
- Prime Infrastructure Services
- wIPS Policy Alarm Encyclopedia

Perform an events search to narrow the results to mobility services engine or Security events only. To view mobility services engine or Security events, choose **Monitor > Events**.

**Note** If there is more than one page of events, the number of pages is displayed with a scroll arrow on each side. Use this to view additional events.
Monitoring CleanAir Air Quality Events

You can use the Prime Infrastructure to view the events generated on the air quality of the wireless network.

To view air quality events, follow these steps:

1. Click **Advanced Search** in the Prime Infrastructure.
   The New Search page appears.
2. In the New Search page, choose **Events** from the Search Category drop-down list.
3. From the Severity drop-down list, choose the type of severity you want to search the air quality events.
4. From the Event Category drop-down list, choose **Performance**.
5. Click **Go**.

   The air quality events page displays the following information:
   - **Severity**—Indicates the severity of the alarm. See Table 5-63 for a list of severity indicator icons.
   - **Failure Source**—Device that generated the alarm.
   - **Date/Time**—The time at which the alarm was generated.

Viewing Air Quality Event Details

To view air quality event details, follow these steps:

1. From the Air Quality Events page, click an item under Failure Source to access the alarm details page.
   See the “Monitoring CleanAir Air Quality Events” section on page 5-146.
2. The air quality event page displays the following information:
   - **Failure Source**—Device that generated the alarm.
   - **Category**—The category this event comes under. In this case, Performance.
   - **Created**—The time stamp at which the event was generated.
   - **Generated by**—The device that generated the event.
   - **Device IP Address**—The IP address of the device that generated the event.
   - **Severity**—The severity of the event.
   - **Alarm Details**—A link to the related alarms associated with this event. Click the link to learn more about the alarm details.
   - **Message**—Describes the air quality index on this access point.

Monitoring Interferer Security Risk Events

You can use the Prime Infrastructure to view the security events generated on your wireless network.

To view interferer security events, follow these steps:

1. Click **Advanced Search** in the Prime Infrastructure.
The New Search page appears.

**Step 2**  In the New Search page, choose **Events** from the Search Category drop-down list.

**Step 3**  From the Severity drop-down list, choose the type of severity you want to search the air quality events.

**Step 4**  From the Event Category drop-down list, choose **Security**.

**Step 5**  Click **Go**.

The interferer security events page displays the following information:

- **Severity**—Indicates the severity of the alarm. See Table 5-63 for a list of severity indicator icons.
- **Failure Source**—Device that generated the alarm.
- **Date/Time**—The time at which the alarm was generated.

---

**Viewing Interferer Security Risk Event Details**

To view interferer security event details, follow these steps:

**Step 1**  In the Interferer Security Event details page, click an item under Failure Source to access the alarm details page. See the “Monitoring Interferer Security Risk Events” section on page 5-146.

**Step 2**  The air quality event page displays the following information:

- **Failure Source**—Device that generated the alarm.
- **Category**—The category this event comes under. In this case, Security.
- **Created**—The time stamp at which the event was generated.
- **Generated by**—The device that generated the event.
- **Device IP Address**—The IP address of the device that generated the event.
- **Severity**—The severity of the event.
- **Alarm Details**—A link to the related alarms associated with this event. Click the link to know more about the alarm details.
- **Message**—Describes the interferer device affecting the access point.

---

**Monitoring Health Monitor Events**

You can use the Prime Infrastructure to view the events generated by the Health Monitor.

To view the health monitor events, follow these steps:

**Step 1**  Click **Advanced Search** in the Prime Infrastructure.

The New Search page appears.

**Step 2**  In the New Search page, choose **Events** from the Search Category drop-down list.

**Step 3**  From the Severity drop-down list, choose the type of severity you want to search the health monitor events.
Step 4  From the Event Category drop-down list, choose the **Prime Infrastructure**.

Step 5  Click Go.

The Health Monitor Events page displays the following information:
- Severity—Indicates the severity of the alarm. See Table 5-63 for a list of severity indicator icons.
- Failure Source—Device that generated the alarm.
- Date/Time—The time at which the alarm was generated.
- Message—Describes the health details.

---

**Viewing Health Monitor Event Details**

To view health monitor event details, follow these steps:

**Step 1**  In the Health Monitor Events page, click an item under Failure Source to access the alarm details page. See the “**Monitoring Health Monitor Events**” section on page 5-147.

**Step 2**  The Health Monitor Events page displays the following information:
- Failure Source—Device that generated the alarm.
- Category—The category this event comes under. In this case, Prime Infrastructure.
- Created—The time stamp at which the event was generated.
- Generated by—The device that generated the event.
- Device IP Address—The IP address of the device that generated the event.
- Severity—The severity of the event.
- Alarm Details—A link to the related alarms associated with this event. Click the link to know more about the alarm details.
- Message—Describes the event through a message.

---

**Working with Events**

You can use the Prime Infrastructure to view mobility services engine and access point events. You can search and display events based on their severity (critical, major, minor, warning, clear, info) and event category or you can search for a mobility services engine and access point by its IP address, MAC address or name.

A successful event search displays the event severity, failure object, date and time of the event, and any messages for each event.

To display events, follow these steps:

**Step 1**  In the Prime Infrastructure, click **Monitor > Events**.

**Step 2**  In the Events page:
• If you want to display the events for a specific element and you know its IP address, MAC address, or Name, enter that value in the Quick Search text box (left pane). Click Go.

• To display events by severity and category, choose the appropriate options from the Severity and Event Category drop-down lists (left pane). Click Search.

Step 3  If the Prime Infrastructure finds events that match the search criteria, it displays a list of these events.

Note  For more information about an event, click the failure object associated with the event. Additionally, you can sort the events summary by each of the column headings.

---

**Monitoring Site Maps**

Maps provide a summary view of all your managed systems on campuses, buildings, outdoor areas, and floors. With the Prime Infrastructure database, you can add maps and view your managed system on realistic campus, building, and floor maps. See the “Monitoring Maps” section on page 6-1 for more information.

**Monitoring Google Earth Maps**

You can enable location presence by mobility server to provide expanded Civic (city, state, postal code, country) and GEO (longitude, latitude) location information beyond the Cisco default setting (campus, building, floor, and X, Y coordinates). This information can then be requested by clients on a demand basis for use by location-based services and applications. Location Presence can be configured when a new campus, building, floor, or outdoor area is being added or configured at a later date. See the “Monitoring Google Earth Maps” section on page 6-78 for more information.
Monitoring Maps

This chapter describes how to add and monitor maps. It contains the following sections:

- About Maps, page 6-1
- Adding a Campus Map, page 6-2
- Adding a Building to a Campus Map, page 6-3
- Adding Floor Areas, page 6-6
- Monitoring Floor Area, page 6-24
- Using the Automatic Hierarchy to Create Maps, page 6-28
- Using the Map Editor, page 6-31
- Adding an Outdoor Area, page 6-39
- Using Chokepoints to Enhance Tag Location Reporting, page 6-40
- Configuring Wi-Fi TDOA Receivers, page 6-43
- Searching Maps, page 6-51
- Using the Map Editor, page 6-52
- Inspecting Location Readiness and Quality, page 6-56
- Monitoring Mesh Networks Using Maps, page 6-59
- Monitoring Tags Using Maps, page 6-65
- Using Planning Mode, page 6-65
- Refresh Options, page 6-70
- Creating a Network Design, page 6-71
- Importing or Exporting WLSE Map Data, page 6-73
- Monitoring Device Details, page 6-74
- Monitoring Google Earth Maps, page 6-78

About Maps

Maps provide a summary view of all your managed systems on campuses, buildings, outdoor areas, and floors.
In addition to the features of the legacy maps, the Cisco Prime Infrastructure 2.0 enables you to use the features of the Next Generation Maps. The Next Generation Maps feature is enabled by default. Use the Administration > User Preferences page to disable or enable this feature.

When you export the maps that have APs placed on them for a given controller would archive the map and the AP placements within the campus/building/floor hierarchy. In the event the APs were to be inadvertently deleted, the archived maps could be imported, restoring the AP placements since the AP names, IP addresses, etc. should not change when rediscovered on the new controller.

The Next Generation Maps feature provides the following benefits:

- Displays a large amount of information on map. When you have numerous clients, interferers and access points, these may clutter the display on the Prime Infrastructure map pages. Also, pages load slowly. Prime Infrastructure 2.0 introduces clustering and layering of information. Information cluster reduces clutter at the high level and reveals more information when you click an object. For details, see the “Monitoring Floor Area” section on page 6-24.

- Simplifies and accelerates the process of adding APs to the map. In the legacy maps, the process of adding access points to maps is manual and tedious. With the Prime Infrastructure 2.0, you can use automated hierarchy creation to add and name access points. For details, see the “Using the Automatic Hierarchy to Create Maps” section on page 6-28.

- Provides High quality map images with easy navigation and zoom/pan controls. In the legacy maps, the map image quality is low and navigating, zooming, and panning is slow. With the Prime Infrastructure 2.0, you can use the next-generation ‘tile-aware’ map engine to load maps faster and zoom/pan easily. Also, Next Generation Maps enables administrators to load high-resolution maps faster and navigate around the map. For details, see the “Panning and Zooming with Next Generation Maps” section on page 6-24.

<table>
<thead>
<tr>
<th>Table 6-1</th>
<th>Process for Working with Maps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>Description</td>
</tr>
<tr>
<td>1. Add a new campus/building map</td>
<td>Choose Monitor &gt; Site Maps. From the Select a command drop-down list, choose New Campus or New Building.</td>
</tr>
<tr>
<td>2. Add a floor map</td>
<td>Choose Monitor &gt; Site Maps. From the Select a command drop-down list, choose New Floor Area.</td>
</tr>
<tr>
<td>3. Use Map Editor</td>
<td>Choose Monitor &gt; Site Maps. From the Select a command drop-down list, choose Map Editor.</td>
</tr>
</tbody>
</table>

Adding a Campus Map

When you navigate to Monitor > Site Maps, you see the “Unassigned Campus” area. This is an area for the Assurance data when the site classification information is unavailable. All the end points or hosts data are aggregated to unassigned campus. “Unassigned” is a default site available in Prime Infrastructure.

To add a single campus map to the Prime Infrastructure database, follow these steps:
Adding a Building to a Campus Map

To add a building to a campus map in the Prime Infrastructure database, follow these steps:

**Step 1** Choose **Monitor > Site Maps** to display the Maps page.

**Step 2** Click the desired campus. The Site Maps > Campus Name page appears.

**Step 3** From the Select a command drop-down list, choose **New Building**, and click **Go**.

**Step 4** In the Campus Name > New Building page, follow these steps to create a virtual building in which to organize related floor plan maps:

a. Enter the building name.

b. Enter the building contact name.

c. Enter the number of floors and basements.
d. Enter the horizontal position (distance from the corner of the building rectangle to the left edge of the campus map) and the vertical position (distance from the corner of the building rectangle to the top edge of the campus map) in feet.

**Note** To change the unit of measurement (feet or meters), choose Monitor > Site Maps, and choose Properties from the Select a command drop-down list.

e. Enter an approximate building horizontal span and vertical span (width and depth on the map) in feet.

**Note** The horizontal and vertical span should be larger than or the same size as any floors that you might add later.

**Tip** You can also use **Ctrl-click** to resize the bounding area in the upper-left corner of the campus map. As you change the size of the bounding area, the Horizontal Span and Vertical Span parameters of the building change to match your actions.

f. Click **Place** to put the building on the campus map. Prime Infrastructure creates a building rectangle scaled to the size of the campus map.

g. Click the building rectangle and drag it to the desired position on the campus map.

**Note** After adding a new building, you can move it from one campus to another without having to recreate it.

h. Click **Save** to save this building and its campus location to the database. Prime Infrastructure saves the building name in the building rectangle on the campus map.

**Note** A hyperlink associated with the building takes you to the corresponding Map page.

**Step 5** (Optional) To assign location presence information for the new outdoor area, do the following:

a. Choose **Edit Location Presence Info** from the Select a command drop-down list. Click **Go**. The Location Presence page appears.

**Note** By default, the Presence Info check box of the Override Child Element is selected. This option should remain selected if you want to propagate the campus location to all buildings and floors on that campus. When adding buildings to the campus map, you can import the campus location information. The campus address cannot be imported to a building if the check box is unselected. This option should be unselected if you want to assign building-specific addresses to buildings on its campus rather than one campus address to all.

b. Click the **Civic Address** or **Advanced** tab.

   i. Civic Address identifies the campus by name, street, house number, house number suffix, city (address line2), state, postal code, and country.
Advanced identifies the campus with expanded civic information such as neighborhood, city
division, country, and postal community name.

**Note**

Each selected field is inclusive of all of those above it. For example, if you choose
Advanced, it can also provide Civic location information upon client demand. The selected
setting must match what is set on the location server level (Services > Mobility Services).

c. By default, the Override Child’s Presence Information check box is selected. There is no need to
alter this setting for standalone buildings.

---

**Adding a Standalone Building**

To add a standalone building to the Prime Infrastructure database, follow these steps:

**Step 1** Choose **Monitor > Site Maps** to display the Maps page.

**Step 2** From the Select a command drop-down list, choose **New Building**, and click **Go**.

**Step 3** In the Maps > New Building page, follow these steps to create a virtual building in which to organize
related floor plan maps:

a. Enter the building name.

b. Enter the building contact name.

**Note**

After adding a new building, you can move it from one campus to another without having to
recreate it.

c. Enter the number of floors and basements.

d. Enter an approximate building horizontal span and vertical span (width and depth on the map) in
feet.

**Note**

To change the unit of measurement (feet or meters), choose **Monitor > Site Maps**, and
choose **Properties** from the Select a command drop-down list.

**Note**

The horizontal and vertical span should be larger than or the same size as any floors that you
might add later.

e. Click **OK** to save this building to the database.

**Step 4** (Optional) To assign location presence information for the new building, do the following:

a. Choose **Location Presence** from the Select a command drop-down list. Click **Go**. The Location
Presence page appears.

b. Click the **Civic** or **Advanced** tab.
Chapter 6  Monitoring Maps

Adding Floor Areas

This section describes how to add floor plans to either a campus building or a standalone building in the Prime Infrastructure database and includes the following topics:

- Adding Floor Areas to a Campus Building, page 6-6
- Adding Floor Plans to a Standalone Building, page 6-9
- Configuring Floor Settings, page 6-11
- Import Map and AP Location Data, page 6-23
- Placing Access Points, page 6-27

Adding Floor Areas to a Campus Building

After you add a building to a campus map, you can add individual floor plan and basement maps to the building.

Note  Use the zoom controls at the top of the campus image to enlarge or decrease the size of the map view and to hide or show the map grid (which displays the map size in feet or meters).

To add a floor area to a campus building, follow these steps:

Step 1  Save your floor plan maps in .PNG, .JPG, .JPEG, or .GIF format.
The maps can be any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.

If there are problems converting the auto-cad file, an error message is displayed. Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. If the native library cannot be loaded, the Prime Infrastructure displays an “unable to convert the auto-cad file” message. If you receive this error, make sure all the required dependencies are met for the native library. To find any dependency problems, use ldd on Linux platforms. The following DLLs must be present under the /webnms/rfdlls Prime Infrastructure installation directory: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problems occur, you might need to install the required libraries and restart the Prime Infrastructure.

An imported auto-cad file can become blurred when you zoom. Without the zoom, the clarity is about the same as the original auto-cad file. Make sure all relevant sections are clearly visible in the original auto-cad file (DWG/DXF) and then import the auto-cad file into .PNG/.GIF format rather than .JPEG or .JPG.

The floor map image is enhanced for zooming and panning. The floor image will not be visible completely until this operation is complete. You can zoom in and out to view the complete map image. For example, if you have a high resolution image (near 181 megapixels) whose size is approximately 60 megabytes, it may take two minutes to appear on the map.

Step 2  Choose **Monitor > Site Maps**.

Step 3  From the Maps Tree View or the Monitor > Site Maps list, choose the applicable campus building to open the Building View page.

Step 4  Hover your mouse cursor over the name within an existing building rectangle to highlight it.

Step 5  From the Select a command drop-down list, choose **New Floor Area**.

Step 6  Click **Go**. The New Floor Area page appears.

Step 7  In the New Floor Area page, follow these steps to add floors to a building in which to organize related floor plan maps:

a. Enter the floor area and contact names.

b. Choose the floor or basement number from the Floor drop-down list.

c. Choose the floor or basement type (RF Model).

d. Enter the floor-to-floor height in feet.
Adding Floor Areas

Chapter 6  Monitoring Maps

Note To change the unit of measurement (feet or meters), choose Monitor > Site Maps, and choose Properties from the Select a command drop-down list.

e. Select the Image or CAD File check box.

f. Browse to and choose the desired floor or basement image or CAD filename, and click Open.

Note If you are importing a CAD file, use the Convert CAD File drop-down list to determine the image file for conversion.

tip We do not recommend a .JPEG (.JPG) format for an auto-cad conversion. Unless a JPEG is specifically required, use .PNG or .GIF format for higher quality images.

g. Click Next. At this point, if a CAD file was specified, a default image preview is generated and loaded.

Note Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. When there are issues loading the native library, the Prime Infrastructure displays the following error: “Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library.” For more information see the Prime Infrastructure online help or Prime Infrastructure documentation.

The names of the CAD file layers are listed with check boxes to the right side of the image indicating which are enabled.

Note When you choose the floor or basement image filename, the Prime Infrastructure displays the image in the building-sized grid.

Note The maps can be any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.

Note The map must be saved in .PNG, .JPG, .JPEG, or .GIF format.

h. If you have CAD file layers, you can select or deselect as many as you want and click Preview to view an updated image. Click Next when you are ready to proceed with the selected layers.

Enter the remaining parameters for the floor area.

i. Either leave the Maintain Aspect Ratio check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio.

j. Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.
Adding Floor Areas

Chapter 6 Monitoring Maps

Adding Floor Plans to a Standalone Building

After you have added a standalone building to the Prime Infrastructure database, you can add individual floor plan maps to the building.

To add floor plans to a standalone building, follow these steps:

Step 1 Save your floor plan maps in .PNG, .JPG, or .GIF format.

Note The maps can be any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.

Step 2 Browse to and import the floor plan maps from anywhere in your file system. You can import CAD files in DXF or DWG formats or any of the formats you created in Step 1.

Tip Use Ctrl-click to resize the image within the building-sized grid.

Note You can zoom in or out to view the map at different sizes and you can add access points.

Adding Floor Areas

Note The horizontal and vertical spans should be smaller than or the same size as the building horizontal and vertical spans in the Prime Infrastructure database.

k. If applicable, enter the horizontal position (distance from the corner of the outdoor area rectangle to the left edge of the campus map) and vertical position (distance from the corner of the outdoor area rectangle to the top edge of the campus map) in feet or meters.

Tip Use Ctrl-click to resize the image within the building-sized grid.

l. If desired, select the Launch Map Editor after floor creation check box to rescale the floor and draw walls.

m. Click OK to save this floor plan to the database. The floor is added to the Maps Tree View and the Monitor > Site Maps list.

Note Use different floor names in each building. If you are adding more than one building to the campus map, do not use a floor name that exists in another building. This overlap causes incorrect mapping information between a floor and a building.

Step 8 Click any of the floor or basement images to view the floor plan or basement map.

Note You can zoom in or out to view the map at different sizes and you can add access points.
Note: If there are problems converting the auto-cad file, an error message is displayed. Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. If the native library cannot be loaded, the Prime Infrastructure displays an “unable to convert the auto-cad file” message. If you receive this error, make sure all the required dependencies are met for the native library. To find any dependency problems, use ldd on Linux platforms. The following DLLs must be present under the /webnms/rfdlls Prime Infrastructure installation directory: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problems occur, you might need to install the required libraries and restart the Prime Infrastructure.

Step 3 Choose Monitor > Site Maps.
Step 4 From the Maps Tree View or the Monitor > Site Maps left sidebar menu, choose the desired building to display the Building View page.
Step 5 From the Select a command drop-down list, choose New Floor Area.
Step 6 Click Go.
Step 7 In the New Floor Area page, add the following information:

- Enter the floor area and contact names.
- Choose the floor or basement number from the Floor drop-down list.
- Choose the floor or basement type (RF Model).
- Enter the floor-to-floor height in feet.
- Select the Image or CAD File check box.
- Browse to and choose the desired floor or basement Image or CAD file, and click Open.

Note: If you are importing a CAD file, use the Convert CAD File drop-down list to determine the image file for conversion.

Tip: A .JPEG (.JPG) format is not recommended for an auto-cad conversion. Unless a .JPEG is specifically required, use a .PNG or .GIF format for higher quality images.

Step 8 Click Next. At this point, if a CAD file was specified, a default image preview is generated and loaded.

Note: Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. When there are issues loading the native library, the Prime Infrastructure displays the following error: "Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library. For more information, see the Prime Infrastructure online help or Prime Infrastructure documentation."

The names of the CAD file layers are listed with check boxes to the right side of the image indicating which are enabled.

Note: When you choose the floor or basement image filename, the Prime Infrastructure displays the image in the building-sized grid.
Note: The maps can be any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.

Note: The map must be saved in .PNG, .JPG, JPEG, or .GIF format.

If you have CAD file layers, you can select or deselect as many as you want and click Preview to view an updated image. Click Next when you are ready to proceed with the selected layers.

Step 9: Enter the remaining parameters for the floor area.

- Either leave the Maintain Aspect Ratio check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio.
- Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.

Note: The horizontal and vertical spans should be smaller than or the same size as the building horizontal and vertical spans in the Prime Infrastructure database.

- If applicable, enter the horizontal position (distance from the corner of the outdoor area rectangle to the left edge of the campus map) and vertical position (distance from the corner of the outdoor area rectangle to the top edge of the campus map) in feet or meters.

Tip: Use Ctrl-click to resize the image within the building-sized grid.

- Adjust the floor characteristics with the Prime Infrastructure map editor by selecting the check box next to Launch Map Editor. See the “Using the Map Editor” section on page 6-31 for more information regarding the map editor feature.

Step 10: Click OK to save this floor plan to the database. The floor is added to the Maps Tree View and the Monitor > Site Maps list.

Step 11: Click any of the floor or basement images to view the floor plan or basement map.

Note: You can zoom in or out to view the map at different sizes and you can add access points.

Configuring Floor Settings

You can modify the appearance of the floor map by selecting or unselecting various floor settings check boxes. The selected floor settings appears in the map image.

The Floor Settings options include the following:

- Access Points
- AP Heatmaps
- AP Mesh Info
Adding Floor Areas

- Clients
- 802.11 Tags
- Rogue APs
- Rogue Adhocs
- Rogue Clients
- Coverage Areas
- Location Regions
- Rails
- Markers
- Chokepoints
- Wi-Fi TDOA Receivers
- Interferers

Use the blue arrows to access floor setting filters for access points, access point heatmaps, clients, 802.11 tags, rogue access points, rogue adhocs, and rogue clients. When filtering options are selected, click OK.

Use the Show MSE data within last drop-down list to choose the timeframe for mobility services engine data. Choose to view mobility services engine data from a range including the past two minutes up to the past 24 hours. This option only appears if a mobility services engine is present on the Prime Infrastructure.

Click Save Settings to make the current view and filter settings your new default for all maps.

Defining Inclusion and Exclusion Regions on a Floor

To further refine location calculations on a floor, you can define the areas that are included (inclusion areas) in the calculations and those areas that are not included (exclusion areas).

For example, you might want to exclude areas such as an atrium or stairwell within a building but include a work area (such as cubicles, labs, or manufacturing floors).

Note

If the MSE to which the floor is synchronized is running the Aeroscout tag engine, then inclusion and exclusion regions are not calculated for tags.
Viewing Floor Component Details

To view details regarding the components displayed on the Floor View, hover your mouse cursor over the applicable icon. A dialog box containing detailed information is displayed. Table 6-2 displays the floor map icons.

Table 6-2 Floor Map Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>Access point icon. The color of the circle indicates the alarm status of the Cisco Radios.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Each access point contains two Cisco Radios. When a single protocol is selected in the Access Point filter page, the entire icon represents this radio. If both protocols are selected, the top half of the icon represents the state of the 802.11a/n radio and the bottom half represents the state of the 802.11b/g/n radio.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If a Cisco Radio is disabled, a small “x” appears in the middle of the icon.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Monitor mode access points are shown with a gray label to distinguish these from other access points.</td>
</tr>
<tr>
<td>🔄</td>
<td>AP heatmaps icon.</td>
</tr>
<tr>
<td>🔄</td>
<td>Client icon. Hover your mouse cursor over the icon to view client details.</td>
</tr>
<tr>
<td>🔄</td>
<td>Tag icon. Hover your mouse cursor over the icon to view tag details.</td>
</tr>
<tr>
<td>🔄</td>
<td>Rogue access point icon. The color of the icon indicates the type of rogue access point. For example, red indicates a malicious rogue access point and blue indicates an unknown type. Hover your mouse cursor over the icon to view rogue access point details.</td>
</tr>
<tr>
<td>🔄</td>
<td>Rogue adhoc icon. Hover your mouse cursor over the icon to view rogue adhoc details.</td>
</tr>
<tr>
<td>🔄</td>
<td>Rogue client icon. Hover your mouse cursor over the icon to view rogue client details.</td>
</tr>
<tr>
<td>🔄</td>
<td>Coverage icon.</td>
</tr>
<tr>
<td>🔄</td>
<td>Location regions icon.</td>
</tr>
<tr>
<td>🔄</td>
<td>Rails icon.</td>
</tr>
<tr>
<td>🔄</td>
<td>Marker icon.</td>
</tr>
</tbody>
</table>
### Adding Floor Areas

#### Cisco 1000 Series Lightweight Access Point Icons

The icons indicate the present status of an access point. The circular part of the icon can be split in half horizontally. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.

**Note**

When the icon is representing 802.11a/n and 802.11b/n, the top half displays the 802.11a/n status, and the bottom half displays the 802.11b/g/n status. When the icon is representing only 802.11b/g/n, the whole icon displays the 802.11b/g/n status. The triangle indicates the more severe color.

Table 6-3 shows the icons used in the Prime Infrastructure user interface Map displays.

#### Table 6-2  **Floor Map Icons (continued)**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon1.png" alt="Chokepoint Icon" /></td>
<td>Chokepoint icon.</td>
</tr>
<tr>
<td><img src="icon2.png" alt="Wi-Fi TDOA Receiver Icon" /></td>
<td>Wi-Fi TDOA receiver icon.</td>
</tr>
<tr>
<td><img src="icon3.png" alt="Interferer Device Icon" /></td>
<td>Interferer device icon.</td>
</tr>
<tr>
<td><img src="icon4.png" alt="Indicates a Guest Client" /></td>
<td>Indicates a guest client that is configured through web auth WLAN on the Prime Infrastructure. <strong>Note</strong> If you create a Guest WLAN on controller and assign that controller to MSE, only then the guests from that controller will show as guest icons.</td>
</tr>
</tbody>
</table>

#### Table 6-3  **Access Points Icons Description**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon5.png" alt="The Green Icon" /></td>
<td>The green icon indicates an access point (AP) with no faults. The top half of the circle represents the optional 802.11a Cisco Radio. The bottom half of the circle represents the state of the 802.11b/g Cisco Radio.</td>
</tr>
<tr>
<td><img src="icon6.png" alt="The Yellow Icon" /></td>
<td>The yellow icon indicates an access point with a minor fault. The top half of the circle represents the optional 802.11a Cisco Radio. The bottom half of the circle represents the state of the 802.11b/g Cisco Radio. <strong>Note</strong> A flashing yellow icon indicates that there has been an 802.11a or 802.11b/g interference, noise, coverage, or load Profile Failure. A flashing yellow icon indicates that there have been 802.11a and 802.11b/g profile failures.</td>
</tr>
<tr>
<td><img src="icon7.png" alt="The Red Icon" /></td>
<td>The red icon indicates an access point (AP) with a major or critical fault. The top half of the circle represents the optional 802.11a Cisco Radio. The bottom half of the circle represents the state of the 802.11b/g Cisco Radio.</td>
</tr>
</tbody>
</table>
### Table 6-3 Access Points Icons Description (continued)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Icon" /></td>
<td>The dimmed icon with a question mark in the middle represents an unreachable access point. It is gray because its status cannot be determined.</td>
</tr>
<tr>
<td><img src="image2.png" alt="Icon" /></td>
<td>The dimmed icon with no question mark in the middle represents an unassociated access point.</td>
</tr>
<tr>
<td><img src="image3.png" alt="Icon" /></td>
<td>The icon with a red “x” in the center of the circle represents an access point that has been administratively disabled.</td>
</tr>
<tr>
<td><img src="image4.png" alt="Icon" /></td>
<td>The icon with the top half green and the lower half yellow indicates that the optional 802.11a Cisco Radio (top) has no faults, and the 802.11b/g Cisco Radio (bottom) has a minor fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.</td>
</tr>
<tr>
<td><img src="image5.png" alt="Icon" /></td>
<td>The icon with the top half green and the lower half red indicates that the optional 802.11a Cisco Radio (top) is operational with no faults, and the 802.11b/g Cisco Radio (bottom) has a major or critical fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.</td>
</tr>
<tr>
<td><img src="image6.png" alt="Icon" /></td>
<td>The icon with the top half yellow and the lower half red indicates that the optional 802.11a Cisco Radio (top) has a minor fault, and the 802.11b/g Cisco Radio (bottom) has a major or critical fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.</td>
</tr>
<tr>
<td><img src="image7.png" alt="Icon" /></td>
<td>The icon with the top half yellow and the lower half green indicates that the optional 802.11a Cisco Radio (top) has a minor fault, and the 802.11b/g Cisco Radio (bottom) is operational with no faults. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.</td>
</tr>
<tr>
<td><img src="image8.png" alt="Icon" /></td>
<td>The icon with the top half red and the lower half green indicates that the optional 802.11a Cisco Radio (top) has a major or critical fault, and the 802.11b/g Cisco Radio (bottom) is operational with no faults. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.</td>
</tr>
</tbody>
</table>
Table 6-3  Access Points Icons Description (continued)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Icon" /></td>
<td>The icon with the top half red and the lower half yellow indicates that the optional 802.11a Cisco Radio (top) has major or critical faults, and the 802.11b/g Cisco Radio (bottom) has a minor fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.</td>
</tr>
<tr>
<td><img src="image2" alt="Icon" /></td>
<td>The icon with a red “x” on the top half (optional 802.11a) shows that the indicated Cisco Radio has been administratively disabled. There are six color coding possibilities as shown.</td>
</tr>
</tbody>
</table>

Each of the access point icons includes a small black arrow that indicates the direction in which the internal Side A antenna points.

Table 6-4 shows some arrow examples used in the Prime Infrastructure user interface map displays.

Table 6-4  Arrows

<table>
<thead>
<tr>
<th>Arrow Examples</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image3" alt="Arrow" /></td>
<td>Zero degrees, or to the right on the map.</td>
</tr>
<tr>
<td><img src="image4" alt="Arrow" /></td>
<td>45 degrees, or to the lower right on the map.</td>
</tr>
<tr>
<td><img src="image5" alt="Arrow" /></td>
<td>90 degrees, or down on the map.</td>
</tr>
</tbody>
</table>

These examples show the first three 45-degree increments allowed, with an additional five at 45-degree increments.
Filtering Access Point Floor Settings

If you enable the access point floor setting and then click the blue arrow to the right of the floor settings, the Access Point Filter dialog box appears with filtering options.

Access point filtering options include the following:

- **Show**—Select this radio button to display the radio status or the access point status.

  **Note** Because the access point icon color is based on the access point status, the icon color might vary depending on the status selected. The default on floor maps is radio status.

- **Protocol**—From the drop-down list, choose which radio types to display (802.11a/n, 802.11b/g/n, or both).

  **Note** The displayed heatmaps correspond to the selected radio type(s).

- **Display**—From the drop-down list, choose what identifying information is displayed for the access points on the map image.
  - **Channels**—Displays the Cisco Radio channel number or Unavailable (if the access point is not connected).
  - **TX Power Level**—Displays the current Cisco Radio transmit power level (with 1 being high) or Unavailable (if the access point is not connected).

  **Note** The power levels differ depending on the type of access point. The 1000 series access points accept a value between 1 and 5, the 1230 access points accept a value between 1 and 7, and the 1240 and 1100 series access points accept a value between 1 and 8.

*Table 6-5 lists the transmit power level numbers and their corresponding power setting.*

<table>
<thead>
<tr>
<th>Transmit Power Level Number</th>
<th>Power Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Maximum power allowed per country code setting</td>
</tr>
<tr>
<td>2</td>
<td>50% power</td>
</tr>
<tr>
<td>3</td>
<td>25% power</td>
</tr>
<tr>
<td>4</td>
<td>12.5 to 6.25% power</td>
</tr>
<tr>
<td>5</td>
<td>6.25 to 0.195% power</td>
</tr>
</tbody>
</table>

**Note** The power levels are defined by the country code setting and are regulated by country. See the following URL for more information:

- **Channel and Tx Power**—Displays both the channel and transmit power level (or Unavailable if the access point is not connected).

- **Coverage Holes**—Displays a percentage of clients whose signal has become weaker until the client lost its connection. Unavailable for unconnected access points, or MonitorOnly for access points in monitor-only mode.

**Note** Coverage holes are areas in which clients cannot receive a signal from the wireless network. When you deploy a wireless network, you must consider the cost of the initial network deployment and the percentage of coverage hole areas. A reasonable coverage hole criterion for launch is between 2 and 10 percent. This means that between two and ten test locations out of 100 random test locations might receive marginal service. After launch, Cisco Unified Wireless Network Solution Radio Resource Management (RRM) identifies these coverage hole areas and reports them to the IT manager, who can fill holes based on user demand.

- **MAC Addresses**—Displays the MAC address of the access point, whether or not the access point is associated to a controller.

- **Names**—Displays the access point name. This is the default value.

- **Controller IP**—Displays the IP address of the controller to which the access point is associated or Not Associated for disassociated access points.

- **Utilization**—Displays the percentage of bandwidth used by the associated client devices (including receiving, transmitting, and channel utilization). Displays Unavailable for disassociated access points and MonitorOnly for access points in monitor-only mode.

- **Profiles**—Displays the load, noise, interference, and coverage components of the corresponding operator-defined thresholds. Displays Okay for thresholds not exceeded, Issue for exceeded thresholds, or Unavailable for unconnected access points.

**Note** Use the Profile Type drop-down list to choose Load, Noise, Interference, or Coverage.

- **CleanAir Status**—Displays the CleanAir status of the access point and whether or not CleanAir is enabled on the access point.

- **Average Air Quality**—Displays the average air quality on this access point. The details include the band and the average air quality.

- **Minimum Air Quality**—Displays the minimum air quality on this access point. The details include the band and the minimum air quality.

- **Average and Minimum Air Quality**—Displays the average and minimum air quality on this access point. The details include the band, average air quality, and minimum air quality.

- **Associated Clients**—Displays the number of associated clients. Unavailable for unconnected access points or MonitorOnly for access points in monitor-only mode.

- **Bridge Group Names**

- **RSSI Cutoff**—From the drop-down list, choose the RSSI cutoff level. The RSSI cutoff ranges from -60 dBm to -90 dBm.

- **Show Detected Interferers**—Select the check box to display all interferers detected by the access point.
• Max. Interferers/label—Choose the maximum number of interferers to be displayed per label from the drop-down list.

Click OK when all applicable filtering criteria are selected.

Filtering Access Point Heatmap Floor Settings

An RF heatmap is a graphical representation of RF wireless data where the values taken by variables are represented in maps as colors. The current heatmap is computed based on the RSSI prediction model, Antenna Orientation, and AP transmit power.

If you enable the Access Point Heatmap floor setting and click the blue arrow to the right of the Floor Settings, the Contributing APs dialog appears with heatmap filtering options.

Prime Infrastructure introduces dynamic heatmaps. When dynamic heatmaps are enabled, the Prime Infrastructure recomputes the heatmaps to represent changed RSSI values.

Access point heatmap filtering options include the following:

• Heatmap Type—Select Coverage, or Air Quality. If you choose Air Quality, you can further filter the heatmap type for access points with average air quality or minimum air quality. Select the appropriate radio button.

  **Note**
  If you have monitor mode access points on the floor plan, you have a choice between IDS or coverage heatmap types. A coverage heatmap excludes monitor mode access points.

  **Note**
  Only APs in Local, FlexConnect, or Bridge mode can contribute to the Coverage and Air Quality Heatmap.

• Total APs—Displays the number of access points positioned on the map.

Select the access point check box(es) to determine which heatmaps are displayed on the image map.

Click OK when all applicable filtering criteria are selected.

Filtering AP Mesh Info Floor Settings

**Note**

The AP Mesh Info check box only appears when bridging access points are added to the floor.

When this check box is selected, the Prime Infrastructure initiates a contact with the controllers and displays information about bridging access points. The following information is displayed:

- Link between the child and the parent access point.
- An arrow that indicates the direction from the child to parent access point.
- A color-coded link that indicates the signal-to-noise ratio (SNR). A green link represents a high SNR (above 25 dB), an amber link represents an acceptable SNR (20-25 dB), and a red link represents a very low SNR (below 20 dB).

If you enable the AP Mesh Info floor setting and click the blue arrow to the right of the floor settings, the Mesh Parent-Child Hierarchical View page appears with mesh filtering options.

You can update the map view by choosing the access points you want to see on the map. From the Quick Selections drop-down list, choose to select only root access point, various hops between the first and the fourth, or select all access points.
Adding Floor Areas

Note
For a child access point to be visible, its parent must also be selected.

Click OK when all applicable filtering criteria are selected.

Filtering Client Floor Settings

Note
The Clients option only appears if a mobility server is added in the Prime Infrastructure.

If you enable the Clients floor setting and click the blue arrow to the right, the Client Filter dialog box appears.

Client filtering options include the following:

- **Show All Clients**—Select the check box to display all clients on the map.
- **Small Icons**—Select the check box to display icons for each client on the map.

Note
If you select the **Show All Clients** check box and **Small Icons** check box, all other drop-down list options are dimmed.

If you unselect the **Small Icons** check box, you can choose if you want the label to display the MAC address, IP address, username, asset name, asset group, or asset category.

If you unselect the **Show All Clients** check box, you can specify how you want the clients filtered and enter a particular SSID.

- **Display**—Choose the client identifier (IP address, username, MAC address, asset name, asset group, or asset category) to display on the map.
- **Filter By**—Choose the parameter by which you want to filter the clients (IP address, username, MAC address, asset name, asset group, asset category, or controller). Once selected, type the specific device in the text box.

Note
If there are multiple IPv6 addresses for a client, then you can specify any one IP address to uniquely identify the client.

- **SSID**—Enter the client SSID in the available text box.
- **Protocol**—Choose All, 802.11a/n, or 802.11b/g/n from the drop-down list.
  - **All**—Displays all the access points in the area.
  - **802.11a/n**—Displays a colored overlay depicting the coverage patterns for the clients with 802.11a/n radios. The colors show the received signal strength from red (–35 dBm) through dark blue (–85 dBm).
  - **802.11b/g/n**—Displays a colored overlay depicting the coverage patterns for the clients with 802.11b/g/n radios. The colors show the received signal strength from red (–35 dBm) through dark blue (–85 dBm). This is the default value.
- **State**—Choose All, Idle, Authenticated, Probing, or Associated from the drop-down list.

Click OK when all applicable filtering criteria are selected.
Filtering 802.11 Tag Floor Settings

If you enable the 802.11 Tags floor setting and then click the blue arrow to the right, the Tag Filter dialog appears.

Tag filtering options include the following:

- **Show All Tags**—Select the check box to display all tags on the map.
- **Small Icons**—Select the check box to display icons for each tag on the map.

**Note**

If you select the Show All Tags check box and Small Icons check box, all other drop-down list options are dimmed.

If you unselect the Small Icons check box, you can choose if you want the label to display MAC address, asset name, asset group, or asset category.

If you unselect the Show All Tags check box, you can specify how you want the tags filtered.

- **Display**—Choose the tag identifier (MAC address, asset name, asset group, or asset category) to display on the map.
- **Filter By**—Choose the parameter by which you want to filter the clients (MAC address, asset name, asset group, asset category, or controller). Once selected, type the specific device in the text box.

Click **OK** when all applicable filtering criteria are selected.

Filtering Rogue AP Floor Settings

If you enable the Rogue APs floor setting and then click the blue arrow to the right, the Rogue AP filter dialog box appears.

Rogue AP filtering options include the following:

- **Show All Rogue APs**—Select the check box to display all rogue access points on the map.
- **Small Icons**—Select the check box to display icons for each rogue access point on the map.

**Note**

If you select the **Show All Rogue APs** check box and **Small Icons** check box, all other drop-down list options are dimmed.

If you unselect the **Show All Rogue APs** check box, you can specify how you want the rogue access points filtered.

- **MAC Address**—If you want to view a particular MAC address, enter it in the MAC Address text box.
- **State**—Use the drop-down list to choose from Alert, Known, Acknowledged, Contained, Threat, or Unknown contained states.
- **On Network**—Use the drop-down list to specify whether or not you want to display rogue access points on the network.

Click **OK** when all applicable filtering criteria are selected.

Filtering Rogue Adhoc Floor Settings

If you enable the Rogue Adhocs floor setting and then click the blue arrow to the right, the Rogue Adhoc filter dialog appears.
Rogue Adhoc filtering options include the following:

- **Show All Rogue Adhocs**—Select the check box to display all rogue adhoc on the map.
- **Small Icons**—Select the check box to display icons for each rogue adhoc on the map.

**Note**

If you select the **Show All Rogue Adhocs** check box and **Small Icons** check box, all other drop-down list options are dimmed.

If you unselect the **Show All Rogue Adhocs** check box, you can specify how you want the rogue adhocs filtered.

- **MAC Address**—If you want to view a particular MAC address, enter it in the MAC Address text box.
- **State**—Use the drop-down list to select from Alert, Known, Acknowledged, Contained, Threat, or Unknown contained states.
- **On Network**—Use the drop-down list to specify whether or not you want to display rogue adhocs on the network.

Click **OK** when all applicable filtering criteria are selected.

### Filtering Rogue Client Floor Settings

If you enable the Rogue Clients floor setting and then click the blue arrow to the right, the Rogue Clients filter dialog appears.

Rogue Clients filtering options include the following:

- **Show All Rogue Clients**—Select the check box to display all rogue clients on the map.
- **Small Icons**—Select the check box to display icons for each rogue client on the map.

**Note**

If you select the **Show All Rogue Clients** check box and **Small Icons** check box, all other drop-down list options are dimmed. If you unselect the **Show All Rogue Clients** check box, you can specify how you want the rogue clients filtered.

- **Assoc. Rogue AP MAC Address**—If you want to view a particular MAC address, enter it in the MAC Address text box.
- **State**—Use the drop-down list to choose from Alert, Contained, Threat, or Unknown contained states.

Click **OK** when all applicable filtering criteria are selected.

### Filtering Interferer Settings

If you enable Interferer floor setting and then click the blue arrow to the right, the Interferers filter dialog box appears.

Interferer filtering options include the following:

- **Show active interferers only**—Select the check box to display all active interferers.
- **Small Icons**—Select the check box to display icons for each interferer on the map.
- **Show Zone of Impact**—Displays the approximate interference impact area. The opacity of the circle denotes its severity. A solid red circle represents a very strong interferer that likely disrupts Wi-Fi communications, a light pink circle represents a weak interferer.
• Click **OK** when all applicable filtering criteria are selected.

**Import Map and AP Location Data**

When converting from autonomous to lightweight access points and from the WLSE to Prime Infrastructure, one of the conversion steps is to manually reenter the access point-related information into the Prime Infrastructure. To speed up this process, you can export the information about access points from the WLSE and import it into the Prime Infrastructure.

---

**Note**
The Prime Infrastructure expects a .tar file and checks for a .tar extension before importing the file. If the file you are trying to import is not a .tar file, the Prime Infrastructure displays an error message and prompts you to import a different file.

---

**Note**
For more information on the WLSE data export functionality (WLSE Version 2.15), see the following URL:


---

To map properties and import a tar file containing WLSE data using the Prime Infrastructure web interface, follow these steps:

---

**Step 1** Choose **Monitor > Site Maps**.

**Step 2** From the Select a command drop-down list, choose **Import Maps**, and click **Go**.

**Step 3** Choose the **WLSE Map and AP Location Data** option, and click **Next**.

**Step 4** In the Import WLSE Map and AP Location Data page, click **Browse** to select the file to import.

**Step 5** Find and select the .tar file to import and click **Open**.

Prime Infrastructure displays the name of the file in the Import From text box.

**Step 6** Click **Import**.

Prime Infrastructure uploads the file and temporarily saves it into a local directory while it is being processed. If the file contains data that cannot be processed, the Prime Infrastructure prompts you to correct the problem and retry. Once the file has been loaded, the Prime Infrastructure displays a report of what is added to the Prime Infrastructure. The report also specifies what cannot be added and why.

If some of the data to be imported already exists, the Prime Infrastructure either uses the existing data in the case of campuses or overwrites the existing data using the imported data in the cases of buildings and floors.

---

**Note**
If there are duplicate names between a WLSE site and building combination and the Prime Infrastructure campus (or top-level building) and building combination, the Prime Infrastructure displays a message in the Pre Execute Import Report indicating that it will delete the existing building.

---

**Step 7** Click **Import** to import the WLSE data.

Prime Infrastructure displays a report indicating what was imported.
Step 8 Choose Monitor > Site Maps to view the imported data.

Monitoring Floor Area

The floor area is the area of each floor of the building measured to the outer surface of the outer walls including the area of lobbies, cellars, elevator shafts, and in multi-dwelling buildings, all the common spaces.

- Panning and Zooming with Next Generation Maps, page 6-24
- Adding Access Points to a Floor Area, page 6-25
- Placing Access Points, page 6-27

Panning and Zooming with Next Generation Maps

Panning
To move the map, click and hold the left mouse button and drag the map to a new place.

You can also move the map North, South, East or West using the pan arrows. These can be found in the top left hand corner of the map (see Figure 6-1).

Figure 6-1 Panning Control

Note You can also perform the panning operations using the arrow keys on a keyboard.

Zooming in and out - changing the scale
The zooming levels depend upon the resolution of an image. A high resolution image may provide more zoom levels. Each zoom level is made of a different style map shown at different scales, each one showing more or less detail. Some maps will be of the same style, but at a smaller or larger scale.

To see a map with more detail you need to zoom in. You can do this using the zoom bar on the left hand side of the map (see Figure 6-2). Click the + sign on the top of the zoom bar. To centre and zoom in on a location, double click the location. To see a map with less detail you need to zoom out. To do this, click the - sign on the bottom of the zoom bar.
Chapter 6 Monitoring Maps

Monitoring Floor Area

Figure 6-2  Zooming Control

You can perform zooming operations using mouse or keyboard. With keyboard, click the + or - signs to zoom in or zoom out. With mouse, use the mouse scroll wheel to zoom in or zoom out or double click to zoom in.

Adding Access Points to a Floor Area

After you add the .PNG, .JPG, .JPEG, or .GIF format floor plan and outdoor area maps to the Prime Infrastructure database, you can position lightweight access point icons on the maps to show where they are installed in the buildings. To add access points to a floor area and outdoor area, follow these steps:

Step 1  Choose Monitor > Site Maps.

Step 2  From the Maps Tree View or the Monitor > Site Maps left sidebar menu, select the applicable floor to open the Floor View page.

Step 3  From the Select a command drop-down list, choose Add Access Points, and click Go.

Step 4  In the Add Access Points page, select the check boxes of the access points that you want to add to the floor area.

Note  If you want to search for access points, enter AP name or MAC address (Ethernet/Radio)/IP in the Search AP [Name/MacAddress (Ethernet/Radio)/IP] text box, and then click Search. The search is case-insensitive.

Note  Only access points that are not yet assigned to any floor or outdoor area appear in the list.

Note  Select the check box at the top of the list to select all access points.

Step 5  When all of the applicable access points are selected, click OK located at the bottom of the access point list.

The Position Access Points page appears.

Each access point you have chosen to add to the floor map is represented by a gray circle (differentiated by access point name or MAC address) and is lined up in the upper left part of the floor map.

Step 6  Click and drag each access point to the appropriate location. Access points turn blue when selected.

Note  When you drag an access point on the map, its horizontal and vertical position appears in the Horizontal and Vertical text boxes.
The small black arrow at the side of each access point represents Side A of each access point, and each access point arrow must correspond with the direction in which the access points were installed. Side A is clearly noted on each 1000 series access point and has no relevance to the 802.11a/n radio. To adjust the directional arrow, choose the appropriate orientation from the Antenna Angle drop-down list.

When selected, the access point details are displayed on the left side of the page. Access point details include the following:

- AP Model—Indicates the model type of the selected access point.
- Protocol—Choose the protocol for this access point from the drop-down list.
- Antenna—Choose the appropriate antenna type for this access point from the drop-down list.
- Antenna/AP Image—The antenna image reflects the antenna selected from the Antenna drop-down list. Click the arrow at the top right of the antenna image to expand the image size.
- Antenna Orientation—Depending on the antenna type, enter the Azimuth and the Elevation orientations in degrees.

The Azimuth option does not appear for Omnidirectional antennas because their pattern is nondirectional in azimuth.

For internal antennas, the same elevation angle applies to both radios.

The antenna angle is relative to the map X axis. Because the origin of the X (horizontal) and Y (vertical) axes is in the upper left corner of the map, 0 degrees points side A of the access point to the right, 90 degrees points side A down, 180 degrees points side A to the left, and so on.

The antenna elevation is used to move the antenna vertically, up or down, to a maximum of 90 degrees.

Make sure each access point is in the correct location on the map and has the correct antenna orientation. Accurate access point positioning is critical when you use the maps to find coverage holes and rogue access points.


When you are finished placing and adjusting each access point, click **Save**.

Clicking Save causes the antenna gain on the access point to correspond to the selected antenna. This might cause the radio to reset.

Prime Infrastructure computes the RF prediction for the entire map. These RF predictions are popularly known as *heat maps* because they show the relative intensity of the RF signals on the coverage area map.
Note
This display is only an approximation of the actual RF signal intensity because it does not take into account the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects of RF signals bouncing off obstructions.

Note
Antenna gain settings have no effect on heatmaps and location calculations. Antenna gain is implicitly associated to the antenna name. Because of this, the following apply:
– If an antenna is used and marked as “Other” in Prime Infrastructure, it is ignored for all heatmap and location calculations;
– If an antenna is used and marked as a Cisco antenna in the Prime Infrastructure, that antenna gain setting (internal value on Prime Infrastructure) is used no matter what gain is set on the controller.

Note
The Heatmap for 3702 AP shows inaccurate details in representation, even if the power level, height and antenna angle are setup at appropriate values.

Note
See the “Placing Access Points” section on page 6-27 for more information on placing access points on a map.

Note
You can change the position of access points by importing or exporting a file. See the “Positioning Wi-Fi TDOA Receivers” section on page 6-44 for more information.

Placing Access Points

To determine the best location of all devices in the wireless LAN coverage areas, you need to consider the access point density and location.

Ensure that no fewer than 3 access points, and preferably 4 or 5, provide coverage to every area where device location is required. The more access points that detect a device, the better. This high level guideline translates into the following best practices, ordered by priority:

1. Most importantly, access points should surround the desired location.
2. One access point should be placed roughly every 50 to 70 linear feet (about 17 to 20 meters). This translates into one access point every 2,500 to 5000 square feet (about 230 to 450 square meters).

Note
The access point must be mounted so that it is under 20 feet high. For best performance, a mounting at 10 feet would be ideal.

Following these guidelines makes it more likely that access points detect tracked devices. Rarely do two physical environments have the same RF characteristics. Users might need to adjust these parameters to their specific environment and requirements.
Note: Devices must be detected at signals greater than –75 dBm for the controllers to forward information to the location appliance. No fewer than three access points should be able to detect any device at signals below –75 dBm.

If you have a ceiling-mounted AP with an integrated omni-directional antenna, the antenna orientation does not really need to be set in the Prime Infrastructure. However, if you mount that same AP on the wall, you must set the antenna orientation to 90 degrees.

Table 6-6 describes the orientation of the access points.

<table>
<thead>
<tr>
<th>Access Point</th>
<th>Antenna Orientation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1140 mounted on the ceiling</td>
<td>The Cisco logo should be pointing to the floor. Elevation: 0 degrees.</td>
</tr>
<tr>
<td>1240 mounted on the ceiling</td>
<td>The antenna should be perpendicular to the access point. Elevation: 0 degrees.</td>
</tr>
<tr>
<td>1240 mounted on the wall</td>
<td>The antenna should be parallel to the access point. Elevation: 0 degrees. If the antenna is perpendicular to the AP then the angle is 90 degrees (up or down does not matter as the dipole is omni).</td>
</tr>
</tbody>
</table>

**Using the Automatic Hierarchy to Create Maps**

Automatic Hierarchy Creation is a way for you to quickly create maps and assign access points to maps in Prime Infrastructure. You can use Automatic Hierarchy Creation to create maps, once you have added wireless LAN controllers to Prime Infrastructure and named your access points. Also, you can use it after adding access points to your network to assign access points to maps in Prime Infrastructure.

Note: To use the Automatic Hierarchy Creation feature, you must have an established naming pattern for your wireless access points that provides the campus, building, floor, or outdoor area names for the maps. For example, San Jose-01-GroundFloor-AP3500i1.

**Step 1** Choose Monitor > Automatic Hierarchy Creation to display the Automatic Hierarchy Creation page.

**Step 2** In the text box, enter the name of an access point on your system. Or, you can choose one from the list. This name is used to create a regular expression to create your maps.
To update a previously created regular expression, click **Load and Continue** next to the expression and update the expression accordingly. To delete a regular expression, click **Delete** next to the expression.

**Step 3** Click **Next**.

**Step 4** If your access point’s name has a delimiter, enter it in the text box and click **Generate basic regex based on delimiter**. The system generates a regular expression that matches your access point’s name based on the delimiter.

For example, using the dash (-) delimiter in the access point name San Jose-01-GroundFloor-AP3500i1, produces the regular expression /(.*)-(.*)-(.*)-(.*)/.

If you have a more complicated access point name, you can manually enter the regular expression.

You are not required to enter the leading and trailing slashes.

As a convention, the Prime Infrastructure displays regular expressions in slashes.

**Step 5** Click **Test**. The system displays the maps that will be created for the access point name and the regular expression entered.

**Step 6** Using the Group fields, assign matching groups to hierarchy types.

For example, if your access point is named: SJC14-4-AP-BREAK-ROOM

In this example, the campus name is SJC, the building name is 14, the floor name is 4, and the AP name is AP-BREAK-ROOM.

Use the regular expression: /((\[A-Z\]+)(\d+)-(\d+)-(\d+)-(\d+))/

From the AP name, the following groups are extracted:

1. SJC
2. 14
3. 4
4. AP-BREAK-ROOM

The matching groups are assigned from left to right, starting at 1.

To make the matching groups match the hierarchy elements, use the drop-down list for each group number to select the appropriate hierarchy element.

This enables you to have almost any ordering of locations in your access point names.

For example, if your access point is named: EastLab-Atrium2-3-SanFrancisco

If you use the regular expression: /((\d+)-(\d+)-(\d+)-(\d+))/

with the following group mapping:

1. Building
2. Device Name
3. Floor
4. Campus
Automatic Hierarchy Creation produces a campus named SanFrancisco, a building under that campus named EastLab, and a floor in EastLab named 3.

Note
The two hierarchy types, Not in device name and Device have no effect, but enable you to skip groups in case you need to use a matching group for some other purpose.

Automatic Hierarchy Creation requires the following groups to be mapped in order to compute a map on which to place the access point:

<table>
<thead>
<tr>
<th>Campus group present in match?</th>
<th>Building group present in match?</th>
<th>Floor group present in match?</th>
<th>Resulting location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Campus &gt; Building &gt; Floor</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Failed match</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Campus &gt; Floor (where Floor is an outdoor area)</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Failed match</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>System Campus &gt; Building &gt; Floor</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Failed match</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Failed match</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Failed match</td>
</tr>
</tbody>
</table>

Automatic Hierarchy Creation attempts to guess the floor index from the floor name. If the floor name is a number, AHC will assign the floor a positive floor index. If the floor name is a negative number or starts with the letter B (for example, b1, -4, or B2), AHC assigns the floor a negative floor index. This indicates that the floor is a basement.

When searching for an existing map on which to place the access point, AHC considers floors in the access point’s building with the same floor index as the access point’s name.

For example, if the map SF > MarketStreet > Sublevel1 exists and has a floor index of -1, then the access point SF-MarketStreet-b1-MON1 will be assigned to that floor.

Step 7 Click Next. You can test against more access points. You may test your regular expression and matching group mapping against more access points by entering the access point names in the Add more device names to test against field, and clicking Add.

You then click Test to test each of the access points names in the table. The result of each test is displayed in the table.

If required, return to the previous step to edit the regular expression or group mapping for the current regular expression.

Step 8 Click Next, then click Save and Apply. This applies the regular expression to the system. The system processes all the access points that are not assigned to a map.

Note You can edit the maps to include floor images, correct dimensions, and so on. When Automatic Hierarchy Creation creates a map, it uses the default dimensions of 20 feet by 20 feet. You will need to edit the created maps to specify the correct dimensions and other attributes.
Maps created using Automatic Hierarchy Creation appear in the maps list with an *incomplete* icon. Once you have edited a map, the *incomplete* icon disappears. You may hide the column for incomplete maps by clicking the Edit View link.

---

**Using the Map Editor**

You use the Map Editor to define, draw, and enhance floor plan information. The map editor allows you to create obstacles so that they can be taken into consideration while computing RF prediction heatmaps for access points. You can also add coverage areas for location appliances that locate clients and tags in that particular area.

The planning mode opens the map editor in the browser window from which the planning tool is launched. If the original browser window has navigated away from the floor page, you need to navigate back to the floor page to launch the map editor.

- Guidelines for Using the Map Editor, page 6-31
- Guidelines for Placing Access Points, page 6-32
- Guidelines for Inclusion and Exclusion Areas on a Floor, page 6-33
- Opening the Map Editor, page 6-34
- Map Editor Icons, page 6-34
- Using the Map Editor to Draw Coverage Areas, page 6-35
- Using the Map Editor to Draw Obstacles, page 6-36
- Defining an Inclusion Region on a Floor, page 6-36
- Defining an Exclusion Region on a Floor, page 6-37
- Defining a Rail Line on a Floor, page 6-38

**Guidelines for Using the Map Editor**

Consider the following when modifying a building or floor map using the map editor:

- We recommend that you use the map editor to draw walls and other obstacles rather than importing an .FPE file from the legacy floor plan editor.
  - If necessary, you can still import .FPE files. To do so, navigate to the desired floor area, choose **Edit Floor Area** from the Select a command drop-down list, click **Go**, select the **FPE File** check box, and browse to choose the .FPE file.

- You can add any number of walls to a floor plan with the map editor; however, the processing power and memory of a client workstation might limit the refresh and rendering aspects of the Prime Infrastructure.
  - We recommend a practical limit of 400 walls per floor for machines with 1 GB RAM or less.

- All walls are used by Prime Infrastructure when generating RF coverage heatmaps.
Guidelines for Placing Access Points

Place access points along the periphery of coverage areas to keep devices close to the exterior of rooms and buildings. Access points placed in the center of these coverage areas provide good data on devices that would otherwise appear equidistant from all other access points.

*Figure 6-3  Access Points Clustered Together*

![Figure 6-3 Access Points Clustered Together]

By increasing overall access point density and moving access points towards the perimeter of the coverage area, location accuracy is greatly improved.

*Figure 6-4  Improved Location Accuracy by Increasing Density*

![Figure 6-4 Improved Location Accuracy by Increasing Density]

In long and narrow coverage areas, avoid placing access points in a straight line. Stagger them so that each access point is more likely to provide a unique snapshot of a device location.

*Figure 6-5  Refrain From Straight Line Placement*

![Figure 6-5 Refrain From Straight Line Placement]
Although the design might provide enough access point density for high bandwidth applications, location suffers because each access point view of a single device is not varied enough; therefore, location is difficult to determine.

Move the access points to the perimeter of the coverage area and stagger them. Each has a greater likelihood of offering a distinctly different view of the device, resulting in higher location accuracy.

**Figure 6-6 Improved Location Accuracy by Staggering Around Perimeter**

![Diagram of access points staggered around perimeter]

Most current wireless handsets support only 802.11b/n, which offers only three non-overlapping channels. Therefore, wireless LANs designed for telephony tend to be less dense than those planned to carry data. Also, when traffic is queued in the Platinum QoS bucket (typically reserved for voice and other latency-sensitive traffic), lightweight access points postpone their scanning functions that allow them to peak at other channels and collect, among other things, device location information. The user has the option to supplement the wireless LAN deployment with access points set to monitor-only mode. Access points that perform only monitoring functions do not provide service to clients and do not create any interference. They simply scan the airwaves for device information.

Less dense wireless LAN installations, such as voice networks, find their location accuracy greatly increased by the addition and proper placement of monitor access points.

**Figure 6-7 Less Dense Wireless LAN Installations**

![Diagram of monitor access points]

Verify coverage using a wireless laptop, handheld, or phone to ensure that no fewer than three access points are detected by the device. To verify client and asset tag location, ensure that the Prime Infrastructure reports client devices and tags within the specified accuracy range (10 m, 90%).

---

**Note**
If you have a ceiling-mounted AP with an integrated omni-directional antenna, the antenna orientation does not really need to be set in the Prime Infrastructure. However, if you mount that same AP on the wall, you must set the antenna orientation to 90 degrees.

---

**Guidelines for Inclusion and Exclusion Areas on a Floor**

Inclusion and exclusion areas can be any polygon shape and must have at least three points.
You can only define one inclusion region on a floor. By default, an inclusion region is defined for each floor when it is added to the Prime Infrastructure. The inclusion region is indicated by a solid aqua line, and generally outlines the region.

You can define multiple exclusion regions on a floor.

Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.

### Opening the Map Editor

Follow these steps to use the map editor:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Monitor &gt; Site Map Design.</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the desired campus. The Site Maps &gt; Campus Name page appears.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click a campus and then click a building.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click the desired floor area. The Site Maps &gt; Campus Name &gt; Building Name &gt; Floor Area Name page appears.</td>
</tr>
<tr>
<td>Step 5</td>
<td>From the Select a command drop-down list, choose <strong>Map Editor</strong>, and click <strong>Go</strong>. The Map Editor page appears.</td>
</tr>
</tbody>
</table>

### Map Editor Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="https://example.com/scale-floor.png" alt="Scale Floor" /></td>
<td>Scale Floor—Click anywhere on the map to start drawing line. Double click to finish the line and enter the new line length in the popup shown. This will modify the floor dimensions to the new dimensions.</td>
</tr>
<tr>
<td><img src="https://example.com/measure-distance.png" alt="Measure Distance" /></td>
<td>Measure Distance—Click anywhere on the map to start drawing line. Double click to finish the line. Measured line length in ft/meters is shown on the top.</td>
</tr>
<tr>
<td><img src="https://example.com/copy-move-obstacles.png" alt="Copy/Move Obstacles" /></td>
<td>Copy/Move Obstacles—Select obstacles either by drawing a box on the map or by clicking the obstacles. To copy obstacles, click <strong>Copy</strong>. This will create new obstacles just above the selected obstacles. To move the obstacles, drag the selected obstacles to new position. Clicking anywhere on the map will unselect all the elements.</td>
</tr>
<tr>
<td><img src="https://example.com/delete-mode.png" alt="Delete Mode" /></td>
<td>Delete Mode—Select the elements to be deleted either by drawing a box on the map or clicking each element. Use Shift key to select multiple elements. Use the Ctrl key to toggle selection of elements, one at a time. Clicking anywhere on the map will unselect all the elements. Click <strong>Delete</strong> to delete the selected elements.</td>
</tr>
</tbody>
</table>
Using the Map Editor to Draw Coverage Areas

If you have a building that is non-rectangular or you want to mark a non-rectangular area within a floor, you can use the map editor to draw a coverage area.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Add the floor plan if it is not already represented in the Prime Infrastructure.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose Monitor &gt; Site Maps.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the Map Name that corresponds to the outdoor area, campus, building, or floor you want to edit.</td>
</tr>
<tr>
<td>Step 4</td>
<td>From the Select a command drop-down list, choose Map Editor, and click Go.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Map Editor page, click the Draw Coverage Area icon on the toolbar. A pop-up appears.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Enter the name of the area that you are defining. Click OK. A drawing tool appears.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Move the drawing tool to the area you want to outline.</td>
</tr>
<tr>
<td></td>
<td>• Click the left mouse button to begin and end drawing a line.</td>
</tr>
<tr>
<td></td>
<td>• When you have completely outlined the area, double-click the left mouse button and the area is highlighted in the page.</td>
</tr>
<tr>
<td></td>
<td>The outlined area must be a closed object to appear highlighted on the map.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Click the disk icon on the toolbar to save the newly drawn area.</td>
</tr>
</tbody>
</table>
Using the Map Editor to Draw Obstacles

Table 6-8 describes the obstacle color coding.

<table>
<thead>
<tr>
<th>Type of obstacle</th>
<th>Color coding</th>
<th>Loss (in dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thick wall</td>
<td></td>
<td>13</td>
</tr>
<tr>
<td>Light wall</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Heavy door</td>
<td></td>
<td>15</td>
</tr>
<tr>
<td>Light door</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Cubicle</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Glass</td>
<td></td>
<td>1.5</td>
</tr>
</tbody>
</table>

Defining an Inclusion Region on a Floor

To define an inclusion area, follow these steps:

**Step 1** Choose Monitor > Site Maps.
**Step 2** Click the name of the appropriate floor area.
**Step 3** From the Select a command drop-down list, choose Map Editor.
**Step 4** Click Go.
**Step 5** At the map, click the aqua box on the toolbar.

**Note** A message box appears reminding you that only one inclusion area can be defined at a time. Defining a new inclusion region automatically removes the previously defined inclusion region. By default, an inclusion region is defined for each floor when it is added to the Prime Infrastructure. The inclusion region is indicated by a solid aqua line and generally outlines the region.

**Step 6** Click OK in the message box that appears. A drawing icon appears to outline the inclusion area.
**Step 7** To begin defining the inclusion area, move the drawing icon to a starting point on the map and click once.
**Step 8** Move the cursor along the boundary of the area you want to include and click to end a border line. Click again to define the next boundary line.
Step 9  Repeat Step 8 until the area is outlined and then double-click the drawing icon. A solid aqua line defines the inclusion area.

Step 10  Choose Save from the Command menu or click the disk icon on the toolbar to save the inclusion region.

**Note**  If you made an error in defining the inclusion area, click the area. The selected area is outlined by a dashed aqua line. Next, click the X icon on the toolbar. The area is removed from the floor map.

Step 11  Select the Location Regions check box if it is not already selected. If you want it to apply to all floor maps, click Save settings. Close the Layers configuration page.

Step 12  To resynchronize the Prime Infrastructure and MSE databases, choose Services > Synchronize Services.

**Note**  If the two DBs are already synchronized then a resynchronization happens automatically every time there is a change. There is no need for an explicit resynch.

Step 13  In the Synchronize page, choose Network Designs from the Synchronize drop-down list and then click Synchronize.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

**Note**  Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.

### Defining an Exclusion Region on a Floor

To further refine location calculations on a floor, you can define areas that are excluded (exclusion areas) in the calculations. For example, you might want to exclude areas such as an atrium or stairwell within a building. As a rule, exclusion areas are generally defined within the borders of an inclusion area.

To define an exclusion area, follow these steps:

**Step 1**  Choose Monitor > Site Maps.

**Step 2**  Click the name of the appropriate floor area.

**Step 3**  From the Select a command drop-down list, choose Map Editor.

**Step 4**  Click Go.

**Step 5**  At the map, click the purple box on the toolbar.

**Step 6**  Click OK in the message box that appears. A drawing icon appears to outline the exclusion area.

**Step 7**  To begin defining the exclusion area, move the drawing icon to the starting point on the map, and click once.

**Step 8**  Move the drawing icon along the boundary of the area you want to exclude. Click once to start a boundary line, and click again to end the boundary line.
Step 9  Repeat Step 8 until the area is outlined and then double-click the drawing icon. The defined exclusion area is shaded in purple when the area is completely defined. The excluded area is shaded in purple.

Step 10  To define additional exclusion regions, repeat Step 5 to Step 9.

Step 11  When all exclusion areas are defined, choose Save from the Command menu or click the disk icon on the toolbar to save the exclusion region.

Note  To delete an exclusion area, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the X icon on the toolbar. The area is removed from the floor map.

Step 12  Select the Location Regions check box if it is not already selected, click Save settings, and close the Layers configuration page when complete.

Step 13  To resynchronize the Prime Infrastructure and location databases, choose Services > Synchronize Services.

Step 14  In the Synchronize page, choose Network Designs from the Synchronize drop-down list and then click Synchronize.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Defining a Rail Line on a Floor

You can define a rail line on a floor that represents a conveyor belt. Additionally, you can define an area around the rail area known as the snap-width to further assist location calculations. This represents the area in which you expect clients to appear. Any client located within the snap-width area is plotted on the rail line (majority) or just outside of the snap-width area (minority).

Note  Rail line configurations do not apply to tags.

The snap-width area is defined in feet or meters (user-defined) and represents the distance that is monitored on either side (east and west or north and south) of the rail.

To define a rail with a floor, follow these steps:

Step 1  Choose Monitor > Site Maps.

Step 2  Click the name of the appropriate floor area.

Step 3  Choose Map Editor from the Select a command drop-down list.

Step 4  Click Go.

Step 5  In the map, click the rail icon (to the right of the purple exclusion icon) on the toolbar.

Step 6  In the message dialog box that appears, enter a snap-width (feet or meters) for the rail and then click OK. A drawing icon appears.

Step 7  Click the drawing icon at the starting point of the rail line. Click again when you want to stop drawing the line or change the direction of the line.

Step 8  Click the drawing icon twice when the rail line is completely drawn on the floor map. The rail line appears on the map and is bordered on either side by the defined snap-width region.
Note: To delete a rail line, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the X icon on the toolbar. The area is removed from the floor map.

Step 9: At the floor map, choose the Layers drop-down list.

Step 10: Select the Rails check box if it is not already selected, click Save settings, and close the Layers configuration pane when complete.

Step 11: To resynchronize the Prime Infrastructure and mobility services engine, choose Services > Synchronize Services.

Step 12: In the Synchronize page, choose Network Designs from the Synchronize drop-down list and then click Synchronize.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

---

**Adding an Outdoor Area**

Note: You can add an outdoor area to a campus map in the Prime Infrastructure database regardless of whether you have added outdoor area maps to the database.

To add an outdoor area to a campus map, follow these steps:

Step 1: If you want to add a map of the outdoor area to the database, save the map in .PNG, .JPG, .JPEG, or .GIF format. Then browse to and import the map from anywhere in your file system.

Note: You do not need a map to add an outdoor area. You can simply define the dimensions of the area to add it to the database. The map can be any size because the Prime Infrastructure automatically resizes the map to fit the workspace.

Step 2: Choose Monitor > Site Maps.

Step 3: Click the desired campus to display the Monitor > Site Maps > Campus View page.

Step 4: From the Select a command drop-down list, choose New Outdoor Area.

Step 5: Click Go. The Create New Area page appears.

Step 6: In the New Outdoor Area page, enter the following information:

- **Name**—The user-defined name of the new outdoor area.
- **Contact**—The user-defined contact name.
- **Area Type (RF Model)**—Cubes And Walled Offices, Drywall Office Only, Outdoor Open Space (default).
- **AP Height (feet)**—Enter the height of the access point.
- **Image File**—Name of the file containing the outdoor area map. Click Browse to find the file.

Step 7: Click Next.
Step 8  Click **Place** to put the outdoor area on the campus map. Prime Infrastructure creates an outdoor area rectangle scaled to the size of the campus map.

Step 9  Click and drag the outdoor area rectangle to the desired position on the campus map.

Step 10  Click **Save** to save this outdoor area and its campus location to the database.

---

**Note**  A hyperlink associated with the outdoor area takes you to the corresponding Maps page.

Step 11  (Optional) To assign location presence information for the new outdoor area, choose **Edit Location Presence Info**, and click **Go**.

---

**Note**  By default, the Override Child Element Presence Info check box is selected. There is no need to alter this setting for outdoor areas.

---

**Using Chokepoints to Enhance Tag Location Reporting**

Installation of chokepoints provides enhanced location information for RFID tags. When an active Cisco-compatible Extensions Version 1-compliant RFID tag enters the range of a chokepoint, it is stimulated by the chokepoint. The MAC address of this chokepoint is then included in the next beacon sent by the stimulated tag. All access points that detect this tag beacon then forward the information to the controller and location appliance.

Using chokepoints in conjunction with active compatible extensions compliant tags provides immediate location information on a tag and its asset. When a Cisco-compatible Extension tag moves out of the range of a chokepoint, its subsequent beacon frames do not contain any identifying chokepoint information. Location determination of the tag defaults to the standard calculation methods based on RSSIs reported by the access point associated with the tag.

- Adding a Chokepoint to a Prime Infrastructure Map, page 6-41
- Positioning Chokepoints, page 6-42
- Adding Wi-Fi TDOA Receivers to the Prime Infrastructure Database, page 6-43
- Adding Wi-Fi TDOA Receivers to a Map, page 6-43
- Positioning Wi-Fi TDOA Receivers, page 6-44
- Managing RF Calibration Models, page 6-45

**Adding Chokepoints to the Prime Infrastructure Database**

Chokepoints are installed and configured as recommended by the Chokepoint vendor. After the chokepoint installation is complete and operational, the chokepoint can be entered into the location database and plotted on a Prime Infrastructure map.

To add a chokepoint to the Prime Infrastructure database, follow these steps:

---

**Step 1**  Choose **Configure > Chokepoints**.

**Step 2**  From the Select a command drop-down list, choose **Add Chokepoints**.
Step 3  Click Go.
Step 4  Enter the MAC address and name for the chokepoint.
Step 5  Select the Entry/Exit Chokepoint check box.
Step 6  Enter the coverage range for the chokepoint.

Note  The Chokepoint range is a visual representation only. It is product-specific. The actual range must be configured separately using the applicable chokepoint vendor software.

Step 7  Click OK.

Note  After the chokepoint is added to the database, it can be placed on the appropriate Prime Infrastructure floor map.

Adding a Chokepoint to a Prime Infrastructure Map

To add the chokepoint to a map, follow these steps:

Step 1  Choose Monitor > Site Maps.
Step 2  In the Maps page, choose the link that corresponds to the floor location of the chokepoint.
Step 3  From the Select a command drop-down list, choose Add Chokepoints.
Step 4  Click Go.

Note  The Add Chokepoints summary page lists all recently added chokepoints that are in the database but are not yet mapped.

Step 5  Select the check box next to the chokepoint that you want to place on the map.
Step 6  Click OK.

A map appears with a chokepoint icon located in the top left-hand corner. You are now ready to place the chokepoint on the map.

Step 7  Left-click the chokepoint icon and drag it to the proper location.

Note  The MAC address, name, and coverage range of the chokepoint appear in the dialog box in the left when you click the chokepoint icon for placement.

Step 8  Click Save.

You are returned to the floor map and the added chokepoint appears on the map.

Note  The newly created chokepoint icon might or might not appear on the map depending on the display settings for that floor.
Chapter 6  Monitoring Maps

Using Chokepoints to Enhance Tag Location Reporting

**Note**  The rings around the chokepoint icon indicate the coverage area. When a CCX tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.

**Note**  The MAC address, name, entry/exit chokepoint, static IP address, and range of the chokepoint appear when you hover your mouse cursor over its map icon.

**Step 9**  If the chokepoint does not appear on the map, select the **Chokepoints** check box located in the Floor Settings menu.

**Note**  Do not click **Save Settings** unless you want to save this display criteria for all maps.

**Note**  You must synchronize the network design to the mobility services engine or location server to push chokepoint information.

---

**Positioning Chokepoints**

To position chokepoints on the map, follow these steps:

**Step 1**  Left-click the **Chokepoint** icon and drag it to the proper location.

**Note**  The MAC address, name, and coverage range of the chokepoint appear in the dialog box in the left when you click the chokepoint icon for placement.

**Step 2**  Click **Save** when the icon is correctly placed on the map.

**Step 3**  The newly created chokepoint icon might or might not appear on the map depending on the display settings for that floor.

**Note**  The rings around the chokepoint icon indicate the coverage area. When a Cisco-compatible Extensions tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. The chokepoint range is provided as a visual only, but chokepoint vendor software is required to actually configure the range. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.

**Note**  The MAC address, name, and range of a chokepoint are displayed when you hover your mouse cursor over its map icon.
Step 4 If the chokepoint does not appear on the map, choose Layers to view a drop-down list of possible elements to display on the map. Select the Chokepoints check box.

Note Do not click Save Settings unless you want to save this display criteria for all maps.

Note You can change the position of chokepoints by importing or exporting a file.

Configuring Wi-Fi TDOA Receivers

- Adding Wi-Fi TDOA Receivers to the Prime Infrastructure Database, page 6-43
- Adding Wi-Fi TDOA Receivers to a Map, page 6-43
- Positioning Wi-Fi TDOA Receivers, page 6-44
- Managing RF Calibration Models, page 6-45
- Managing Location Presence Information, page 6-50

Adding Wi-Fi TDOA Receivers to the Prime Infrastructure Database

To add Wi-Fi TDOA receivers to the Prime Infrastructure database, follow these steps:

Step 1 Choose Configure > WiFi TDOA Receivers.
Step 2 From the Select a command drop-down list, choose Add WiFi TDOA Receivers.
Step 3 Click Go.
Step 4 Enter the MAC address, name, and static IP address for the Wi-Fi TDOA receiver.

Note Wi-Fi TDOA receivers are configured separately using the Wi-Fi TDOA receiver vendor software.

Step 5 Click OK to save the Wi-Fi TDOA receiver entry to the database.

Note After the Wi-Fi TDOA receiver is added to the database, place it on the appropriate Prime Infrastructure floor map. See the “Adding Wi-Fi TDOA Receivers to the Prime Infrastructure Database” section on page 6-43 for more information.

Adding Wi-Fi TDOA Receivers to a Map

To add a WiFi TDOA receiver to a map, follow these steps:
Step 1 Choose Monitor > Site Maps.
Step 2 Choose the link that corresponds to the floor location of the Wi-Fi TDOA receiver.
Step 3 From the Select a command drop-down list, choose Add WiFi TDOA Receivers.
Step 4 Click Go.

Note: The Add WiFi TDOA Receivers summary page lists all recently added Wi-Fi TDOA receivers that are in the database but are not yet mapped.

Step 5 Select the check box next to the Wi-Fi TDOA receiver to be added to the map.
Step 6 Click OK.

A map appears with a green WiFi TDOA receiver icon located in the top left-hand corner. You are now ready to position the Wi-Fi TDOA receiver on the map.

Positioning Wi-Fi TDOA Receivers

To position Wi-Fi TDOA receivers on the map, follow these steps:

Step 1 Left-click the WiFi TDOA receiver icon and drag it to the proper location.

Note: The MAC address and name of the Wi-Fi TDOA receiver appear in the left pane when you click the WiFi TDOA receiver icon for placement.

Step 2 Click Save when the icon is correctly placed on the map.

Note: The MAC address of the Wi-Fi TDOA receiver appears when you hover your mouse cursor over its map icon.

Step 3 If the chokepoint does not appear on the map, click Layers to view a drop-down list of possible elements to display on the map. Select the WiFi TDOA Receivers check box.

Note: Do not select Save Settings unless you want to save this display criteria for all maps.

Note: You can change the position of Wi-Fi TDOA Receivers by importing or exporting a file.
Managing RF Calibration Models

If the provided RF models do not sufficiently characterize the floor layout, you can create a calibration model that is applied to the floor and better represents the attenuation characteristics of that floor. The calibration models are used as RF overlays with measured RF signal characteristics that can be applied to different floor areas. This enables the Cisco WLAN solution installation team to lay out one floor in a multi-floor area, use the RF calibration tool to measure, save the RF characteristics of that floor as a new calibration model, and apply that calibration model to all the other floors with the same physical layout.

You can collect data for a calibration using one of two methods:

- Point mode data collection—Calibration points are selected and their coverage area is calculated one location at a time.
- Linear mode data collection—A series of linear paths are selected and then calculated as you traverse the path. This approach is generally faster than the point mode data collection. You can also employ point mode data collection to augment data collection for locations missed by the linear paths.

Note Calibration models can only be applied to clients, rogue clients, and rogue access points. Calibration for tags is done using the Aeroscout System Manager. See the following URL for details on tag calibration at: http://support.aeroscout.com.

Note We recommend client device that supports both 802.11a/n and 802.11b/g/n radios to expedite the calibration process for both spectrums.

Use a laptop or other wireless device to open a browser to Prime Infrastructure server and perform the calibration process.

- Accessing Current Calibration Models, page 6-45
- Applying Calibration Models to Maps, page 6-46
- Viewing Calibration Model Properties, page 6-46
- Viewing Calibration Model Details, page 6-46
- Creating New Calibration Models, page 6-47
- Starting Calibration Process, page 6-47
- Calibrating, page 6-49
- Apply the Model to the Floor, page 6-50
- Deleting Calibration Models, page 6-50

Accessing Current Calibration Models

To access current calibration models, follow these steps:

**Step 1** Choose **Monitor > Site Maps**.

**Step 2** From the Select a command drop-down list, choose **RF Calibration Models**. The Model Name and Status for each calibration model are listed.
Step 3

Click the model name to access a specific calibration model.

---

**Applying Calibration Models to Maps**

To apply a current calibration model to a map, follow these steps:

**Step 1** Choose Monitor > Site Maps.

**Step 2** From the Select a command drop-down list, choose RF Calibration Models.

**Step 3** Click the model name to access the applicable calibration model.

**Step 4** From the Select a command drop-down list, choose Apply to Maps.

**Step 5** Click Go.

---

**Viewing Calibration Model Properties**

To view or edit current calibration models, follow these steps:

**Step 1** Choose Monitor > Site Maps.

**Step 2** From the Select a command drop-down list, choose RF Calibration Models.

**Step 3** Click the model name to access the applicable calibration model.

**Step 4** From the Select a command drop-down list, choose Properties.

**Step 5** Click Go to view or edit calibration model details. See the “Viewing Calibration Model Properties” section on page 6-46 for more information.

---

**Viewing Calibration Model Details**

To edit calibration model details, follow these steps:

**Step 1** Choose Monitor > Site Maps.

**Step 2** From the Select a command drop-down list, choose RF Calibration Models.

**Step 3** Click the model name to access the applicable calibration model.

**Step 4** From the Select a command drop-down list, choose Properties.

**Step 5** Click Go.

**Step 6** The following parameters might be edited:

- Sweep Client Power for Location—Click to enable. You might want to enable this if a high density of access points exists and transmit power is reduced or unknown. The sweeping range of client transmit power might improve accuracy but scalability is negatively affected.

- HeatMap Binsize—Choose 4, 8, 16, or 32 from the drop-down list.
• HeatMap Cutoff—Determine the heatmap cutoff. We recommend a low heatmap cutoff especially if the access point density is high and RF propagation conditions are favorable. A higher cutoff value increases scalability but might cause difficulty when locating clients.

**Step 7** When any necessary changes have been made or to exit the page, click **OK**.

### Creating New Calibration Models

To create a new calibration model, follow these steps:

**Step 1** Choose **Monitor > Site Maps**.

**Step 2** From the Select a command drop-down list, choose **RF Calibration Models**.

**Step 3** Click **Go**.

**Step 4** From the Select a command drop-down list, choose **Create New Model**.

**Step 5** Click **Go**.

**Step 6** Enter a model name, and click **OK**.

The new model appears along with the other RF calibration models with a status of Not Yet Calibrated.

### Starting Calibration Process

To start the calibration process, follow these steps:

**Step 1** Click the model name to open the Calibration Model > Model Name page.

**Step 2** From the Select a command drop-down list, choose **Add Data Points**.

**Step 3** Click **Go**.

**Step 4** Enter the MAC address of the device being used to perform the calibration. Manually-entered MAC addresses must be delimited with colons (such as FF:FF:FF:FF:FF:FF).

**Note** If this process is being performed from a mobile device connected to the Prime Infrastructure through the Cisco Centralized architecture, the MAC address text box is automatically populated with the device address.

**Step 5** Choose the appropriate campus, building, floor, or outdoor area where the calibration is performed.

**Note** The calibration in the outdoor area is supported in Release 1.0.x and later. You can use this option to add the calibration data points to the outdoor area. The data points can be added to the outdoor area using the same procedure for calibration.

**Step 6** Click **Next**.

**Step 7** When the chosen floor map and access point locations appear, a grid of plus marks (+) indicates the locations where data collection for calibration is performed.
Using these locations as guidelines, you can perform either a point or linear collection of data by appropriate placement of either the Calibration Point pop-up (point) or the Start and Finish pop-ups (linear) that appear on the map when the respective options are displayed.

If you want to perform a point collection of data for the calibration, do the following:

a. Choose **Point** from the Collection Method drop-down list and select the **Show Data points** check box if not already selected. A calibration point pop-up appears on the map.

b. Position the tip of the calibration point pop-up at a data point (+), and click **Go**. A dialog box appears showing the progress of the data collection.

**Note** Rotate the calibrating client laptop during data collection so that the client is heard evenly by all access points in the vicinity.

c. When the data collection is complete for a selected data point and the coverage area is plotted on the map, move the calibration point pop-up to another data point, and click **Go**.

**Note** The coverage area plotted on the map is color-coded and corresponds with the specific wireless LAN standard used to collect that data. Information on color-coding is provided in legend on the left side of the page. Additionally, the progress of the calibration process is indicated by two status bars above the legend, one for 802.11a/n and one for 802.11b/g/n.

**Note** To delete data points for locations selected in error, click **Delete** and move the black square that appears over the appropriate data points. Resize the square as necessary by pressing **Ctrl** and moving the mouse.

d. Repeat point collection Steps a. to c. until the calibration status bar of the relevant spectrums (802.11a/n, 802.11b/g/n) display as ‘done.’

**Note** The calibration status bar indicates data collection for the calibration as done after roughly 50 distinct locations and 150 measurements have been gathered. For every location point saved in the calibration process, more than one data point is gathered. The progress of the calibration process is indicated by two status bars above the legend, one for 802.11b/g/n and one for 802.11a/n.

If you want to perform a linear collection of data for the calibration, do the following:

a. Choose **Linear** from the Collection Method drop-down list, and select the **Show Data points** check box if not already selected. A line appears on the map with both Start and Finish pop-ups.

b. Position the tip of the Start pop-up at the starting data point.

c. Position the Finish pop-up at the ending data point.

d. Position yourself with your laptop at the starting data point, and click **Go**. Walk steadily towards the end point along the defined path. A dialog box appears to show that data collection is in process.

**Note** Do not stop data collection until you reach the end point even if the data collection bar indicates completion.
Note: Only Intel and Cisco adapters have been tested. Make sure Enable Cisco-compatible Extensions and Enable Radio Management Support are enabled in the Cisco-compatible Extension Options.

e. Press the space bar (or Done on the data collection panel) when you reach the end point. The collection pane displays the number of samples taken before it closes to reveal the map. The map displays all the coverage areas where data was collected.

Note: To delete data points for locations selected in error, click Delete and move the black square that appears over the appropriate data points. Resize the square as necessary by pressing the Ctrl and moving the mouse.

Note: The coverage area is color-coded and corresponds with the specific wireless LAN standard used to collect that data. Information on color-coding is provided in legend on the left-hand side of the page.

f. Repeat linear collection Steps b to e until the status bar for the respective spectrum is filled in (done).

Note: You can augment linear collection with point mode data collection to address missed coverage areas.

Step 8 Click the name of the calibration model at the top of the page to return to the main page for that model to calibrate the data points.

Step 9 Choose Calibrate from the Select a command drop-down list, and click Go.

Step 10 Click the Inspect Location Quality link when calibration completes. A map displays showing RSSI readings displays.

Step 11 To use the newly created calibration model, you must apply the model to the floor on which it was created (and on any other floors with similar attenuation characteristics as well). Choose Monitor > Site Maps and find the specific floor to which the model is applied. At the floor map interface, choose Edit Floor Area from the drop-down list, and click Go.

Step 12 From the Floor Type (RF Model) drop-down list, choose the newly created calibration model. Click OK to apply the model to the floor.

Note: This process can be repeated for as many models and floors as needed. After a model is applied to a floor, all location determination performed on that floor is done using the specific collected attenuation data from the calibration model.

Calibrating

To compute the collected data points, follow these steps:

Step 1 Click the model name to open the Calibration Model > Model Name page.
Apply the Model to the Floor

To use the newly created calibration model, you must apply the model to the floor on which it was created (along with other floors with similar attenuation characteristics).

To apply the model to the floor, follow these steps:

Step 1  Choose Monitor > Site Maps.
Step 2  Locate the specific floor to which the model is applied.
Step 3  From the Select a command drop-down list, choose Edit Floor Area.
Step 4  Click Go.
Step 5  From the Floor Type (RF Model) drop-down list, choose the newly-created calibration model.
Step 6  Click OK to apply the model to the floor.

This process can be repeated for as many models and floors as needed. After a model is applied to a floor, all location determination performed on that floor is done using the specific collected attenuation data from the calibration model.

Deleting Calibration Models

To delete a calibration model, follow these steps:

Step 1  Click the model name to open the Calibration Model > Model Name page.
Step 2  From the Select a command drop-down list, choose Delete Model.
Step 3  Click Go.

Managing Location Presence Information

You can enable location presence through mobility services engine to provide expanded Civic (city, state, postal code, country) and GEO (longitude, latitude) location information beyond the Cisco default setting (campus, building, floor, and X, Y coordinates). This information can then be requested by clients on a demand basis for use by location-based services and applications. See the “Enabling Location Presence for Mobility Services” section on page 16-49 for more information on enabling location presence.

To view or edit current location presence information for a current map, follow these steps:

Step 1  Choose Monitor > Site Maps.
Step 2  Select the check box of the map.
Step 3  From the Select a command drop-down list, choose Location Presence.
Step 4  Click Go.

Searching Maps

You can use the following parameters in the Search Maps page:
- Search for
- Map Name
- Search in
- Save Search
- Items per page

After you click Go, the map search results page appears (see Table 6-9).
Using the Map Editor

You can use the Prime Infrastructure map editor to define, draw, and enhance floor plan information.

- Opening the Map Editor, page 6-52
- Using the Map Editor to Draw Polygon Areas, page 6-53
- Defining an Inclusion Region on a Floor, page 6-53
- Defining an Exclusion Region on a Floor, page 6-55
- Defining a Rail Line on a Floor, page 6-55

Opening the Map Editor

Follow these steps to use the map editor:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Monitor &gt; Site Maps to display the Maps page.</td>
</tr>
<tr>
<td>2</td>
<td>Click the desired campus. The Site Maps &gt; Campus Name page appears.</td>
</tr>
<tr>
<td>3</td>
<td>Click a campus and then click a building.</td>
</tr>
<tr>
<td>4</td>
<td>Click the desired floor area. The Site Maps &gt; Campus Name &gt; Building Name &gt; Floor Area Name page appears.</td>
</tr>
<tr>
<td>5</td>
<td>From the Select a command drop-down list, choose Map Editor, and click Go. The Map Editor page appears.</td>
</tr>
</tbody>
</table>

Note: Make sure that the floor plan images are properly scaled so that all white space outside of the external walls is removed. To make sure that floor dimensions are accurate, click the compass tool on the toolbar.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Position the reference length. When you do, the Scale menu appears with the line length supplied. Enter the dimensions (width and height) of the reference length, and click OK.</td>
</tr>
<tr>
<td>7</td>
<td>Determine the propagation pattern from the Antenna Mode drop-down list.</td>
</tr>
<tr>
<td>8</td>
<td>Make antenna adjustments by sliding the antenna orientation bar to the desired degree of direction.</td>
</tr>
<tr>
<td>9</td>
<td>Choose the desired access point.</td>
</tr>
</tbody>
</table>

Table 6-9 Map Search Results

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Clicking an item in the Name column provides a map of an existing building with individual floor area maps for each floor.</td>
</tr>
<tr>
<td>Type</td>
<td>Campus, building, or floor area.</td>
</tr>
<tr>
<td>Total APs</td>
<td>Displays the total number of Cisco Radios detected.</td>
</tr>
<tr>
<td>a/n Radios</td>
<td>Displays the number of 802.11a/n Cisco Radios.</td>
</tr>
<tr>
<td>b/g/n Radios</td>
<td>Displays the number of 802.11b/g/n Cisco Radios.</td>
</tr>
</tbody>
</table>
Using the Map Editor to Draw Polygon Areas

If you have a building that is non-rectangular or you want to mark a non-rectangular area within a floor, you can use the map editor to draw a polygon-shaped area.

---

**Step 1** Add the floor plan if it is not already represented in the Prime Infrastructure (see the “Adding Floor Areas” section on page 6-6).

**Step 2** Choose **Monitor > Site Maps**.

**Step 3** Click the Map Name that corresponds to the outdoor area, campus, building, or floor you want to edit.

**Step 4** From the Select a command drop-down list, choose **Map Editor**, and click **Go**.

**Step 5** If the Map Editor page, click the **Add Perimeter** icon on the toolbar.

A pop-up appears.

**Step 6** Enter the name of the area that you are defining. Click **OK**.

A drawing tool appears.

**Step 7** Move the drawing tool to the area you want to outline.

- Click the left mouse button to begin and end drawing a line.
- When you have completely outlined the area, double-click the left mouse button and the area is highlighted in the page.

The outlined area must be a closed object to appear highlighted on the map.

**Step 8** Click the disk icon on the toolbar to save the newly drawn area.

**Step 9** Choose **Command > Exit** to close the window. You are returned to the original floor plan.

---

**Note** When you return to the original floor plan view after exiting the map editor, the newly drawn area is not visible; however, it appears in the Planning Model page when you add elements.

**Step 10** Choose **Planning Mode** from the Select a command drop-down list to begin adding elements to the newly defined polygon-shaped area. See **Table 6-8** for the obstacle color coding.

---

**Note** The RF prediction heatmaps for access points approximates of the actual RF signal intensity. It takes into account the attenuation of obstacles drawn using the Map Editor but it does not take into account the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects of RF signals bouncing off obstructions. The thick wall (color-coded orange) with a loss of 13 dB might not be enough to contain the RF signal beyond the walls of the heatmap.

---

**Defining an Inclusion Region on a Floor**

To define an inclusion area, follow these steps:
**Using the Map Editor**

**Chapter 6  Monitoring Maps**

**Step 1**  Choose **Monitor > Site Maps**.

**Step 2**  Click the name of the appropriate floor area.

**Step 3**  From the Select a command drop-down list, choose **Map Editor**.

**Step 4**  Click **Go**.

**Step 5**  At the map, click the aqua box on the toolbar.

---

**Note** A message box appears reminding you that only one inclusion area can be defined at a time. Defining a new inclusion region automatically removes the previously defined inclusion region. By default, an inclusion region is defined for each floor when it is added to the Prime Infrastructure. The inclusion region is indicated by a solid aqua line and generally outlines the region.

**Step 6**  Click **OK** in the message box that appears. A drawing icon appears to outline the inclusion area.

**Step 7**  To begin defining the inclusion area, move the drawing icon to a starting point on the map and click once.

**Step 8**  Move the cursor along the boundary of the area you want to include and click to end a border line. Click again to define the next boundary line.

**Step 9**  Repeat **Step 8** until the area is outlined and then double-click the drawing icon. A solid aqua line defines the inclusion area.

**Step 10**  Choose **Save** from the Command menu or click the **disk** icon on the toolbar to save the inclusion region.

---

**Note** If you made an error in defining the inclusion area, click the area. The selected area is outlined by a dashed aqua line. Next, click the **X** icon on the toolbar. The area is removed from the floor map.

**Step 11**  To return to the floor map to enable inclusion regions on heatmaps, choose **Exit** from the Command menu.

**Step 12**  Select the **Location Regions** check box if it is not already selected. If you want it to apply to all floor maps, click **Save settings**. Close the Layers configuration page.

**Step 13**  To resynchronize the Prime Infrastructure and MSE databases, choose **Services > Synchronize Services**.

---

**Note** If the two DBs are already synchronized then a resynchronization happens automatically every time there is a change. There is no need for an explicit resynch.

**Step 14**  In the Synchronize page, choose **Network Designs** from the Synchronize drop-down list and then click **Synchronize**.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

---

**Note** Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.
Defining an Exclusion Region on a Floor

To further refine location calculations on a floor, you can define areas that are excluded (exclusion areas) in the calculations. For example, you might want to exclude areas such as an atrium or stairwell within a building. As a rule, exclusion areas are generally defined within the borders of an inclusion area.

To define an exclusion area, follow these steps:

**Step 1** Choose **Monitor > Site Maps**.

**Step 2** Click the name of the appropriate floor area.

**Step 3** From the Select a command drop-down list, choose **Map Editor**.

**Step 4** Click **Go**.

**Step 5** At the map, click the purple box on the toolbar.

**Step 6** Click **OK** in the message box that appears. A drawing icon appears to outline the exclusion area.

**Step 7** To begin defining the exclusion area, move the drawing icon to the starting point on the map, and click once.

**Step 8** Move the drawing icon along the boundary of the area you want to exclude. Click once to start a boundary line, and click again to end the boundary line.

**Step 9** Repeat **Step 8** until the area is outlined and then double-click the drawing icon. The defined exclusion area is shaded in purple when the area is completely defined. The excluded area is shaded in purple.

**Step 10** To define additional exclusion regions, repeat **Step 5** to **Step 9**.

**Step 11** When all exclusion areas are defined, choose **Save** from the Command menu or click the disk icon on the toolbar to save the exclusion region.

**Note** To delete an exclusion area, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the X icon on the toolbar. The area is removed from the floor map.

**Step 12** To return to the floor map to enable exclusion regions on heatmaps, choose **Exit** from the Command menu.

**Step 13** Select the **Location Regions** check box if it is not already selected, click **Save settings**, and close the Layers configuration page when complete.

**Step 14** To resynchronize the Prime Infrastructure and location databases, choose **Services > Synchronize Services**.

**Step 15** In the Synchronize page, choose **Network Designs** from the Synchronize drop-down list and then click **Synchronize**.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Defining a Rail Line on a Floor

You can define a rail line on a floor that represents a conveyor belt. Additionally, you can define an area around the rail area known as the snap-width to further assist location calculations. This represents the area in which you expect clients to appear. Any client located within the snap-width area is plotted on the rail line (majority) or just outside of the snap-width area (minority).
Inspecting Location Readiness and Quality

You can configure Prime Infrastructure to verify the ability of the existing access point deployment to estimate the true location of a client, rogue client, rogue access point, or tag within 10 meters at least 90% of the time. The location readiness calculation is based on the number and placement of access points.

You can also check the location quality and the ability of a given location to meet the location specification (10 m, 90%) based on data points gathered during a physical inspection and calibration.
Inspecting Location Readiness

The Inspect Location Readiness feature is a distance-based predictive tool that can point out problem areas with access point placement.

To access the Inspect Location Readiness tool, follow these steps:

**Step 1** Choose Monitor > Site Maps.

**Step 2** Click the applicable floor area name to view the map.

**Note** If RSSI is not displayed, you can enable AP Heatmaps by selecting the AP Heatmaps check box on the left sidebar menu.

**Note** If clients, tags, and access points are not displayed, verify that their respective check boxes are selected on the left sidebar menu. Licenses for both clients and tags must also be purchased for each to be tracked.

**Step 3** From the Select a command drop-down list, choose Inspect Location Readiness.

**Step 4** Click Go.

A color-coded map appears showing those areas that meet (indicated by Yes) and do not meet (indicated by No) the ten meter, 90% location specification.

Inspecting Location Quality Using Calibration Data

After completing a calibration model based on data points generated during a physical tour of the area, you can inspect the location quality of the access points.

To inspect location quality based on calibration, follow these steps:

**Step 1** Choose Monitor > Site Maps.

**Step 2** Choose RF Calibration Model from the Select a command list. Click Go.

A list of calibration models appears.

**Step 3** Click the appropriate calibration model.

Details on the calibration including date of last calibration, number of data points by signal type (802.11a, 802.11 b/g) used in the calibration, location, and coverage are displayed.

**Step 4** In the same page, click the Inspect Location Quality link found under the Calibration Floors heading.

A color-coded map noting percentage of location errors appears.

**Note** You can modify the distance selected to see the effect on the location errors.
Inspecting VoWLAN Readiness

The VoWLAN Readiness (voice readiness) tool allows you to check the RF coverage to determine if it is sufficient for your voice needs. This tool verifies RSSI levels after access points have been installed. To access the VoWLAN Readiness Tool (VRT), follow these steps:

**Step 1** Choose Monitor > Site Maps.

**Step 2** Click the applicable floor area name.

**Step 3** From the Select a command drop-down list, choose Inspect VoWLAN Readiness.

**Step 4** Choose the applicable Band, AP Transmit Power, and Client parameters from the drop-down lists.

*Note* By default, the region map displays the b/g/n band for Cisco Phone-based RSSI threshold. The new settings cannot be saved.

**Step 5** Depending on the selected client, the following RSSI values might not be editable:

- Cisco Phone—RSSI values are not editable.
- Custom—RSSI values are editable with the following ranges:
  - Low threshold between -95dBm to -45dBm
  - High threshold between -90dBm to -40dBm

**Step 6** The following color schemes indicate whether or not the area is voice ready:

- Green—Yes
- Yellow—Marginal
- Red—No

*Note* The accuracy of the Green/Yellow/Red regions depends on the RF environment and whether or not the floor is calibrated. If the floor is calibrated, the accuracy of the regions is enhanced.

Troubleshooting Voice RF Coverage Issues

- Floors with either calibration or no calibration data are treated as follows:
  - Set the AP Transmit field to Max (the maximum downlink power settings). If the map still shows some yellow or red regions, more access points are required to cover the floor.
  - If the calibrated model shows red or yellow regions (where voice is expected to be deployed) with the AP Transmit field set to Current, increasing the power level of the access points might help.
Monitoring Mesh Networks Using Maps

You can access and view details for the following elements from a mesh network map in the Prime Infrastructure:

- Mesh Link Statistics
- Mesh Access Points
- Mesh Access Point Neighbors

Details on how this information is accessed and displayed for each of these items is detailed in this section.

- Monitoring Mesh Access Points Using Maps, page 6-60
- Monitoring Mesh Access Point Neighbors Using Maps, page 6-62
- Viewing the Mesh Network Hierarchy, page 6-62
- Using Mesh Filters to Modify Map Display of Maps and Mesh Links, page 6-63

Monitoring Mesh Link Statistics Using Maps

You can view the SNR for a specific mesh network link, view the number of packets transmitted and received on that link, and initiate a link test in the Monitor > Site Maps page.

To view details on a specific mesh link between two mesh access points or a mesh access point and a root access point, follow these steps:

**Step 1** Choose Monitor > Site Maps.

**Step 2** Click the map name that corresponds to the outdoor area, campus, building, or floor you want to monitor.

**Step 3** From the left sidebar menu, click the arrow to the right of AP Mesh Info. The Mesh Filter dialog box appears.

**Step 4** Move the cursor over the colored dot next to each mesh access point child to view details on the link between it and its parent. Table 6-10 summarizes the parameters that appear.

The Bridging Link information appears.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information fetched on</td>
<td>Date and time that information was compiled.</td>
</tr>
<tr>
<td>Link SNR</td>
<td>Link signal-to-noise ratio (SNR).</td>
</tr>
<tr>
<td>Link Type</td>
<td>Hierarchical link relationship.</td>
</tr>
</tbody>
</table>
Monitoring Mesh Networks Using Maps

Step 5  Click either Link Test, Child to Parent or Link Test, Parent to Child. After the link test is complete, a results page appears.

Note  A link test runs for 30 seconds.

Note  You cannot run link tests for both links (child-to-parent and parent-to-child) at the same time.

Step 6  To view a graphical representation of SNR statistics over a period of time, click the arrow on the link. A page with multiple SNR graphs appears.

The following graphs are displayed for the link:

- **SNR Up**—Plots the RSSI values of the neighbor from the perspective of the access point.
- **SNR Down**—Plots the RSSI values that the neighbor reports to the access point.
- **Link SNR**—Plots a weighed and filtered measurement based on the SNR Up value.
- **The Adjusted Link Metric**—Plots the value used to determine the least cost path to the root access point. This value represents the ease of getting the rooftop access point and accounts for the number of hops. The lower the ease value, the less likely the path is used.
- **The Unadjusted Link Metric**—Plots the least cost path to get to the root access point unadjusted by the number of hops. The higher the value for the unadjusted link, the better the path.

### Monitoring Mesh Access Points Using Maps

You can view the following summary information for a mesh access point from a mesh network map:

- Parent
- Number of children
- Hop count
- Role
- Group name
- Backhaul interface
- Data Rate
To view summary and detailed configuration information for a mesh access point from a mesh network map, follow these steps:

**Step 1** Choose **Monitor > Site Maps**.

**Step 2** Click the map name that corresponds to the outdoor area, campus, building, or floor location of the access point you want to monitor.

**Step 3** To view summary configuration information for an access point, hover your mouse cursor over the access point that you want to monitor. A dialog box with configuration information for the selected access point appears.

**Step 4** To view detailed configuration information for an access point, double-click the access point appearing on the map. The configuration details for the access point appear.

**Note** For more details on the View Mesh Neighbors link in the access point dialog box, see the “Monitoring Mesh Access Point Neighbors Using Maps” section on page 6-62. If the access point has an IP address, a Run Ping Test link is also visible at the bottom of the mesh access point dialog box.

**Step 5** In the Access Point Details configuration page, follow these steps to view configuration details for the mesh access point:

- **a.** Click the **General** tab to view the overall configuration of the mesh access point such as the AP name, MAC address, AP Up time, associated controllers (registered and primary) operational status, and software version.

  **Note** The software version for mesh access points is appended with the letter *m* and the word *mesh* appears in parentheses.

- **b.** Click the **Interface** tab to view configuration details for the interfaces supported on the mesh access point. Interface options are radio and Ethernet.

- **c.** Click the **Mesh Links** tab to view parent and neighbor details (name, MAC address, packet error rate, and link details) for the mesh access point. You can also initiate link tests from this page.

- **d.** Click the **Mesh Statistics** tab to view details on the bridging, queue, and security statistics for the mesh access point. For more details on mesh statistics, see the “Mesh Statistics Tab” section on page 5-81.
Chapter 6  Monitoring Maps

Monitoring Mesh Access Point Neighbors Using Maps

To view details on neighbors of a mesh access point from a mesh network map, follow these steps:

**Step 1**  Choose Monitor > Site Maps.

**Step 2**  Click the map name that corresponds to the outdoor area, campus, building, or floor you want to monitor.

**Step 3**  To view detailed information on mesh links for a mesh access point, click the arrow portion of the access point label. The Access Points page appears.

**Step 4**  Click the Mesh Links tab.

**Note**  You can also view mesh link details for neighbors of a selected access point by clicking the View Mesh Neighbors link on the Mesh tab of the access point configuration summary dialog box, which appears when you hover your mouse cursor over an access point on a map.

**Note**  Signal-to-noise (SNR) appears in the View Mesh Neighbors dialog box.

**Note**  In addition to listing the current and past neighbors in the dialog box that appears, labels are added to the mesh access points map icons to identify the selected access point, the neighbor access point, and the child access point. Click the clear link of the selected access point to remove the relationship labels from the map.

**Note**  The drop-down lists at the top of the mesh neighbors page indicate the resolution of the map (100%) displayed and how often the information displayed is updated (every 5 mins). You can modify these default values.

Viewing the Mesh Network Hierarchy

You can view the parent-child relationship of mesh access points within a mesh network in an easily navigable display. You can also filter which access points are displayed in the map view by selecting only access points of interest.

To view the mesh network hierarchy for a selected network, follow these steps:

**Step 1**  Choose Monitor > Site Maps.

**Step 2**  Click the map name you want to display.

**Step 3**  Select the AP Mesh Info check box in the left sidebar menu if it is not already selected.

**Note**  The AP Mesh Info check box is only selectable if mesh access points are present on the map. It must be selected to view the mesh hierarchy.
Step 4  Click the blue arrow to the right of the AP Mesh Info to display the Mesh Parent-Child Hierarchical View.

Step 5  Click the plus (+) sign next to a mesh access point to display its children.

All subordinate mesh access points are displayed when a negative (-) sign appears next to the parent mesh access point entry. For example, the access point, *indoor-mesh-45-rap2*, has only one child, *indoor-mesh-44-map2*.

Step 6  Hover your mouse cursor over the colored dot next to each mesh access point child to view details on the link between it and its parent. Table 6-11 summarizes the parameters that appear.

The color of the dot also provides a quick reference point of the SNR strength:

- A green dot represents a high SNR (above 25 dB).
- An amber dot represents an acceptable SNR (20-25 dB).
- A red dot represents a low SNR (below 20 dB).
- A black dot indicates a root access point.

**Table 6-11  Bridging Link Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information fetched on</td>
<td>Date and time that information was compiled.</td>
</tr>
<tr>
<td>Link SNR</td>
<td>Link signal-to-noise ratio (SNR).</td>
</tr>
<tr>
<td>Link Type</td>
<td>Hierarchical link relationship.</td>
</tr>
<tr>
<td>SNR Up</td>
<td>Signal-to-noise radio for the uplink (dB).</td>
</tr>
<tr>
<td>SNR Down</td>
<td>Signal-to-noise radio for the downlink (dB).</td>
</tr>
<tr>
<td>PER</td>
<td>The packet error rate for the link.</td>
</tr>
<tr>
<td>Tx Parent Packets</td>
<td>The TX packets to a node while acting as a parent.</td>
</tr>
<tr>
<td>Rx Parent Packets</td>
<td>The RX packets to a node while acting as a parent.</td>
</tr>
<tr>
<td>Time of Last Hello</td>
<td>Date and time of last hello.</td>
</tr>
</tbody>
</table>

Using Mesh Filters to Modify Map Display of Maps and Mesh Links

In the mesh hierarchical page, you can also define mesh filters to determine which mesh access points display on the map based on hop values as well as what labels display for mesh links.

Mesh access points are filtered by the number of hops between them and their root access point.

To use mesh filtering, follow these steps:

**Step 1**  To modify what label and color displays for a mesh link, follow these steps:

a.  In the Mesh Parent-Child Hierarchical View, choose an option from the Link Label drop-down list. Options are None, Link SNR, and Packet Error Rate.

b.  In the Mesh Parent-Child Hierarchical View, choose an option from the Link Color drop-down list to define which parameter (Link SNR or Packet Error Rate) determines the color of the mesh link on the map.
Note: The color of the link provides a quick reference point of the SNR strength or Packet Error Rate. Table 6-12 defines the different link colors.

Table 6-12  Definition for SNR and Packet Error Rate Link Color

<table>
<thead>
<tr>
<th>Link Color</th>
<th>Link SNR</th>
<th>Packet Error Rate (PER)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Represents a SNR above 25 dB (high value)</td>
<td>Represents a PER of one percent (1%) or lower</td>
</tr>
<tr>
<td>Amber</td>
<td>Represents a SNR between 20 and 25 dB (acceptable value)</td>
<td>Represents a PER that is less than ten percent (10%) and greater than one percent (1%)</td>
</tr>
<tr>
<td>Red</td>
<td>Represents a SNR below 20 dB (low value)</td>
<td>Represents a PER that is greater than ten percent (10%)</td>
</tr>
</tbody>
</table>

Note: The Link label and color settings are reflected on the map immediately. You can display both SNR and PER values simultaneously.

Step 2  To modify which mesh access points display based on the number of hops between them and their parents, do the following:

a. In the Mesh Parent-Child Hierarchical View, choose the appropriate options from the Quick Selections drop-down list. A description of the options is provided in Table 6-13.

Table 6-13  Quick Selection Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select only Root APs</td>
<td>Choose this setting if you want the map view to display root access points only.</td>
</tr>
<tr>
<td>Select up to 1st hops</td>
<td>Choose this setting if you want the map view to display 1st hops only.</td>
</tr>
<tr>
<td>Select up to 2nd hops</td>
<td>Choose this setting if you want the map view to display 2nd hops only.</td>
</tr>
<tr>
<td>Select up to 3rd hops</td>
<td>Choose this setting if you want the map view to display 3rd hops only.</td>
</tr>
<tr>
<td>Select up to 4th hops</td>
<td>Choose this setting if you want the map view to display 4th hops only.</td>
</tr>
<tr>
<td>Select All</td>
<td>Select this setting if you want the map view to display all access points.</td>
</tr>
</tbody>
</table>

b. Click Update Map View to refresh the screen and display the map view with the selected options.

Note: Map view information is retrieved from the Prime Infrastructure database and is updated every 15 minutes.
Monitoring Tags Using Maps

On an Prime Infrastructure map, you can review the name of the access point that generated the signal for a tagged asset, its strength of signal and when the location information was last updated for the asset. This information is displayed by simply hovering the mouse cursor over the asset tag icon on the map.

To enable tag location status on a map, follow these steps:

**Step 1** Choose **Monitor > Site Maps**.

**Step 2** Choose **Campus > Building > Floor** for the applicable mobility services engine and tag.

**Step 3** Select the **802.11 Tags** check box in the Floor Settings pane (left), if not already selected.

**Note** Do not click **Save Settings** unless you want to save changes made to the Floor Settings across all maps.

**Step 4** Hover the mouse cursor over a tag icon (yellow tag) and a summary of its configuration appears in a dialog box.

**Step 5** Click the **tag** icon to see tag details in a new window.

Using Planning Mode

You can calculate the recommended number and location of access points based on whether data and/or voice traffic and/or location are active.

**Note** Based on the throughput specified for each protocol (802.11a or 802.11 b/g), planning mode calculates the total number of access points required that would provide optimum coverage in your network.
To access the Planning Mode feature, follow these steps:

**Step 1** Choose Monitor > Site Maps.
**Step 2** Select the desired campus or building from the Name list.
**Step 3** Click the desired floor area in the Building.
**Step 4** From the Select a command drop-down list, choose Planning Mode.
**Step 5** Click Go.

**Note**
Planning mode does not use AP type or Antenna pattern information for calculating the number of access points required. The calculation is based on the access point coverage area or the number of users per access point.

**Planning Mode options:**
- Add APs—Enables you to add access points on a map. See the “Using Planning Mode to Calculate Access Point Requirements” section on page 6-67 for details.
- Delete APs—Deletes the selected access points.
- Map Editor—Opens the Map Editor window. See the “Using the Map Editor” section on page 6-52 for more details.
- Synchronize with Deployment—Synchronizes your planning mode access points with the current deployment scenario.
- Generate Proposal—View a planning summary of the current access points deployment.
- Planned AP Association Tool—Allows you to perform add, delete or import an AP Association from an excel or CSV file. Once an access point is defined, it can be associated to a base radio MAC address using the Planned AP Association Tool. If the AP is not discovered they get pushed into a standby bucket and get associated when discovered.

**Note**
AP association is subjected to a limitation that AP should not belong to any floor or outdoor area. If the AP is already assigned to a floor or outdoor area, then the standby bucket holds the AP and when removed from the floor or outdoor, get positioned to the given floor. One Mac address cannot be put into bucket for multiple floor or outdoor areas.

**Note**
The map synchronizations works only if the AP is associated to a base radio MAC address and not to its Ethernet MAC address.
Using Planning Mode to Calculate Access Point Requirements

Prime Infrastructure planning mode enables you to calculate the number of access points required to cover an area by placing fictitious access points on a map and allowing you to view the coverage area. Based on the throughput specified for each protocol (802.11a/n or 802.11b/g/n), planning mode calculates the total number of access points required to provide optimum coverage in your network. You can calculate the recommended number and location of access points based on the following criteria:

- traffic type active on the network: data or voice traffic or both
- location accuracy requirements
- number of active users
- number of users per square footage

To calculate the recommended number and placement of access points for a given deployment, follow these steps:

**Step 1** Choose Monitor > Site Maps.

The Site Map page appears.

**Step 2** Select the appropriate location link from the list that appears.

A color-coded map appears showing placement of all installed elements (access points, clients, tags) and their relative signal strength.

**Step 3** Choose Planning Mode from the Select a command drop-down list (top-right), and click Go. A blank floor map appears.

**Step 4** Click Add APs.

**Step 5** In the page that appears, drag the dashed-line rectangle over the map location for which you want to calculate the recommended access points.

**Note** Adjust the size or placement of the rectangle by selecting the edge of the rectangle and holding down the Ctrl key. Move the mouse as necessary to outline the targeted location. When you use the next-generation maps mode, the rectangle is resizable by dragging on the handles on its edges and corners.

**Step 6** Choose Automatic from the Add APs drop-down list.

**Step 7** Choose the AP Type and the appropriate antenna and protocol for that access point.

**Step 8** Choose the target throughput for the access point.

**Step 9** Select the check box(es) next to the service(s) that is used on the floor. Options are Data/Coverage (default), Voice, Location, and Location with Monitor Mode APs. (see Table 6-14).

**Note** You must select at least one service or an error occurs.

**Note** If you select the Advanced Options check box, two additional access point planning options appear: Demand and Override Coverage per AP. Additionally, a Safety Margin field appears for the Data/Coverage and Voice safety margin options.
### Table 6-14 Definition of Services Option

<table>
<thead>
<tr>
<th>Service Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data/Coverage</strong></td>
<td>Select this check box if data traffic is transmitted on the wireless LAN. The following densities are used depending on the band and data rates:</td>
</tr>
<tr>
<td>Band</td>
<td>Path Loss Model (dBm)</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.3</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.3</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.5</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.5</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.3</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.3</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.5</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.5</td>
</tr>
</tbody>
</table>

If you select the Advanced Options check box, you can select the desired safety margin (aggressive, safe, or very safe) of the signal strength threshold for data.

- Aggressive = Minimum (–3 dBm)
- Safe = Medium (0 dBm)
- Very Safe = Maximum (+3 dBm)

<table>
<thead>
<tr>
<th><strong>Voice</strong></th>
<th>Select the Voice check box if voice traffic is transmitted on the wireless LAN.</th>
</tr>
</thead>
</table>

If you select the Advanced Options check box, you can select the desired safety margin (aggressive, safe, very safe or 7920-enabled) of the signal strength threshold for voice.

- Aggressive = Minimum [–78 dBm (802.11a/b/g)]
- Safe = Medium [–75 dBm (802.11a/b/g)]
- Very Safe = Maximum [–72 dBm (802.11a/b/g)]
- 7920_enabled = [–72 dBm (802.11a); –67 dBm (802.11b/g)]

<table>
<thead>
<tr>
<th><strong>Location</strong></th>
<th>Select this check box to ensure that the recommended access point calculation provides the true location of an element within 10 meters at least 90% of the time.</th>
</tr>
</thead>
</table>

To meet the criteria, access points are collocated within 70 feet of each other in a hexagonal pattern employing staggered and perimeter placement.

Note Each service option includes all services that are listed above it. For example, if you select the Location check box, the calculation considers data/coverage, voice, and location in determining the optimum number of access points required.
### Table 6-15 Definition of Advanced Services

<table>
<thead>
<tr>
<th>Service Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data/Coverage</strong></td>
<td>Select this check box, if data traffic is transmitted on the wireless LAN. The following densities are used depending on the band and data rates:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Band</th>
<th>Path Loss Model (dBm)</th>
<th>Date Rate (Mb/s)</th>
<th>Area (Sq. ft.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>–3.3</td>
<td>10-12</td>
<td>6000</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.3</td>
<td>15-18</td>
<td>4500</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.5</td>
<td>10-12</td>
<td>5000</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.5</td>
<td>15-18</td>
<td>3250</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.3</td>
<td>5</td>
<td>6500</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.3</td>
<td>6</td>
<td>4500</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.5</td>
<td>5</td>
<td>5500</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.5</td>
<td>6</td>
<td>3500</td>
</tr>
</tbody>
</table>

If you select the **Advanced Options** check box, you can select the desired safety margin (aggressive, safe, or very safe) of the signal strength threshold for data.

- Aggressive = Minimum (–3 dBm)
- Safe = Medium (0 dBm)
- Very Safe = Maximum (+3 dBm)

| **Voice** | Select the voice check box if voice traffic is transmitted on the wireless LAN. |

If you select the **Advanced Options** check box, you can select the desired safety margin (aggressive, safe, very safe or 7920-enabled) of the signal strength threshold for voice.

- Aggressive = Minimum [–78 dBm (802.11a/b/g)]
- Safe = Medium [–75 dBm (802.11a/b/g)]
- Very Safe = Maximum [–72 dBm (802.11a/b/g)]
- 7920_enabled = [–72 dBm (802.11a); –67 dBm (802.11b/g)]

| **Location** | Select this check box to ensure that the recommended access point calculation provides the true location of an element within 10 meters at least 90% of the time. |

To meet the criteria, access points are collocated within 70 feet of each other in a hexagonal pattern employing staggered and perimeter placement.

| **Demand** | Select this check box if you want to use the total number of users or user ratio per access point as a basis for the access point calculation. |

Note: Each service option includes all services that are listed above it. For example, if you select the Location check box, the calculation considers data/coverage, voice, and location in determining the optimum number of access points required.
Table 6-15  Definition of Advanced Services (continued)

<table>
<thead>
<tr>
<th>Service Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Override Coverage per AP</td>
<td>Select this check box if you want to specify square foot coverage as the basis for access point coverage.</td>
</tr>
<tr>
<td>Safety Margin</td>
<td>Select this check box to qualify relative signal strength requirements for data and voice service in the access point calculation. Options are: Aggressive, Safe, Very Safe, and 7920-enabled (voice only). Select Aggressive to require minimal signal strength requirements in the calculation and Very Safe to request the highest signal strength.</td>
</tr>
</tbody>
</table>

Step 10  Click Calculate.

The recommended number of access points given the selected services appears.

Note  Recommended calculations assume the need for consistently strong signals unless adjusted downward by the safety margin advanced option. In some cases, the recommended number of access points is higher than what is required.

Note  Walls are not used or accounted for in planning mode calculations.

Step 11  Click Apply to generate a map that shows proposed deployment of the recommended access points in the selected area based on the selected services and parameters.

Step 12  Choose Generate Proposal to display a textual and graphical report of the recommended access point number and deployment based on the given input.

Refresh Options

To prepare for monitoring your wireless LANs, become familiar with the various refresh options for a map.

- Load—The Load option in the left sidebar menu refreshes map data from the Prime Infrastructure database on demand.
- Auto Refresh—The Auto Refresh option provides an interval drop-down list to set how often to refresh the map data from the database.
- Refresh from network—By clicking the Refresh from network icon to the right of the Auto Refresh drop-down list, you can refresh the map status and statistics directly from the controller through an SNMP fetch rather than polled data from the Prime Infrastructure database that is five to fifteen minutes older.

Note  If you have monitor mode access points on the floor plan, you have a choice between IDS or coverage heatmap types. A coverage heatmap excludes monitor mode access points, and an IDS heatmap includes them.
Creating a Network Design

After access points have been installed and have joined a controller, and the Prime Infrastructure has been configured to manage the controllers, set up a network design. A network design is a representation within the Prime Infrastructure of the physical placement of access points throughout facilities. A hierarchy of a single campus, the buildings that comprise that campus, and the floors of each building constitute a single network design. These steps assume that the location appliance is set to poll the controllers in that network, as well as be configured to synchronize with that specific network design, to track devices in that environment. The concept and steps to perform synchronization between the Prime Infrastructure and the mobility service engine are explained in the Cisco 3350 Mobility Services Engine Configuration Guide.

Designing a Network

To design a network, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Open the Prime Infrastructure web interface and log in.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>To create or edit a network design, you must log into the Prime Infrastructure and have SuperUser, Admin, or ConfigManager access privileges.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Choose Monitor &gt; Site Maps.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>From the drop-down list on the right-hand side, choose either New Campus or New Building, depending on the size of the network design and the organization of maps. If you chose New Campus, continue to Step 4. To create a building without a campus, skip to Step 14.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Go.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Enter a name for the campus network design, a contact name, and the file path to the campus image file. .bmps and .jpgs are importable.</td>
</tr>
<tr>
<td>Note</td>
<td>You can use the Browse... button to navigate to the location.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Click Next.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td>Select the Maintain Aspect Ratio check box. Enabling this check box causes the horizontal span of the campus to be 5000 feet and adjusts the vertical span according to the aspect ratio of the image file. Adjusting either the horizontal or vertical span changes the other field in accordance with the image ratio. You should unselect the Maintain Aspect Ratio check box if you want to override this automatic adjustment. You could then adjust both span values to match the real world campus dimensions.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Click OK.</td>
</tr>
</tbody>
</table>
Creating a Network Design

Chapter 6  Monitoring Maps

Step 9  In the Monitor > Site Maps page, click the hyperlink associated with the above-made campus map. A page showing the new campus image is displayed.

Step 10  From the Select a command menu on the upper right of the page, choose New Building, and click Go.

Step 11  Enter the name of the building, the contact person, the number of floors and basements in the building, and the dimensions. Click OK.

Step 12  Indicate which building on the campus map is the correct building by clicking the blue box in the upper left of the campus image and dragging it to the intended location. To resize the blue box, hold down the Ctrl key and click and drag to adjust its horizontal size. You can also enter dimensions of the building by entering numerical values in the Horizontal Span and Vertical Span fields and click Place. After resizing, reposition the blue box if necessary by clicking it and dragging it to the desired location. Click Save.

Step 13  Prime Infrastructure is then returned to the campus image with the newly created building highlighted in a green box. Click the green box.

Step 14  To create a building without a campus, choose New Building and click Go.

Step 15  Enter the name, contact information, number of floors and basements, and dimension information of the building. Click Save. Prime Infrastructure is returned to the Monitor > Site Maps page.

Step 16  Click the hyperlink associated with the newly created building.

Step 17  In the Monitor > Site Maps > Campus Name > Building Name page, from the drop-down list and choose New Floor Area. Click Go.

Step 18  Enter a name for the floor, a contact, a floor number, floor type, and height at which the access points are installed and the path of the floor image. Click Next.

Note  The Floor Type (RF Model) field specifies the type of environment on that specific floor. This RF Model indicates the amount of RF signal attenuation likely to be present on that floor. If the available models do not properly characterize a floor's makeup, details on how to create RF models specific to a floor's attenuation characteristics are available in the Cisco 3350 Mobility Services Engine Configuration Guide.

Step 19  If the floor area is a different dimension than the building, adjust floor dimensions by either making numerical changes to the text fields under the Dimensions heading or by holding the Ctrl key and clicking and dragging the blue box around the floor image. If the floor's location is offset from the upper left corner of the building, change the placement of the floor within the building by either clicking and dragging the blue box to the desired location or by altering the numerical values under the Coordinates of top left corner heading. After making changes to any numerical values, click Place.

Step 20  Adjust the characteristics of the floor with Prime Infrastructure map editor by selecting the check box next to Launch Map Editor. For an explanation of the map editor feature, see the “Using the Map Editor” section on page 6-52.

Step 21  At the image of the new floor (Monitor > Site Maps > CampusName > BuildingName > FloorName), go to the drop-down list on the upper right and choose Add Access Points. Click Go.

Step 22  All access points that are connected to controllers are displayed. Even controllers that Prime Infrastructure is configured to manage but which have not yet been added to another floor map are displayed. Select the access points to be placed on the specific floor map by checking the boxes to the left of the access point entries. Select the box to the left of the Name column to select all access points. Click OK.
Step 23 Each access point you have chosen to add to the floor map is represented by a gray circle (differentiated by access point name or MAC address) and is lined up in the upper left part of the floor map. Drag each access point to the appropriate location. (Access points turn blue when you click them to relocate them.) The small black arrow at the side of each access point represents Side A of each access point, and each arrow of the access point must correspond with the direction in which the access points were installed. (Side A is clearly noted on each 1000 series access point and has no relevance to the 802.11a/n radio.)

Step 24 To adjust the directional arrow, choose the appropriate orientation on the Antenna Angle drop-down list. Click Save when you are finished placing and adjusting each direction of the access point.

Note Access point placement and direction must directly reflect the actual access point deployment or the system cannot pinpoint the device location.

Step 25 Repeat these steps to create campuses, buildings, and floors until each device location is properly detailed in a network design.

**Importing or Exporting WLSE Map Data**

When you convert an access point from autonomous to CAPWAP and from the WLSE to Prime Infrastructure, one of the conversion steps is to manually re-enter the access point information into the Prime Infrastructure. This can be a time-consuming step. To speed up the process, you can export the information about access points from the WLSE and import it into the Prime Infrastructure.

Note Prime Infrastructure expects a .tar file and checks for a .tar extension before importing the file. If the file you are trying to import is not a .tar file, the Prime Infrastructure displays an error message and prompts you to import a different file.

To map properties and import a tar file containing WLSE data using the Prime Infrastructure web interface, follow these steps. For more information on the WLSE data export functionality (WLSE version 2.15), see http://<WLSE_IP_ADDRESS>:1741/debug/export/exportSite.jsp.

Step 1 Choose Monitor > Site Maps.
Step 2 Choose Properties from the Select a command drop-down list, and click Go.
Step 3 In the Export/Import AP/LS/SP Placement, click Browse to select the file to import.
Step 4 Find and select the .tar file to import and click Open.
Prime Infrastructure displays the name of the file in the Import From field.
Step 5 Click Import.
Prime Infrastructure uploads the file and temporarily saves it into a local directory while it is being processed. If the file contains data that cannot be processed, the Prime Infrastructure prompts you to correct the problem and retry. After the file has been loaded, the Prime Infrastructure displays a report of what is added to the Prime Infrastructure. The report also specifies what cannot be added and why.

If some of the data to be imported already exists, the Prime Infrastructure either uses the existing data in the case of campuses or overwrites the existing data using the imported data in the cases of buildings and floors.
If there are duplicate names between a WLSE site and building combination and an Prime Infrastructure campus (or top-level building) and building combination, the Prime Infrastructure displays a message in the Pre Execute Import Report indicating that it will delete the existing building.

**Step 6**  
Click **Import** to import the WLSE data. 
Prime Infrastructure displays a report indicating what was imported.

---

**Note**  
Because a WLSE file has no floor number information, the structure of the floor index calculation after WLSE is imported into the Prime Infrastructure is in descending order. You can click the floor image to go directly to the appropriate floor page.

**Step 7**  
Choose **Monitor > Site Maps** to verify the imported data.

---

**Monitoring Device Details**

**Access Point Details**

Hover your mouse cursor over an access point icon to view access point details. Click the appropriate tab to view access point and radio information.

**Note**  
Monitor mode access points are shown with gray labels to distinguish them from other access points.

The AP Info tab includes the following access point information:

- MAC address
- Access point model
- Controller
- Location
- Access point height
- Access point uptime
- LWAPP uptime

**Note**  
From the AP Info tab, you can run a ping test by clicking the **Run Ping Test** link.

The 802.11 tabs includes the following radio information:

- Channel number
- Extension channel
- Channel width
- Transmit power level
- Client count
Note The number of clients associated to access points might not match the total number of clients.

- Receiving and transmitting utilization percentages
- Channel utilization percentage

Note Total utilization = (Rx + Tx + Channel utilization) scaled to 100%.

- Antenna name and angle
- Elevation angle

Note From either of the 802.11 tabs, you can view Rx neighbors and radio details for this access point by clicking the appropriate link (View Rx Neighbors or View Radio Details).

- Dot11n Enabled
- CleanAir Status—Displays the CleanAir status of the access point, whether or not CleanAir is enabled on the access point.
- Average Air Quality—Displays the average air quality on this access point.
- Minimum Air Quality—Displays the minimum air quality on this access point.

Client Details
Hover your mouse cursor over a client icon to view client details.

Client details information includes the following:
- Username
- IP address
- Asset name, group, and category
- Status
- Auth
- SSID
- Access point name
- Protocol
- Port number
- Last location

Tag Details
Hover your mouse cursor over a tag icon to view tag details.

Tag details includes the following:
- Asset name, group, and category
- Type
- Battery life
Monitoring Device Details

- Last located

Rogue Access Point Details
Hover your mouse cursor over an access point icon to view rogue access point details.
Rogue access point details includes the following:
- Classification type—Friendly, malicious, or unknown.
- State
- Detecting access points
- Type
- Rogue clients
- First seen
- Last seen
- On network
- Last located

Rogue Adhoc Details
Hover your mouse cursor over an access point icon to view rogue ad hoc details.

Rogue Client Details
Hover your mouse cursor over an access point icon to view rogue client details.

Interferer Details
Hover your mouse cursor over an interferer icon to view its details. Interferer details includes the following:
- Interferer Name—The name of the interfering device.
- Affected Channels—The channel the interfering device is affecting.
- Detected Time—The time at which the interference was detected.
- Severity—The severity index of the interfering device.
- Duty Cycle—The duty cycle (in percentage) of the interfering device.
- RSSI (dBm)—The Received Signal Strength Indicator of the interfering device.
Rogue client details includes the following:
- State
- Associated rogue access point
- Detecting access points
- First seen
- Last seen
- Last located

Floor View Navigation

The main Floor View navigation pane provides access to multiple map functions.
This navigation pane includes the following functionality:

- **Zoom In/Zoom Out**—Click the magnifying glass icon with the plus sign (+) to enlarge the map view. Click the magnifying glass icon with the minus sign (-) to decrease the size of the map view.
- **Map Size**—See the “Panning and Zooming with Next Generation Maps” section on page 6-24.
- **Show Grid**—Click to show or hide the grid that displays distance in feet on the map.
- **RSSI Legend**—Hover your mouse cursor over the RSSI Legend icon to display the RSSI color scheme (ranging from red/-35 dBm to dark blue/-90 dBm).
- **Add Access Points**—Click to open the Add Access Points page. For more information, see the “Adding Access Points to a Floor Area” section on page 6-25.
- **Remove Access Points**—Click to open the Remove Access Points page. Select the access points that you want to remove and click **OK**.
- **Position Access Points**—Click to open the Position Access Points page.
- **Add Chokepoints**—Click to open the Add Chokepoints page. For more information, see the *Cisco Context-Aware Services Configuration Guide*.
- **Add WiFi TDOA Receivers**—Click to open the Add Wi-Fi TDOA Receivers page. For more information, see the *Cisco Context-Aware Services Configuration Guide*.
- **Auto Refresh**—From the drop-down list, choose the length of time between each system refresh.
- **Refresh from Network**—Click to initiate an immediate refresh of the current data.
- **Planning Mode**—Click to open the Planning Mode window. For more information, see the “Using Planning Mode” section on page 6-65 for more information.
- **Map Editor**—Click to open the Map Editor.

**Full Screen**—Click to increase the size of the map to full screen. Once there, click **Exit Full Screen** to return to the normal view.

### Understanding RF Heatmap Calculation

A radio frequency heat map is a graphical representation of the strength of the RF signals. Because WLANs are very dynamic and nondeterministic in nature, administrators can never be certain of the coverage at a particular moment. To help combat this challenge, the Prime Infrastructure provides a map of your floor plan along with visual cues as to the Wi-Fi coverage of the floor. These maps are called heatmaps because they are similar to the colored maps used to show varying levels of heat in oceanography or geographical sciences. Color is used to show the various levels of signal strength. The different shades in the "heatmap" reflect differing signal strengths.

This color visualization is extremely useful. At one glance, you can see the current state of coverage (without having to walk around measuring it), the signal strength, and any gaps or "holes" in the WLAN. Because floor plans and heat maps are very intuitive, this system greatly enhances the speed and ease with which you support your organization and troubleshoot specific problems.

The RF heatmap calculation is based on an internal grid. Depending on the exact positioning of an obstacle in that grid, the RF heatmap, within a few feet or meters of the obstacle, might or might not account for the obstacle attenuation.

In detail, grid squares partially affected by an obstacle crossing the grid square might or might not incorporate the obstacle attenuation according to the geometry of the access point, obstacle, and grid.

For example, consider a wall crossing one grid square. The midpoint of the grid square is behind the wall from the AP, so the whole grid square is colored with attenuation, including (unfortunately) the top left corner that is actually in front of the wall.
The midpoint of the grid square is on the same side of the wall as the AP, so the whole grid square is not colored with attenuation, including (unfortunately) the bottom right corner that is actually behind the wall from the AP.

**Dynamic Heatmap Calculation**

The RF heatmap calculation can be static or dynamic. By default, it is dynamic, to configure it to be static, disable the dynamic heatmap option in the map properties page. Prime Infrastructure server maintains the current list of all APs RSSI strength for all APs. The neighbor AP RSSI strength is used to modify the RF heatmaps for all APs. The main purpose of the dynamic heatmap feature is to recompute the RF heatmaps due to obstacles.

**Monitoring Google Earth Maps**

Within Monitor > Google Earth Maps, you can create an outdoor location, import a file, view Google Earth maps, and specify Google Earth settings.

- Creating an Outdoor Location Using Google Earth, page 6-78
- Importing a File into Prime Infrastructure, page 6-82
- Viewing Google Earth Maps, page 6-83
- Adding Google Earth Location Launch Points to Access Point Pages, page 6-84
- Google Earth Settings, page 6-84

**Creating an Outdoor Location Using Google Earth**

To group the access points together into outdoor locations, use the Latitude/Longitude geographical coordinates for each access point. These coordinates are provided in two ways:

- Importing a KML (Google Keyhole Markup Language) File
- Importing a CSV File (Spreadsheet format with comma-separated values)
- Understanding Geographical Coordinates for Google Earth, page 6-78
- Creating and Importing Coordinates in Google Earth (KML File), page 6-79
- Creating and Importing Coordinates as a CSV File, page 6-81

**Understanding Geographical Coordinates for Google Earth**

The following geographical information is required for each access point:

- Longitude (East or West)—Angular distance in degrees relative to Prime Meridian. Values west of Meridian range from –180 to 0 degrees. Values east of Meridian range from 0 to 180 degrees. The default is 0.
- Coordinates in degrees, minutes, seconds, direction:
Chapter 6      Monitoring Maps

Monitoring Google Earth Maps

– Degrees (−180 to 180)
– Minutes (0 to 59)
– Seconds (00.00 to 59.99)
– Direction—East or West (E, W)

Decimal format (converted from degrees, minutes, and seconds):
– Longitude can range from −179.59.59.99 W to 179.59.59.99 E

• Latitude (North or South)—Angular distance in degrees relative to the Equator. Values south of the Equator range from −90 to 0 degrees. Values north of the Equator range from 0 to 90 degrees. The default is 0.

Coordinates in degrees, minutes, seconds, direction:
– Degrees (−90 to 90)
– Minutes (0 to 59)
– Seconds (00.00 to 59.99)
– Direction—North or South (N, S)

Decimal format (converted from degrees, minutes, and seconds):
– Latitude can range from −89.59.59.99 S to 89.59.59.99 N

• Altitude—Height or distance of the access point from the surface of the earth in meters. If not provided, value defaults to 0. Values range from 0 to 99999.

• Tilt—Values range from 0 to 90 degrees (cannot be negative). A tilt value of 0 degrees indicates viewing from directly above the access point. A tilt value of 90 degrees indicates viewing along the horizon. Values range from 0 to 90. The default azimuth angle is 0.

• Range—Distance in meters from the point specified by longitude and latitude to the point where the access point is being viewed (the Look At position) (camera range above sea level). Values range from 0 to 999999.

• Heading—Compass direction in degrees. The default is 0 (North). Values range from 0 to ±180 degrees.

• Altitude Mode—Indicates how the <altitude> specified for the Look At point is interpreted.
  – Clamped to ground—Ignores the <altitude> specification and places the Look At position on the ground. This is the default.
  – Relative to ground—Interprets the <altitude> as a value in meters above the ground.
  – Absolute—Interprets the <altitude> as a value in meters above sea level.

• Extend to ground—Indicates whether or not the access point is attached to a mast.

Creating and Importing Coordinates in Google Earth (KML File)

The geographical coordinates can be created in Google Earth and imported. Either a folder or individual placemarks can be created. Creating a folder helps group all the Placemarks into a single folder and allows you to save the folder as a single KML (a.k.a. XML) file. If individual Placemarks are created, each Placemark must be individually saved.

Follow these steps to create a folder in Google Earth:

Step 1    Launch Google Earth.
**Step 2**  In the Places page on the left sidebar menu, choose My Places or Temporary Places.

**Step 3**  Right-click Temporary Places and select Add > Folder from the drop-down lists.

---

**Note**  By using a KML file, folders can be created hierarchically to any depth. For example, you can create folders and placemarks organized by country, city, state, zip.

This is not applicable for CSV. In CSV there can be only one level of hierarchy.

---

**Step 4**  Enter the following information (optional):

- Name—Folder name
- Description—Folder description
- View—Includes latitude, longitude, range, heading, and tilt

---

**Note**  If the View coordinates (latitude, longitude, range, heading, and tilt) are specified, this information is used to “fly” or advance to the correct location when Google Earth is first loaded.

If no coordinates are specified, the latitude and longitude information is derived using the minimum and maximum latitude and longitude of all access points within this group or folder.

---

**Step 5**  Click OK to save the folder. After the folder is created, it can be selected from the Places page to create Placemarks.

---

To create Placemarks, follow these steps:

---

**Step 1**  Launch Google Earth.

**Step 2**  In the Places page on the left sidebar, select My Places or Temporary Places.

**Step 3**  Select the folder that you previously created.

**Step 4**  Right-click your created folder and select Add > Placemark from the drop-down lists.

**Step 5**  Configure the following parameters, if applicable:

- Name—The Placemark name must contain the name, MAC address, or IP address of the appropriate access point.

---

**Note**  The MAC address refers to base radio MAC not Ethernet MAC.

- Latitude—Provides the current coordinate for the folder if the placemark is created inside the folder or the coordinate for the placemark (if not created inside a folder). This field is automatically filled depending on where the yellow Placemark icon is located on the map. Use your mouse to move the Placemark to the correct location or enter the correct coordinate in the Latitude text box.

- Longitude—Provides the current coordinate for the folder if the placemark is created inside the folder or the coordinate for the placemark (if not created inside a folder). This field is automatically filled depending on where the yellow Placemark icon is located on the map. Use your mouse to move the Placemark to the correct location or enter the correct coordinate in the Longitude text box.

- Description (optional)—Field is ignored by the Prime Infrastructure.
Style, Color (optional)—Field is ignored by the Prime Infrastructure.

View—Allows you to configure the Latitude, Longitude, Range, Heading and Tilt coordinates. See the “Understanding Geographical Coordinates for Google Earth” section on page 6-78 for more information on these geographical coordinates.

- Longitude and latitude are automatically filled depending on where the yellow Placemark icon is located on the map. Use your mouse to click and move the Placemark to the correct location.
- All of the coordinates can be entered manually.

Altitude—Enter the altitude in meters in the text box or use the Ground to Space slide bar to indicate the altitude.

- Clamped to ground—Indicates that the Look At position is on the ground. This is the default.
- Relative to ground—Interprets the <altitude> as a value in meters above the ground.
- Absolute—Interprets the <altitude> as a value in meters above sea level.
- Extend to ground—For Relative to ground or Absolute settings, indicates whether or not the access point is attached to a mast.

**Step 6** When all coordinates are entered, click **Snapshot current view** or click **Reset** to return the coordinates to the original settings.

**Note** For more information regarding Google Earth, see to the Google Earth online help.

**Step 7** Click **OK**.

**Step 8** Repeat these steps for all placemarks you want to add.

**Step 9** When all placemarks are created, save the folder as a .kmz file (KML Zip file) or as a .kml file.

**Note** A .kmz file should contain only one .kml file.

**Note** To save the folder, right-click the folder, select **Save as** from the drop-down list, navigate to the correct location on your computer, and click **Save**. Both .kmz and .kml files can be imported into the Prime Infrastructure.

---

**Creating and Importing Coordinates as a CSV File**

To create a CSV file to import into the Prime Infrastructure, follow these steps:

**Step 1** Open a flat file and provide the necessary information as a comma-separated list. The Table 6-16 lists the potential data, whether the data is optional or required, and the parameters of the data.

**Note** For more information regarding the geographical coordinates listed in Table 6-16, see the “Understanding Geographical Coordinates for Google Earth” section on page 6-78.
Monitoring Google Earth Maps

To import a Google KML or a CSV into the Google Earth Maps feature of the Prime Infrastructure, follow these steps:

Step 1 Log in to the Prime Infrastructure.
Step 2 Choose Monitor > Google Earth Maps.
Step 3 From the Select a command drop-down list, choose Import Google KML or Import CSV.
Step 4 Click Go.
Step 5 Use the Browse button to navigate to the .kml, .kmz, or .csv file on your computer.
Step 6 When the file name path is displayed in the text box, click Next.

The input file is parsed and validated for the following:

- Access points specified in the uploaded file are validated (the specified access points must be available within the Prime Infrastructure).
- Range validations are performed for tilt, heading, range, and other geographical coordinates fields. If longitude and latitude are provided, range validations are performed; if not, the value is defaulted to 0.

---

**Table 6-16 Potential Fields for the CSV File**

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;FolderName&quot;</td>
<td>&quot;Value Optional&quot;</td>
<td>Max Length: 32</td>
</tr>
<tr>
<td>&quot;FolderState&quot;</td>
<td>&quot;Value Optional&quot;</td>
<td>Permitted Values: true/false</td>
</tr>
<tr>
<td>&quot;FolderLongitude&quot;</td>
<td>&quot;Value Optional&quot;</td>
<td>Range: 0 to ±180</td>
</tr>
<tr>
<td>&quot;FolderLatitude&quot;</td>
<td>&quot;Value Optional&quot;</td>
<td>Range: 0 to ±90</td>
</tr>
<tr>
<td>&quot;FolderAltitude&quot;</td>
<td>&quot;Value Optional&quot;</td>
<td>Range: 0 to 99999</td>
</tr>
<tr>
<td>&quot;FolderRange&quot;</td>
<td>&quot;Value Optional&quot;</td>
<td>Range: 0 to 99999</td>
</tr>
<tr>
<td>&quot;FolderTilt&quot;</td>
<td>&quot;Value Optional&quot;</td>
<td>Range: 0 to 90</td>
</tr>
<tr>
<td>&quot;FolderHeading&quot;</td>
<td>&quot;Value Optional&quot;</td>
<td>Range: 0 to ±180</td>
</tr>
<tr>
<td>&quot;FolderGeoAddress&quot;</td>
<td>&quot;Value Optional&quot;</td>
<td>Max Length: 128</td>
</tr>
<tr>
<td>&quot;FolderGeoCity&quot;</td>
<td>&quot;Value Optional&quot;</td>
<td>Max Length: 64</td>
</tr>
<tr>
<td>&quot;FolderGeoState&quot;</td>
<td>&quot;Value Optional&quot;</td>
<td>Max Length: 40</td>
</tr>
<tr>
<td>&quot;FolderGeoZip&quot;</td>
<td>&quot;Value Optional&quot;</td>
<td>Max Length: 12</td>
</tr>
<tr>
<td>&quot;FolderGeoCountry&quot;</td>
<td>&quot;Value Optional&quot;</td>
<td>Max Length: 64</td>
</tr>
<tr>
<td>&quot;AP_Name&quot;</td>
<td>&quot;Value Required&quot;</td>
<td>Max Length: 32</td>
</tr>
<tr>
<td>&quot;AP_Longitude&quot;</td>
<td>&quot;Value Required&quot;</td>
<td>Range: 0 to ±180</td>
</tr>
<tr>
<td>&quot;AP.getLatitude&quot;</td>
<td>&quot;Value Required&quot;</td>
<td>Range: 0 to ±90</td>
</tr>
</tbody>
</table>

Step 2 Save the .csv file. The file is now ready to import into the Prime Infrastructure.

---

Importing a File into Prime Infrastructure

To import a Google KML or a CSV into the Google Earth Maps feature of the Prime Infrastructure, follow these steps:

Step 1 Log in to the Prime Infrastructure.
Step 2 Choose Monitor > Google Earth Maps.
Step 3 From the Select a command drop-down list, choose Import Google KML or Import CSV.
Step 4 Click Go.
Step 5 Use the Browse button to navigate to the .kml, .kmz, or .csv file on your computer.
Step 6 When the file name path is displayed in the text box, click Next.

The input file is parsed and validated for the following:

- Access points specified in the uploaded file are validated (the specified access points must be available within the Prime Infrastructure).
- Range validations are performed for tilt, heading, range, and other geographical coordinates fields. If longitude and latitude are provided, range validations are performed; if not, the value is defaulted to 0.
Step 7  
After the files pass all validation checks, review the file details and click **Save**.

If the uploaded information was saved previously, the information is overwritten accordingly:
- If the folder was uploaded previously, the coordinates are updated for the folder.
- If access points were uploaded previously, the coordinates are updated for the access points.
- Existing access points in the folder are not removed.
- New folders, as needed, are created and access points are placed accordingly.

### Viewing Google Earth Maps

To view Google Earth maps, follow these steps:

**Step 1**  
Log in to the Prime Infrastructure.

**Step 2**  
Choose **Monitor > Google Earth Maps**. The Google Earth Maps page displays all folders and the number of access points included within each folder.

**Step 3**  
Click **Launch** for the map you want to view. Google Earth opens in a separate page and displays the location and its access points.

**Note**  
To use this feature, you must have Google Earth installed on your computer and configured to auto-launch when data is sent from the server. You can download Google Earth from the Google website: [http://www.google.com/earth/index.html](http://www.google.com/earth/index.html).

### Viewing Google Earth Map Details

To view details for a Google Earth Map folder, follow these steps:

**Step 1**  
In the Google Earth Map page, click the folder name to open the details page for this folder. The Google Earth Details provide the access point names and MAC or IP addresses.

**Note**  
To delete an access point, select the applicable check box and click **Delete**. To delete the entire folder, select the check box next to **Folder Name** and click **Delete**. Deleting a folder also deletes all subfolders and access points inside the folder.
Adding Google Earth Location Launch Points to Access Point Pages

You can expand the number of Google Earth Location launch points within the Prime Infrastructure by adding it to the Access Point summary and detail pages.

To add a Google Earth Location launch point to the Access Point summary and details page, follow these steps:

**Step 1** Choose Monitor > Access Points.

**Step 2** In the Access Point summary page, click the Edit View link next to page heading.

**Step 3** In the Edit View page, highlight Google Earth Location in the left-hand column. Click Show.

The Google Earth Location column heading moves into the View Information column.

**Note** The View Information listings, top-to-bottom, reflect the left-to-right order of the columns as they appear on the Access Point summary page.

**Step 4** To change the display order of the columns, highlight the Google Earth Location entry and click the Up and Down buttons as needed. Click Submit.

You are returned to the Access Points summary page, and a Google Earth launch link is in the display.

**Note** The launch link also appears in the general summary page of the Access Points details page (Monitor > Access Points > AP Name).

Google Earth Settings

Access point related settings can be defined from the Google Earth Settings page. To configure access point settings for the Google Earth Maps feature, follow these steps:

**Step 1** Choose Monitor > Google Earth Maps.

**Step 2** Configure the following parameters:

- Refresh Settings—Select the Refresh from Network check box to enable this on-demand refresh.
  
  This option is applied only once and then disabled.

**Caution** Because this refresh occurs directly from the network, it could take a long period of time to collect data according to the number of access points.
• Layers—Layer filters for access points, access point heat maps, and access point mesh information can be selected and saved. Select the check box to activate the applicable layer and click > to open the filter page.

**Note** These settings apply when Google Earth sends the request for the next refresh.

- Access Points—From the AP Filter drop-down list, choose to display channels, Tx power level, coverage holes, MAC addresses, names, controller IP, utilization, profiles, or clients.

**Note** If the access point layer is not checked, no data is returned, and an error message is returned to Google Earth as a Placemark without an icon.

- AP Heatmap—From the Protocol drop-down list, choose 802.11a/n, 802.11b/g/n, 802.11a/n & 802.11b/g/n, or None. Select the cutoff from the RSSI Cutoff drop-down list (-60 to -90 dBm).

**Note** If the protocol chosen is both 802.11a/n and 802.11b/g/n, the heat maps are generated for both and overlayed on top of each other. The order cannot be defined. To prevent this overlay, you must turn off individual overlay in Google Earth or change it in the Google Earth Settings on the Prime Infrastructure.

- AP Mesh Info—Choose Link SNR, Packet Error Rate, or none from the Link Label drop-down list. Choose Link SNR or Packet Error Rate from the Link Color drop-down list.

**Note** When the AP Mesh Info check box is chosen, Mesh Links are also automatically shown.

**Step 3** Click **Save Settings** to confirm these changes or **Cancel** to close the page without saving the changes.
Managing User Accounts

The Cisco Prime Infrastructure Administration enables you to schedule tasks, administer accounts, and configure local and external authentication and authorization. Also, set logging options, configure mail servers, and data management related to configuring the data retain periods. Information is available about the types of the Prime Infrastructure licenses and how to install a license.

Organizations need an easy and cost-effective method to manage and control wireless network segments using a single management platform. They need a solution that supports limiting an individual administrator to manage or control the wireless LAN.

This chapter describes the administrative tasks to perform with the Prime Infrastructure.

- Managing the Prime Infrastructure User Accounts, page 7-1
- Viewing the Audit Trail, page 7-7
- Managing the Prime Infrastructure Guest User Accounts, page 7-9
- Adding a New User, page 7-12
- Managing Lobby Ambassador Accounts, page 7-14

Managing the Prime Infrastructure User Accounts

This section describes how to configure global e-mail parameters and manage the Prime Infrastructure user accounts.

- Configuring the Prime Infrastructure User Accounts, page 7-2
- Deleting the Prime Infrastructure User Accounts, page 7-3
- Changing Passwords, page 7-4
- Monitoring Active Sessions, page 7-4
- Viewing or Editing User Account Information, page 7-5
- Viewing or Editing Group Information, page 7-6
- Audit Trail Details Page, page 7-8
- Viewing the Audit Trail, page 7-7
- Creating Guest User Accounts, page 7-8
- Logging in to the Prime Infrastructure User Interface as a Lobby Ambassador, page 7-16
Configuring the Prime Infrastructure User Accounts

This section describes how to configure a Prime Infrastructure user. The accounting portion of the AAA framework is not implemented at this time. Besides complete access, you can give administrative access with differentiated privileges to certain user groups. Prime Infrastructure supports external user authentication using these access restrictions and authenticates the users against the TACACS+ and RADIUS servers.

The username and password supplied by you at install time are always authenticated, but the steps you take here create additional superusers. If the password is lost or forgotten, you must run a utility to reset the password to another user-defined password.

To configure a new user account to the Prime Infrastructure, follow these steps:

**Step 1**
Start the Prime Infrastructure server.

**Step 2**
Log into the Prime Infrastructure user interface as root.

*Note*
We recommend that you create a new superuser assigned to the SuperUsers group.

**Step 3**
Choose **Administration > AAA**. The Change Password page appears.

**Step 4**
In the Old Password text box, enter the current password that you want to change.

**Step 5**
Enter the username and password for the new the Prime Infrastructure user account. You must enter the password twice.

*Note*
These entries are case sensitive.

**Step 6**
Choose **User Groups** from the left sidebar menu. The All Groups page displays the following group names.

*Note*
Some usergroups cannot be combined with other usergroups. For instance, you cannot choose both lobby ambassador and monitor lite.

- **System Monitoring**—Allows users to monitor the Prime Infrastructure operations.
- **ConfigManagers**—Allows users to monitor and configure the Prime Infrastructure operations.
- **Admin**—Allows users to monitor and configure the Prime Infrastructure operations and perform all system administration tasks.

*Note*
If you choose admin account and log in as such on the controller, you can also see the guest users under Local Net Admin.

- **SuperUsers**—Allows users to monitor and configure the Prime Infrastructure operations and perform all system administration tasks including administering Prime Infrastructure user accounts and passwords. Superusers tasks can be changed.
- **Users Assistant**—Allows only local net user administration. User assistants cannot configure or monitor controllers. They must access the Configure > Controller page to configure these local net features.
Managing the Prime Infrastructure User Accounts

Note: If you create a user assistant user, log in as that user, and choose Monitor > Controller, you receive a “permission denied” message, which is an expected behavior.

- Lobby Ambassador—Allows access for configuration and management of only Guest User user accounts.
- Monitor lite—Allows monitoring of assets location.
- Root—Allows users to monitor and configure the Prime Infrastructure operations and perform all system administration tasks including changing any passwords. Only one user can be assigned to this group and is determined upon installation. It cannot be removed from the system, and no task changes can be made for this user.

Step 7: Click the name of the user group to which you assigned the new user account. The Group Detail > User Group page shows a list of this permitted operations of the group.

From this page you can also show an audit trail of login and logout patterns or export a task list.

Step 8: Make any desired changes by selecting or unselecting the appropriate check boxes for task permissions and members.

Note: Any changes you make affect all members of this user group.

Note: To view complete details in the Monitor > Client details page and to perform operations such as Radio Measurement, users in User Defined groups need permission for Monitor Clients, View Alerts & Events, Configure Controllers, and Client Location.

Step 9: Click Submit to save your changes or Cancel to leave the settings unchanged.

Deleting the Prime Infrastructure User Accounts

To delete a Prime Infrastructure user account, follow these steps:

Step 1: Start the Prime Infrastructure server.
Step 2: Log into the Prime Infrastructure user interface as a user assigned to the SuperUsers group.
Step 3: Choose Administration > AAA.
Step 4: Choose Users from the left sidebar menu to display the Users page.
Step 5: Select the check box to the left of the user account(s) to be deleted.
Step 6: From the Select a command drop-down list, choose Delete User(s), and click Go.

When prompted, click OK to confirm your decision. The user account is deleted and can no longer be used.
Changing Passwords

To change the password for a Prime Infrastructure user account, follow these steps:

Step 1  Start the Prime Infrastructure server.
Step 2  Log into the Prime Infrastructure user interface as a user assigned to the SuperUsers group.
Step 3  Choose Administration > AAA to display the Change Password page.
Step 4  Enter your old password.
Step 5  Enter the new password in both the New Password and Confirm New Password text boxes.
Step 6  Click Save to save your changes. The password for this user account has been changed and can be used immediately.

Changing the Root User Password using CLI

To change the password for a root user using the command-line interface, follow these steps:

Step 1  Log into the system as administrator.
Step 2  Using the command-line interface (CLI), enter the following commands:

```
VMNCS/admin# ncs password ?
ftpuser  Modifies ftp username and password
root     Modifies root user login password

VMNCS/admin# ncs password root ?
password  Modifies root user login password

VMNCS/admin# ncs password root password ? <password>
<WORD>  Type in root user login password (Max Size - 80)
```

Monitoring Active Sessions

To view a list of active users, follow the steps:

Step 1  Choose Administration > AAA.
Step 2  From the left sidebar menu, choose Active Sessions. The Active Sessions page appears.

The user highlighted in red represents your current login. If a column heading is a hyperlink, click the heading to sort the list of active sessions in descending or ascending order along that column. The sort direction is toggled each time the hyperlink is clicked.

The Active Sessions page has the following columns:

- Username—The logged in username.
- IP/Host Name—The IP address or the hostname of the machine on which the browser is running. If the hostname of the user machine is not in DNS, the IP address is displayed.
• Login Time—The time at which the user logged in to the Prime Infrastructure. All times are based on the Prime Infrastructure server machine time.

• Last Access Time—The time at which the user last accessed Prime Infrastructure. All times are based on the Prime Infrastructure server machine time.

Note The time displayed in this column is usually a few seconds behind the current system time because Last Access Time is updated frequently by the updates to the alarm status dashlet.

• Login Method:
  – Regular: Sessions created for users who log into the Prime Infrastructure directly through a browser.

• User Groups: The list of groups to which the user belongs.

• Audit trail icon: Link to page that displays the audit trail (previous login times) for that user.

### Viewing or Editing User Account Information

To see the group the user is assigned to or to adjust a password or group assignment for that user, follow these steps:

**Step 1** Choose **Administration > AAA**.

**Step 2** From the left sidebar menu, choose **Users**.

**Step 3** Click a user in the User Name column. The User Detail : User Group page appears.

You can see which group is assigned to this user or change a password or group assignment.

### Setting the Lobby Ambassador Defaults

If you choose a Lobby Ambassador from the User Name column, a Lobby Ambassador Defaults tab appears. All of the guest user accounts created by the lobby ambassador have these credentials by default. If the default values are not specified, the lobby ambassador must provide the required guest user credential fields.

Note If no default profile is chosen on this tab, the defaults do not get applied to this lobby ambassador. The lobby ambassador account does get created, and you can create users with any credentials you choose.

**Step 1** Use the Profile drop-down list to choose the guest user to connect to.

Wired-guest is an example of a profile that might be defined to indicate traffic that is originating from wired LAN ports. See the “Configuring Wired Guest Access” section on page 9-47.

**Step 2** Choose a user role to manage the amount of bandwidth allocated to specific users within the network. They are predefined by the administrator and are associated with the guests’ access (such as contractor, customer, partner, vendor, visitor, and so on).
Step 3 Choose **Limited** or **Unlimited** at the Lifetime radio button.

- For the limited option, you choose the period of time that the guest user account is active using the hours and minutes drop-down lists. The default value for Limited is one day (8 hours).
- When **unlimited** is chosen, no expiration date for the guest account exists.

Step 4 Use the Apply to drop-down list to choose from the following options. What you choose determines what additional parameters appear.

- Indoor area—A campus, building, or floor.
- Outdoor area—A campus or outdoor area.
- Controller list—A list of controller(s) with the selected profile created.
- Config Group—Those config group names configured on the Prime Infrastructure.

Step 5 Enter the email ID of the host to whom the guest account credentials are sent.

**Note** This field is optional. The lobby ambassador user can enter any email id of his preference at the time of creating a guest user.

Step 6 Provide a brief description of the account.

Step 7 If you want to supply disclaimer text, enter it.

Select the **Defaults Editable** check box if you want to allow the lobby ambassador to override these configured defaults. This allows the Lobby Ambassadors to modify Guest User default settings while creating guest account from the Lobby Ambassador portal.

**Note** If no default profile is selected on this tab, the defaults are not applied to this Lobby Ambassador. However, the Lobby Ambassador account is created, and the Lobby Ambassador can create users with credentials as desired.

Step 8 Select the **Max User Creations Allowed** check box to set limits on the number of guest users that can be created by the lobby ambassador in a given time period. The time period is defined in hours, days, or weeks.

Step 9 Click the **Preview Current Logo** link to see what is currently being used as a logo, and then you can click to enable it or browse to another location to update the logo.

Step 10 If you want additional page header text, you can enter it at the Print Page Header Text field.

Step 11 Click **Submit**.

---

**Viewing or Editing Group Information**

To see specific tasks the user is permitted to do within the defined group or make changes to the tasks, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 Choose **Users** from the left sidebar menu.

Step 3 Click the group link in the **Member Of** column. The Group Detail: **User Group** page appears.
Chapter 7  Managing User Accounts

Viewing the Audit Trail

Click the icon in the Users page to view the configuration changes performed by individual users. The Audit Trail page appears.

This page enables you to view the following data:

- **User**—User login name.
- **Operation**—Type of operation audited.
- **Time**—Time operation was audited.
- **Status**—Success or failure.
- **Reason**—Indicates any login failure reason, for example, invalid password.
- **Configuration Changes**—This field provides a Details link if there are any configuration changes. Click the Details link for more information on the configuration changes done by an individual user. The entries list the change of values for individual parameters between the Prime Infrastructure and Controller. For more information on Audit Trail Details, see “Audit Trail Details Page” section on page 7-8.

You will see the Details link only when you make configuration changes to the wireless devices.

The audit trail entries could be logged for individual controller changes. For example, if a template is applied on multiple controllers, then there are multiple audit entries for each controller to which the template has been applied to.
Audit Trail Details Page

The Configuration Changes column in the Audit Trail list page contains a Details link if there are changes to the configuration. Click the Details link to view the Audit Trail Details for a specific User. The Audit Trail Details dialog box shows the attribute-level differences when a User changes the configuration from either the Templates or Configuration side.

Table 7-1 describes the fields in the Audit Trail Details dialog box.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prime Infrastructure Username</td>
<td>The username who triggered this audit trail.</td>
</tr>
<tr>
<td>Object Name</td>
<td>The name of the object that has triggered this audit trail.</td>
</tr>
<tr>
<td>Operation Time</td>
<td>The date and time at which the audit entry was made.</td>
</tr>
</tbody>
</table>
| Configuration Changes         | Lists the attributes that have been changed as a result of a user action in the Prime Infrastructure and the controller. For example, the attributes could be:  
  - Quality of service  
  - Admin Status  
  - MAC Filters |

Creating Guest User Accounts

You can use the Cisco Lobby Ambassador to create guest user accounts in the Prime Infrastructure. A guest network provided by an enterprise allows access to the Internet for a guest without compromising the host. The web authentication is provided with or without a supplicant or client, so a guest needs to initiate a VPN tunnel to their desired destinations.

Both wired and wireless guest user access is supported. Wired guest access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or specific ports in a conference room. Like wireless guest user accounts, wired guest access ports are added to the network using the lobby ambassador feature.

The network administrator must first set up a lobby ambassador account. Guest user accounts are for visitors, temporary workers, and so on, who need network access. A lobby ambassador account has limited configuration privileges and only allows access to the screens used to configure and manage guest user accounts.

The lobby ambassador can create the following types of guest user accounts:

- A guest user account with a limited lifetime. After the specified time period, the guest user account automatically expires.
- A guest user account with an unlimited lifetime. This account never expires.
Managing the Prime Infrastructure Guest User Accounts

Prime Infrastructure guest user accounts are managed with the use of templates. This section describes how to manage the Prime Infrastructure user accounts.

- Configuring a Guest User Template, page 11-55
- Scheduling the Prime Infrastructure Guest User Accounts, page 7-10
- Printing or E-mailing the Prime Infrastructure Guest User Details, page 7-11
- Saving Guest Accounts on a Device, page 7-11
Scheduling the Prime Infrastructure Guest User Accounts

A lobby ambassador is able to schedule automatic creation of a guest user account. The validity and recurrence of the account can be defined. The generation of a new password on every schedule is optional and is enabled by selecting a check box. For scheduled users, the password is automatically generated and is automatically sent by e-mail to the host of the guest. The e-mail address for the host is configured on the New User page. After clicking Save, the Guest User Details page displays the password. From this page, you can e-mail or printer the account credentials.

To schedule a recurring guest user account in the Prime Infrastructure, follow these steps:

Step 1 Log in to the Prime Infrastructure user interface as lobby ambassador.
Step 2 Choose Schedule Guest User from the Guest User page.

Note You can also schedule guest users from the Configure > Controller Template Launch Pad > Security > Guest User option.

Step 3 In the Guest Users > Scheduling page, enter the guest username. The maximum is 24 characters.
Step 4 Select the check box to generate a username and password on every schedule. If this is enabled, a different password is supplied for each day (up to the number of days chosen). If this is disabled (unselected), one password is supplied for a span of days. The generation of a new password on every schedule is optional.
Step 5 Select a Profile ID from the drop-down list. This is the SSID to which this guest user applies and must be a WLAN that has Layer 3 authentication policy configured. Your administrator can advise which Profile ID to use.
Step 6 Enter a description of the guest user account.
Step 7 Choose limited or unlimited.

- Limited—From the drop-down list, choose days, hours, or minutes for the lifetime of this guest user account. The maximum is 365 days.
  - Start time—Date and time when the guest user account begins.
  - End time—Date and time when the guest user account expires.
- Unlimited—This user account never expires.
- Days of the week—Select the check box for the days of the week that apply to this guest user account.
Step 8 Choose Apply To to restrict a guest user to a confined area by selecting a campus, building, or floor so that when applied, only those controllers and associated access points are available. You can use AP grouping to enforce access point level restrictions that determine which SSIDs to broadcast. Those access points are then assigned to the respective floors. You can also restrict the guest user to specific listed controllers or a configuration group, which is a group of controllers that has been preconfigured by the administrator.

From the drop-down lists, choose one of the following:

- Controller List—Select the check box for the controller(s) to which the guest user account is associated.
- Indoor Area—Choose the applicable campus, building, and floor.
- Outdoor Area—Choose the applicable campus and outdoor area.
Managing the Prime Infrastructure Guest User Accounts

• **Config group**—Choose the configuration group to which the guest user account belongs.

**Step 9** Enter the e-mail address to send the guest user account credentials. Each time the scheduled time comes up, the guest user account credentials are e-mailed to the specified e-mail address.

**Step 10** Review the disclaimer information. Use the scroll bar to move up and down.

**Step 11** Click **Save** to save your changes or **Cancel** to leave the settings unchanged.

---

**Printing or E-mailing the Prime Infrastructure Guest User Details**

The lobby ambassador can print or e-mail the guest user account details to the host or person who welcomes guests.

The e-mail and print copy shows the following details:

- Username—Guest user account name.
- Password—Password for the guest user account.
- Start time—Data and time when the guest user account begins.
- End time—Date and time when the guest user account expires.
- Profile ID—Profile assigned to the guest user. Your administrator can advise which Profile ID to use.
- Disclaimer—Disclaimer information for the guest user.

When creating the guest user account and applying the account to a list of controllers, area, or configuration group, a link is provided to e-mail or print the guest user account details. You can also print guest user account details from the Guest Users List page.

To print guest user details from the Guest Users List page, follow these steps:

**Step 1** Log into the Prime Infrastructure user interface as lobby ambassador.

**Step 2** On the Guest User page, select the check box next to User Name, choose **Print/E-mail User Details** from the Select a command drop-down list, and click **Go**.

- If printing, click **Print** and from the print page, select a printer, and click **Print** or **Cancel**.
- If e-mailing, click **E-mail** and from the e-mail page, enter the subject text and the e-mail address of the recipient. Click **Send** or **Cancel**.

**Note** You can also print or e-mail user details from the Configure > Controller Template Launch Pad > Security > Guest User option.

---

**Saving Guest Accounts on a Device**

Select the **Save Guest Accounts on Device** check box to save guest accounts to a WLC flash so that they are maintained across WLC reboots.
Adding a New User

The Add User page allows the administrator to set up a new user login including username, password, groups assigned to the user, and virtual domains for the user.

Note You can only assign virtual domains to a newly created user which you own. By assigning virtual domains to a user, the user is restricted to information applicable to those virtual domains.

- Adding User Names, Passwords, and Groups, page 7-12
- Assigning a Virtual Domain, page 7-13

Adding User Names, Passwords, and Groups

To add a new user, follow these steps:

Step 1 Choose Administration > AAA.
Step 2 From the left sidebar menu, choose Users.
Step 3 From the Select a command drop-down list, choose Add User.
Step 4 Click Go. The Users page appears.
Step 5 Enter a new Username.
Step 6 Enter and confirm a password for this account.
Step 7 Select the check box(es) of the groups to which this user is assigned.

Note If the user belongs to Lobby Ambassador, Monitor Lite, Northbound API, or Users Assistant group, the user cannot belong to any other group.

- Admin—Allows users to monitor and configure the Prime Infrastructure operations and perform all system administration tasks.
- ConfigManagers—Allows users to monitor and configure the Prime Infrastructure operations.
- System Monitoring—Allows users to monitor the Prime Infrastructure operations.
• Users Assistant—Allows local net user administration only.
• Lobby Ambassador—Allows guest access for configuration and management only of user accounts. If Lobby Ambassador is selected, a Lobby Ambassador Defaults tab appears.
• Monitor Lite—Allows monitoring of assets location.
• North Bound API User—A user group used by the Prime Infrastructure Web Service consumers. That is, any North Bound APIs.

Note If you are creating a North Bound API user from TACACS or RADIUS, the default user domain should be root.

Note North Bound API Users cannot be assigned a Virtual Domain. When a North Bound API group is selected, the Virtual Domains tab is not available.

• SuperUsers—Allows users to monitor and configure the Prime Infrastructure operations and perform all system administration tasks including administering the Prime Infrastructure user accounts and passwords. Superuser tasks can be changed.
• Root—This group is only assignable to ‘root’ user and that assignment cannot be changed.
• User Defined.

Assigning a Virtual Domain

To assign a virtual domain to this user, follow these steps:

Step 1 Click the Virtual Domains tab. This tab displays all virtual domains available and assigned to this user.

Note The Virtual Domains tab enables the administrator to assign virtual domains for each user. By assigning virtual domains to a user, the user is restricted to information applicable to those virtual domains.

Note North Bound API Users cannot be assigned a Virtual Domain. When a North Bound API group is selected, the Virtual Domains tab is not available.

Step 2 Click to highlight the virtual domain in the Available Virtual Domains list that you want to assign to this user.

Note You can select more than one virtual domain by holding down the Shift or Control key.

Step 3 Click Add >. The virtual domain moves from the Available Virtual Domains to the Selected Virtual Domains list.
Managing Lobby Ambassador Accounts

You can use the Cisco Lobby Ambassador to create guest user accounts in the Prime Infrastructure. A guest network provided by an enterprise allows access to the Internet for a guest without compromising the host. The web authentication is provided with or without a supplicant or client, so a guest needs to initiate a VPN tunnel to their desired destinations.

Both wired and wireless guest user access is supported. Wired guest access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or specific ports in a conference room. Like wireless guest user accounts, wired guest access ports are added to the network using the lobby ambassador feature.

The network administrator must first set up a lobby ambassador account. Guest user accounts are for visitors, temporary workers, and so on, who need network access. A lobby ambassador account has limited configuration privileges and only allows access to the pages used to configure and manage guest user accounts.

The lobby ambassador can create the following types of guest user accounts:

- A guest user account with a limited lifetime. After the specified time period, the guest user account automatically expires.
- A guest user account with an unlimited lifetime. This account never expires.
- A guest user account that is activated at a predefined time in the future. The lobby ambassador defines the beginning and end of the valid time period.

Creating a Lobby Ambassador Account, page 7-14
Editing a Lobby Ambassador Account, page 7-16
Logging in to the Prime Infrastructure User Interface as a Lobby Ambassador, page 7-16
Logging the Lobby Ambassador Activities, page 7-17

Creating a Lobby Ambassador Account

Note

A group that has the SuperUser/administrator privileges (by default) can create a lobby ambassador account.

To create a lobby ambassador account in the Prime Infrastructure, follow these steps:

Step 1 Log into the Prime Infrastructure user interface as an administrator.
Step 2 Choose Administration > AAA.
Step 3 From the left sidebar menu, choose Users.
Step 4 From the Select a command drop-down list, choose Add User.

Step 5 Click Go.

Step 6 Enter the username.

Step 7 Enter the password. Reenter to confirm the password. Password requirements include the following:

- The password must have a minimum of eight characters.
- The password must include at least three of the following elements: lowercase letters, uppercase letters, numbers, or special characters.

Step 8 In the Groups Assigned to this User section, select the Lobby Ambassador check box to access the Lobby Ambassador Defaults tab.

The Lobby Ambassador Defaults tab has the following parameters:

- Profile—The default profile to which the guest users would connect.
- Lifetime—Limited or Unlimited.

Note By default, the lifetime is limited to eight hours.

- Apply to—From the drop-down list, choose one of the following:
  - Indoor Area—Campus, Building, and Floor.
  - Outdoor Area—Campus, Outdoor Area.
  - Controller List—List of controller(s) on which the selected profile is created.
  - Config Groups—Config group names configured on the Prime Infrastructure.
- Email ID—The e-mail ID of the host to whom the guest account credentials are sent.

Note This field is optional. The lobby ambassador user can enter any email id of his preference at the time of creating a guest user.

- Description—A brief description of this account.
- Disclaimer—The default disclaimer text.
- Defaults Editable—Select this check box if you want to allow the lobby ambassador to override these configured defaults. This allows the lobby ambassador to modify these Guest User Account default settings while creating Guest Accounts from the Lobby Ambassador portal.

Note If no default profile is selected on this tab, the defaults are not applied to this Lobby Ambassador. However, the Lobby Ambassador account is created and the Lobby Ambassador can create users with credentials as desired.

- Max User Creation Allowed—Select this check box to set limits on the number of guest users that can be created by the Lobby Ambassador in a given time period. The time period is defined in hours, days, or weeks.
- Click Submit. The name of the new lobby ambassador account is listed and the account can be used immediately.
Editing a Lobby Ambassador Account

The Lobby Ambassador default credentials can be edited from the username link on the Prime Infrastructure user list page.

To edit the Lobby Ambassador default credentials, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log into the Prime Infrastructure user interface as an administrator.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Choose Administration &gt; AAA.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the left sidebar menu, choose Users.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click the applicable Lobby Ambassador account in the User Name column.</td>
</tr>
<tr>
<td>Step 5</td>
<td>From the Lobby Ambassador Defaults page, edit the credentials as necessary.</td>
</tr>
</tbody>
</table>

Note: While editing, if the Profile selection is removed (changed to Select a profile), the defaults are removed for this Lobby Ambassador. The user must reconfigure the defaults to reinforce them.

Step 6 Click Submit.

Logging in to the Prime Infrastructure User Interface as a Lobby Ambassador

When you log in as a lobby ambassador, you have access to the guest user template page in the Prime Infrastructure. You can then configure guest user accounts (through templates).

To log into the Prime Infrastructure user interface through a web browser, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Launch Internet Explorer 8 or later on your computer.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>Some Prime Infrastructure features might not function properly if you use a web browser other than Internet Explorer 8 or later on a Windows workstation.</td>
</tr>
</tbody>
</table>

| Step 2 | In the browser address line, enter https://Prime Infrastructure-ip-address (such as https://1.1.1.1), where Prime Infrastructure-ip-address is the IP address of the computer on which the Prime Infrastructure is installed. Your administrator can provide this IP address. |

| Step 3 | When the Prime Infrastructure user interface displays the Login window, enter your username and password. |

Note All entries are case sensitive.

Note The lobby ambassador can only define guest users templates.

Step 4 Click Submit to log into the Prime Infrastructure. Prime Infrastructure user interface is now active and available for use. The Guest Users page is displayed. This page provides a summary of all created Guest Users.
To exit the Prime Infrastructure user interface, close the browser window or click **Logout** in the upper right corner of the page. Exiting a Prime Infrastructure user interface session does not shut down the Prime Infrastructure on the server.

---

**Note**

When a system administrator stops the Prime Infrastructure server during a Prime Infrastructure session, the session ends, and the web browser displays this message: “The page cannot be displayed.” Your session does not reassociate to the Prime Infrastructure when the server restarts. You must restart the Prime Infrastructure session.

---

### Logging the Lobby Ambassador Activities

The following activities are logged for each lobby ambassador account:

- Lobby ambassador login—Prime Infrastructure logs the authentication operation results for all users.
- Guest user creation—When a lobby ambassador creates a guest user account, the Prime Infrastructure logs the guest username.
- Guest user deletion—When a lobby ambassador deletes the guest user account, the Prime Infrastructure logs the deleted guest username.
- Account updates—Prime Infrastructure logs the details of any updates made to the guest user account. For example, increasing the life time.

To view the lobby ambassador activities, follow these steps:

---

**Note**

You must have administrative permissions to open this window.

---

**Step 1**

Log into the Prime Infrastructure user interface as an administrator.

**Step 2**

Choose **Administration > AAA > Groups** from the left sidebar menu to display the All Groups page.

**Step 3**

On the All Groups page, click the **Audit Trail** icon for the lobby ambassador account you want to view. The Audit Trail page for the lobby ambassador appears.

This page enables you to view a list of lobby ambassador activities over time.

- **User**—User login name
- **Operation**—Type of operation audited
- **Time**—Time operation was audited
- **Status**—Success or failure

**Step 4**

To clear the audit trail, choose **Clear Audit Trail** from the Select a command drop-down list, and click **Go**.
Managing Lobby Ambassador Accounts
Configuring Mobility Groups

This chapter describes mobility groups and explains how to configure them on the Cisco Prime Infrastructure.

- Information About Mobility, page 8-1
- Symmetric Tunneling, page 8-5
- Overview of Mobility Groups, page 8-5
- Configuring Mobility Groups, page 8-8
- Mobility Anchors, page 8-11
- Configuring Multiple Country Codes, page 8-11
- Configuring Controller Config Groups, page 8-12
- Reporting Config Groups, page 8-16
- Downloading Software, page 8-17

Information About Mobility

Mobility, or roaming, is an ability of a wireless client to maintain its association seamlessly from one access point to another securely and with as little latency as possible. This section explains how mobility works when controllers are included in a wireless network.

When a wireless client associates and authenticates to an access point, the controller places an entry for that client in its client database. This entry includes the MAC and IP addresses of the client, security context and associations, quality of service (QoS) contexts, the WLANs, and the associated access point. The controller uses this information to forward frames and manage traffic to and from the wireless client. Figure 8-1 illustrates a wireless client roaming from one access point to another when both access points are joined to the same controller.
When the wireless client moves its association from one access point to another, the controller simply updates the client database with the newly associated access point. If necessary, new security context and associations are established as well.

The process becomes more complicated, however, when a client roams from an access point joined to one controller to an access point joined to a different controller. The process also varies based on whether the controllers are operating on the same subnet. Figure 8-2 illustrates inter-controller roaming, which occurs when the wireless LAN interfaces of a controller are on the same IP subnet.
When the client associates to an access point joined to a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database entry is updated for the new access point. This process remains invisible to the user.

**Note**

All clients configured with 802.1X/Wi-Fi Protected Access (WPA) security complete a full authentication to comply with the IEEE standard.

**Figure 8-3** illustrates *inter-subnet roaming*, which occurs when the wireless LAN interfaces of a controller are on different IP subnets.
Inter-subnet roaming is similar to inter-controller roaming in that the controllers exchange mobility messages on how the client roams. However, instead of moving the client database entry to the new controller, the original controller marks the client with an “Anchor” entry in its own client database. The database entry is copied to the new controller client database and marked with a “Foreign” entry in the new controller. The roam remains invisible to the wireless client, and the client maintains its original IP address.

After an inter-subnet roam, data flows in an asymmetric traffic path to and from the wireless client. Traffic from the client to the network is forwarded directly into the network by the foreign controller. Traffic to the client arrives at the anchor controller, which forwards the traffic to the foreign controller in an EtherIP tunnel. The foreign controller then forwards the data to the client. If a wireless client roams to a new foreign controller, the client database entry is moved from the original foreign controller to the new foreign controller, but the original anchor controller is always maintained. If the client moves back to the original controller, it becomes local again.

In inter-subnet roaming, WLANs on both anchor and foreign controllers need to have the same network access privileges and no source-based routing or source-based firewalls in place. Otherwise, the clients might have network connectivity problems after the handoff.

**Note**

Currently, multicast traffic cannot be passed during inter-subnet roaming. In other words, avoid designing an inter-subnet network for Spectralink phones that need to send multicast traffic while using push to talk.

**Note**

Both inter-controller roaming and inter-subnet roaming require the controllers to be in the same mobility group. See the next two sections for a description of mobility groups and instructions for configuring them.
Symmetric Tunneling

With symmetric mobility tunneling, the controller provides inter-subnet mobility for clients roaming from one access point to another within a wireless LAN. The client traffic on the wired network is directly routed by the foreign controller. If a router has Reverse Path Filtering (RPF) enabled (which provides additional checks on incoming packets), the communication is blocked. Symmetric mobility tunneling allows the client traffic to reach the controller designated as the anchor, even with RPF enabled. You enable or disable symmetric tunneling by choosing Configure > Controller and then System > General from the left sidebar menu.

**Note**
All controllers in a mobility group should have the same symmetric tunneling mode.

**Note**
For symmetric tunneling to take effect, a reboot is required.

With this guest tunneling N+1 redundancy feature, the time it takes for a client to join another access point following a controller failure is decreased because a failure is quickly identified, the clients are moved away from the problem controller, and the clients are anchored to another controller.

See the “Configuring Controller Templates” section on page 11-4 for instructions on configuring this feature within a template.

Overview of Mobility Groups

A set of controllers can be configured as a mobility group to allow seamless client roaming within a group of controllers. By creating a mobility group, you can enable multiple controllers in a network to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers can share the context and state of client devices and controller loading information. With this information, the network can support inter-controller wireless LAN roaming and controller redundancy.

**Note**
Clients do not roam across mobility groups.

Figure 8-4 shows an example of a mobility group.
As shown in Figure 8-4, each controller is configured with a list of the other members of the mobility group. Whenever a new client joins a controller, the controller sends out a unicast message to all of the controllers in the mobility group. The controller to which the client was previously connected passes on the status of the client. All mobility exchange traffic between controllers is carried over a CAPWAP tunnel.

Examples:

1. A 4404-100 controller supports up to 100 access points. Therefore, a mobility group consisting of 24 4404-100 controllers supports up to 2400 access points (24 * 100 = 2400 access points).

2. A 4402-25 controller supports up to 25 access points, and a 4402-50 controller supports up to 50 access points. Therefore, a mobility group consisting of 12 4402-25 controllers and 12 4402-50 controllers supports up to 900 access points (12 * 25 + 12 * 50 = 300 + 600 = 900 access points).

Mobility groups enable you to limit roaming between different floors, buildings, or campuses in the same enterprise by assigning different mobility group names to different controllers within the same wireless network. Figure 8-5 shows the results of creating distinct mobility group names for two groups of controllers.
Overview of Mobility Groups

The controllers in the ABC mobility group recognize and communicate with each other through their access points and through their shared subnets. The controllers in the ABC mobility group do not recognize or communicate with the XYZ controllers, which are in a different mobility group. Likewise, the controllers in the XYZ mobility group do not recognize or communicate with the controllers in the ABC mobility group. This feature ensures mobility group isolation across the network.

**Note**
Clients might roam between access points in different mobility groups, provided they can detect them. However, their session information is not carried between controllers in different mobility groups.

When to Include Controllers in a Mobility Group

If it is possible for a wireless client in your network to roam from an access point joined to one controller to an access point joined to another controller, both controllers should be in the same mobility group.
Configuring Mobility Groups

Chapter 8      Configuring Mobility Groups

Messaging among Mobility Groups

The controller provides inter-subnet mobility for clients by sending mobility messages to other member controllers. There can be up to 72 members in the list with up to 24 in the same mobility group. In the Prime Infrastructure and controller software releases 5.0, two improvements have been made to mobility messaging, each of which is especially useful when sending messages to the full list of mobility members:

- Sending Mobile Announce messages within the same group first and then to other groups in the list
  The controller sends a Mobile Announce message to members in the mobility list each time a new client associates to it. In the Prime Infrastructure and controller software releases prior to 5.0, the controller sends this message to all members in the list irrespective of the group to which they belong. However, in controller software release 5.0, the controller sends the message only to those members that are in the same group as the controller and then includes all of the other members while sending retries.

- Sending Mobile Announce messages using multicast instead of unicast
  In the Prime Infrastructure and controller software releases prior to 5.0, the controller might be configured to use multicast to send the mobile announce messages, which requires sending a copy of the messages to every mobility member. This behavior is not efficient because many messages (such as Mobile Announce, PMK Update, AP List Update, and IDS Shun) are meant for all members in the group. In the Prime Infrastructure and controller software releases 5.0, the controller uses multicast mode to send the Mobile Announce messages. This behavior allows the controller to send only one copy of the message to the network, which destines it to the multicast group containing all the mobility members. To derive the maximum benefit from multicast messaging, we recommend that it be enabled or disabled on all group members.

Configuring Mobility Groups

This section provides instructions for configuring mobility groups.

Note
You can also configure mobility groups using the controller. See the Cisco Wireless LAN Controller Configuration Guide for instructions.

Prerequisites

Before you add controllers to a mobility group, you must verify that the following requirements have been met for all controllers that are to be included in the group:

- All controllers must be configured for the same LWAPP transport mode (Layer 2 or Layer 3).
  
  Note
  You can verify and, if necessary, change the LWAPP transport mode in the System > General page.

- IP connectivity must exist between the management interfaces of all devices.
  
  Note
  You can verify IP connectivity by pinging the controllers.
All controllers must be configured with the same mobility group name.

**Note** For the Cisco WiSM, both controllers should be configured with the same mobility group name for seamless routing among 300 access points.

All devices must be configured with the same virtual interface IP address.

**Note** If all the controllers within a mobility group are not using the same virtual interface, inter-controller roaming might appear to work, but the hand-off does not complete, and the client loses connectivity for a period of time.

You must have gathered the MAC address and IP address of every controller that is to be included in the mobility group. This information is necessary because you configure all controllers with the MAC address and IP address of all the other mobility group members.

**Note** You can find the MAC and IP addresses of the other controllers to be included in the mobility group in the Configure > Controllers page.

To add each WLC controller into mobility groups and configure them, follow these steps:

**Step 1** Choose **Configure > Controllers**.

This page shows the list of all the controllers you added in Step 1. The mobility group names and the IP address of each controller that is currently a member of the mobility group is listed.

**Step 2** Choose the first controller by clicking the WLC IP address. You then access the controller templates interface for the controller you are managing.

**Step 3** Choose **System > Mobility Groups** from the left sidebar menu. The existing Mobility Group members are listed in the page.

**Step 4** You see a list of available controllers. From the Select a command drop-down list in the upper right-hand corner, choose **Add Group Members** and then click **Go**.

**Step 5** If no controllers were found to add to the mobility group, you can add the members manually by clicking the “To add members manually to the Mobility Group click here” link. The Mobility Group Member page appears.

**Step 6** In the Member MAC Address text box, enter the MAC address of the controller to be added.

**Step 7** In the Member IP Address text box, enter the management interface IP address of the controller to be added.

**Note** If you are configuring the mobility group in a network where Network Address Translation (NAT) is enabled, enter the IP address sent to the controller from the NAT device rather than the management interface IP address of the controller. Otherwise, mobility fails among controllers in the mobility group.

**Step 8** Enter the multicast group IP address to be used for multicast mobility messages in the Multicast Address text box. The group address of the local mobility member must be the same as the group address of the local controller.

**Step 9** In the Group Name text box, enter the name of the mobility group.
Step 10  Click Save.
Step 11  Repeat the Steps 1 through 9 for the remaining WLC devices.

Setting the Mobility Scalability Parameters

To set the mobility message parameters, follow these steps:

Note  You must complete the steps in the “Configuring Mobility Groups” section on page 8-8 prior to setting the mobility scalability parameters.

Step 1  Choose Configure > Controllers.
Step 2  Choose an IP address of a controller whose software version is 5.0 or later.
Step 3  Choose System > Multicast from the left sidebar menu. The Multicast page appears.
Step 4  From the Ethernet Multicast Support drop-down list, specify if you want to disable the ability for the controller to use multicast mode to send Mobile Announce messages to mobility members. Otherwise, you can choose Multicast or Unicast from the drop-down list.
Step 5  If you chose multicast in Step 4, you must enter the group IP address at the Multicast Group Address field to begin multicast mobility messaging. You must configure this IP address for the local mobility group, but it is optional for other groups within the mobility list. If you do not configure the IP address for other (non-local) groups, the controllers use unicast mode to send mobility messages to those members.
Step 6  Select the Global Multicast Mode check box to make the multicast mode available globally.
Step 7  Select the Enable IGMP Snooping check box to enable IGMP snooping.
Step 8  Choose Enable from the Multicast Mobility Mode drop-down list to change the IGMP snooping status or to set the IGMP timeout. When IGMP snooping is enabled, the controller gathers IGMP reports from the clients and then sends each access point a list of the clients listening to any multicast group. The access point then forwards the multicast packets only to those clients.

The timeout interval has a range of 3 to 300 and a default value of 60. When the timeout expires, the controller sends a query to all WLANs. Those clients which are listening in the multicast group then send a packet back to the controller.
Step 9  If you enabled the Multicast Mobility Mode, enter the mobility group multicast address.
Step 10  Select the Multicast Direct check box to enable videos to be streamed over a wireless network.
Step 11  Specify the Session Banner information, which is the error information sent to the client if the client is denied or dropped from a Media Stream.

a. State—Select the check box to activate the Session Banner. If not activated, the Session Banner is not sent to the client
b. URL—A web address reported to the client
c. Email—An e-mail address reported to the client
d. Phone—A telephone number reported to the client
e. Note—A note reported to the client
Note: All media streams on a controller share this configuration.

Step 12: Click Save.

Mobility Anchors

Mobility anchors are a subset of a mobility group specified as the anchor controllers for a WLAN. This feature can be used to restrict a WLAN to a single subnet, regardless of the entry point of a client into the network. In this way, users can access a public or guest WLAN throughout an enterprise but still be restricted to a specific subnet. Guest WLAN can also be used to provide geographic load balancing because WLANs can represent a particular section of a building (such as a lobby, a restaurant, and so on). For more information about Mobility Anchors, and how to configure a new WLAN and guest anchor controller, see the Mobility Anchors section in the Cisco Prime Infrastructure 2.0 User Guide.

Configuring Multiple Country Codes

You can configure one or more countries on a controller. After countries are configured on a controller, the corresponding 802.11a/n DCA channels are available for selection. At least one DCA channel must be selected for the 802.11a/n network. When the country codes are changed, the DCA channels are automatically changed in coordination.

Note: 802.11a/n and 802.11b/n networks for controllers and access points must be disabled before configuring a country on a controller. To disable 802.11a/n or 802.11b/n networks, choose Configure > Controllers, select the desired controller you want to disable, choose 802.11a/n or 802.11b/g/n from the left sidebar menu, and then choose Parameters. The Network Status is the first check box.

Note: To configure multiple country codes outside of a mobility group, see the “Configuring Security Parameters” section on page 9-90.

To add multiple controllers that are defined in a configuration group and then set the DCA channels, follow these steps:

Step 1: Choose Configure > Controller Config Groups.
Step 2: Choose Add Config Groups from the Select a command drop-down list, and click Go.
Step 3: Create a config group by entering the group name and mobility group name.
Step 4: Click Save. The Config Groups page appears.
Step 5: Click the Controllers tab. The Controllers page appears.
Step 6: Highlight the controllers you want to add, and click Add. The controller is added to the Group Controllers page.
Chapter 8      Configuring Mobility Groups

Configuring Controller Config Groups

By creating a config group, you can group controllers that should have the same mobility group name and similar configuration. You can assign templates to the group and push templates to all the controllers in a group. You can add, delete, or remove config groups, and download software, IDS signatures, or a customized web authentication page to controllers in the selected config groups. You can also save the current configuration to nonvolatile (flash) memory to controllers in selected config groups.

Note: A controller cannot be a member of more than one mobility group. Adding a controller to one mobility group removes that controller from any other mobility group to which it is already a member.

For information about applying templates to either individual controllers or controllers in selected Config Groups, see the “Using Templates” section on page 11-1.

By choosing Configure > Controller Config Groups, you can view a summary of all config groups in the Prime Infrastructure database. When you choose Add Config Groups from the Select a command drop-down list, the page displays a table with the following columns:

- Group Name: Name of the config group.
- Templates: Number of templates applied to config group.

Adding New Group

To add a config group, follow these steps:

Step 1  Choose Configure > Controller Config Groups.
Step 2  From the Select a command drop-down list, choose Add Config Group, and click Go. The Add New Group page appears.
Step 3  Enter the new config group name. It must be unique across all groups. If Enable Background Audit is selected, the network and controller audits occur for this config group. If Enable Enforcement is selected, the templates are automatically applied during the audit if any discrepancies are found.
Chapter 8  Configuring Mobility Groups

Configuring Controller Config Groups

To configure a config group, follow these steps:

Step 1  Choose Configure > Controller Config Groups, and click a group name in the Group Name column. The Config Group page appears.

Step 2  Click the General tab. The following options for the config group appear:

- Group Name: Name of the config group
  - Enable Background Audit—If selected, all the templates that are part of this group are audited against the controller during network and controller audits.
  - Enable Enforcement—If selected, the templates are automatically applied during the audit if any discrepancies are found.

  Note  The audit and enforcement of the config group template happens when the selected audit mode is Template based audit.

- Enable Mobility Group—If selected, the mobility group name is pushed to all controllers in the group.

- Mobility Group Name: Mobility Group Name that is pushed to all controllers in the group. The Mobility Group Name can also be modified here.

  Note  A controller can be part of multiple config groups.

- Last Modified On: Date and time config group was last modified.

Step 4  Other templates created in the Prime Infrastructure can be assigned to a config group. The same WLAN template can be assigned to more than one config group. Choose from the following:

- Select and add later: Click to add a template at a later time.

- Copy templates from a controller: Click to copy templates from another controller. Choose a controller from a list of current controllers to copy its applied template to the new config group. Only the templates are copied.

  Note  The order of the templates is important when dealing with radio templates. For example, if the template list includes radio templates that require the radio network to be disabled prior to applying the radio parameters, the template to disable the radio network must be added to the template first.

Step 5  Click Save. The Config Groups page appears.
Configuring Controller Config Groups

Step 3 You must click the Apply/Schedule tab to distribute the specified mobility group name to the group controllers and to create mobility group members on each of the group controllers.

Step 4 Click Save.

Adding or Removing Controllers from a Config Group

To add or remove controllers from a config group, follow these steps:

Step 1 Choose Configure > Controller Config Groups, and click a group name in the Group Name column.
Step 2 Click the Controllers tab. The columns in the table display the IP address of the controller, the config group name the controller belongs to, and the mobility group name of the controller.
Step 3 Click to highlight the row of the controller you want to add to the group.
Step 4 Click Add.

Note If you want to remove a controller from the group, highlight the controller in the Group Controllers box and click Remove.

Step 5 You must click the Apply/Schedule tab, and click Apply to add or remove the controllers to the config groups.
Step 6 Click Save Selection.

Adding or Removing Templates from the Config Group

To add or remove templates from the config group, follow these steps:

Step 1 Choose Configure > Controller Config Groups, and click a group name in the Group Name column.
Step 2 Click the Templates tab. The Remaining Templates table displays the item number of all available templates, the template name, and the type and use of the template.
Step 3 Click to highlight the row of the template you want to add to the group.
Step 4 Click Add to move the highlighted template to the Group Templates column.

Note If you want to remove a template from the group, highlight the template in the Remaining Templates box, and click Remove.

Step 5 You must click the Apply/Schedule tab, and click Apply to add or remove the templates to the config groups.
Step 6 Click Save Selection.
Applying or Scheduling Config Groups

Note  The scheduling function allows you to schedule a start day and time for provisioning.

To apply the mobility groups, mobility members, and templates to all the controllers in a config group, follow these steps:

Step 1  Choose Configure > Controller Config Groups, and click a group name in the Group Name column.
Step 2  Click the Apply/Schedule tab to access this page.
Step 3  Click Apply to start the provisioning of mobility groups, mobility members, and templates to all the controllers in the config group. After you apply, you can leave this page or log out of the Prime Infrastructure. The process continues, and you can return later to this page to view a report.

Note  Do not perform any other config group functions during the apply provisioning.

A report is generated and appears in the Recent Apply Report page. It shows which mobility group, mobility member, or template were successfully applied to each of the controllers.

Note  If you want to print the report as shown on the page, you must choose landscape page orientation.

Step 4  Enter a starting date in the text box or use the calendar icon to choose a start date.
Step 5  Choose the starting time using the hours and minutes drop-down lists.
Step 6  Click Schedule to start the provisioning at the scheduled time.

Auditing Config Groups

The Config Groups Audit page allows you to verify if the configuration complies of the controller with the group templates and mobility group. During the audit, you can leave this screen or log out of the Prime Infrastructure. The process continues, and you can return to this page later to view a report.

Note  Do not perform any other config group functions during the audit verification.

To perform a config group audit, follow these steps:

Step 1  Choose Configure > Controller Config Groups, and click a group name in the Group Name column.
Step 2  Click the Audit tab to access this page.
Step 3  Click to highlight a controller from the Controllers tab, choose >> (Add), and Save Selection.
Step 4  Click to highlight a template from the Templates tab, choose >> (Add), and Save Selection.
Step 5  Click Audit to begin the auditing process.
A report is generated and the current configuration on each controller is compared with that in the config group templates. The report displays the audit status, the number of templates in sync, and the number of templates out of sync.

**Note** This audit does not enforce the Prime Infrastructure configuration to the device. It only identifies the discrepancies.

**Step 6** Click **Details** to view the Controller Audit Report details.

**Step 7** Double-click a line item to open the Attribute Differences page. This page displays the attribute, its value in the Prime Infrastructure, and its value in the controller.

**Note** Click **Retain Prime Infrastructure Value** to push all attributes in the Attribute Differences page to the device.

**Step 8** Click **Close** to return to the Controller Audit Report page.

### Rebooting Config Groups

To reboot a config group, follow these steps:

**Step 1** Choose **Configure > Controller Config Groups**, and click a group name in the Group Name column.

**Step 2** Click the **Reboot** tab.

**Step 3** Select the **Cascade Reboot** check box if you want to reboot one controller at a time, waiting for that controller to come up before rebooting the next controller.

**Step 4** Click **Reboot** to reboot all controllers in the config group at the same time. During the reboot, you can leave this page or logout of the Prime Infrastructure. The process continues, and you can return later to this page and view a report.

The Recent Reboot Report page shows when each controller was rebooted and what the controller status is after the reboot. If the Prime Infrastructure is unable to reboot the controller, a failure is shown.

**Note** If you want to print the report as shown on the page, you must choose landscape page orientation.

### Reporting Config Groups

To display all recently applied reports under a specified group name, follow these steps:

**Step 1** Choose **Configure > Controller Config Groups**, and click a group name in the Group Name column.
**Downloading Software**

To download software to all controllers in the selected groups after you have a config group established, follow these steps:

**Step 1** Choose **Configure > Controller Config Groups**.

**Step 2** Select the check box to choose one or more config groups names on the Config Groups page.

**Step 3** Choose **Download Software** from the Select a command drop-down list, and click **Go**.

**Step 4** The Download Software to Controller page appears. The IP address of the controller to receive the bundle and the current status are displayed. Choose **local machine** from the File is Located On field.

**Step 5** Enter the maximum number of times the controller should attempt to download the signature file in the **Maximum Retries** field.

**Step 6** Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the **Timeout** field.

**Step 7** The signature files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click **Browse** to navigate to it. The controller uses this local filename as a base name and then adds _custom.sgi as a suffix.

If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On field, and the server filename is populated for you and retried.

**Step 8** Click **OK**.

**Downloading IDS Signatures**

To download Intrusion Detection System (IDS) signature files from your config group to a local TFTP server, follow these steps:

**Step 1** Choose **Configure > Controller Config Groups**.
Step 2  Select the check box to choose one or more config groups on the Config Groups page.
Step 3  Choose **Download IDS Signatures** from the Select a command drop-down list, and click **Go**.
Step 4  The Download IDS Signatures to Controller page appears. The IP address of the controller to receive the bundle and the current status are displayed. Choose **local machine** from the File is Located On field.
Step 5  Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries field.
Step 6  Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the Timeout field.
Step 7  The signature files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click **Browse** to navigate to it. The controller uses this local filename as a base name and then adds _custom.sgi as a suffix.

If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On field, and the server filename is populated for you and retried.
Step 8  Click **OK**.

---

**Downloading Customized WebAuth**

To download customized web authentication, follow these steps:

---

Step 1  Choose **Configure > Controller Config Groups**.
Step 2  Select the check box to choose one or more config groups on the Config Groups page.
Step 3  Choose **Download Customized WebAuth** from the Select a command drop-down list, and click **Go**.
Step 4  The Download Customized Web Auth Bundle to Controller page appears. The IP address of the controller to receive the bundle and the current status are displayed.
Step 5  Choose **local machine** from the File is Located On field.
Configuring Devices

This chapter describes how to configure devices in Prime Infrastructure database. It contains the following sections:

- Configuring Controllers, page 9-1
- Configuring Existing Controllers, page 9-23
- Configuring Third-Party Controllers and Access Points, page 9-168
- Configuring Access Points, page 9-171
- Configuring Switches, page 9-205
- Configuring Spectrum Experts, page 9-215
- Configuring Chokepoints, page 9-219
- Configuring Spectrum Experts, page 9-222
- Configuring Wi-Fi TDOA Receivers, page 9-223
- Configuring Scheduled Configuration Tasks, page 9-227
- Configuring Auto Provisioning for Controllers, page 9-227
- Configuring Redundancy on Controllers, page 9-228
- Configuring wIPS Profiles, page 9-228
- Configuring ACS View Servers, page 9-237
- Configuring TFTP or FTP Servers, page 9-238
- Interactive Graphs, page 9-239

Configuring Controllers

This section describes how to configure controllers in the Prime Infrastructure database. Choose **Configure > Controllers** to access the following:

- A summary of all controllers in the Prime Infrastructure database.
- The ability to add, remove, and reboot selected controllers.
- The ability to download software from the Prime Infrastructure server to selected controllers.
- The ability to save the current configuration to nonvolatile (flash) memory on selected controllers.
- The ability to view audit reports for selected controllers.
The controllers data table contains the following columns:

- **Check box**—Select the applicable controller.
- **IP Address**—Local network IP address of the controller management interface.
  - Click the title to sort the list items.
  - Click a list item to display parameters for that IP address. See the “Configuring Controllers Properties” section on page 9-24.
  - Click the icon to the right of the IP address to launch the controller web user interface in a new browser window.
- **Device Name**—Indicates the name of the controller. Click the **Controller Name** link to sort the list by controller name.
- **Device Type**—Click to sort by type. Based on the series, device types are grouped. For example:
  - WLC2100—21xx Series Wireless LAN Controllers
  - 2500—25xx Series Wireless LAN Controllers
  - 4400—44xx Series Wireless LAN Controllers
  - 5500—55xx Series Wireless LAN Controllers
  - 7500—75xx Series Wireless LAN Controllers
  - WiSM—WiSM (slot number, port number)
  - WiSM2—WiSM2 (slot number, port number)
- **Location**—Indicates the location of the controller.
- **Software Version**—The operating system release.version.dot.maintenance number of the code currently running on the controller.
- **Mobility Group Name**—Name of the mobility or WPS group.
- **Reachability Status**—Reachable or not reachable.

| Note | Reachability status is updated based on the last execution information of the Device Status background task. For updating the current status, choose Administration > Background Tasks, and choose Execute Now from the Select a command drop-down list. |

- **Audit Status**
  - Not Available—No audit occurred on this switch.
  - Identical—No configuration differences were discovered.
  - Mismatch—Configuration differences were discovered.

Click the **Audit Status** link to access the audit report. In the Audit Report page, choose Audit Now from the Select a command drop-down list to run a new audit for this controller. See the “Understanding the Controller Audit Report” section on page 9-3 for more information on audit reports.

| Note | Audit status is updated based on the last execution information of either the Configuration Sync background task or the Audit Now option located in the Controllers page. To get the current status, either choose Administration > Background Tasks and choose Execute Now or Audit Now from the Select a command drop-down list. |
Use the Search feature to search for a specific controller. See the Search Methods section in the Cisco Prime Infrastructure 2.0 User Guide for additional information.

- Understanding the Controller Audit Report, page 9-3
- Adding Controllers, page 9-4
- Bulk Update of Controller Credentials, page 9-7
- Removing Controllers from the Prime Infrastructure, page 9-8
- Rebooting Controllers, page 9-8
- Downloading Software to Controllers, page 9-9
- Downloading IDS Signatures, page 9-14
- Downloading a Customized WebAuthentication Bundle to a Controller, page 9-15
- Downloading a Vendor Device Certificate, page 9-16
- Downloading a Vendor CA Certificate, page 9-17
- Saving the Configuration to Flash, page 9-18
- Refreshing the Configuration from the Controller, page 9-18
- Discovering Templates from the Controller, page 9-19
- Updating Credentials in the Prime Infrastructure, page 9-19
- Viewing Templates Applied to a Controller, page 9-20
- Using the Audit Now Feature, page 9-21
- Viewing the Latest Network Audit Report, page 9-22

Understanding the Controller Audit Report

The Controller Audit Report displays the following information depending on the type of audit selected in Administration > Settings > Audit and on which parameters the audit is performed:

- Applied template discrepancies (Template Based Audit only)
- Config group template discrepancies (Template Based Audit only)
- Total enforcements for config groups with background audit enabled (Template Based Audit only)
  - If the total enforcement count is greater than zero, this number appears as a link. Click the link to view a list of the enforcements made from the Prime Infrastructure.
- Failed for config groups with background audit enabled (Template Based Audit only)
  - If the failed enforcement count is greater than zero, this number appears as a link. Click the link to view the failures returned from the device.
- Other Prime Infrastructure discrepancies

Note

The controller audit report indicates if the audit was performed on all parameters or on a selected set of parameters.
A current Controller Audit Report can be accessed in the Configure > Controllers page by clicking a value in the Audit Status column.

You can audit a controller by choosing Audit Now from the Select a command drop-down list in the Configure > Controllers page (See the “Using the Audit Now Feature” section on page 9-21 for more information) or by clicking Audit Now in the Controller Audit Report.

Adding Controllers

**Note** You cannot add or configure Cisco Catalyst 3850 Series Switches or Cisco 5760 Series Wireless LAN Controllers using the Classic view. To add or configure these devices, use the Lifecycle view.

After adding a device in the Converged view with profile, if you edit the device (which is associated with Credential Profile) in classic view, the Credential Profile association of the device is removed.

**Note** You do not need to specify CLI credentials for WLC devices in order for Prime Infrastructure to manage them. As long as you specify SNMP credentials, the WLC devices will be in Managed state.

You can add controllers one at a time or in batches.

To add controllers, follow these steps:

**Step 1** Choose Configure > Controllers.

**Step 2** From the Select a command drop-down list, choose Add Controllers, and click Go. The Add Controller page appears.

**Step 3** Choose one of the following:

- If you want to add one controller or use commas to separate multiple controllers, leave the Add Format Type drop-down list at Device Info.
- If you want to add multiple controllers by importing a CSV file, choose File from the Add Format Type drop-down list. The CSV file allows you to generate your own import file and add the devices you want.

**Note** When a controller is removed from the system, the associated access points are not removed automatically and therefore remain in the system. These disassociated access points must be removed manually.

**Note** If you are adding a controller into the Prime Infrastructure across a GRE link using IPsec or a lower MTU link with multiple fragments, you might need to adjust the Maximum VarBinds per Get PDU and Maximum VarBinds per Set PDU. If it is set too high, the controller might fail to be added into the Prime Infrastructure. To adjust the Maximum VarBinds per Get PDU or Maximum VarBinds per Set PDU, do the following: Stop the Prime Infrastructure, choose Administration > Settings > SNMP Settings, and edit the Maximum VarBinds per Get PDU and Maximum VarBinds per Set PDU values to 50 or lower.
Note: If you reduce the Maximum VarBinds per Get PDU or Maximum VarBinds per Set PDU value, applying the configurations to the device might fail.

Step 4 If you chose Device Info, enter the IP address of the controller you want to add. If you want to add multiple controllers, use a comma between the string of IP addresses.

Note: If a partial byte boundary is used and the IP address appears to be broadcast (without regard to the partial byte boundary), there is a limitation on adding the controllers into the Prime Infrastructure. For example, 10.0.2.255/23 cannot be added but 10.0.2.254/23 can.

If you chose File, click Browse to find the location of the CSV file you want to import.

The first row of the CSV file is used to describe the columns included. The first row of the CSV file is used to describe the columns included. The IP Address column is mandatory. The following example shows a sample CSV file.

```
ip_address,network_mask,snmp_version,snmp_community,snmpv3_user_name,snmpv3_auth_type,snmpv3_auth_password,snmpv3_privacy_type,snmpv3_privacy_password,snmp_retries,snmp_timeout,protocol,telnet_username,telnet_password,enable_password,telnet_timeout
209.165.200.225,255.255.255.224,v2,public,,,,,,3,10,telnet,cisco,cisco,cisco,60
209.165.200.226,255.255.255.224,v2,public,,,,,,3,10,,cisco,cisco,cisco,60
209.165.200.227,255.255.255.224,v2,public,,,,,,3,10,telnet,cisco,cisco,cisco,60
```

The CSV files can contain the following fields:
- ip_address
- network_mask
- snmp_version
- snmp_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout
- protocol
- telnet_username
- telnet_password
- enable_password
- telnet_timeout

Step 5 Select the Verify Telnet/SSH Credentials check box if you want this controller to verify Telnet/SSH credentials. You might want to leave this unselected (or disabled) because of the substantial time it takes for discovery of the devices.
Chapter 9      Configuring Devices

Note Enter SNMP parameters for the write access, if available. If you enter read-only access parameters, the controller is added but the Prime Infrastructure is unable to modify the configuration and the Prime Infrastructure can not be registered as a trap receiver on that Controller.

Step 6 Use the Version drop-down list to choose v1, v2, or v3.

Step 7 In the Retries text box, enter the number of times that attempts are made to discover the controller.

Step 8 Provide the client session timeout value in seconds. This determines the maximum amount of time allowed for a client before it is forced to reauthenticate.

Step 9 In the Community field, enter either public or private (for v1 and v2 only).

Note If you go back and later change the community mode, you must perform a refresh config for that controller.

Step 10 Choose None, HMAC-SHA, or HMAC-MD5 (for v3 only) for the authorization type.

Step 11 Enter the authorization password (for v3 only).

Step 12 Enter None, CBC-DES, or CFB-AES-128 (for v3 only) for the privacy type.

Step 13 Enter the privacy password (for v3 only).

Step 14 Enter the Telnet credentials information for the controller. If you chose the File option and added multiple controllers, the information applies to all specified controllers. If you added controllers from a CSV file, the username and password information is obtained from the CSV file.

Note The Telnet/SSH username must have sufficient privileges to execute commands in CLI templates.

The default username and password is admin.

Step 15 Enter the retries and timeout values. The default retries number is 3, and the default retry timeout is 1 minute.

Step 16 Click OK.

Note If you fail to add a device to the Prime Infrastructure, and if the error message ‘Sparse table not supported’ occurs, verify that the Prime Infrastructure and WLC versions are compatible and retry. For information on compatible versions, see the following URL: http://www.cisco.com/en/US/docs/wireless/controller/5500/tech_notes/Wireless_Software_Compatibility_Matrix.html.

Note When a controller is added to the Prime Infrastructure, the Prime Infrastructure acts as a TRAP receiver and the following traps are enabled on the controller: 802.11 Disassociation, 802.11 Deauthentication, and 802.11 Authenticated.
Chapter 9  Configuring Devices

Configuring Controllers

Note

To update the credentials of multiple controllers in a bulk, choose **Bulk Update Controllers** from the Select a command drop-down list. The Bulk Update Controllers page appears. You can choose a CSV file. The CSV file contains a list of controllers to be updated, one controller per line. Each line is a comma separated list of controller attributes. The first line describes the attributes included. The IP address attribute is mandatory. For details, see the *Cisco Prime Infrastructure Configuration Guide*.

Note

After adding a controller, it is placed temporarily in the Monitor > Unknown Devices page while the Prime Infrastructure attempts to communicate with the controller that you have added. Once communication with the controller has been successful, the controller moves from the Monitor > Unknown Devices page to the Monitor > Controllers page. If the Prime Infrastructure is unable to successfully communicate with a controller, it remains in the Monitor > Unknown Devices and an error condition an error message is displayed. To access the Unknown Devices page, choose Configure > Unknown Devices.

See the **Configuring Third-Party Controllers and Access Points** on page 9-168 for more information on how to add third-party controllers and AP.

**Bulk Update of Controller Credentials**

You can update multiple controllers credentials by importing a CSV file.

To update controller(s) information in bulk, follow these steps:

**Step 1**  Choose **Configure > Controllers**.

**Step 2**  Select the check box(es) of the applicable controller(s).

**Step 3**  From the Select a command drop-down list, choose **Bulk Update Controller**. The Bulk Update Controllers page appears.

**Step 4**  Enter the CSV filename in the Select CSV File text box or click **Browse** to locate the desired file.

**Step 5**  Click **Update and Sync**.

**Sample CSV File for the Bulk Update of Controller Credentials**

The first row of the CSV file is used to describe the columns included. The IP Address column is mandatory. The following example shows a sample CSV file.

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name, snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries, snmp_timeout, protocol, telnet_username, telnet_password, enable_password, telnet_timeout
209.165.200.225, 255.255.255.224, v2, public, , , , , , , , , , ,
209.165.200.226, 255.255.255.224, v2, public, , , , , , , , , , ,
209.165.200.227, 255.255.255.224, v2, public, , , , , , , , , , ,
```

The CSV files can contain the following fields:

- **ip_address**
- **network_mask**
- **snmp_version**
- **snmp_community**
- **snmpv3_user_name**
- **snmpv3_auth_type**
- **snmpv3_auth_password**
- **snmpv3_privacy_type**
- **snmpv3_privacy_password**
- **snmp_retries**
- **snmp_timeout**
- **protocol**
- **telnet_username**
- **telnet_password**
- **enable_password**
- **telnet_timeout**
Configuring Controllers

- ip_address
- network_mask
- snmp_version
- snmp_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout
- protocol
- telnet_username
- telnet_password
- enable_password
- telnet_timeout

Removing Controllers from the Prime Infrastructure

To remove a controller, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Select the check box(es) of the applicable controller(s).

**Step 3** From the Select a command drop-down list, choose **Remove Controllers**.

**Step 4** Click **Go**.

**Step 5** Click **OK** in the pop-up dialog box to confirm the deletion.

**Note**
When a controller is removed from the system, the associated access points are not removed automatically and, therefore, remain in the system. These disassociated access points must be removed manually.

Rebooting Controllers

To reboot a controller, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Select the check box(es) of the applicable controller(s).
Step 3  From the Select a command drop-down list, choose **Reboot Controllers**.

Step 4  Click **Go**. The Reboot Controllers page appears.

| Note | Save the current controller configuration prior to rebooting. |

Step 5  Select the Reboot Controller options that must be applied.

- **Save Config to Flash**—Data is saved to the controller in non-volatile RAM (NVRAM) and is preserved in the event of a power cycle. If the controller is rebooted, all applied changes are lost unless the configuration has been saved.
- **Reboot APs**—Select the check box to enable a reboot of the access point after making any other updates.
- **Swap AP Image**—Indicates whether or not to reboot controllers and APs by swapping AP images. This could be either Yes or No.

| Note | Options are disabled unless the Reboot APs check box is selected. |

Step 6  Click **OK** to reboot the controller with the optional configuration selected.

### Downloading Software to Controllers

Both File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) are supported for uploading and downloading files to and from the Prime Infrastructure. In previous software releases, only TFTP was supported.

- [Downloading Software (FTP), page 9-9](#)
- [Downloading Software (TFTP), page 9-11](#)
- [Configuring IPaddr Upload Configuration/Logs from the Controller, page 9-13](#)

### Downloading Software (FTP)

To download software to a controller, follow these steps:

Step 1  Choose **Configure > Controllers**.

Step 2  Select the check box(es) of the applicable controller(s).

Step 3  From the Select a command drop-down list, choose **Download Software (FTP)**.

Step 4  Click **Go**.

| Note | Software can also be downloaded by choosing **Configure > Controllers > IPaddr > System > Commands > Upload/Download Commands > Download Software**. |

The IP address of the controller and its current status appears in the Download Software to Controller page.
Step 5  
Select the download type.

**Note**  
The pre-download option is displayed only when all selected controllers are using the Release 7.0.x.x or later.

- **Now**—Executes the download software operation immediately. If you select this option, proceed with Step 7.

**Note**  
After the download is successful, reboot the controllers to enable the new software.

- **Scheduled**—Specify the scheduled download options.
  - **Schedule download to controller**—Select this check box to schedule download software to controller.
  - **Pre-download software to APs**—Select this check box to schedule the pre-download software to APs. The APs download the image and then reboot when the controller reboots.

**Note**  
To see Image Predownload status per AP, enable the task in the Administration > Background Task > AP Image Predownload Task page, and run an AP Image Predownload report from the Report Launch Pad.

Step 6  
If you selected the Scheduled option under Download type, enter the schedule details.

- **Task Name**—Enter a Scheduled Task Name to identify this scheduled software download task.
- **Reboot Type**—Indicates whether the reboot type is manual, automatic, or scheduled.

**Note**  
Reboot Type Automatic can be set when the only Download software to controller option is selected.

- **Download date/time**—Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date. Choose the time from the hours and minutes drop-down lists.
- **Reboot date/time**—This option appears only if you select the reboot type as “Scheduled”. Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date to reboot the controller. Choose the time from the hours and minutes drop-down lists.

**Note**  
Schedule enough time (at least 30mins) between Download and Reboot so that all APs can complete the software pre-download.

**Note**  
If any one of the AP is in pre-download progress state at the time of scheduled reboot, the controller will not reboot. In such a case, wait for the pre-download to finish for all the APs and reboot the controller manually.

- **Notification (Optional)**—Enter the e-mail address of recipient to send notifications via e-mail.
Note To receive e-mail notifications, configure the Prime Infrastructure mail server in the Administration > Settings > Mail Server Configuration page.

**Step 7** Enter the FTP credentials including username, password, and port.

Note You cannot use special characters such as $, ' \, %, &, (, ), ;, ”, <, >, , ?, and | as part of the FTP password. The special characters such as @, #, ^, *, ~, _, -, +, =, {, }, :, ., and / are allowed in password. The special character "!" (exclamation mark) works when the password policy is disabled.

**Step 8** In the File is located on option, select either the **Local machine** or **FTP Server** radio button.

Note If you choose FTP Server, choose **Default Server** or **New** from the Server Name drop-down list.

Note The software files are uploaded to the FTP directory specified during the install.

**Step 9** Specify the local filename or click **Browse** to navigate to the appropriate file.

Note If you chose FTP Server previously, specify the server filename.

**Step 10** Click **Download**.

Note If the transfer times out for some reason, you can choose the FTP server option in the File is located on field; the server filename is populated and retried.

### Downloading Software (TFTP)

To download software to a controller, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Select the check box(es) of the applicable controller(s).

**Step 3** In the Select a command drop-down list, choose **Download Software (TFTP)**.

**Step 4** Click **Go**.

Note Software can also be downloaded from Configure > Controllers > IPaddr > System > Commands > Upload/Download Commands > Download Software.

The IP address of the controller and its current status are displayed in the Download Software to Controller page.
Step 5  Select the download type.

The pre-download option is displayed only when all selected controllers are using the Release 7.0.x.x or later.

- Now—Executes the download software operation immediately. If you select this option, proceed with Step 7.

After the download is successful, reboot the controllers to enable the new software.

- Scheduled—Specify the scheduled download options.
  - Download software to controller—Select this option to schedule download software to controller.
  - Pre-download software to APs—Select this option to schedule the pre-download software to APs. The APs download the image and then reboot when the controller reboots.

To see Image Predownload status per AP, enable the task in the Administration > Background Task > AP Image Predownload Task page, and run an AP Image Predownload report from the Report Launch Pad.

Step 6  If you selected the Scheduled option under Download type, enter the schedule detail.

- Task Name—Enter a scheduled task name to identify this scheduled software download task.

- Reboot Type—Indicates whether the reboot type is manual, automatic, or scheduled.

Reboot Type Automatic can be set when only Download software to controller option is selected.

- Download date/time—Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date. Choose the time from the hours and minutes drop-down lists.

- Reboot date/time—This option appears only if you select the reboot type as “Scheduled”. Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date to reboot the controller. Choose the time from the hours and minutes drop-down lists.

Schedule enough time (at least 30 minutes) between Download and Reboot so that all APs can complete the software pre-download.

If any one of the APs is in pre-download progress state at the time of scheduled reboot, the controller does not reboot. In such a case, wait for the pre-download to finish for all the APs and reboot the controller manually.

- Notification (Optional)—Enter the e-mail address of recipient to send notifications via e-mail.
Configuring Devices

Configuring Controllers

To receive e-mail notifications, configure the Prime Infrastructure mail server in the Administration > Settings > Mail Server Configuration page.

Step 7  From the File is located on field, choose Local machine or TFTP server.

Note  If you choose TFTP server, choose the Default Server or add a New server using the Server Name drop-down list.

Step 8  From the Maximum Retries field, enter the maximum number of tries the controller should attempt to download the software.

Step 9  In the Timeout field, enter the maximum amount of time (in seconds) before the controller times out while attempting to download the software.

Note  The software files are uploaded to the TFTP directory specified during the install.

Step 10  Specify the local filename or click Browse to navigate to the appropriate file.

Note  If you selected TFTP server previously, specify the server filename.

Step 11  Click Download.

Tip  If the transfer times out for some reason, you can choose the TFTP server option in the File is located on field; the server filename is populated and retried.

Configuring IPaddr Upload Configuration/Logs from the Controller

To upload files from the controller, follow these steps:

Step 1  Choose Configure > Controllers.

Step 2  Click an IP address in the IP address column.

Step 3  From the left sidebar menu, choose System > Commands.

Step 4  Select the FTP or TFTP radio button.

Note  Both File Transfer Protocol (FTP) and Trivial Transfer Protocol (TFTP) are supported for uploading and downloading files to and from the Prime Infrastructure. In previous software releases, only TFTP was supported.

Step 5  From the Upload/Download Commands drop-down list, choose Upload File from Controller.

Step 6  Click Go to access this page.
• FTP Credentials Information—Enter the FTP username, password, and port if you selected the FTP radio button previously.

• TFTP or FTP Server Information:
  – Server Name—From the drop-down list, choose Default Server or New.
  – IP Address—IP address of the controller. This is automatically populated if the default server is selected.
  – File Type—Select from configuration, event log, message log, trap log, crash file, signature files, or PAC.
  – Enter the Upload to File from /(root)/Prime Infrastructure-tftp/ or /(root)/Prime Infrastructure-ftp/ filename.
  – Select whether or not Prime Infrastructure saves the information before backing up the configuration.

**Note**
Prime Infrastructure uses an integral TFTP and FTP server. This means that third-party TFTP and FTP servers cannot run on the same workstation as the Prime Infrastructure, because the Prime Infrastructure and the third-party servers use the same communication port.

**Step 7**
Click OK. The selected file is uploaded to your TFTP or FTP server and named what you entered in the File Name text box.

---

### Downloading IDS Signatures

To download Intrusion Detection System (IDS) signature files to a controller, follow these steps:

**Step 1**
Choose Configure > Controllers.

**Step 2**
Select the check box(es) of the applicable controller(s).

**Step 3**
From the Select a command drop-down list, choose Download IDS Signatures.

**Step 4**
Click Go.

**Note**
IDS signature files can also be downloaded from Configure > Controllers > IPaddr > System > Commands > Upload/Download Commands > Download IDS Signatures.

In the Download IDS Signatures to Controller page, the controller IP address and its current status appears.

**Step 5**
Copy the signature file (*.sig) to the default directory on your TFTP server.

**Step 6**
In the File is located on option, select the Local machine radio button.

**Note**
If you know the filename and path relative to the server root directory, you can also select the TFTP server radio button.

**Step 7**
In the Maximum Retries text box, enter the maximum number of tries the controller should attempt to download the signature file.
Chapter 9 Configuring Devices

Configuring Controllers

Step 8 In the Timeout text box, enter the maximum amount of time (in seconds) before the controller times out while attempting to download the signature file.

Note The signature files are uploaded to the c:\tftp directory.

Step 9 Specify the local filename or click Browse to navigate to the appropriate file. The controller uses this local filename as a base name and adds _custom.sgi as a suffix.

Note If you chose TFTP server previously, specify the server filename.

Step 10 Click Download.

Tip If the transfer times out for some reason, you can choose the TFTP server option in the File is located on field; the server filename is populated and retried.

Note The local machine option initiates a two-step operation. First, the local file is copied from the administrator workstation to the Prime Infrastructure own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in the Prime Infrastructure server TFTP directory, and the downloaded web page now automatically populates the filename.

Downloading a Customized WebAuthentication Bundle to a Controller

To download customized web authentication bundle to a controller, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Select the check box(es) of the applicable controller(s).
Step 3 From the Select a command drop-down list, choose Download Customized WebAuth.
Step 4 Click Go.

A customized web authentication bundle can also be downloaded from Configure > Controllers > IPaddr > System > Commands > Upload/Download Commands > Download Customized Web Auth.

In the Download Customized WebAuth bundle to Controller page, the controller IP address and its current status appears.

Step 5 Select the Local machine radio button in the File is located on field.

Note If you know the filename and path relative to the server root directory, you can also select the TFTP server radio button.
Note For a local machine download, either .zip or .tar file options exists but the Prime Infrastructure does the conversion of .zip to .tar automatically. If you choose a TFTP server download, only .tar files are specified.

Step 6 In the Maximum Retries text box, enter the maximum number of tries the controller should attempt to download the file.

Step 7 In the Timeout text box, enter the maximum amount of time (in seconds) before the controller times out while attempting to download the file.

Note Prime Infrastructure Server Files In field specifies where the Prime Infrastructure server files are located.

Step 8 Specify the local filename or click Browse to navigate to the appropriate file. The controller uses this local filename as a base name and adds _custom.sgi as a suffix.

Step 9 Click Download.

Tip If the transfer times out for some reason, you can select the TFTP server radio button in the File is located on field; the server filename is populated and retried.

Step 10 The local machine option initiates a two-step operation. First, the local file is copied from the administrator workstation to the Prime Infrastructure own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in the Prime Infrastructure server TFTP directory, and the downloaded web page now automatically populates the filename.

Step 11 After completing the download, you are directed to a new page and are able to authenticate.

**Downloading a Vendor Device Certificate**

Each wireless device (controller, access point, and client) has its own device certificate. If you want to use your own vendor-specific device certificate, it must be downloaded to the controller.

To download a vendor device certificate to a controller, follow these steps:

Step 1 Choose Configure > Controllers.

Step 2 You can download the certificate in one of two ways:

a. Select the check box(es) of the applicable controller(s).

b. From the Select a command drop-down list, choose Download Vendor Device Certificate.

c. Click Go.

-or-

a. Click the IP address of the desired controller.

b. Choose System > Commands from the left sidebar menu.

c. From the Upload/Download Commands drop-down list, choose Download Vendor Device Certificate.
d. Click Go.

**Step 3**
In the Certificate Password text box, enter the password used to protect the certificate.

**Step 4**
Reenter the password in the Confirm Password text box.

**Step 5**
In the File is located on field, select the Local machine or TFTP server radio button.

---

**Note**
If the certificate is located on the TFTP server, enter the server filename. If it is located on the local machine, enter the local filename by clicking Browse.

**Step 6**
Enter the TFTP server name in the Server Name field. The default is the Prime Infrastructure server.

**Step 7**
Enter the server IP address.

**Step 8**
In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.

**Step 9**
In the Timeout text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

**Step 10**
In the Local File Name text box, enter the directory path of the certificate.

**Step 11**
In the Server File Name text box, enter the name of the certificate.

**Step 12**
Click Download.

---

**Downloading a Vendor CA Certificate**

Controllers and access points have a certificate authority (CA) certificate that is used to sign and validate device certificates. The controller is shipped with a Cisco-installed CA certificate. This certificate might be used by EAP-TLS and EAP-FAST (when not using PACs) to authenticate wireless clients during local EAP authentication. However, if you want to use your own vendor-specific CA certificate, it must be downloaded to the controller.

To download a vendor CA certificate to the controller, follow these steps:

**Step 1**
Choose Configure > Controllers.

**Step 2**
You can download the certificate in one of two ways:

a. Select the check box(es) of the applicable controller(s).

b. From the Select a command drop-down list, choose Download Vendor CA Certificate.

c. Click Go.

- or -

da. Click the IP address of the desired controller.

b. Choose System > Commands from the left sidebar menu.

c. From the Upload/Download Commands drop-down list, choose Download Vendor CA Certificate.

d. Click Go.

**Step 3**
In the File is located on field, Select the Local machine or TFTP server radio button.
Note If the certificate is located on the TFTP server, enter the server file name. If it is located on the local machine, enter the local filename by clicking Browse.

Step 4 Enter the TFTP server name in the Server Name text box. The default is the Prime Infrastructure server.
Step 5 Enter the server IP address.
Step 6 In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.
Step 7 In the Timeout text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.
Step 8 In the Local File Name text box, enter the directory path of the certificate.
Step 9 In the Server File Name text box, enter the name of the certificate.
Step 10 Click OK.

Saving the Configuration to Flash

To save the configuration to flash memory, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Select the check box(es) for the applicable controller(s).
Step 3 From the Select a command drop-down list, choose Save Config to Flash.
Step 4 Click Go.

Refreshing the Configuration from the Controller

The Refresh Config from Controller command will not work when there is a custom rogue AP rule specified on the controller.

To refresh the configuration from the controller, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Select the check box(es) for the applicable controller(s).
Step 3 From the Select a command drop-down list, choose Refresh Config from Controller.
Step 4 Click Go.
Step 5 At the Configuration Change prompt, select the Retain or Delete radio button.
Step 6 Click Go.
Discovering Templates from the Controller

Prior to software Release 5.1, templates were detected when a controller was detected, and every configuration found on the Prime Infrastructure for a controller had an associated template. Now templates are not automatically detected with controller discovery, and you can specify which Prime Infrastructure configurations you want to have associated templates.

Note
The templates that are discovered do not retrieve management or local user passwords.

The following rules apply for template discovery:

- Template Discovery discovers templates that are not found in the Prime Infrastructure.
- Existing templates are not discovered.
- Template Discovery does not retrieve dynamic interface configurations for a controller. You must create a new template to apply the dynamic interface configurations on a controller.

To discover current templates, follow these steps:

Step 1  Choose Configure > Controllers.

Step 2  Select the check box of the controller for which you want to discover templates.

Step 3  From the Select a command drop-down list, choose Discover Templates from Controller.

Step 4  Click Go. The Discover Templates page displays the number of discovered templates, each template type and each template name.

Note
You can select the Enabling this option will create association between discovered templates and the device listed above check box so that discovered templates are associated to the configuration on the device and are shown as applied on that controller.

Note
Template discovery refreshes configuration from the controller prior to discovering templates. Click OK in the warning dialog box to continue with the discovery.

Note
For the TACACS+ Server templates, the configuration on the controller with same server IP address and port number but different server types are aggregated into one single template with the corresponding Server Types set on the Discovered Template. For the TACACS+ Server templates, the Admin Status on the discovered template reflects the value of Admin Status on the first configuration from the controller with same Server IP address and port number.

Updating Credentials in the Prime Infrastructure

To update SNMP/Telnet credential details in the Prime Infrastructure for multiple controllers, there is no configuration available. To perform this mass update, you need to go to each device and update the SNMP and Telnet credentials.
To update the SNMP/Telnet credentials, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Select the check box for each controller to which you want to update SNMP/Telnet credentials.

**Step 3** From the Select a command drop-down list, choose **Update Credentials in Prime Infrastructure**. The Update Credentials in the Prime Infrastructure page appears.

**Step 4** Select the **SNMP Parameters** check box and configure the following parameters:

- **Note**: SNMP write access parameters are needed for modifying controller configuration. With read-only access parameters, configuration can only be displayed.

- Version—Choose from v1, v2, or v3.
- Retries—Indicates the number of controller discovery attempts.
- Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The valid range is 2 to 90 seconds. The default is 2 seconds.
- Community—Public or Private.
- Verify SNMP Credentials—Select this check box to verify SNMP credentials.

**Step 5** Select the **Telnet/SSH Parameters** check box and configure the following parameters:

- User Name—Enter the username.
- Password/Confirm Password—Enter and confirm the password.
- Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The valid range is 2 to 90 seconds. The default is 60 seconds.

---

**Viewing Templates Applied to a Controller**

You can view all templates currently applied to a specific controller.

**Note**: Only templates applied in this partition are displayed.

To view applied templates, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Select the check box for the applicable controller.

**Step 3** From the Select a command drop-down list, choose **Templates Applied to a Controller**.

**Step 4** Click **Go**. The Templates Applied to a Controller page displays each applied template name, template type, the date the template was last saved, and the date the template was last applied.
Using the Audit Now Feature

You can audit a controller by choosing **Audit Now** from the Select a command drop-down list in the Configure > Controllers page or by choosing **Audit Now** directly from the Select a command drop-down list.

| Note | A current Controller Audit Report can be accessed in the Configure > Controllers page by clicking a value in the Audit Status column. |

To audit a controller, follow these steps:

1. **Step 1** Choose **Configure > Controllers**.
2. **Step 2** Select the check box for the applicable controller.
3. **Step 3** From the Select a command drop-down list, choose **Audit Now**.
4. **Step 4** Click **Go**.
5. **Step 5** Click **OK** in the pop-up dialog box if you want to remove the template associations from configuration objects in the database as well as template associations for this controller from associated config groups (Template based audit only).

The Audit Report displays:

- Device Name
- Time of Audit
- Audit Status
- Applied and Config Group Template Discrepancies information including the following:
  - Template type (template name)
  - Template application method
  - Audit status (For example, mismatch, identical)
  - Template attribute
  - Value in Prime Infrastructure
  - Value in Controller
- Other Prime Infrastructure Discrepancies including the following:
  - Configuration type (name)
  - Audit Status (For example, mismatch, identical)
  - Attribute
  - Value in Prime Infrastructure
- Value in Controller

- Total enforcements for config groups with background audit enabled—If discrepancies are found during the audit in regards to the config groups enabled for background audit and if the enforcement is enabled, this section lists the enforcements made during the controller audit.

- Failed Enforcements for Config Groups with background audit enabled—Click the link to view a list of failure details (including the reason for the failure) returned by the device.

- Restore Prime Infrastructure Values to Controller or Refresh Config from Controller—If there are config differences found as a result of the audit, you can either click **Restore Prime Infrastructure Values to controller** or **Refresh Config from controller** to bring the Prime Infrastructure configuration in sync with the controller.
  
  - Choose **Restore Prime Infrastructure Values to Controller** to push the discrepancies to the device.
  
  - Choose **Refresh config from controller** to pick up the device for this configuration from the device.

---

**Note**

Templates are not refreshed as a result of clicking **Refresh Config from Controller**.

---

### Viewing the Latest Network Audit Report

The Network Audit Report shows the time of the audit, the IP address of the selected controller, and the synchronization status.

---

**Note**

This method shows the report from the network audit task and not an on-demand audit per controller.

To view the latest network audit report for the selected controllers, follow these steps:

---

**Step 1** Choose **Configure > Controllers**.

**Step 2** Select the check box for the applicable controller.

**Step 3** From the Select a command drop-down list, choose **View Latest Network Configuration Audit Report**.

**Step 4** Click **Go**.

The Audit Summary displays the time of the audit, the IP address of the selected controller, and the audit status. The Audit Details display the config differences, if applicable.

---

**Note**

Use the General and Schedule tabs to revise Audit Report parameters.

---

### Command Buttons

- **Save**—Click to save changes made to the current parameters.
- Save and Run—Click to save the changes to the current parameters and run the report.
- Run Now—Click to run the audit report based on existing parameters.
- Export Now—Click to export the report results. The supported export formats is PDF and CSV.
- Cancel—Click to cancel any changes made to the existing parameters.

**Note**
From the All Controllers page, click the Audit Status column value to view the latest audit details page for the selected controller. This method has similar information as the Network Audit report on the Reports menu, but this report is interactive and per controller.

**Note**
To run an on-demand audit report, choose which controller you want to run the report on and choose Audit Now from the Select a command drop-down list. If you run an on-demand audit report and configuration differences are detected, you are given the option to retain the existing controller or Prime Infrastructure values.

### Configuring Existing Controllers

- Replacing an Old Controller Model with a New Model, page 9-24
- Configuring Controllers Properties, page 9-24
- Configuring Controller System Parameters, page 9-25
- Configuring Controller WLANs, page 9-64
- Configuring FlexConnect Parameters, page 9-86
- Configuring Security Parameters, page 9-90
- Configuring Cisco Access Points, page 9-118
- Configuring 802.11 Parameters, page 9-120
- Configuring 802.11a/n Parameters, page 9-127
- Configuring 802.11b/g/n Parameters, page 9-139
- Configuring Mesh Parameters, page 9-149
- Configuring Port Parameters, page 9-152
- Configuring Controllers Management Parameters, page 9-152
- Configuring Location Configurations, page 9-159
- Configuring IPv6, page 9-161
- Configuring Proxy Mobile IPv6, page 9-163
- Configuring mDNS, page 9-165
- Configuring AVC Profiles, page 9-166
- Configuring NetFlow, page 9-167
Replacing an Old Controller Model with a New Model

When you want to replace an old controller model with a new one without changing the IP address, do the following:

- First delete the old controller from Prime Infrastructure and wait for the confirmation popup that the deletion is complete.
- Replace the controller with the new model in the setup with same IP.
- Re-add the IP address to the Prime Infrastructure.

Configuring Controllers Properties

To configure the properties for current controllers, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Configure &gt; Controllers</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the IP address of the applicable controller.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the left sidebar menu, choose <strong>Properties &gt; Settings</strong>. The following parameters appear:</td>
</tr>
</tbody>
</table>

- **General Parameters:**
  - Name—Name assigned to the controller.
  - Type—Controller type.
  - Restore on Cold Start Trap—Select to enable a restore on a cold start trap.
  - Auto Refresh on Save Config Trap—Select to enable an automatic refresh on a Save Config trap.
  - Trap Destination Port—Read-only.
  - Software Version—Read-only.
  - Location—Location of the controller.
  - Contact—The contact person for this controller.
  - Most Recent Backup—The date and time of the most recent backup.
  - Save Before Backup—Select to enable a save before backup.

- **SNMP Parameters:**
  - Note: SNMP write access parameters are needed for modifying controller configuration. With read-only access parameters, configuration can only be displayed.
  - Version—Choose from v1, v2, or v3.
  - Retries—Indicates the number of controller discovery attempts.
  - Timeout (seconds)—Client Session timeout. Sets the maximum amount of time allowed a client before it is forced to reauthenticate.
  - Community—Public or Private.
  - Access Mode—Read Write
Note Community settings only apply to v1 and v2.

- User Name—Enter a username.
- Auth. Type—Choose an authentication type from the drop-down list or choose None.
- Auth. Password—Enter an authentication password.
- Privacy Type—Choose a privacy type from the drop-down list or choose None.
- Privacy Password—Enter a privacy password.

Note User Name, Auth. Type, Auth. Password, Privacy Type, and Privacy Password only display for v3.

- Telnet/SSH Parameters:
  - User Name—Enter the username. (Default username is admin.)

Note The Telnet/SSH username must have sufficient privileges to execute commands in CLI templates.

  - Password/Confirm Password—Enter and confirm the password. (Default password is admin.)
  - Retries—Indicate the number of allowed retry attempts. The default is three.
  - Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The default is 60 seconds.

Note Default values are used if the Telnet/SSH parameters are left blank.

**Step 4** If you made changes to this controller properties, click **Save** to confirm the changes, **Reset** to return to the previous or default settings, or **Cancel** to return to the Configure > Controllers page without making any changes to these settings.

**Configuring Controller System Parameters**

This section describes how to configure the controller system parameters and contains the following topics:

- Managing General System Properties for Controllers, page 9-26
- Configuring Controller System Commands, page 9-32
- Configuring Controller System Interfaces, page 9-39
- Configuring Controller System Interface Groups, page 9-42
- Configuring Controller Network Routes, page 9-49
- Configuring Controller Spanning Tree Protocol Parameters, page 9-50
- Configuring Controller Mobility Groups, page 9-51
Managing General System Properties for Controllers

To view the general system parameters for a current controller, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click the IP address of the applicable controller.

**Step 3** From the left sidebar menu, choose **System > General**. The following parameters appear:

- **802.3x Flow Control Mode**—Disable or enable. See the “802.3x Flow Control” section on page 9-30 for more information.

- **802.3 Bridging**—Disable or enable. See the “Configuring 802.3 Bridging” section on page 9-30 for more information.

- **Web Radius Authentication**—Choose PAP, CHAP, or MD5-CHAP.
  - **PAP**—Password Authentication Protocol. Authentication method where user information (username and password) is transmitted in clear text.
  - **CHAP**—Challenge Handshake Authentication Protocol. Authentication method where user information is encrypted for transmission.
  - **MD5-CHAP**—Message Digest 5 Challenge Handshake Authentication Protocol. With MD5, passwords are hashed using the Message Digest 5 algorithm.

- **AP Primary Discovery Timeout**—Enter a value between 30 and 3600 seconds.

The access point maintains a list of backup controllers and periodically sends primary discovery requests to each entry in the list. When configured, the primary discovery request timer specifies the amount of time that a controller has to respond to the discovery request of the access point before the access point assumes that the controller cannot be joined and waits for a discovery response from the next controller in the list.

- **CAPWAP Transport Mode**—Layer 3 or Layer 2. See the “Lightweight Access Point Protocol Transport Mode” section on page 9-30 for more information.

- **Current LWAPP Operating Mode**—Automatically populated.

- **Broadcast Forwarding**—Disable or enable.

- **LAG Mode**—Choose **Disable** if you want to disable LAG.
Link aggregation (LAG) is a partial implementation of the 802.3ad port aggregation standard. It bundles all of the controller distribution system ports into a single 802.3ad port channel, thereby reducing the number of IP addresses needed to configure the ports on your controller. When LAG is enabled, the system dynamically manages port redundancy and load balances access points transparently to the user.

**Note** LAG is disabled by default on the Cisco 5500 and 4400 series controllers but enabled by default on the Cisco WiSM and the controller in the Catalyst 3750G Integrated Wireless LAN Controller Switch.

See the “Link Aggregation” section on page 9-31 for more information.

- Ethernet Multicast Support
  - Disable—Select to disable multicast support on the controller.
  - Unicast—Select if the controller, upon receiving a multicast packet, forwards the packets to all the associated access points.

  **Note** FlexConnect supports only unicast mode.

  - Multicast—Select to enable multicast support on the controller.

- Aggressive Load Balancing—Disable or enable. See the “Aggressive Load Balancing” section on page 9-31 for more information on load balancing.

- Peer to Peer Blocking Mode
  - Disable—Same-subnet clients communicate through the controller.
  - Enable—Same-subnet clients communicate through a higher-level router.

- Over Air Provision AP Mode—Disable or enable.

Over-the-air provisioning (OTAP) is supported by Cisco 5500 and 4400 series controllers. If this feature is enabled on the controller, all associated access points transmit wireless CAPWAP or LWAPP neighbor messages, and new access points receive the controller IP address from these messages. This feature is disabled by default and should remain disabled when all access points are installed.

**Note** Disabling OTAP on the controller does not disable it on the access point. OTAP cannot be disabled on the access point.

**Note** You can find additional information about OTAP at the following URL:

- AP Fallback—Disable or enable.

  **Note** Enabling AP Fallback causes an access point which lost a primary controller connection to automatically return to service when the primary controller returns.
• AP Failover Priority—Disable or enable.

  **Note** To configure failover priority settings for access points, you must first enable the AP Failover Priority feature. See the “AP Failover Priority” section on page 9-29 for more information.

• AppleTalk Bridging—Disable or enable.

• Fast SSID change—Disable or enable.

  When fast SSID changing is enabled, the controller allows clients to move between SSIDs. When the client sends a new association for a different SSID, the client entry in the controller connection table is cleared before the client is added to the new SSID. When fast SSID changing is disabled, the controller enforces a delay before clients are allowed to move to a new SSID.

  **Note** If enabled, the client connects instantly to the controller between SSIDs without having appreciable loss of connectivity.

• Master Controller Mode—Disable or enable.

  **Note** Because the master controller is normally not used in a deployed network, the master controller setting is automatically disabled upon reboot or OS code upgrade.

• Wireless Management—Disable or enable. See the “Wireless Management” section on page 9-32 for more information.

• Symmetric Tunneling Mode

• ACL Counters—Disable or enable. The number of hits are displayed in the ACL Rule page. See the “Configuring Access Control Lists” section on page 9-105 or the “Configuring IPaddr > Access Control List > listname Rules” section on page 9-105 for more information.

• Multicast Mobility Mode—Disable or enable. See the “Setting the Mobility Scalability Parameters” section on page 9-53 for more information.

• Default Mobility Domain Name—Enter domain name.

• Mobility Anchor Group Keep Alive Interval—Enter the amount of delay time allowed between tries for a client attempting to join another access point. See the “Mobility Anchor Group Keep Alive Interval” section on page 9-32 for more information.

  **Tip** When you hover your mouse cursor over the parameter text box, the valid range for that field appears.

• Mobility Anchor Group Keep Alive Retries—Enter number of allowable retries.

  **Tip** When you hover your mouse cursor over the parameter text box, the valid range for that field appears.

• RF Network Name—Enter network name.

• User Idle Timeout (seconds)—Enter timeout in seconds.
AP Failover Priority

When a controller fails, the backup controller configured for the access point suddenly receives a number of Discovery and Join requests. If the controller becomes overloaded, it might reject some of the access points.

By assigning failover priority to an access point, you have some control over which access points are rejected. When the backup controller is overloaded, join requests of access points configured with a higher priority levels take precedence over lower-priority access points.

To configure failover priority settings for access points, you must first enable the AP Failover Priority feature.

To enable the AP Failover Priority feature, follow these steps:

Step 1  Choose Configure > Controllers.
Step 2  Click the IP address of the applicable controller.
Step 3  From the left sidebar menu, choose System > General.
Step 4  From the AP Failover Priority drop-down list, choose Enabled.

To configure an access point failover priority, follow these steps:

Step 1  Choose Configure > Access Points > AP Name.
Step 2  From the AP Failover Priority drop-down list, choose the applicable priority (Low, Medium, High, Critical).

Note  The default priority is Low.
Configuring 802.3 Bridging

The controller supports 802.3 frames and applications that use them, such as those typically used for cash registers and cash register servers. However, to make these applications work with the controller, the 802.3 frames must be bridged on the controller.

Support for raw 802.3 frames allows the controller to bridge non-IP frames for applications not running over IP. Only this raw 802.3 frame format is currently supported.

To configure 802.3 bridging using the Prime Infrastructure release 4.1 or later, follow these steps:

- **Step 1** Choose **Configure > Controllers**.
- **Step 2** Click the IP address of the applicable controller.
- **Step 3** Choose **System > General** to access the General page.
- **Step 4** From the 802.3 Bridging drop-down list, choose **Enable** to enable 802.3 bridging on your controller or **Disable** to disable this feature. The default value is Disable.
- **Step 5** Click **Save** to confirm your changes.

802.3x Flow Control

Flow control is a technique for ensuring that a transmitting entity, such as a modem, does not overwhelm a receiving entity with data. When the buffers on the receiving device are full, a message is sent to the sending device to suspend the transmission until the data in the buffers has been processed.

By default, flow control is disabled. You can only enable a Cisco switch to receive PAUSE frames but not to send them.

Lightweight Access Point Protocol Transport Mode

Lightweight Access Point Protocol transport mode indicates the communications layer between controllers and access points. Selections are Layer 2 or Layer 3.

To convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 lightweight access point transport mode using the Prime Infrastructure user interface, follow these steps:

- **Note** Cisco IOS-based lightweight access points do not support Layer 2 lightweight access point mode. These access points can only be run with Layer 3.

- **Note** This procedure causes your access points to go offline until the controller reboots and the associated access points reassociate to the controller.

- **Step 1** Make sure that all controllers and access points are on the same subnet.

- **Note** You must configure the controllers and associated access points to operate in Layer 2 mode before completing the conversion.
Step 2 Log into the Prime Infrastructure user interface. Then follow these steps to change the lightweight access point transport mode from Layer 3 to Layer 2:

a. Choose **Configure > Controllers**.
b. Click the IP address of the applicable controller.
c. Choose **System > General** to access the General page.
d. Change lightweight access point transport mode to Layer2 and click **Save**.
e. If the Prime Infrastructure displays the following message, click **OK**:

Please reboot the system for the CAPWAP Mode change to take effect.

Step 3 To restart the Prime Infrastructure, follow these steps:

a. Choose **System > Commands**.
b. From the Administrative Commands drop-down list, choose **Save Config To Flash**, and click **Go** to save the changed configuration to the controller.
c. Click **OK** to continue.
d. From the Administrative Commands drop-down list, choose **Reboot**, and click **Go** to reboot the controller.
e. Click **OK** to confirm the save and reboot.

Step 4 After the controller reboots, follow these steps to verify that the CAPWAP transport mode is now Layer 2:

a. Choose **Configure > Controllers**.
b. Click the IP address of the applicable controller.
c. Verify that the current CAPWAP transport mode is Layer2 from the general drop-down list.

You have completed the CAPWAP transport mode conversion from Layer 3 to Layer 2. The operating system software now controls all communications between controllers and access points on the same subnet.

---

**Aggressive Load Balancing**

Aggressive load balancing actively balances the load between the mobile clients and their associated access points.

**Link Aggregation**

Link aggregation allows you to reduce the number of IP addresses needed to configure the ports on your controller by grouping all the physical ports and creating a link aggregation group (LAG). In a 4402 model, two ports are combined to form a LAG whereas in a 4404 model, all four ports are combined to form a LAG.

If LAG is enabled on a controller, the following configuration changes occur:

- Any dynamic interfaces that you have created are deleted. This is done to prevent configuration inconsistencies in the interface database.
• Interfaces cannot be created with the “Dynamic AP Manager” flag set.

Note You cannot create more than one LAG on a controller.

The advantages of creating a LAG include the following:
• Assurance that, if one of the links goes down, the traffic is moved to the other links in the LAG. As long as one of the physical ports is working, the system remains functional.
• No need to configure separate backup ports for each interface.
• Multiple AP-manager interfaces are not required because only one logical port is visible to the application.

Note When you make changes to the LAG configuration, the controller has to be rebooted for the changes to take effect.

When you hover your mouse cursor over the parameter text box, the valid range for that field appears.

Wireless Management

Because of IPsec operation, management via wireless is only available to operators logging in across WPA, Static WEP, or VPN Pass Through WLANs. Wireless management is not available to clients attempting to log in via an IPsec WLAN.

Mobility Anchor Group Keep Alive Interval

Indicate the delay between tries for clients attempting to join another access point. This decreases the time it takes for a client to join another access point following a controller failure because the failure is quickly identified, the clients are moved away from the problem controller, and the clients are anchored to another controller.

When you hover your mouse cursor over the parameter text box, the valid range for that field appears.

Configuring Controller System Commands

To view the System Command parameters for current controllers, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click the IP address of the applicable controller.
Step 3 From the left sidebar menu, choose System > Commands. The following parameters appear:
  • Administrative
    – Reboot—This command enables you to confirm the restart of your controller after saving your configuration changes. Open and confirm a new session and log into the controller to avoid loosing a system connection.
- Save Config to Flash—Data is saved to the controller in non-volatile RAM (NVRAM) and is preserved in the event of a power cycle. If the controller is rebooted, all applied changes are lost unless the configuration has been saved.

- Reset to Factory Default—Choose this command to return the controller to its original settings. See the “Restoring Factory Defaults” section on page 9-34 for more information.

- Ping From Controller—Send a ping to a network element. This pop-up dialog box allows you to tell the controller to send a ping request to a specified IP address. This is useful for determining if there is connectivity between the controller and a particular IP station. If you click OK, three pings are sent and the results of the ping are displayed in the pop-up. If a reply to the ping is not received, it shows No Reply Received from IP xxx.xxx.xxx.xxx, otherwise it shows Reply received from IP xxx.xxx.xxx.xxx: (send count = 3, receive count = n).

• Configuration

- Audit Config—See the “Viewing the Latest Network Audit Report” section on page 9-22.

- Refresh Config From Controller—See the “Refreshing the Configuration from the Controller” section on page 9-18.

- Restore Config To Controller—Choose this command to restore the configuration from the Prime Infrastructure database to the controller.

- Set System Time—See the “Setting the Controller Time and Date” section on page 9-34.

• Upload/Download Commands

Note Select the FTP or TFTP radio button. Both File Transfer Protocol (FTP) and Trivial Transfer Protocol (TFTP) are supported for uploading and downloading files to and from the Prime Infrastructure. In previous software releases, only TFTP was supported.

- Upload File from Controller—See the “Uploading Configuration/Logs from Controllers” section on page 9-35.

- Download Config—See the “Downloading Configurations to Controllers” section on page 9-35.

- Download Software—Choose this command to download software to the selected controller or all controllers in the selected groups after you have a configuration group established. See the “Downloading Software to a Controller” section on page 9-36.

- Download Web Auth Cert—Choose this command to access the Download Web Auth Certificate to Controller page. See the “Downloading a Web Admin Certificate to a Controller” section on page 9-37.

- Download Web Admin Cert—Choose this command to access the Download Web Admin Certificate to Controller page. See the “Downloading a Web Admin Certificate to a Controller” section on page 9-37.

- Download IDS Signatures—Choose this command to download customized signatures to the standard signature file currently on the controller. See the “Downloading Signature Files” section on page 9-114 for more information.

- Download Customized Web Auth—Choose this command to download a customized Web authentication page to the controller. A customized web page is created to establish a username and password for user web access. See the “Downloading a Customized Web Authentication Bundle to a Controller” section on page 9-15.

- Download Vendor Device Certificate—Choose this command to download your own vendor-specific device certificate to the controller to replace the current wireless device certificate. See the “Downloading a Vendor Device Certificate” section on page 9-16.
- Download Vendor CA Certificate—Choose this command to download your own vendor-specific certificate authority (CA) to the controller to replace the current CA. See the “Downloading a Vendor CA Certificate” section on page 9-17.

- RRM Commands
  - RRM 802.11a/n Reset—Resets Remote Radio Management for 802.11a/n Cisco Radios.
  - 802.11b/g/n Reset—Resets Remote Radio Management for 802.11b/g/n Cisco Radios.
  - 802.11a/n Channel Update—Updates access point dynamic channel algorithm for 802.11a/n Cisco Radios.
  - 802.11b/g/n Channel Update—Updates access point dynamic channel algorithm for 802.11b/g/n Cisco Radios.
  - 802.11a/n Power Update—Updates access point dynamic transmit power algorithm for 802.11a/n Cisco Radios.
  - 802.11b/g/n Power Update—Updates access point dynamic transmit power algorithm for 802.11b/g/n Cisco Radios.

Restoring Factory Defaults

Choose Configure > Controllers, and click an IP address in the IP Address column. From the left sidebar menu, choose System > Commands, and from the Administrative Commands drop-down list, choose Reset to Factory Default, and click Go to access this page.

This command enables you to reset the controller configuration to the factory default. This overwrites all applied and saved configuration parameters. You are prompted for confirmation to reinitialize your controller.

All configuration data files are deleted, and upon reboot, the controller is restored to its original non-configured state. This removes all IP configuration, and you need a serial connection to restore its base configuration.

**Note**

After confirming configuration removal, you must reboot the controller and select the Reboot Without Saving option.

Setting the Controller Time and Date

Choose Configure > Controllers, and click an IP address under the IP Address column. From the left sidebar menu, choose System > Commands, and from the Configuration Commands drop-down list choose Set System Time, and click Go to access this page.

Use this command to manually set the current time and date on the controller. To use a Network Time Server to set or refresh the current time, see the “Configuring an NTP Server Template” section on page 11-9 page. The following parameters appear:

- Current Time—Shows the time currently being used by the system.
- Month/Day/Year—Choose the month/day/year from the drop-down list.
- Hour/Minutes/Seconds—Choose the hour/minutes/seconds from the drop-down list.
- Delta (hours)—Enter the positive or negative hour offset from GMT (Greenwich Mean Time).
- Delta (minutes)—Enter the positive or negative minute offset from GMT.
Daylight Savings—Select to enable Daylight Savings Time.

**Command Buttons**
- Set Date and Time
- Set Time Zone
- Cancel

**Uploading Configuration/Logs from Controllers**

To upload files from the controller, follow these steps:

**Step 1** Choose Configure > Controllers.
**Step 2** Click an IP address in the IP Address column.
**Step 3** From the left sidebar menu, choose System > Commands.
**Step 4** From the Upload/Download Commands drop-down list, choose Upload File from Controller.
**Step 5** Click Go to access this page.

Use this command to upload files from your controller to a local TFTP (Trivial File Transfer Protocol) server. The following fields appear:
- IP Address—IP address of the controller.
- Status—Upload NOT_INITIATED, or other state.
- Enter the TFTP server name, or New and the new TFTP server name.
- Verify and/or enter the IP Address of the TFTP server.
- Select the file type—Configuration file, Event Log, Message Log, Trap Log, Crash File.
- Enter the Upload to File from /(root)/Prime Infrastructure-tftp/ filename.
- Choose whether or not Prime Infrastructure saves before backing up the configuration.
**Step 6** Click OK. The selected file is uploaded to your TFTP server and named what you entered in the File Name text box.

**Note**
Prime Infrastructure uses an integral TFTP server. This means that third-party TFTP servers cannot run on the same workstation as Prime Infrastructure, because the Cisco Prime Infrastructure and the third-party TFTP servers use the same communication port.

**Downloading Configurations to Controllers**

To download configuration files, follow these steps:

**Step 1** Choose Configure > Controllers.
**Step 2** Click an IP address in the IP Address column.
**Step 3** From the left sidebar menu, choose System > Commands.
Configuring Existing Controllers

Chapter 9 Configuring Devices

Step 4 From the Upload/Download Commands drop-down list, choose Download Config.

Step 5 Click Go to access this page.

Use this command to download and install a configuration file to your controller from a local TFTP (Trivial File Transfer Protocol) server. The following parameters appear:

**Note** Prime Infrastructure uses an integral TFTP server. This means that third-party TFTP servers cannot run on the same workstation as Prime Infrastructure, because the Prime Infrastructure and the third-party TFTP servers use the same communication port.

- IP Address—IP address of the controller.
- Status—Status of the certificate, for example, NOT_INITIATED.

### TFTP Servers

- Server Name—Choose Default Server or New from the drop-down list. When you choose New, type in the IP address.
- Server Address—IP address of the server.
- Maximum Retries—How many times to retry if the download fails.
- Timeout—How long to allow between retries.
- File Name—Enter or choose the filename to download by clicking Browse.

### Downloading Software to a Controller

To download software, follow these steps:

Step 1 Choose Configure > Controllers.

Step 2 Click an IP address in the IP Address column.

Step 3 From the left sidebar menu, choose System > Commands.

Step 4 From the Upload/Download Commands drop-down list, choose Download Software.

Step 5 Click Go to access this page.

Use this command to download and install a new Operating System software to your controller from a local TFTP (Trivial File Transfer Protocol) server.

**Note** Prime Infrastructure uses an integral TFTP server. This means that third-party TFTP servers cannot run on the same workstation as Prime Infrastructure, because the Prime Infrastructure and the third-party TFTP servers use the same communication port.

- IP Address—IP address of the controller to receive the software.
- Current Software Version—The software version currently running on the controller.
- Status—Status of the software, for example, NOT_INITIATED.
- TFTP Server on Cisco Prime Infrastructure System—Select the check box enable the built-in Cisco Prime Infrastructure TFTP server.
• Server IP Address—Indicates the IP address of the TFTP server to send the software to the controller when you have disabled the built-in the Prime Infrastructure TFTP server.
• Maximum Retries—Maximum number of unsuccessful attempts before the download is abandoned.
• Timeout—Maximum number of seconds before the download is abandoned.
• File Name—Enter or select the filename to download by clicking Browse.

### Downloading a Web Admin Certificate to a Controller

To download a Web Admin Certificate, follow these steps:

1. Choose Configure > Controllers.
2. Click an IP address in the IP Address column.
3. From the left sidebar menu, choose System > Commands.
4. From the Upload/Download Commands drop-down list, choose Download WEB Admin Cert.
5. Click Go to access this page.

This page enables you to download a web administration certificate to the controller. The following parameters appear:

> Caution

Each certificate has a variable-length embedded RSA Key. The RSA key length varies from 512 bits, which is relatively insecure, to thousands of bits, which is very secure. When you are obtaining a new certificate from a certificate authority (such as the Microsoft CA), Make sure the RSA key embedded in the certificate is at least 768 Bits.

- IP Address—IP address of the controller to receive the certificate.
- Status—Status of the certificate, for example, NOT_INITIATED.

### TFTP Servers

- Server Name—Use the drop-down list to choose the Default Server or New. When you select New, type in the IP address.
- Server Address—IP address of the server.
- Maximum Retries—Maximum number of times each download operation can be attempted.
- Timeout (seconds)—The amount of time allowed for each download operation.
- File Name—File name of the certificate.
- Password—Password to access the certificate.

### Downloading IDS Signatures

To download a IDS Signature, follow these steps:

1. Choose Configure > Controllers.
Chapter 9  Configuring Devices

Configuring Existing Controllers

Step 2  Click an IP address in the IP Address column.
Step 3  From the left sidebar menu, choose System > Commands.
Step 4  From the Upload/Download Commands drop-down list, choose Download IDS Signatures.
Step 5  Click Go to access this page.

Use this command to download IDS (Intrusion Detection System) signature files from your controller to a local TFTP (Trivial File Transfer Protocol) server. The following parameters appear:
- IP Address—IP address of the controller.
- Status—Download NOT_INITIATED, TRANSFER_SUCCESSFUL or other state.

---

Downloading a Customized Web Auth Bundle to a Controller

To download a customized web authentication page to the controller, follow these steps:

Step 1  Choose Configure > Controllers.
Step 2  Click an IP address in the IP Address column.
Step 3  From the left sidebar menu, choose System > Commands.
Step 4  From the Upload/Download Commands drop-down list, choose Download Customized Web Auth.

The following parameters appear:
- IP Address—IP address of the controller to receive the bundle.
- Status—State of download: NOT_INITIATED, TRANSFER_SUCCESSFUL, TRANSFER_FAILED, NOT_RESPONDING.

---

Before downloading the customized Web authentication bundle, follow these steps:

Step 1  Click the indicated link to download the example login.tar bundle file from the server.
The link is the highlighted word “here” near the bottom of the page.
Step 2  Edit the login.html file and save it as a .tar or .zip file.
Step 3  Download the .tar or .zip file to the controller.
The file contains the pages and image files required for the web authentication display.

Note  The controller accepts a .tar or .zip file of up to 1 MB in size. The 1 MB limit includes the total size of uncompressed files in the bundle.

---

TFTP Servers

To set up one or more TFTP servers, configure the following parameters:
- File is located on—Choose Local machine or TFTP server. The default is local machine (Prime Infrastructure internal server).
• Server Name—Use the drop-down list to choose one of the following:
  – New—Set up a new server. Enter the server name and IP address in the text boxes provided.
  – Default Server—The server name (editable) and IP address (read-only) are automatically added.
• Server IP Address—IP address of the server.
• Maximum Retries—Maximum number of unsuccessful attempts before the download is abandoned.
• Timeout—Maximum number of seconds before the download is abandoned.
• Prime Infrastructure Server Files In—C:\ftp or other specified file directory on the local machine.
• Local File Name—Filename of the Web authentication bundle on the local machine. Click Browse to locate the file.
• Server File Name—Filename on a remote TFTP server.

When completed, these fields and settings are repopulated in the page and do not need to be entered again.

Command Buttons

• OK—The file is downloaded from the local machine or TFTP server with the name shown in the File Name text box.
• Cancel

Configuring Controller System Interfaces

This section describes how to configure controller system interfaces and contains the following topics:

• Adding an Interface, page 9-40
• Viewing Current Interface Details, page 9-41
• Deleting a Dynamic Interface, page 9-42
• NAC Integration, page 9-44
• Configuring Wired Guest Access, page 9-47

To view existing interfaces, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click the IP address of the applicable controller.
Step 3 From the left sidebar menu, choose System > Interfaces. The following parameters appear:
  • Check box—Select the dynamic interface for deletion. Choose Delete Dynamic Interfaces from the Select a command drop-down list.
  • Interface Name—User-defined name for this interface (For example, Management, Service-Port, Virtual).
  • VLAN Identifier—VLAN identifier between 0 (untagged) and 4096, or N/A.
  • Quarantine—Select the check box if the interface has a quarantine VLAN ID configured on it.
  • IP Address—IP address of this interface.
• Interface Type—Static (Management, AP-Manager, Service-Port, and Virtual interfaces) or Dynamic (operator-defined interfaces).
• AP Management Status—Displays the status of AP Management interfaces. The parameters include Enabled, Disabled, and N/A.

Note Only the management port can be configured as Redundancy Management Interface port.

Adding an Interface

To add an interface, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click the IP address of the applicable controller.
Step 3 From the left sidebar menu, choose System > Interfaces.
Step 4 From the Select a command drop-down list, choose Add Interface.
Step 5 Enter the necessary parameters:
  • Interface Name—User-defined name for this interface (Management, Service-Port, Virtual, and VLAN n).
  • Wired Interface—Select the check box to mark the interface as wired.
  • Interface Address
    – VLAN Identifier—1 through 4096, or 0 = untagged.
    – Quarantine—Enable/disable to quarantine a VLAN. Select the check box to enable.
    – IP Address—IP address of the interface.
    – Gateway—Gateway address of the interface.
  • Physical Information
    – Port Number—The port that is used by the interface.
    – Primary Port Number (active)—The port that is currently used by the interface.
    – Secondary Port Number—The port that is used by the interface when the primary port is down.

Note Primary and secondary port numbers are only present in Cisco 4400 Series Wireless LAN controllers.

Note The secondary port is used when the primary port shuts down. When the primary port is reactivated, the Cisco 4400 Series Wireless LAN controller transfers the interfaces back to the primary port.

  – AP Management—Select to enable access point management.
  • DHCP Information
- Primary DHCP Server—IP address of the primary DHCP server.
- Secondary DHCP Server—IP address of the secondary DHCP server.
- Access Control List—User-defined ACL name (or none).
- mDNS Profile—Drop-down list from which you can choose the mDNS profile. The default option is none.

### Viewing Current Interface Details

To view details for a current interface, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click the IP address of the applicable controller.

**Step 3** From the left sidebar menu, choose **System > Interfaces**.

**Step 4** Select the Interface Name for the applicable interface. The Interface Details page opens.

**Step 5** View or edit the following interface parameters:

**Note** Changing the Interface parameters causes the WLANs to be temporarily disabled and thus might result in loss of connectivity for some clients.

- Interface Address
  - VLAN Identifier—1 through 4096, or 0 = untagged.
  - Guest LAN
  - Quarantine—Enable/disable to quarantine a VLAN. Select the check box to enable.
  - IP Address—IP address of the interface.
  - Gateway—Gateway address of the interface.

- Physical Information
  - Primary Port Number (active)—The port that is currently used by the interface.
  - Secondary Port Number—The port that is used by the interface when the primary port is down.

**Note** Primary and secondary port numbers are only present in Cisco 4400 Series Wireless LAN Controllers.

**Note** The secondary port is used when the primary port shuts down. When the primary port is reactivated, the Cisco 4400 Series Wireless LAN Controller transfers the interfaces back to the primary port.

- AP Management—Select to enable access point management.

- DHCP Information
  - Primary DHCP Server—IP address of the primary DHCP server.
Configuring Existing Controllers

Chapter 9      Configuring Devices

Configuring Devices

Step 6 Click **Save** to confirm any changes made. Click **Audit** to audit the device values.

Deleting a Dynamic Interface

To delete a dynamic interface, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click the IP address of the applicable controller.

**Step 3** From the left sidebar menu, choose **System > Interfaces**.

**Step 4** Select the check box of the dynamic interface that you want to delete.

**Step 5** From the Select a command drop-down list, choose **Delete Dynamic Interfaces**.

**Step 6** Click **OK** to confirm the deletion.

*Note* The dynamic interface cannot be deleted if it has been assigned to interface group.

Configuring Controller System Interface Groups

*Note* The Interface Groups feature is supported by controller software release 7.0.116.0 and later.

This section describes how to configure controller system interface groups and contains the following topics:

- **Adding an Interface Group**, page 9-42
- **Deleting an Interface Group**, page 9-43
- **Viewing Interface Groups**, page 9-44

Adding an Interface Group

To add an interface group, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click the IP address of the applicable controller.

**Step 3** From the left sidebar menu, choose **System > Interface Groups**.

**Step 4** From the Select a command drop-down list, choose **Add Interface Group**.

**Step 5** Enter the necessary parameters:

- Secondary DHCP Server—IP address of the secondary DHCP server.
- Access Control List
  - ACL Name—User-defined name of the access control list (or none).

**Step 6** Click **Save** to confirm any changes made. Click **Audit** to audit the device values.
### Configuring Existing Controllers

- **Name**—User-defined name for this interface group (group1, group2).
- **Description**—(Optional) Description for the Interface group.
- **Quarantine**—Enable/disable to quarantine a VLAN. Select the check box to enable.
- **mDNS Profile**—Drop-down list from which you can choose the mDNS profile. The default option is none.

**Step 6**  
Click **Add**.  
The Interface dialog box appears.

**Step 7**  
Select the interfaces that you want to add to the group, and click **OK**.  
To remove an Interface from the Interface group, from the Interface Group page, select the Interface and click **Remove**.

**Step 8**  
Once you are done with adding the interfaces in the Interface Group page, click any of the following buttons:
- **Save** to confirm any changes made.
- **Cancel** to discard the changes.

**Note**
- The number of interfaces that can be added to an interface group depends upon the type of the controller.
- Guest LAN interfaces cannot be part of interface groups.
- An Interface group name must be different from the Interface name.

### Deleting an Interface Group

To delete an interface group, follow these steps:

**Step 1**  
Choose **Configure > Controllers**.

**Step 2**  
Click the IP address of the applicable controller.

**Step 3**  
From the left sidebar menu, choose **System > Interface Groups**.

**Step 4**  
Select the check box of the interface group that you want to delete.

**Step 5**  
From the Select a command drop-down list, choose **Delete Interface Group**, and click **Go**.

**Step 6**  
Click **OK** to confirm the deletion.

**Note**
- The Interface Group cannot be deleted if it has been assigned to WLAN(s).
- The Interface Group cannot be deleted if it has been assigned to AP Group(s).
- The Interface Group cannot be deleted if it has been assigned to Foreign Controller Mapping for the WLAN(s).
- The Interface Group Template cannot be deleted if it has been assigned to WLAN Template(s).
- The Interface Group Template cannot be deleted if it has been assigned to AP Group Template(s).
Configuring Existing Controllers

Viewing Interface Groups

To view existing interface groups, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click the IP address of the applicable controller.

**Step 3** From the left sidebar menu, choose **System > Interface Groups**. The following parameters appear:

- **Name**—User-defined name for the interface group (For example, group1, group2).
- **Description**—(Optional) Description for the Interface Group.
- **Interfaces**—Count of the number of interfaces belonging to the group.

**Step 4** Click the Interface group name link.

The Interface Groups Details page appears with the Interface group details as well as the details of the Interfaces that form part of that particular Interface group.

NAC Integration

The Cisco NAC appliance, also known as Cisco Clean Access (CCA), is a Network Admission Control (NAC) product that allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network. It identifies whether machines are compliant with security policies and repairs vulnerabilities before permitting access to the network. The NAC appliance is available in two modes: in-band and out-of-band. Customers can deploy both modes if desired, each geared toward certain types of access (in-band for supporting wireless users and out-of-band for supporting wired users, for example).

For more information on NAC Out-of-Band Integration, see the applicable section in the *Cisco Prime Infrastructure Configuration Guide*.

- Guidelines for Using SNMP NAC, page 9-44
- Configuring NAC Out-of-Band Integration (SNMP NAC), page 9-45

Guidelines for Using SNMP NAC

Follow these guidelines when using SNMP NAC out-of-band integration:

- The NAC appliance supports up to 3500 users, and the controller supports up to 5000 users. Therefore, multiple NAC appliances might need to be deployed.

- Because the NAC appliance supports static VLAN mapping, you must configure a unique quarantine VLAN for each interface configured on the controller. For example, you might configure a quarantine VLAN of 110 on controller 1 and a quarantine VLAN of 120 on controller 2. However, if two WLANs or guest LANs use the same distribution system interface, they must use the same quarantine VLAN, provided they have one NAC appliance deployed in the network. The NAC appliance supports unique quarantine-to-access VLAN mapping.
• For posture reassessment based on session expiry, you must configure the session timeout on both the NAC appliance and the WLAN, making sure that the session expiry on the WLAN is greater than that on the NAC appliance.

• When a session timeout is configured on an open WLAN, the timing out of clients in the Quarantine state is determined by the timer on the NAC appliance. Once the session timeout expires for WLANs using web authentication, clients deauthenticate from the controller and must perform posture validation again.

• NAC out-of-band integration is supported only on WLANs configured for FlexConnect central switching. It is not supported for use on WLANs configured for FlexConnect local switching.

• If you want to enable NAC on an access point group VLAN, you must first enable NAC on the WLAN. Then you can enable or disable NAC on the access point group VLAN. If you ever decide to disable NAC on the WLAN, be sure to disable it on the access point group VLAN as well.

• NAC out-of-band integration is not supported for use with the WLAN AAA override feature.

• All Layer 2 and Layer 3 authentication occurs in the quarantine VLAN. To use external web authentication, you must configure the NAC appliance to allow HTTP traffic to and from external web servers and to allow the redirect URL in the quarantine VLAN.

  **Note**  
  See the Cisco NAC appliance configuration guides for configuration instructions at the following URL:  

### Guidelines for Using RADIUS NAC

Follow these guidelines when using RADIUS NAC:

• RADIUS NAC is available only for WLAN with 802.1x/WPA/WPA2 Layer 2 security.

• RADIUS NAC cannot be enabled when FlexConnect local switching is enabled.

• AAA override should be enabled to configure RADIUS NAC.

### Configuring NAC Out-of-Band Integration (SNMP NAC)

To configure SNMP NAC out-of-band integration, follow these steps:

**Step 1**  
To configure the quarantine VLAN for a dynamic interface, follow these steps:

a. Choose **Configure > Controller**.

b. Choose which controller you are configuring for out-of-band integration by clicking it in the IP Address column.

c. Choose **System > Interfaces** from the left sidebar menu.

d. Choose **Add Interface** from the Select a command drop-down list.

e. In the Interface Name text box, enter a name for this interface, such as “quarantine.”

f. In the VLAN Identifier text box, enter a non-zero value for the access VLAN ID, such as “10.”

g. Select the **Quarantine** check box if the interface has a quarantine VLAN ID configured on it.
We recommend that you configure unique quarantine VLANs throughout your network. If multiple controllers are configured in the same mobility group and access interfaces on all controllers are in the same subnet, it is mandatory to have the same quarantine VLAN if there is only one NAC appliance in the network. If multiple controllers are configured in the same mobility group and access interfaces on all controllers are in different subnets, it is mandatory to have different quarantine VLANs if there is only one NAC appliance in the network.

h. Configure any remaining fields for this interface, such as the IP address, netmask, and default gateway.

i. Enter an IP address for the primary and secondary DHCP server.

j. Click Save. You are now ready to create a NAC-enabled WLAN or Guest LAN.

Step 2
To configure NAC out-of-band support on a WLAN or guest LAN, follow these steps:

a. Choose WLANs > WLAN from the left sidebar menu.

b. Choose Add a WLAN from the Select a command drop-down list, and click Go.

c. If you have a template established that you want to apply to this controller, choose the guest LAN template name from the drop-down list. Otherwise, click the click here link to create a new template. For more information on setting up the template, see the “Configuring Wired Guest Access” section on page 9-47 section.

d. Click the Advanced tab.

e. To configure SNMP NAC support for this WLAN or guest LAN, choose SNMP NAC from the NAC Stage drop-down list. To disable SNMP NAC support, choose None from the NAC Stage drop-down list, which is the default value.

f. Click Apply to commit your changes.

Step 3
To configure NAC out-of-band support for a specific AP group, follow these steps:

a. Choose WLANs > AP Groups VLAN from the left sidebar menu to open the AP Groups page.

b. Click the name of the desired AP group.

c. From the Interface Name drop-down list, choose the quarantine enabled interface.

d. To configure SNMP NAC support for this AP group, choose SNMP NAC from the Nac State drop-down list. To disable NAC out-of-band support, choose None from the Nac State drop-down list, which is the default value.

e. Click Apply to commit your changes.

Step 4
To see the current state of the client (either Quarantine or Access), follow these steps:

a. Choose Monitor > Clients to open the Clients. Perform a search for clients.
Configuring Wired Guest Access

Wired Guest Access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or specific ports in a conference room.

Like wireless guest user accounts, wired guest access ports are added to the network using the Lobby Ambassador feature.

Wired Guest Access can be configured in a standalone configuration or in a dual controller configuration employing an anchor and foreign controller. This latter configuration is used to further isolate wired guest access traffic but is not required for deployment of wired guest access.

Wired Guest Access ports initially terminate on a Layer 2 access switch or switch port which is configured with VLAN interfaces for wired guest access traffic.

The wired guest traffic is then trunked from the access switch to a wireless LAN controller. This controller is configured with an interface that is mapped to a wired guest access VLAN on the access switch.

If two controllers are being used, the controller (foreign) that receives the wired guest traffic from the switch then forwards the wired guest traffic to an anchor controller that is also configured for wired guest access. After successful hand off of the wired guest traffic to the anchor controller, a bidirectional Ethernet over IP (EoIP) tunnel is established between the foreign and anchor controllers to handle this traffic.

**Note**
Although wired guest access is managed by anchor and foreign anchors when two controllers are deployed, mobility is not supported for wired guest access clients. In this case, DHCP and web authentication for the client are handled by the anchor controller.

**Note**
You can specify how much bandwidth a wired guest user is allocated in the network by configuring and assigning a role and bandwidth contract.

To configure and enable wired guest user access on the network, follow these steps:

**Step 1**
To configure a dynamic interface for wired guest user access, choose **Configure > Controllers** and after IP address, choose **System > Interfaces**.

**Step 2**
Choose **Add Interface** from the Select a command drop-down list, and click **Go**.

**Step 3**
Enter a name and VLAN ID for the new interface.

**Step 4**
Select the **Guest LAN** check box.

**Step 5**
Enter the primary and secondary port number.

**Step 6**
Click **Save**. You are now ready to create a wired LAN for guest access.

**Step 7**
To configure a wired LAN for guest user access, choose **WLANs > WLAN configuration** from the left sidebar menu.

**Step 8**
Choose **Add a WLAN** from the Select a command drop-down list, and click **Go**.

b. Click the MAC address of the desired client to open the Clients > Detail page. The NAC state appears as access, invalid, or quarantine in the Security Information section.
Chapter 9      Configuring Devices

### Configuring Existing Controllers

#### Step 9
If you have a template established that you want to apply to this controller, choose the guest LAN template name from the drop-down list. Otherwise, click the click here link to create a new template.

#### Step 10
In the WLAN > New Template general page, enter a name in the Profile Name text box that identifies the guest LAN. Do not use any spaces in the name entered.

#### Step 11
Select the Enabled check box for the WLAN Status field.

#### Step 12
From the Ingress Interface drop-down list, choose the VLAN that you created in Step 3. This VLAN provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

#### Step 13
From the Egress Interface drop-down list, choose the name of the interface. This WLAN provides a path out of the controller for wired guest client traffic.

**Note**
If you have only one controller in the configuration, choose management from the Egress Interface drop-down list.

#### Step 14
Click the Security > Layer 3 tab to modify the default security policy (web authentication) or to assign WLAN specific web authentication (login, logout, login failure) pages and the server source.

- **a.** To change the security policy to passthrough, select the Web Policy check box and select the Passthrough radio button. This option allows users to access the network without entering a username or password.
  
  An Email Input check box appears. Select this check box if you want users to be prompted for their e-mail address when attempting to connect to the network.

- **b.** To specify custom web authentication pages, unselect the Global WebAuth Configuration Enabled check box.

When the Web Auth Type drop-down list appears, choose one of the following options to define the web login page for the wireless guest users:

- **Default Internal**—Displays the default web login page for the controller. This is the default value.

- **Customized Web Auth**—Displays custom web login, login failure, and logout pages. When the customized option is selected, three separate drop-down lists for login, login failure, and logout page selection appear. You do not need to define a customized page for all three of the options. Choose None from the appropriate drop-down list if you do not want to display a customized page for that option.

  These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files. For specifics on downloading custom pages, see the “Downloading a Customized WebAuthentication Bundle to a Controller” section on page 9-15.

- **External**—Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.

  You can select specific RADIUS or LDAP servers to provide external authentication in the Security > AAA pane. To do so, continue with Step 17.

  **Note**
The RADIUS and LDAP external servers must be already configured to have selectable options in the Security > AAA pane. You can configure these servers on the RADIUS Authentication Servers, TACACS+ Authentication Servers page, and LDAP Servers page.

#### Step 15
If you selected External as the Web Authentication Type in Step 14, choose Security > AAA and choose up to three RADIUS and LDAP servers using the drop-down lists.

#### Step 16
Click Save.
Chapter 9  Configuring Devices

Configuring Existing Controllers

Step 17  Repeat this process if a second (anchor) controller is being used in the network.

Creating an Ingress Interface

To create an Ingress interface, follow these steps:

Step 1  Choose Add Interface from the Select a command drop-down list, and click Go.
Step 2  Click an interface name. The Interfaces Details : New Config page appears.
Step 3  In the Interface Name text box, enter a name for this interface, such as guestinterface.
Step 4  Enter a VLAN identifier for the new interface.
Step 5  Select the Guest LAN check box.
Step 6  Enter the primary and secondary port numbers.
Step 7  Click Save.

Creating an Egress Interface

To create an Egress interface, follow these steps:

Step 1  Choose Add Interface from the Select a command drop-down list, and click Go.
Step 2  Click an interface name. The Interfaces Details : New Config page appears.
Step 3  In the Interface Name text box, enter a name for this interface, such as quarantine.
Step 4  In the VLAN Identifier text box, enter a non-zero value for the access VLAN ID, such as 10.
Step 5  Select the Quarantine check box and enter a non-zero value for the quarantine VLAN ID, such as 110.
Note  You can have NAC-support enabled on the WLAN or guest WLAN template Advanced tab for interfaces with Quarantine enabled.
Step 6  Enter the IP address, netmask, and default gateway.
Step 7  Enter the primary and secondary port numbers.
Step 8  Provide an IP address for the primary and secondary DHCP server.
Step 9  Configure any remaining fields for this interface, and click Save.
You are now ready to create a wired LAN for guest access.

Configuring Controller Network Routes

The Network Route page enables you to add a route to the controller service port. This route allows you to direct all Service Port traffic to the designated management IP address.
- Viewing Existing Network Routes, page 9-50
- Adding a Network Route, page 9-50

**Viewing Existing Network Routes**

To view existing network routes, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Configure &gt; Controllers.</td>
</tr>
<tr>
<td>2</td>
<td>Click the IP address of the applicable controller.</td>
</tr>
<tr>
<td>3</td>
<td>From the left sidebar menu, choose System &gt; Network Route. The following parameters appear:</td>
</tr>
<tr>
<td></td>
<td>- IP Address—The IP address of the network route.</td>
</tr>
<tr>
<td></td>
<td>- IP Netmask—Network mask of the route.</td>
</tr>
<tr>
<td></td>
<td>- Gateway IP Address—Gateway IP address of the network route.</td>
</tr>
</tbody>
</table>

**Adding a Network Route**

To add a network route, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Configure &gt; Controllers.</td>
</tr>
<tr>
<td>2</td>
<td>Click the IP address of the applicable controller.</td>
</tr>
<tr>
<td>3</td>
<td>From the left sidebar menu, choose System &gt; Network Route.</td>
</tr>
<tr>
<td>4</td>
<td>From the Select a command drop-down list, choose Add Network Route.</td>
</tr>
<tr>
<td>5</td>
<td>Click Go.</td>
</tr>
<tr>
<td>6</td>
<td>Enter the IP address, IP Netmask, and Gateway IP address information.</td>
</tr>
<tr>
<td>7</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

**Configuring Controller Spanning Tree Protocol Parameters**

Spanning Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

To view or manage current STP parameters, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Configure &gt; Controllers.</td>
</tr>
<tr>
<td>2</td>
<td>Click the IP address of the applicable controller.</td>
</tr>
<tr>
<td>3</td>
<td>From the left sidebar menu, choose System &gt; Spanning Tree Protocol. The Spanning Tree Protocol page displays the following parameters:</td>
</tr>
<tr>
<td></td>
<td>- Protocol Spec—The current protocol specification.</td>
</tr>
<tr>
<td></td>
<td>- Admin Status—Select this check box to enable.</td>
</tr>
<tr>
<td></td>
<td>- Priority—The numerical priority number of the ideal switch.</td>
</tr>
</tbody>
</table>
Maximum Age (seconds)—The amount of time (in seconds) before the received protocol information recorded for a port is discarded.

Hello Time (seconds)—Determines how often (in seconds) the switch broadcasts its hello message to other switches.

Forward Delay (seconds)—The time spent (in seconds) by a port in the learning/listening states of the switches.

---

### Configuring Controller Mobility Groups

By creating a mobility group, you can enable multiple network controllers to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers can share the context and state of client devices and controller loading information. With this information, the network can support inter-controller wireless LAN roaming and controller redundancy.

**Note**

If it is possible for a wireless client in your network to roam from an access point joined to one controller to an access point joined to another controller, both controllers should be in the same mobility group.

- Messaging Among Mobility Groups, page 9-51
- Mobility Group Prerequisites, page 9-51
- Viewing Current Mobility Group Members, page 9-52
- Adding Mobility Group Members from a List of Controllers, page 9-52
- Manually Adding Mobility Group Members, page 9-52
- Setting the Mobility Scalability Parameters, page 9-53

### Messaging Among Mobility Groups

The controller provides inter-subnet mobility for clients by sending mobility messages to other member controllers:

- There can be up to 72 members in the list with up to 24 in the same mobility group.
- The controller sends a Mobile Announce message to members in the mobility list each time a new client associates to it.
- In the Prime Infrastructure and controller software release 5.0, the controller uses multicast mode to send the Mobile Announce messages. This allows the controller to send only one copy of the message to the network, which delivers it to the multicast group containing all the mobility members.

**Note**

For more information regarding mobility groups, see the *Cisco Prime Prime Infrastructure Configuration Guide*.

### Mobility Group Prerequisites

Before you add controllers to a mobility group, you must verify that the following requirements have been met for all controllers that are to be included in the group:

- All controllers must be configured for the same CAPWAP transport mode (Layer 2 or Layer 3).
Chapter 9       Configuring Devices

Configuring Existing Controllers

- IP connectivity must exist between the management interfaces of all devices.
- All controllers must be configured with the same mobility group name.
- All devices must be configured with the same virtual interface IP address.
- Availability of MAC and IP addresses of each controller to be included in the mobility group (to configure the controllers with the MAC address and IP address of all the other mobility group members).

Viewing Current Mobility Group Members

To view current mobility group members, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Configure &gt; Controllers</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the IP address of the applicable controller.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the left sidebar menu, choose <strong>System &gt; Mobility Groups</strong>.</td>
</tr>
</tbody>
</table>

**Note**
To delete a group member, select a check box for the applicable group member, choose **Delete Group Members**, and click **Go**.

Adding Mobility Group Members from a List of Controllers

To add a mobility group member from a list of existing controllers, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Configure &gt; Controllers</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the IP address of the applicable controller.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the left sidebar menu, choose <strong>System &gt; Mobility Groups</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>From the Select a command drop-down list, choose <strong>Add Group Members</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Go</strong>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Select the check box(es) for the controller to be added to the mobility group.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

Manually Adding Mobility Group Members

If no controllers were found to add to the mobility group, you can add members manually. To manually add members to the mobility group, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Click the <strong>click here</strong> link from the Mobility Group Member details page.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Member MAC Address text box, enter the MAC address of the controller to be added.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Member IP Address text box, enter the management interface IP address of the controller to be added.</td>
</tr>
</tbody>
</table>
### Configuring Existing Controllers

**Step 4** Enter the multicast group IP address to be used for multicast mobility messages in the Multicast Address text box. The local mobility member group address must be the same as the local controller group address.

**Step 5** In the Group Name text box, enter the name of the mobility group.

**Step 6** Click **Save**.

**Step 7** Repeat Steps 1 through 6 for the remaining WLC devices.

### Setting the Mobility Scalability Parameters

**Note** Mobility Groups must be configured prior to setting the mobility scalability parameters.

To set the mobility message parameters, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click an IP address of a controller whose software version is 5.0 or later.

**Step 3** From the left sidebar menu, choose **System > General**.

**Step 4** From the Multicast Mobility Mode drop-down list, specify if you want to enable or disable the ability for the controller to use multicast mode to send Mobile Announce messages to mobility members.

**Step 5** If you enabled multicast messaging by setting multicast mobility mode to enabled, you must enter the group IP address at the Mobility Group Multicast-address field to begin multicast mobility messaging. You must configure this IP address for the local mobility group but it is optional for other groups within the mobility list. If you do not configure the IP address for other (non-local) groups, the controllers use unicast mode to send mobility messages to those members.

**Step 6** Click **Save**.

### Configuring Controller Network Time Protocol

To add a new NTP Server, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click the IP address of the applicable controller.

**Step 3** From the left sidebar menu, choose **System > Network Time Protocol**.

**Step 4** From the Select a command drop-down list, choose **Add NTP Server**.

**Step 5** Click **Go**.
Step 6 From the Select a template to apply to this controller drop-down list, choose the applicable template to apply to this controller.

Command Buttons

- Apply
- Cancel

To create a New Template for NTP Servers, use the click here link to access the template creation page (Configure NTP Servers > New Template).

NTP general parameters include the following:
- Template Name—Enter the new NTP Template name.

  Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- Server Address—Enter the NTP server IP address.
- No. of Controllers Applied To—Number of controllers to which this template is applied (read-only).

Background Scanning on 1510s in Mesh Networks

Background scanning allows Cisco Aironet 1510 Access Points to actively and continuously monitor neighboring channels for more optimal paths and parents. Because the access points are searching on neighboring channels as well as the current channel, the list of optimal alternate paths and parents is greater.

Identifying this information prior to the loss of a parent results in a faster transfer and the best link possible for the access points. Additionally, access points might switch to a new channel if a link on that channel is found to be better than the current channel in terms of fewer hops, stronger signal-to-noise ratio (SNR), and so on.

Background scanning on other channels and data collection from neighbors on those channels are performed on the primary backhaul between two access points:

The primary backhaul for 1510s operate on the 802.11a link.

Background scanning is enabled on a global basis on the associated controller of the access point.

Note Latency might increase for voice calls when they are switched to a new channel.

Note In the EMEA regulatory domain, locating neighbors on other channels might take longer given DFS requirements.

Background Scanning Scenarios

A few scenarios are provided below to better illustrate how background scanning operates.
In Figure 9-1, when the mesh access point (MAP1) initially comes up, it is aware of both root access points (RAP1 and RAP2) as possible parents. It chooses RAP2 as its parent because the route through RAP2 is better in terms of hops, SNR, and so on. After the link is established, background scanning (once enabled) continuously monitors all channels in search of a more optimal path and parent. RAP2 continues to act as parent for MAP1 and communicates on channel 2 until either the link goes down or a more optimal path is located on another channel.

Figure 9-1  Mesh Access Point (MAP1) Selects a Parent

In Figure 9-2, the link between MAP1 and RAP2 is lost. Data from ongoing background scanning identifies RAP1 and channel 1 as the next best parent and communication path for MAP1 so that link is established immediately without the need for additional scanning after the link to RAP2 goes down.

Figure 9-2  Background Scanning Identifies a New Parent

Enabling Background Scanning

To enable background scanning on an AP1510 RAP or MAP, follow these steps:
Configuring Existing Controllers

Chapter 9 Configuring Devices

Step 1 Choose Configure > Controllers.

Note You can also enable this on the Controllers template. See the “Configuring Mesh Templates” section on page 11-110.

Step 2 Choose Mesh > Mesh Settings from the left sidebar menu. The Mesh Settings page appears.

Step 3 Select the Background Scanning check box to enable background scanning or unselect it to disable the feature. The default value is disabled.

Step 4 Click Save.

Configuring Controller QoS Profiles

To make modifications to the quality of service profiles, follow these steps:

Step 1 Choose Configure > Controllers.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose System > QoS Profiles. The following parameters appear:

- Bronze—For Background
- Gold—For Video Applications
- Platinum—For Voice Applications
- Silver—For Best Effort

Step 4 Click the applicable profile to view or edit profile parameters.

Step 5 Set the following values in the Per-User Bandwidth Contracts group box (all have a default of 0 or Off):

- Average Data Rate—The average data rate for non-UDP traffic.
- Burst Data Rate—The peak data rate for non-UDP traffic.
- Average Real-time Rate—The average data rate for UDP traffic.
- Burst Real-time Rate—The peak data rate for UDP traffic.

Step 6 Set the following values for the Over-the-Air QoS group box:

- Maximum QoS RF Usage Per AP (%)—The maximum air bandwidth available to clients. The default is 100%.
- QoS Queue Depth—The depth of queue for a class of client. The packets with a greater value are dropped at the access point.

Step 7 Set the following values in the WLAN QoS group box:

- Maximum Priority
- Unicast Default Priority
- Multicast Default Priority

Step 8 Set the following value in the Wired QoS Protocol group box:

- Wired QoS Protocol—Choose 802.1P to activate 802.1P priority tags or None to deactivate 802.1P priority tags.
Step 9  Click Save.

Configuring Controller DHCP Scopes

- Viewing Current DHCP Scopes, page 9-57
- Adding a New DHCP Scope, page 9-57

Viewing Current DHCP Scopes

To view current DHCP (Dynamic Host Configuration Protocol) scopes, follow these steps:

Step 1  Choose Configure > Controllers.
Step 2  Click the IP address of the applicable controller.
Step 3  From the left sidebar menu, choose System > DHCP Scopes.
The following DHCP Scopes information appears:
- Pool Address
- Lease Time
- Status

Adding a New DHCP Scope

To add a new DHCP Scope, follow these steps:

Step 1  Choose Configure > Controllers.
Step 2  Click the IP address of the applicable controller.
Step 3  From the left sidebar menu, choose System > DHCP Scopes.
Step 4  From the Select a command drop-down list, choose Add DHCP Scope.
Step 5  Enter the following information:
- Scope Name
- Lease Time (in seconds)
- Network
- Netmask
- Pool Start Address
- Pool End Address
- DNS Domain Name
- Status
- Router Addresses—Enter which IP addresses are already in use and should therefore be excluded. For example, you should enter the IP address of your company router. In doing so, this IP address is blocked from use by another client.
• DNS Servers—Enter the IP address of the DNS server(s). Each DNS server must be able to update a client DNS entry to match the IP address assigned by this DHCP scope.

• NetBios Servers—Enter the IP address of the Microsoft Network Basic Input Output System (NetBIOS) name server(s), such as a Windows Internet Naming Service (WINS) server.

Step 6 Click Save.

Configuring Controller User Roles

• Viewing Current Local Net User Roles, page 9-58
• Adding a New Local Net User Role, page 9-58

Viewing Current Local Net User Roles

To view current local net user roles, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click the IP address of the applicable controller.
Step 3 From the left sidebar menu, choose System > User Roles.

The following Local Net User Role parameters appear:

• Template Name

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

• Role Name
• Average Data Rate—The average data rate for non-UDP traffic.
• Burst Data Rate—The peak data rate for non-UDP traffic.
• Average Real-time Rate—The average data rate for UDP traffic.
• Burst Real-time Rate—The peak data rate for UDP traffic.

Step 4 Click a Template Name to view the User Role details.

Adding a New Local Net User Role

To add a new local net user role, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click the IP address of the applicable controller.
Step 3 From the left sidebar menu, choose System > User Roles.
Step 4 From the Select a command drop-down list, choose Add User Role.
Step 5 Select a template from the Select a template to apply to this controller drop-down list.
Configuring Existing Controllers

Chapter 9  Configuring Devices

Configuring Devices

Step 6  Click Apply.

To create a new template for local net user roles, click the click here link to access the template creation page. See the “Configuring User Roles Controller Templates” section on page 11-9 for more information about User Role templates.

Configuring a Global Access Point Password

The AP Username Password page enables you to set a global password that all access points inherit as they join a controller. When you are adding an access point, you can also choose to accept this global username and password or override it on a per-access point basis. See the “Configuring AP Configuration Templates” section on page 11-126 to view where the global password is displayed and how it can be overridden on a per-access point basis.

Also in controller software release 5.0, after an access point joins the controller, the access point enables console port security and you are prompted for your username and password whenever you log into the access point console port. When you log in, you are in non-privileged mode and you must enter the enable password to use the privileged mode.

To establish a global username and password, follow these steps:

Step 1  Choose Configure > Controllers.
Step 2  Click an IP address of a controller with a Release 5.0 or later.
Step 3  From the left sidebar menu, choose System > AP Username Password.
Step 4  Enter the username and password that you want to be inherited by all access points that join the controller.

Note  For Cisco IOS access points, you must also enter and confirm an enable password.

Step 5  Click Save.

Configuring Global CDP

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices.

Note  CDP is enabled on the Ethernet and radio ports of a bridge by default.

Note  Global Interface CDP configuration is applied to only the APs with CDP enabled at AP level.

To configure a Global CDP, perform the following steps:
Chapter 9  Configuring Devices

Configuring Existing Controllers

Step 1  Choose Configure > Controllers.

Step 2  Choose the IP address of the desired controller.

Step 3  From the left sidebar menu, choose System > Global CDP Configuration from the left sidebar menu. The Global CDP Configuration page appears.

Step 4  In the Global CDP group box, configure the following parameters:

- CDP on controller—Choose enable or disable CDP on the controller.

  Note  This configuration cannot be applied on WiSM2 controllers.

- Global CDP on APs—Choose to enable or disable CDP on the access points.

- Refresh-time Interval (seconds)—In the Refresh Time Interval field, enter the time in seconds at which CDP messages are generated. The default is 60.

- Holdtime (seconds)—Enter the time in seconds before the CDP neighbor entry expires. The default is 180.

- CDP Advertisement Version—Enter which version of the CDP protocol to use. The default is v1.

Step 5  In the CDP for Ethernet Interfaces group box, select the slots of Ethernet interfaces for which you want to enable CDP.

  Note  CDP for Ethernet Interfaces fields are supported for Controller Release 7.0.110.2 and later.

Step 6  In the CDP for Radio Interfaces group box, select the slots of Radio interfaces for which you want to enable CDP.

  Note  CDP for Radio Interfaces fields are supported for Controller Release 7.0.110.2 and later.

Step 7  Click Save.

Configuring AP 802.1X Supplicant Credentials

You can configure 802.1X authentication between lightweight access points and the switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning. You can set global authentication settings that all access points inherit as they join the controller. This includes all access points that are currently joined to the controller and any that join in the future.

If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point. See the “Configuring Access Point Details” section on page 9-184 for more information.

To enable global supplicant credentials, follow these steps:

Step 1  Choose Configure > Controllers.

Step 2  Choose the IP address of the desired controller.
Step 3  From the left sidebar menu, choose System > AP 802.1X Supplicant Credentials.
Step 4  Select the Global Supplicant Credentials check box.
Step 5  Enter the supplicant username.
Step 6  Enter and confirm the applicable password.
Step 7  Click Save.

Note  Once saved, you can click Audit to perform an audit on this controller. See the “Understanding the Controller Audit Report” section on page 9-3.

Configuring Controller DHCP

To configure DHCP (Dynamic Host Configuration Protocol) information for a controller, follow these steps:

Step 1  Choose Configure > Controllers.
Step 2  Choose the IP address of the desired controller.
Step 3  From the left sidebar menu, choose System > DHCP.
Step 4  Add or modify the following parameters:

- DHCP Option 82 Remote Id Field Format—Choose AP-MAC, AP-MAC-SSID, AP-ETHMAC, or AP-NAME-SSID from the drop-down list.

  Note  To set the format for RemoteID field in DHCP option 82
  If Ap-Mac is selected, then set the RemoteID format as AP-Mac. If Ap-Mac-ssid is selected, then set the RemoteID format as AP-Mac:SSID.

- DHCP Proxy—Select the check box to enable DHCP by proxy.

  Note  When DHCP proxy is enabled on the controller, the controller unicasts DHCP requests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the WLAN or the WLAN itself.

Step 5  Enter the DHCP Timeout in seconds after which the DHCP request times out. The default setting is 5. Allowed values range from 5 to 120 seconds.

  Note  DHCP Timeout is applicable for Controller Release 7.0.114.74 and later.

Step 6  Click Save.
Note Once saved, you can click **Audit** to perform an audit on this controller. See the “Understanding the Controller Audit Report” section on page 9-3.

### Configuring Controller Multicast Mode

Prime Infrastructure provides an option to configure IGMP (Internet Group Management Protocol) snooping and timeout values on the controller.

To configure multicast mode and IGMP snooping for a controller, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click the IP address of the desired controller.

**Step 3** From the left sidebar menu, choose **System > Multicast**.

**Step 4** Choose **Disable**, **Unicast**, or **Multicast** from the Ethernet Multicast Support drop-down list.

**Note** IGMP Snooping and timeout can be set only if Ethernet Multicast mode is Enabled.

**Step 5** If Multicast is selected, enter the multicast group IP address.

**Step 6** Select the Enable Global Multicast Mode check box to make the multicast mode available globally.

**Step 7** Select to enable IGMP Snooping.

**Step 8** Choose **Enable** from the Multicast Mobility Mode drop-down list to change the IGMP snooping status or to set the IGMP timeout. When IGMP snooping is enabled, the controller gathers IGMP reports from the clients and then sends each access point a list of the clients listening to any multicast group. The access point then forwards the multicast packets only to those clients.

The timeout interval has a range of 3 to 300 and a default value of 60. When the timeout expires, the controller sends a query to all WLANs. Those clients which are listening in the multicast group then send a packet back to the controller.

**Step 9** If you enabled the Multicast Mobility Mode, enter the mobility group multicast address.

**Step 10** Select the **Multicast Direct feature** check box to enable videos to be streamed over a wireless network.

**Step 11** Choose **Enable** from the Multicast Mobility Mode drop-down list to change MLD configuration.

**Step 12** Select the **Enable MLD Snooping** check box to enable IPv6 MLD snooping. If you have selected this check box, configure the following parameters:

- **MLD Timeout**—Enter the MLD timeout value in seconds. The timeout has a range of 3 to 7200 and a default value of 60.
- **MLD Query Interval**—Enter the MLD query interval timeout value in seconds. The interval has a range of 15 to 2400 and a default value of 20.

**Note** Internet Group Management Protocol (IGMP) snooping enables you to limit the flooding of multicast traffic for IPv4. For IPv6, Multicast Listener Discovery (MLD) snooping is used.
Step 13 Specify the Session Banner information, which is the error information sent to the client if the client is denied or dropped from a Media Stream.

a. State—Select the check box to activate the Session Banner. If not activated, the Session Banner is not sent to the client.

b. URL—a web address reported to the client

c. Email—an e-mail address reported to the client

d. Phone—a telephone number reported to the client

e. Note—a note reported to the client

Note All Media Streams on a Controller share this configuration.

Step 14 Click Save.

Note Once saved, you can click Audit to perform an audit on this controller. See the “Understanding the Controller Audit Report” section on page 9-3.

Configuring Access Point Timer Settings

Advanced timer configuration for FlexConnect and local mode is available for the controller on Prime Infrastructure.

Note This feature is only supported on Release 6.0 controllers and later.

- Configuring Advanced Timers, page 9-63
- Access Point Timer Settings for Local Mode, page 9-64
- Access Point Timer Settings for FlexConnect Mode, page 9-64

Configuring Advanced Timers

To configure the advanced timers, follow these steps:

Step 1 Choose Configure > Controllers.

Step 2 Choose the controller for which you want to set timer configuration.

Step 3 From the left sidebar menu, choose System > AP Timers.

Step 4 Select the applicable access point mode (Local mode or FlexConnect mode).

Step 5 See the “Access Point Timer Settings for Local Mode” section on page 9-64 or the “Access Point Timer Settings for FlexConnect Mode” section on page 9-64 for more information on each mode configuration.
Access Point Timer Settings for Local Mode

To reduce the failure detection time, you can configure the fast heartbeat interval (between the controller and the access point) with a smaller timeout value. When the fast heartbeat timer expires (at every heartbeat interval), the access point determines if any data packets have been received from the controller within the last interval. If no packets have been received, the access point sends a fast echo request to the controller. You can then enter a value between 10 and 15 seconds.

Access Point Timer Settings for FlexConnect Mode

Once selected, you can configure the FlexConnect timeout value. Select the AP Primary Discovery Timeout check box to enable the timeout value. Enter a value between 30 and 3600 seconds.

Note

5500 series controllers accept access point fast heartbeat timer values in the range of 1-10.

Configuring Controller WLANs

Because controllers can support 512 WLAN configurations, the Prime Infrastructure provides an effective way to enable or disable multiple WLANs at a specified time for a given controller.

To view a summary of the wireless local access networks (WLANs) that you have configured on your network, follow these steps:

Step 1  Choose Configure > Controllers.
Step 2  Click the IP address of the applicable controller.
Step 3  From the left sidebar menu, choose WLANs > WLAN Configuration. The Configure WLAN Summary page appears. This WLAN Configuration page contains the values found in Table 9-1.

Table 9-1  WLAN Configuration Summary Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check box</td>
<td>Select the WLAN for deletion. Choose Delete WLANs from the Select a command drop-down list.</td>
</tr>
<tr>
<td>WLAN ID</td>
<td>Identification number of the WLAN.</td>
</tr>
<tr>
<td>Profile Name</td>
<td>User-defined profile name specified when creating the WLAN template. Profile Name is the WLAN name.</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier being broadcast by.</td>
</tr>
<tr>
<td>WLAN/Guest LAN</td>
<td>Specifies if it is a WLAN or guest LAN.</td>
</tr>
<tr>
<td>Security Policies</td>
<td>Security policies enabled on the WLAN.</td>
</tr>
</tbody>
</table>
Viewing WLAN Details

To view WLAN details, choose WLANs. The WLAN Details page appears.

Use the tabs (General, Security, QoS, and Advanced) to view or edit parameters for the WLAN.

- **General Tab, page 9-65**
- **Security Tab, page 9-66**
- **QoS Tab, page 9-71**
- **Advanced Tab, page 9-72**
- **Policy Configuration Tab, page 9-77**

**General Tab**

The General tab includes the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Status of the WLAN is either enabled or disabled.</td>
</tr>
<tr>
<td>Task List</td>
<td>If a task is scheduled in Configure &gt; Scheduled Configuration Tasks, you have a link to view the scheduled configuration task.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>Depending on the WLAN template used for this controller, these parameters might or might not be available.</td>
</tr>
<tr>
<td>Note</td>
<td>To configure a start time for the WLAN status to be enabled, select the Schedule Status check box. Choose the hours and minutes from the drop-down lists. Click the calendar icon to select the applicable date.</td>
</tr>
</tbody>
</table>

- Guest LAN—Indicates whether or not this WLAN is a Guest LAN.
- Profile Name
- SSID
- Status—Select the Enabled check box to enable this WLAN.

- Schedule Status
- Security Policies—Identifies the security policies set using the Security tab (includes security policies such as None, 802.1X, Static WEP, Static WEP-802.1X, WPA+WPA2, and CKIP). Changes to the security policies appear after the page is saved.
- Radio Policy—Choose any of the following from the drop-down list:
  - All, 802.11a only, 802.11g only, 802.11b/g only, 802.11a/g only.
- Interface/Interface Group—Choose from the drop-down list.
• Broadcast SSID—Select the check box to enable.
• Egress Interface—Select the name of the applicable interface. This WLAN provides a path out of the controller for wired guest client traffic.

**Note** If you only have one controller in the configuration, choose Management from the Egress Interface drop-down list.

• Ingress Interface—Choose the applicable VLAN from the drop-down list. This interface provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

### Security Tab

The Security tab includes three additional tabs: Layer 2, Layer 3, and AAA Servers.

#### Layer 2 Security

Use the Layer 2 Security drop-down list to choose between None, 802.1x, Static WEP, Cranite, Static WEP-802.1x, WPA1+WPA2, and CKIP. These parameters are described in the Table 9-2.

Mac Filtering—Select the check box if you want to filter clients by MAC address.

**Note** Mac Filtering, Max-Clients, Client Profiling are not supported with FlexConnect Local Authentication.

<table>
<thead>
<tr>
<th>Table 9-2</th>
<th>Layer 2 Security Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| None      | • No Layer 2 security selected.  
|          |   – FT Enable—Select the check box to enable Fast Transition (FT) between access points.  
|          |   **Note** The fast transition feature is not supported with FlexConnect mode.  
|          |   – Over the DS—Select the check box to enable the fast transition over a distributed system.  
|          |   – Reassociation Timeout—Time in seconds after which fast transition reassociation times out. The default is 20 seconds, and the valid range is 1 to 100.  
|          |   **Note** To enable Over the DS or Reassociation Timeout, you should enable fast transition.  |
| 802.1x    | 802.11 Data Encryption:  
|          |   • Type—WEP  
|          |   • Key Size—40, 104, or 128 bits.  |
Configuring Existing Controllers

Table 9-2  Layer 2 Security Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static WEP</td>
<td>802.11 Data Encryption:</td>
</tr>
<tr>
<td></td>
<td>• Type</td>
</tr>
<tr>
<td></td>
<td>• Key Size—Not set, 40, 104, or 128 bits.</td>
</tr>
<tr>
<td></td>
<td>• Key Index—1 to 4.</td>
</tr>
<tr>
<td></td>
<td>• Encryption Key</td>
</tr>
<tr>
<td></td>
<td>• Encryption Key Format—ASCII or HEX.</td>
</tr>
<tr>
<td></td>
<td>• Allowed Shared Key Authentication—Select the check box to enable shared key authentication.</td>
</tr>
<tr>
<td>Cranite</td>
<td>Configure the WLAN to use the FIPS140-2 compliant Cranite Wireless Wall Software Suite, which uses AES encryption and VPN tunnels to encrypt and verify all data frames carried by the Cisco Wireless LAN Solution.</td>
</tr>
<tr>
<td>Static WEP-802.1X</td>
<td>Use this setting to enable both Static WEP and 802.1X policies. If this option is selected, static WEP and 802.1X parameters are displayed at the bottom of the page.</td>
</tr>
<tr>
<td></td>
<td>Static WEP encryption parameters:</td>
</tr>
<tr>
<td></td>
<td>• 802.11 Data Encryption</td>
</tr>
<tr>
<td></td>
<td>• Type</td>
</tr>
<tr>
<td></td>
<td>• Key Size—Not set, 40, 104, or 128 bits.</td>
</tr>
<tr>
<td></td>
<td>• Key Index—1 to 4.</td>
</tr>
<tr>
<td></td>
<td>• Encryption Key</td>
</tr>
<tr>
<td></td>
<td>• Encryption Key Format—ASCII or HEX.</td>
</tr>
<tr>
<td></td>
<td>• Allowed Shared Key Authentication—Select the check box to enable.</td>
</tr>
</tbody>
</table>
### Table 9-2  Layer 2 Security Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA+WPA2</td>
<td>Use this setting to enable WPA, WPA2, or both. WPA enables Wi-Fi Protected Access with TKIP-MIC Data Encryption or AES. When WPA+WPA2 is selected, you can use Cisco Centralized Key Management (CCKM) authentication key management, which allows fast exchange when a client roams from one access point to another. When WPA+WPA2 is selected as the Layer 2 security policy and preshared key is enabled, neither CCKM nor 802.1X can be enabled; although, both CCKM and 802.1X can be enabled at the same time.</td>
</tr>
<tr>
<td></td>
<td>- Mac Filtering—Enables MAC address filtering.</td>
</tr>
<tr>
<td></td>
<td>Note Mac Filtering and Max-Clients are not supported with FlexConnect Local Authentication.</td>
</tr>
<tr>
<td></td>
<td>- FT Enable—Select the check box to enable fast transition between access points.</td>
</tr>
<tr>
<td></td>
<td>Note Fast transition is not supported with FlexConnect mode.</td>
</tr>
<tr>
<td></td>
<td>- Over the DS—Select the check box to enable the fast transition over a distributed system.</td>
</tr>
<tr>
<td></td>
<td>- Reassociation Timeout—Time in seconds after which fast transition reassociation times out. The default is 20 seconds, and the valid range is 1 to 100.</td>
</tr>
<tr>
<td></td>
<td>Note To enable Over the DS or Reassociation Timeout, fast transition should be enabled.</td>
</tr>
<tr>
<td></td>
<td>WPA+WPA2 parameters:</td>
</tr>
<tr>
<td></td>
<td>- WPA1—Select the check box to enable WPA1.</td>
</tr>
<tr>
<td></td>
<td>- WPA2—Select the check box to enable WPA2.</td>
</tr>
<tr>
<td></td>
<td>Authentication Key Management:</td>
</tr>
<tr>
<td></td>
<td>- FT802.1X—Select the check box to enable FT802.1X.</td>
</tr>
<tr>
<td></td>
<td>- 802.1X—Select the check box to enable 802.1X.</td>
</tr>
<tr>
<td></td>
<td>- CCKM—Select the check box to enable CCKM.</td>
</tr>
<tr>
<td></td>
<td>- PSK—Select the check box to enable PSK.</td>
</tr>
<tr>
<td></td>
<td>- FTPSK—Select the check box to enable FTPSK.</td>
</tr>
<tr>
<td></td>
<td>Note Enable WPA2 and fast transition to set FT802.1X or FTPSK.</td>
</tr>
</tbody>
</table>
Use the Layer 3 Security drop-down list to choose between None, VPN Pass Through, and IPsec (Internet Protocol Security). The page parameters change according to the selection you make.

**Note** Depending on the type of WLAN, the Layer 3 parameters might or might not be available.

**Note** If you choose VPN pass through, you must enter the VPN gateway address.

**Note** IPsec is a suite of protocols for securing IP communications by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for establishing cryptographic keys.

Web Policy—Select the check box to specify policies such as authentication, pass through, conditional web redirect, or WebAuth on MAC Filter Failure. This section also allows you to enable guest users to view customized login pages.

**Note** If you choose Pass Through, the Email Input check box appears. Select this check box if you want users to be prompted for their e-mail addresses when attempting to connect to the network.

Preauthentication ACL—Lists IPv4, IPv6, and WebAuth ACLs to be used for traffic between the client and the controller.

---

**Table 9-2 Layer 2 Security Options (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| CKIP  | Cisco Key Integrity Protocol. A Cisco access point advertises support for CKIP in beacon and probe response packets. CKIP can be configured only when Aironet IE is enabled on the WAN.  
  **Note** CKIP is not supported on 10xx access points.  
  CKIP parameters:  
  - 802.11 Data Encryption  
    - Type  
    - Key Size—Not set, 40, 104, or 128 bits.  
    - Key Index—1 to 4.  
    - Encryption Key  
    - Encryption Key Format—ASCII or HEX.  
  - MMH Mode—Select the check box to enable.  
  - Key Permutation—Select the check box to enable. |
IPv6 ACL mapping for WLANs is supported from Controller Release 7.2.x.

To allow guest users to view customized login pages, follow these steps:

**Step 1** Unselect the **Global WebAuth Configuration** check box.

**Step 2** Choose **Web Auth Type** from the drop-down list on the Security > Layer 3 tab.

- Default Internal—The guest user receives the default login page.
- Customized WebAuth—Customized login pages can be downloaded from the Upload/Download Commands page. See the “Downloading a Customized Web Authentication Page” section on page 11-62 for more information.
  - Choose **Web Auth Login Page**, **Web Auth Login Failure Page**, or **Web Auth Logout Page** from the drop-down lists.
  - Choose **None** from any of the drop-down lists if you do not want to display a customized page for that option.
- External—The guest user is redirected to an external login page. Enter the login page URL in the External Web Auth URL text box.

If External is selected, you can select up to three RADIUS and LDAP servers in the Security > AAA page. See the “AAA Servers” section on page 9-70 for more information.

### AAA Servers

Select RADIUS and LDAP servers to override the use of default servers on the current WLAN.

- RADIUS Servers—Use the drop-down lists to choose authentication and accounting servers. With this selection, the default RADIUS server for the specified WLAN overrides the RADIUS server that is configured for the network. If all three RADIUS servers are configured for a particular WLAN, server 1 has the highest priority, and so on.
- LDAP Servers—If no LDAP servers are chosen from the drop-down lists, Prime Infrastructure uses the default LDAP server order from the database.
- Local EAP Authorization—Allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the back-end system becomes disrupted or the external authentication server fails.

Select the check box to enable if you have an EAP profile configured. Select the profile from the drop-down list.

- Allow AAA Override—When enabled, if a client has conflicting AAA and controller WLAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the operating system moves clients from the default Cisco WLAN solution to a VLAN returned by the AAA server and predefined in the controller interface configuration (only when configured for MAC filtering, 802.1X, or WPA operation).

In all cases, the operating system also uses QoS and ACL provided by the AAA server as long as they are predefined in the controller interface configuration. (This VLAN switching by AAA override is also referred to as identity networking.)
When AAA override is disabled, all client authentication defaults to the controller authentication parameter settings, and authentication is only performed by the AAA server if the controller WLANs do not contain any client-specific authentication parameters.

**QoS Tab**

- **Quality of service (QoS)**—From the drop-down list, choose **Platinum** (voice), **Gold** (video), **Silver** (best effort), or **Bronze** (background).
  - Services such as VoIP should be set to gold. Non-discriminating services such as text messaging can be set to bronze.
- **NBAR Visibility**—Check box that you enable to view the classification of applications based on the Network Based Application Recognition (NBAR) deep packet inspection technology.
- **AVC Profile**—Drop-down list from which you can choose an Application Visibility and Control (AVC) profile for the WLAN.
- **NetFlow Monitor**—Drop-down list from which you can choose a NetFlow monitor for the WLAN.
- **Override Per-User Rate Limits**—The wireless rate limits can be defined on both upstream and downstream traffic. To define the data rates on a per-user basis, configure the following:
  - **Average Data Rate**—Define the average data rate for TCP traffic per user or per SSID by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile.
  - **Burst Data Rate**—Define the peak data rate for TCP traffic per user or per SSID by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile. The Burst Data Rate should be greater than or equal to the Average Data Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.
  - **Average Real-Time Rate**—Define the average real-time rate for UDP traffic per user or per SSID by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile.
  - **Burst Real-Time Rate**—Define the peak real-time rate for UDP traffic per user or per SSID by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile. The Burst Real-Time Rate should be greater than or equal to the Average Real-Time Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.
- **Override Per-SSID Rate Limits**—To define the data rates on a per SSID basis, configure the following:
  - **Average Data Rate**—Define the average data rate TCP traffic per user or per SSID by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile.
  - **Burst Data Rate**—Define the peak data rate for TCP traffic per user or per SSID by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile. The Burst Data Rate should be greater than or equal to the Average Data Rate. Otherwise, the QoS policy may block traffic in the WLANs.
  - **Average Real-Time Rate**—Define the average real-time rate for UDP traffic per user or per SSID by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile.
- Burst Real-Time Rate—Define the peak real-time rate for UDP traffic per user or per SSID by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile. The Burst Real-Time Rate should be greater than or equal to the Average Real-Time Rate. Otherwise, the QoS policy may block traffic in the WLANs.

- WMM Parameters
  - WMM Policy—Choose Disabled, Allowed (to allow clients to communicate with the WLAN), or Required (to make it mandatory for clients to have WMM enabled for communication).
  - 7920 AP CAC—Select the check box to enable support on Cisco 7920 phones.
  - 7920 Client CAC—Select the check box to enable WLAN support for older versions of the software on 7920 phones. The CAC limit is set on the access point for newer versions of software.

Advanced Tab

- FlexConnect Local Switching—Select this check box to enable FlexConnect local switching. When enabled, the FlexConnect access point handles client authentication and switches client packets locally. See the “Configuring FlexConnect” section on page 12-4 for more information.

  **Note**  
  FlexConnect local switching applies only to Cisco 1130/1240/1250 series access points. It is not supported with L2TP, PPTP, CRANITE, and FORTRESS authentications. It does not apply to WLAN IDs 9-16.

- Enable FlexConnect local authentication by selecting the FlexConnect Local Auth check box. Local authentication is useful where you cannot maintain the criteria, which is a remote office setup of minimum bandwidth of 128 kbps with the roundtrip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes. In local switching, the authentication capabilities are present in the access point itself. Therefore, local authentication reduces the latency requirements of the branch office.

  **Note**  
  Local authentication can only be enabled on the WLAN of a FlexConnect AP that is in local switching mode.

Local authentication is not supported in the following scenarios:

- Guest Authentication cannot be performed on a FlexConnect local authentication-enabled WLAN.
- RRM information is not available at the controller for the FlexConnect local authentication-enabled WLAN.
- Local RADIUS is not supported.
- Once the client has been authenticated, roaming is supported only after the WLC and the other FlexConnects in the group are updated with the client information.

- Session Timeout (secs)—Set the maximum time a client session can continue before reauthentication.
- Override Interface ACL—Lists IPv4 and IPv6 access control list (ACL) that overrides the ACL configured for the interface on this WLAN.
• **Learn Client IP Address**—When you enable hybrid-REAP local switching, the Learn Client IP Address check box is enabled by default. However, if the client is configured with Fortress Layer 2 encryption, the controller cannot learn the client IP address, and the controller periodically drops the client. Disable this option so that the controller maintains the client connection without waiting to learn the client IP address. The ability to disable this option is supported only with hybrid-REAP local switching; it is not supported with hybrid-REAP central switching.

• **VLAN Based Central Switching**—Select or unselect the VLAN based Central Switching check box to enable or disable central switching on a locally switched WLAN based on AAA overridden VLAN.

• **Central DHCP Processing**—Select or unselect the Central DHCP Processing check box to enable or disable the feature. When you enable this feature, 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.

• **Override DNS**—Select or unselect the Override DNS check box to enable or disable the overriding of the DNS server address on the interface assigned to the locally switched WLAN. When you override DNS in centrally switched WLANs, the clients get their DNS server IP address from the AP, not from the controller.

• **NAT-PAT**—Select or unselect the NAT-PAT check box to enable or disable Network Address Translation (NAT) and Port Address Translation (PAT) on locally switched WLANs. You must enable Central DHCP Processing to enable NAT and PAT.

• **Aironet IE**—Select the check box to enable support for Aironet information elements (IEs) for this WLAN.
  - 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 controller sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the controller and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the association request.

• **IPv6**—Select the check box to enable IPv6.

  **Note**  
  Layer 3 security must be set to None for IPv6 to be enabled.

• **Diagnostic Channel**—Click to enable the diagnostics. When enabled, clients can connect to this WLAN for diagnostic purposes.

  **Note**  
  The results of the diagnostic tests are stored in the SNMP table, and the Prime Infrastructure polls these tables to display the results.

• **Override Interface ACL**—Choose a defined access control list (ACL) from the drop-down list. When the ACL is selected, the WLAN associates the ACL to the WLAN.

  **Note**  
  Choosing an ACL is optional, and the default is None.

  For more information, see the “Configuring an Access Control List Template” section on page 11-65.

• **Peer to Peer Blocking**—From the drop-down list, choose **Disable**, **Drop**, or **Forward-Up Stream**.
This option allows users to configure peer-to-peer blocking for individual clients rather than universally for all WLAN clients.

**Note** For controller Release 7.2.x and later, the Forward Up Stream is same as Drop for locally switched clients.

- **Wi-Fi Direct Client Policy**—Devices that are Wi-Fi Direct capable can connect directly to each other quickly and conveniently to do tasks such as printing, synchronization, and sharing of data. Wi-Fi Direct devices might associate with multiple peer-to-peer (P2P) devices and with infrastructure wireless LANs (WLANs) concurrently. You can use the controller to configure the Wi-Fi Direct Client Policy, on a per-WLAN basis, where you can allow or disallow association of Wi-Fi devices with infrastructure WLANs, or disable Wi-Fi Direct Client Policy for WLANs altogether. From the Wi-Fi Direct Clients Policy drop-down list, choose one of the following options:
  
  - **Disabled**—Disables the Wi-Fi Direct Clients Policy for the WLAN and deauthenticates all Wi-Fi Direct capable clients.
  
  - **Allow**—Allows the Wi-Fi Direct clients to associate with an infrastructure WLAN.
  
  - **Not-Allow**—Disallows the Wi-Fi Direct clients from associating with an infrastructure WLAN.

**Note** The Wi-Fi Direct Clients Policy is applicable to WLANs that have APs in local mode only.

**Note** The Wi-Fi Direct Clients Policy is applicable for controller Release 7.2.x. and later.

- **Client Exclusion**—Select the check box to enable automatic client exclusion. If it is enabled, set the timeout value in seconds for disabled client machines.
  
  - Client machines are excluded by MAC address, and their status can be observed.
  
  - A timeout setting of 0 indicates that administrative control is required to reenable the client.

**Note** When session timeout is not set, the excluded client remains and does not time out from the excluded state. It does not imply that the exclusion feature is disabled.

- **Media Session Snooping**—Select the check box to enable media session snooping. This feature enables access points to detect the establishment, termination, and failure of voice calls and then report them to the controller and Prime Infrastructure. It can be enabled or disabled for each WLAN. When media session snooping is enabled, the access point radios advertise this WLAN snoop for Session Initiation Protocol (SIP) voice packets. Any packets destined to or originating from port number 5060 are considered for further inspection. The access point tracks whether Wi-Fi Multimedia (WMM) and non-WMM clients are establishing a call, already on an active call, or in the process of ending a call and then notify the controller of any major call events.

- **KTS based CAC**—Select the check box to enable KTS-based CAC support per WLAN.
  
  WLC supports TSPEC-based CAC and SIP based CAC. But there are certain phones that work with different protocols for CAC, which are based on the Key Telephone System (KTS). For supporting CAC with KTS-based SIP clients, WLC should understand and process the bandwidth request message from those clients, to allocate the required bandwidth on the AP radio, in addition to handling and sending certain other messages, as part of this protocol.
Note: The KTS CAC configuration is only supported by Cisco 5508, 7500, WISM2, and 2500 controllers that run controller software Release 7.2.x. This feature is not supported by Cisco 4400 series controllers.

Note: The voice parameters appear only if you choose Platinum (voice) from the quality of service (QoS) drop-down list on the QoS tab.

- **NAC State**—From the NAC State drop-down list, choose **SNMP NAC** or **Radius NAC**. SIP errors that are discovered generate traps that appear on the Client Troubleshooting and Alarms pages. The controller can integrate with the NAC appliance in out-of-band mode, where the NAC appliance remains in the data path only until clients have been analyzed and cleaned. Out-of-band mode reduces the traffic load on the NAC appliance and enables centralized NAC processing. See the “NAC Integration” section on page 9-44 for more information.

Note: You can enable RADIUS NAC on WLAN with open authentication and MAC filtering. If you are using local web authentication with RADIUS NAC, the Layer 3 web authentication must also be enabled.

- **Passive Client**—If the check box is selected, it enables passive clients on your WLAN.
  
  Passive clients are wireless devices like scales and printers that are configured with a static IP address. These clients do not transmit any IP information such as IP address, subnet mask, and gateway information during association with an access point. As a result, when passive clients are used, the controller never knows the IP address unless they use DHCP.

  Wireless LAN controllers currently act as a proxy for ARP requests. On receiving an ARP request, the controller responds with an ARP response instead of passing the request directly to the client. This has two advantages:
  
  - The upstream device that sends out the ARP request to the client cannot know where the client is located.
  - Reserves power for battery-operated devices like mobile phones and printers as they do not need to respond to every ARP request.

  Because the wireless controller does not have any IP-related information about passive clients, it cannot respond to any ARP requests. The current behavior does not allow the transfer of ARP requests to passive clients. Therefore, any application that tries to access a passive client fails.

  This feature enables ARP requests and responses to be exchanged between wired and wireless clients on a per VLAN/WLAN basis. This feature enables the user to mark a desired WLAN for presence of proxy ARP thereby enabling the controller to pass the ARP requests until the client gets to RUN state.

Note: This feature is supported only on the 2100, 5500, 5760 and 3850 series controllers.

- **DTIM Period (in beacon intervals)**—For 802.11a/n and 802.11b/g/n, specify the frequency of the DTIM packet sent in the wireless medium. This period can be configured for every WLAN (except guest WLAN) on all Version 6.0 and later controllers.

- **DHCP**
- DHCP Server—Select the check box to override the DHCP server, and enter the IP address of the DHCP server.

  **Note**  For some WLAN configurations, this setting is required.

- DHCP Addr. Assignment—If you select the **Required** check box, clients connected to this WLAN get an IP address from the default DHCP server.

**• Management Frame Protection (MFP)**

- MFP Signature Generation—If the check box is selected, it enables signature generation for the 802.11 management frames transmitted by an access point associated with this WLAN. With signature generation, changes to the transmitted management frames by an intruder are detected and reported.

- MFP Client Protection—From the drop-down list, choose **Enabled**, **Disabled**, or **Required** for individual WLAN configurations.

  **Note**  The **Enabled** parameter is the same as the **Optional** parameter that you choose from the MFP Client Protection drop-down list in the WLC graphical user interface.

- MFP Version—Displays the Management Frame Protection version.

  **Note**  Client-side MFP is available only for those WLANs configured to support CCXv5 (or later) clients. In addition, WPA1 must first be configured.

**• Foreign Controller Mapping**—Click this link to configure foreign controller mappings. This takes you to the Foreign Controller configuration page. In this configuration page, choose a foreign controller from the Foreign Controller drop-down list and choose an interface or interface group from the Interface/Interface Group drop-down list. After choosing the required options, click **Add** to complete the adding of a foreign controller.

**• Client Profiling**—Select the check box to enable or disable profiling of all the clients that are associated with the WLAN.

  **Note**  Client Profiling is not supported with FlexConnect local authentication.

  **Note**  Client Profiling is configurable only when you select the **DHCP Address Assignment** check box.

  **Note**  Client profiling is supported for controllers Release 7.2.x.

- mDNS Snooping—Select the mDNS Snooping check box to enable mDNS snooping on the WLAN.

- mDNS Profile—From the mDNS Profile drop-down list from which you can choose the mDNS profile for the WLAN. The default value is default-mdns-profile.
Policy Configuration Tab

To add a policy to WLAN, follow these steps:

Step 1  Click Add Row.
Step 2  Select a policy name that you want to map to the WLAN, from the drop-down list.
Step 3  Enter the priority. The priority ranges from 1 to 16.

Note  Two policies cannot have same priority.

Step 4  Click Save.

If you want to delete a policy, select the check box corresponding to the policy that you want to delete and click Delete.

Configuring Mobile Concierge (802.11u)

Mobile Concierge is a solution that enables 802.1X capable clients to interwork with external networks. The Mobile Concierge feature provides service availability information to clients and can help them to associate available networks.

The services offered by the network can be broadly classified into two protocols:

- 802.11u MSAP
- 802.11u HotSpot 2.0

The following guidelines and limitations apply to Mobile Concierge:

- Mobile Concierge is not supported on FlexConnect Access Points.
- 802.11u configuration upload is not supported. If you perform a configuration upgrade and upload a configuration on the controller, the HotSpot configuration on the WLANs is lost.

To configure Mobile Concierge (802.11u) Groups, follow these steps:

Step 1  Choose Configure > Controllers.
Step 2  Click the IP address of the applicable controller.
Step 3  From the left sidebar menu, choose WLANs > WLAN Configuration.
Step 4  Click the Hot Spot tab.
Step 5  On the General tab, configure the following fields:

- Select the 802.11u Status check box to enable 802.11u on the WLAN.
- Select the Internet Access check box to enable this WLAN to provide Internet services.
- From the Network Type drop-down list, choose the network type that best describes the 802.11u you want to configure on this WLAN. The following options are available:
  - Private Network
  - Private Network with Guest Access
  - Chargeable Public Network
Free Public Network
Emergency Services Only Network
Personal Device Network
Test or Experimental
Wildcard

Choose the authentication type that you want to configure for the 802.11u parameters on this network:
- Not configured
- Acceptance of Terms and Conditions
- Online Enrollment
- HTTP/HTTPS Redirection

In the HESSID field, enter the Homogenous Extended Service Set Identifier value. The HESSID is a 6-octet MAC address that identifies the homogeneous ESS.

**Step 6** On the Others tab, configure the following fields:
- In the OUI List group box, enter the following details:
  - OUI name
  - Is Beacon
  - OUI Index

  Click **Add** to add the OUI (Organizationally Unique Identifier) entry to this WLAN.

- In the Domain List group box, enter the following details:
  - Domain Name—The domain name operating in the 802.11 access network.
  - Domain Index—Choose the domain index from the drop-down list.

  Click **Add** to add the domain entry to this WLAN.

**Step 7** On the Realm tab, configure the following fields:
- In the OUI List section, enter the following details:
  - Realm Name—The realm name.
  - Realm Index—The realm index.

  Click **Add** to add the domain entry to this WLAN.

**Step 8** On the Service Advertisement tab, configure the following fields:
- Select the **MSAP Enable** check box to enable service advertisements.
- If you enabled MSAP in the previous step, you must provide a server index. Enter the server index for this WLAN. The server index field uniquely identifies an MSAP server instance serving a venue that is reachable through the BSSID.
Step 9  On the HotSpot 2.0 tab, configure the following fields:

- Choose the Enable option from the HotSpot2 Enable drop-down list.
- In the WAM Metrics group box, specify the following:
  - WAN Link Status—The link status. The valid range is 1 to 3.
  - WAN SIM Link Status—The symmetric link status. For example, you can configure the uplink and downlink to have different speeds or same speeds.
  - Down Link Speed—The downlink speed. The maximum value is 4,194,304 kbps.
  - Up Link Speed—The uplink speed. The maximum value is 4,194,304 kbps.
- In the Operator Name List group box, specify the following:
  - Operator Name—Specify the name of the 802.11 operator.
  - Operator Index—Select an operator index. The range is from 1 to 32.
  - Language Code—An ISO-14962-1997 encoded string defining the language. This string is a three character language code.
  
  Click Add to add the operator details. The operator details are displayed in a tabular form.

- In the Port Config List, specify the following:
  - IP Protocol—The IP protocol that you want to enable. The following options are ESP, FTP, ICMP, and IKEV2.
  - Port No—The port number that is enabled on this WLAN.
  - Status—The status of the port.
- On the Policy Configuration tab, configure the following fields:
  - Policy Name—Name of the policy.
  - Policy Priority—Configure policy priority between 1 and 16. No two policies can have same priority.

Note  Only 16 Policy mappings are allowed per WLAN. Selected policy template for the mapping will be applied first if it does not exist on the controller.

Step 10  Click Save.

Adding a WLAN

To add a WLAN, follow these steps:
## Step 1
Choose Configure > Controllers.

## Step 2
Click the IP address of the appropriate controller.

## Step 3
From the left sidebar menu, choose WLANs > WLAN Configuration.

## Step 4
From the Select a command drop-down list, choose Add a WLAN.

## Step 5
Click Go to open the WLAN Details: Add from Template page.

## Step 6
Choose a template from the Select a template to apply to this controller drop-down list.

## Step 7
Click Apply.

**Note**
To create a new template for WLANs, use the click here link in this page, or choose Configure > Controller Template Launch Pad > WLANs > WLAN.

### Deleting a WLAN

To delete a WLAN, follow these steps:

## Step 1
Choose Configure > Controllers.

## Step 2
Click the IP address of the appropriate controller.

## Step 3
From the left sidebar menu, choose WLANs > WLAN Configuration.

## Step 4
Select the check boxes of the WLANs that you want to delete.

## Step 5
From the Select a command drop-down list, choose Delete a WLAN.

## Step 6
Click Go.

## Step 7
Click OK to confirm the deletion.

### Managing WLAN Status Schedules

Prime Infrastructure enables you to change the status of more than one WLAN at a time on a given controller. You can select multiple WLANs and select the date and time for that status change to take place.

To schedule multiple WLANs for a status change, follow these steps:

## Step 1
Choose Configure > Controllers.

## Step 2
Click the IP address of the appropriate controller.

## Step 3
From the left sidebar menu, choose WLANs > WLAN Configuration.

## Step 4
Select the check boxes of the WLANs that you want to schedule for a status change.

## Step 5
From the Select a command drop-down list, choose Schedule Status to open the WLAN Schedule Task Detail page.

The selected WLANs are listed at the top of the page.
Step 6 Enter a Scheduled Task Name to identify this status change schedule.

Step 7 Choose the new Admin Status (Enabled or Disabled) from the drop-down list.

Step 8 Choose the schedule time using the hours and minutes drop-down lists.

Step 9 Click the calendar icon to choose a schedule date or enter the date in the text box (MM/DD/YYYY).

Step 10 Select the appropriate Recurrence radio button to determine the frequency of the status change (Daily, Weekly, or No Recurrence).

Step 11 Click Submit to initiate the status change schedule.

Note For more information on the WLAN Configuration Scheduled Task results, see the Viewing WLAN Configuration Scheduled Task Results section in the Cisco Prime Infrastructure 2.0 User Guide.

Mobility Anchors

Mobility anchors are one or more controllers defined as anchors for the WLAN. Clients (802.11 mobile stations such as a laptop) are always attached to one of the anchors.

This feature can be used to restrict a WLAN to a single subnet, regardless of the entry point of the client into the network. In this way, users can access a public or guest WLAN throughout an enterprise but still be restricted to a specific subnet. Guest WLAN can also be used to provide geographical load balancing because WLANs can represent a particular section of a building (such as a lobby, restaurant, and so on).

When a client first associates to a controller of a mobility group that has been preconfigured as a mobility anchor for a WLAN, the client associates to the controller locally, and a local session is created for the client. Clients can be anchored only to preconfigured anchor controllers of the WLAN. For a given WLAN, you should configure the same set of anchor controllers on all controllers in the mobility group.

When a client first associates to a controller of a mobility group that has not been configured as a mobility anchor for a WLAN, the client associates to the controller locally, a local session is created for the client, and the controller is announced to the other controllers in the same mobility group. If the announcement is not answered, the controller contacts one of the anchor controllers configured for the WLAN and creates a foreign session for the client on the local switch. Packets from the client are encapsulated and delivered to the wired network. Packets to the client are received by the anchor controller and forwarded to the foreign controller through a mobility tunnel using EitherIP. The foreign controller decapsulates the packets and forwards them to the client.

Note A 2000 series controller cannot be designated as an anchor for a WLAN. However, a WLAN created on a 2000 series controllers can have a 4100 series controller or a 4400 series controller as its anchor.

Note The L2TP Layer 3 security policies are unavailable for WLANs configured with a mobility anchor.

To view the real time status of mobility anchors for a specific WLAN, follow these steps:

Step 1 Choose Configure > Controllers.
Configuring Existing Controllers

Chapter 9 Configuring Devices

Configuring WLANs AP Groups

Site-specific VLANs or AP groups limit the broadcast domains to a minimum by segmenting a WLAN into different broadcast domains. Benefits of this include more effective management of load balancing and bandwidth allocation.

To open this page, follow these steps:

**Step 1** Choose Configure > Controllers.

**Step 2** Click a controller IP address.

**Step 3** From the left sidebar menu, choose WLAN > AP Groups.

This page displays a summary of the AP groups configured on your network. From here you can add, remove, or view details of an AP group. Click the AP group name on the Access Points tab to view or edit its access point(s). Click the WLAN Profiles tab to view, edit, add, or delete WLAN profiles.

Adding Access Point Groups

To add a new access point group, follow these steps:

**Step 1** Choose Configure > Controllers.

**Step 2** Click a controller IP address.

**Step 3** From the left sidebar menu, choose WLAN > AP Groups.

**Note** AP Groups (for 5.2 and later controllers) is referred to as AP Group VLANs for controllers prior to 5.2.

**Step 4** From the Select a command drop-down list, choose Add AP Groups.
Step 5  Click **Go**.

In the AP Groups details page, you can add access points and WLAN profiles to this access point group.

Step 6  Enter a name and group description for the access point group.

**Note**  The group description is optional.

Step 7  To add access points to the group, follow these steps:

a.  Click the **Access Points** tab.

b.  Click **Add**. The access point page displays parameters for available access points. Click the access point name to view or edit parameters for one of the available access points.

c.  Select the check box(es) of the access point(s) you want to add.

d.  Click **Select**.

Step 8  To add a WLAN profile, click the **WLAN Profiles** tab and configure the following parameters:

a.  Click **Add**.

**Note**  To display all available WLAN profile names, delete the current WLAN profile name from the text box. When the current WLAN profile name is deleted from the text box, all available WLAN profiles appear in the drop-down list.

**Note**  Each access point is limited to 16 WLAN profiles. Each access point broadcasts all WLAN profiles unless the WLAN override feature is enabled. The WLAN override feature allows you to disable any of the 16 WLAN profiles per access point.

**Note**  The WLAN override feature applies only to older controllers that do not support the 512 WLAN feature (can support up to 512 WLAN profiles).

b.  Type a WLAN profile name or choose one from the WLAN Profile Name drop-down list.

c.  Enter an interface/interface group or choose one from the Interface/Interface Group drop-down list.

**Note**  To display all available interfaces, delete the current interface in the Interface text box. When the current interface is deleted from the Interface text box, all available interfaces appear in the drop-down list.

d.  Select the **NAC Override** check box, if applicable. NAC override is disabled by default.

e.  Specify the policy configuration parameters by clicking the **Add/Edit** link.

  - Policy Name—Name of the policy.

  - Policy Priority—Configure policy priority between 1 and 16. No two policies can have same priority.
Chapter 9  Configuring Devices

Configuring Existing Controllers

Note Only 16 Policy mappings are allowed per WLAN. Selected policy template for the mapping will be applied first if it does not exist on the controller.

f. When access points and WLAN profiles are added, click Save.

Step 9 If you want to add a RF profile, click the RF Profiles tab and configure the following parameters:

- 802.11a—Drop-down list from which you can choose an RF profile for APs with 802.11a radios.
- 802.11b—Drop-down list from which you can choose an RF profile for APs with 802.11b radios.
- When RF profiles are added, click Save.

Note Use the Click here link to add a new RF profile. See the “Configuring RF Profiles Templates (802.11)” section on page 11-81 for more information.

Note Changing the WLAN-interface mapping in an AP Group removes the local VLAN mapping for FlexConnect APs in this group. These mappings need to be reconfigured after applying this change.

Deleting Access Point Groups

To delete an access point group, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click a controller IP address.
Step 3 From the left sidebar menu, choose WLAN > AP Groups.
Step 4 Select the check box(es) of the access point group(s) that you want to delete.
Step 5 From the Select a command drop-down list, choose Delete AP Groups.
Step 6 Click OK to confirm the deletion.

Auditing Access Point Groups

You can audit the access point group to determine if the Prime Infrastructure and device values differ. To audit an access point group, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click a controller IP address.
Step 3 From the left sidebar menu, choose WLAN > AP Groups.
Step 4 Click the name of the access point group that you want to audit.
Configuring Policy on a Controller

The Policy Configuration Templates page enables you to configure the device-based policies on a controller. You can configure policies for a user or a device on the network. The maximum number of policies that you can configure is 64. For more information about policy configuration templates, see the “Configuring Policy Configuration Templates” section on page 11-39.

Note Policies are not applied on WLANs and AP groups if AAA override is configured on the controller.

To configure Policy Configuration templates, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.
Step 2 Click Policy Configuration or choose WLANs > Policy Configuration from the left sidebar menu.
Step 3 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go.
Step 4 Configure the following fields:
   • Policy Name—Name of the policy.
   • Policy Role—The user type or the user group the user belongs to. For example, student, employee.
   • EAP Type—EAP authentication method used by the client. The available types are as follows:
     - LEAP
     - EAP-FAST
     - EAP-TLS
     - PEAP
   • Device Type—Drop-down list from which you can choose a type of device.
   • VLAN—VLAN associated with the policy.
   • ACL—Drop-down list from which you can choose an IPv4 ACL for the policy.
   • QoS—Drop-down list from which you can choose the QoS policy that can be one of the follows:
     - Platinum (Voice)—Assures a high QoS for Voice over Wireless.
     - Gold (Video)—Supports the high-quality video applications.
     - Silver (Best Effort)—Supports the normal bandwidth for clients.
     - Bronze (Background)—Provides the lowest bandwidth for guest services.
   • Session Timeout—Maximum amount of time, in seconds, before a client is forced to reauthenticate. The default value is 0 seconds.

Note Click Audit located at the bottom of the page.
• Sleeping Client Timeout—Maximum amount of time, in hours, before a guest client is forced to reauthenticate. The default value is 12 hours. The range is from 1 to 720 hours.

## Configuring FlexConnect Parameters

FlexConnect 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 a controller in each office. There is no deployment restriction on the number of FlexConnect access points per location. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller.

- Configuring FlexConnect AP Groups, page 9-86
- Auditing a FlexConnect Group, page 9-90

### Configuring FlexConnect AP Groups

To view a list of existing FlexConnect AP groups, follow these steps:

1. Choose Configure > Controllers.
2. Click the IP address of the applicable controller.
3. From the left sidebar menu, choose FlexConnect > FlexConnect AP Groups. The FlexConnect AP Groups page opens.
   - Group Name—The name of the FlexConnect AP group. Click the group name to view its details.

   **Note**
   Use the check box to select a group for deletion.

### Configuring a FlexConnect AP Group

To configure a FlexConnect access point group, follow these steps:

1. Choose Configure > Controllers.
2. Click the IP address of the applicable controller.
3. From the left sidebar menu, choose FlexConnect > FlexConnect AP Groups.
4. From the Select a command drop-down list, click *Add FlexConnect AP Group* to open the FlexConnect AP Group > Add From Template pane.
5. Choose a template from the Select a template to apply to this controller drop-down list.
6. Click Apply.
Note To make modifications to an existing FlexConnect AP Group, click the existing group in the Group Name column of the FlexConnect AP Group page.
To delete an existing group, select the check box of the group you want to remove, and choose Delete FlexConnect AP Group from the Select a command drop-down list.

Step 7 Configure the following FlexConnect AP Group parameters:

- **General tab**
  - Template Name—The name of the template applied to this controller.
  - Primary Radius—From the drop-down list, choose the primary radius authentication server present on the controller.
  
  **Note** If the selected or configured Radius Authentication Server is not present on the controller with version less than 7.4, the template will fail.

  **Note** You must configure the RADIUS server configuration on the controller before you apply FlexConnect RADIUS server configuration from the Prime Infrastructure.

  - Secondary Radius—From the drop-down list, choose the secondary radius authentication server present on the controller.

  **Note** If a RADIUS authentication server is not present on the controller, the Prime Infrastructure configured RADIUS server does not apply.

- **FlexConnect AP tab**
  - Ethernet MAC—Select the check box to apply to the FlexConnect group.
  
  **Note** An AP Ethernet MAC address cannot exist in more than one FlexConnect group on the same controller. The controller does not allow you to set an AP Ethernet MAC in a FlexConnect group if it is already present in another FlexConnect group.

  - Add AP—Click to add an additional FlexConnect AP (present in the Prime Infrastructure) to an existing FlexConnect group. When you click Add AP, only those access points that are part of this FlexConnect group is listed.

Step 8 If you want to enable local authentication for a FlexConnect group, click the **FlexConnect Configuration** tab.

**Note** Make sure that the Primary RADIUS Server and Secondary RADIUS Server parameters are set to None on the General tab.

Step 9 Select the **FlexConnect Local Authentication Enable** check box to enable local authentication for this FlexConnect group. The default value is unselected.
Step 10  To allow a FlexConnect access point to authenticate clients using LEAP, select the LEAP check box. Otherwise, to allow a FlexConnect access point to authenticate clients using EAP-FAST, select the EAP-FAST check box.

If you have selected the EAP-FAST check box, then you are required to provide the EAP-FAST key as well as confirm the EAP-FAST key.

Step 11  Perform one of the following, depending on how you want Protected Access Credentials (PACs) to be provisioned:

- To use manual PAC provisioning, enter the key used to encrypt and decrypt PACs in the EAP=FAST Key text box. The key must be 32 hexadecimal characters.
- To allow PACs to be sent automatically to clients that do not have one during PAC provisioning, select the Ignore Server Key check box.

Step 12  In the EAP-FAST Authority ID text box, enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.

Step 13  In the EAP-FAST Authority Info text box, enter the authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.

Step 14  In the EAP-FAST PAC Timeout text box, specify a PAC timeout value by entering the number of seconds for the PAC to remain visible in the edit text box. The valid range is 2 to 4095 seconds.

Note  To see if an individual access point belongs to a FlexConnect group, click the Users configured in the group link. It advances you to the FlexConnect AP Group page which shows the names of the groups and the access points that belong in it.

Step 15  Click the Image Upgrade tab and configure the following:

- FlexConnect AP Upgrade—Select the check box if you want to upgrade the FlexConnect access points.
- Slave Maximum Retry Count—Specify the maximum retries for the slave to undertake to start the download from the master in the FlexConnect group. This option is available only if you select the FlexConnect AP Upgrade check box.

Note  You are allowed to add an access point as a master access point only if the FlexConnect AP Upgrade check box is enabled on the General tab.

Step 16  Click the VLAN-ACL Mapping tab to view, add, edit, or remove a VLAN ACL mapping.

a. Click Add Row.
b. Enter a VLAN ID. The valid VLAN ID range is 1—4094.
c. From the Ingress ACL drop-down list, choose an Ingress ACL.
d. From the Egress AC drop-down list, choose an Egress ACL.
e. Click Save.

Step 17  Click the WLAN-ACL Mapping tab, and select the FlexConnect access control list for external web authentication.

a. Click Add Row.
b. From the WLAN Profile Name drop-down list, choose a WLAN profile.
c. From the WebAuth ACL drop-down list, choose a WebAuth ACL.
d. Click Save.

**Note** You can add up to a maximum of 16 WebAuth ACLs.

**Step 18** Click the **WebPolicy ACL** tab and select the FlexConnect access control list to be added as a web policy.

a. Click Add Row.

b. From the Web-Policy ACL drop-down list, choose a WebPolicy ACL.

c. Click Save.

**Note** You can add up to a maximum of 16 Web-Policy ACLs.

**Step 19** Click the **Local Split** tab to view, add, edit, or remove a Local Split ACL mapping.

a. Click Add Row.

b. From the WLAN Profile Name drop-down list, choose a WLAN profile.

**Note** Only the FlexConnect central switching WLANs are displayed in the WLAN Profile Name drop-down list.

c. From the Local-Split ACL drop-down list, choose a FlexConnect ACL.

d. Click Save.

**Step 20** Click the **Central DHCP** tab to view, add, edit, or remove a Central DHCP processing.

a. Click Add Row.

b. From the WLAN Profile Name drop-down list, choose a WLAN profile.

**Note** Only the FlexConnect local switching WLANs are displayed in the WLAN Profile Name drop-down list.

c. From the Central DHCP drop-down list, choose **Enable** or **Disable**. When you enable this feature, 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.

d. From the Override DNS drop-down list, choose **Enable** or **Disable**. You can enable or disable the overriding of the DNS server address on the interface assigned to the locally switched WLAN. When you override DNS in centrally switched WLANs, the clients get their DNS server IP address from the AP, not from the controller.

e. From the NAT-PAT drop-down list, choose **Enable** or **Disable**. You can enable or disable Network Address Translation (NAT) and Port Address Translation (PAT) on locally switched WLANs. You must enable Central DHCP Processing to enable NAT and PAT.

f. Click Save.

**Step 21** Click **Save**.
Auditing a FlexConnect Group

If the FlexConnect configuration changes over a period of time either on the Prime Infrastructure or the controller, you can audit the configuration. The changes are visible in subsequent pages. You can specify to refresh the Prime Infrastructure or the controller to synchronize the configuration.

Configuring Security Parameters

- Configuring Controller File Encryption, page 9-90
- Configuring Controllers > IPaddr > Security > AAA, page 9-91
- Configuring Controllers > IPaddr > Security > Local EAP, page 9-100
- Configuring User Login Policies, page 9-104
- Managing Manually Disabled Clients, page 9-104
- Configuring Access Control Lists, page 9-105
- Configuring CPU Access Control Lists, page 9-107
- Configuring the IDS Sensor List, page 9-108
- Configuring CA Certificates, page 9-108
- Configuring ID Certificates, page 9-109
- Configuring Controllers > IPaddr > Security > Web Auth Certificate, page 9-110
- Configuring Wireless Protection Policies, page 9-110
- Configuring Rogue Policies, page 9-111
- Configuring Rogue AP Rules, page 9-112
- Configuring Client Exclusion Policies, page 9-113
- Configuring Controller Standard Signature Parameters, page 9-113
- Configuring Custom Signatures, page 9-117
- Configuring AP Authentication and MFP, page 9-118

Configuring Controller File Encryption

To configure a controller file encryption, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click the IP address of the applicable controller.

**Step 3** From the left sidebar menu, choose **Security > File Encryption**. File encryption ensures that data is encrypted when you upload or download the controller configuration file from a TFTP server.

File Encryption parameters include the following:

- File Encryption—If this option is enabled, the data in the controller configuration file is encrypted when it is uploaded or downloaded through the TFTP server.
- Encryption Key—A text string of exactly 16 characters.
• Confirm Encryption Key—Enter the encryption key.

Configuring Controllers > IPaddr > Security > AAA

This section describes how to configure controller security AAA parameters and contains the following topics:

• Configuring AAA General Parameters, page 9-91
• Configuring AAA RADIUS Auth Servers, page 9-91
• Configuring AAA RADIUS Acct Servers, page 9-92
• Configuring AAA RADIUS Fallback Parameters, page 9-93
• Configuring AAA LDAP Servers, page 9-94
• Configuring AAA TACACS+ Servers, page 9-96
• Configuring AAA Local Net Users, page 9-96
• Configuring AAA MAC Filtering, page 9-97
• Configuring AAA AP/MSE Authorization, page 9-98
• Configuring AAA Web Auth Configuration, page 9-99

Configuring AAA General Parameters

The General page allows you to configure the local database entries on a controller.

To configure the local database entries, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click the IP address of the applicable controller.
Step 3 From the left sidebar menu, choose Security > AAA > General.
Step 4 Enter the maximum number of allowed database entries. This amount becomes effective on the next reboot. The valid range is 512 - 2048.

Configuring AAA RADIUS Auth Servers

To view a summary of existing RADIUS authentication servers, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click the IP address of the applicable controller.
Step 3 From the left sidebar menu, choose Security > AAA > RADIUS Auth Servers. The following RADIUS Auth Servers parameters appear:

• Server Index—Access priority number for the RADIUS server (display only). Click to go to Configure IPaddr > RADIUS Authentication Server.
Server Address—IP address of the RADIUS server (read-only).
Port Number—Controller port number (read-only).
Admin Status—Enable or Disable.
Network User—Enable or Disable.
Management User—Enable or Disable.

Adding an Authentication Server

To add an authentication server, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click the IP address of the applicable controller.
Step 3 From the left sidebar menu, choose Security > AAA > RADIUS Auth Servers.
Step 4 From the Select a command drop-down list, choose Add Auth Server to open the Radius Authentication Server > Add From Template page.
Step 5 Choose a template from the Select a template to apply to this controller drop-down list.
Step 6 Click Apply.

Note To create a new template for Radius authentication servers, choose Configure > Controller Templates > Security > RADIUS Auth Servers.

Configuring AAA RADIUS Acct Servers

To view a summary of existing RADIUS accounting servers, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click the IP address of the applicable controller.
Step 3 From the left sidebar menu, choose Security > AAA > RADIUS Acct Servers. RADIUS Acct Server parameters include the following:

- Server Index—Access priority number for the RADIUS server (read-only). Click to open the Radius Acct Servers Details page.

Note To edit or audit the current accounting server parameters, click the Server Index for the applicable accounting server.

- Server Address—IP address of the RADIUS server (read-only).
- Port Number—Controller port number (read-only).
- Admin Status—Enable or Disable.
Adding an Accounting Server

To add an accounting server, follow these steps:

**Step 1** Choose Configure > Controllers.

**Step 2** Click the IP address of the applicable controller.

**Step 3** From the left sidebar menu, choose Security > AAA > RADIUS Acct Servers.

**Step 4** From the Select a command drop-down list, choose Add Acct Server to open the Radius Acct Servers Details > Add From Template page.

**Step 5** Choose a template from the Select a template to apply to this controller drop-down list.

**Step 6** From the drop-down list, choose a controller to apply to this template.

**Step 7** Click Apply.

*Note* To create a new template for Radius accounting servers, choose Configure > Controller Templates Launch Pad > Security > RADIUS Acct Servers.

Deleting an Accounting Server

To delete an accounting server, follow these steps:

**Step 1** Choose Configure > Controllers.

**Step 2** Click the IP address of the applicable controller.

**Step 3** From the left sidebar menu, choose Security > AAA > RADIUS Acct Servers.

**Step 4** Select the check box(es) for the applicable accounting server(s).

**Step 5** From the Select a command drop-down list, choose Delete Acct Server.

**Step 6** Click Go.

**Step 7** Click OK in the pop-up dialog box to confirm the deletion.

Configuring AAA RADIUS Fallback Parameters

To configure RADIUS fallback parameters, follow these steps:
Configuring Existing Controllers

Chapter 9  Configuring Devices

Configuring Existing Controllers

Configuring Devices

Step 1
Choose **Configure > Controllers**.

Step 2
Click the IP address of the applicable controller.

Step 3
From the left sidebar menu, choose **Security > AAA > RADIUS Fallback**.

Step 4
Add or modify the following parameters:
- RADIUS FallbackMode
- Username
- Time Interval

Step 5
Click **Save**.

**Note**
Click **Audit** to check the present configuration status of the Prime Infrastructure and controller.

Configuring AAA LDAP Servers

This page enables you to add and delete LDAP servers to this controller.

To access the LDAP Servers page, follow these steps:

**Step 1**
Choose **Configure > Controllers**.

**Step 2**
Click the IP address of the applicable controller.

**Step 3**
From the left sidebar menu, choose **Security > AAA > LDAP Servers**.

This page displays LDAP servers currently used by this controller and contains the following parameters:
- Check box—Select the check box to choose an LDAP server for deletion.
- Server Index—A number assigned to identify the LDAP server.
- Server Address—The LDAP server IP address.
- Port Number—The port number used to communicate with the LDAP server.
- Admin Status—Server template status.
  Indicates if use of the LDAP server template is enabled or disabled.

**Note**
Click the index number to go the LDAP server configuration page.

**Note**
If the title of a column is a link, click it to toggle between ascending and descending order.

**Note**
Prime Infrastructure now supports LDAP configuration for both an anonymous or authenticated bind.
For more information, see the “Configuring New LDAP Bind Requests” section on page 9-95.
LDAP Servers Select a command Drop-Down List Options

Adding LDAP Server

To add a LDAP Server, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click the IP address of the applicable controller.
Step 3 From the left sidebar menu, choose Security > AAA > LDAP Servers.
Step 4 From the Select a command drop-down list, choose Add LDAP Server.
Step 5 Click Go.

Deleting LDAP Servers

To delete the LDAP Server, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click the IP address of the applicable controller.
Step 3 From the left sidebar menu, choose Security > AAA > LDAP Servers.
Step 4 Select the check box(es) of the LDAP servers that you want to delete.
Step 5 From the Select a command drop-down list, choose Delete LDAP Servers.
Step 6 Click Go.

Configuring New LDAP Bind Requests

Prime Infrastructure now supports LDAP configuration for both an anonymous or authenticated bind. A bind is a socket opening that performs a lookup.

To configure LDAP bind requests, follow these steps:

Step 1 Choose Configure > Controller.
Step 2 From the left sidebar menu, choose Security > AAA > LDAP Servers.
Step 3 From the Bind Type drop-down list, choose Authenticated or Anonymous. If you choose Authenticated, you must enter a bind username and password as well.
Step 4 In the Server User Base DN text box, enter the distinguished name of the subtree in the LDAP server that contains a list of all the users.
Step 5 In the Server User Attribute text box, enter the attribute that contains the username in the LDAP server.
Step 6 In the Server User Type text box, enter the ObjectType attribute that identifies the user.
Step 7 In the Retransmit Timeout text box, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.
Step 8 Select the Admin Status check box if you want the LDAP server to have administrative privileges.
Configuring Existing Controllers

Configuring AAA TACACS+ Servers

This page enables you to add and delete TACACS+ servers to this controller.

To access the TACACS+ Servers page, follow these steps:

Step 1  Choose Configure > Controllers.

Step 2  Click the IP address of the applicable controller.

Step 3  From the left sidebar menu, choose Security > AAA > TACACS+ Servers.

This page displays TACACS+ servers currently used by this controller and contains the following parameters:

- Check box—Select the check box to choose a TACACS+ server for deletion.
- Server Type—The TACACS+ server type—accounting, authorization, or authentication.
- Server Index—A number assigned to identify the TACACS+ server and set its use priority. Click the index number to go the TACACS+ server configuration page.
- Server Address—The TACACS+ server IP address.
- Port Number—The port number used to communicate with the TACACS+ server.
- Admin Status—Server template status.
  Indicates if use of the TACACS+ server template is enabled.

If the title of a column is a link, click it to toggle between ascending and descending order.

The Select a command drop-down list has the following options:

- Add TACACS+ Server—Choose this option, then click Go to add a TACACS+ server to the controller.
- Delete TACACS+ Servers—Choose this option, then click Go to delete all TACACS+ servers with a selected check box from the controller.

Configuring AAA Local Net Users

This page provides a summary of the existing local network user controllers for clients who are allowed to access a specific WLAN. This is an administrative bypass of the RADIUS authentication process. Layer 3 Web Authentication must be enabled. The client information is passed to the RADIUS authentication server first, and if the client information does not match a RADIUS database entry, this local database is polled. Clients located in this database are granted access to network services if the RADIUS authentication fails or does not exist.

- Deleting a Local Net User, page 9-97

To view existing local network users, follow these steps:

Step 1  Choose Configure > Controllers.

Step 2  Click the IP address of the applicable controller.
Step 3  From the left sidebar menu, choose Security > AAA > Local Net Users. The Local Net Users page displays the following local net user parameters:

- Username—User-defined identification.
- WLAN ID—Any WLAN ID, 1 through 16; 0 for all WLANs; 17 for third-party WLAN that this local net user is allowed to access.
- Description—Optional user-defined description.

Deleting a Local Net User

To delete a local net user, follow these steps:

**Step 1**  Choose Configure > Controllers.

**Step 2**  Click the IP address of the applicable controller.

**Step 3**  From the left sidebar menu, choose Security > AAA > Local Net Users.

**Step 4**  Select the check box(es) for the applicable local net user(s).

**Step 5**  From the Select a command drop-down list, choose Delete Local Net Users.

**Step 6**  Click Go.

**Step 7**  Click OK in the dialog box to confirm the deletion.

Configuring AAA MAC Filtering

This page enables you to view MAC Filter information.

**Note**  You cannot use MAC address in the broadcast range.

To access the MAC Filtering page, follow these steps:

**Step 1**  Choose Configure > Controllers.

**Step 2**  Click the IP address of the applicable controller.

**Step 3**  From the left sidebar menu, choose Security > AAA > MAC Filtering. The MAC Filtering page displays the following parameters:

- **MAC Filter Parameters**
  - RADIUS Compatibility Mode—User-defined RADIUS server compatibility: Cisco ACS, FreeRADIUS, or Other.
  - MAC Delimiter—The MAC delimiters can be Colon (xx:xx:xx:xx:xx:xx), Hyphen (xx-xx-xx-xx-xx-xx), Single Hyphen (xxxxxx-xxxxxx), or No Delimiter (xxxxxxxxxxxx), as required by the RADIUS server.

- **MAC Filters**
  - MAC Address—Client MAC address. Click to open Configure IPaddr > MAC Filter.
  - WLAN ID—1 through 16, 17 = Third-party AP WLAN, or 0 = all WLANs.
Configuring Existing Controllers

Chapter 9 Configuring Devices

- Interface—Displays the associated Interface Name.
- Description—Displays an optional user-defined description.

**Step 4**
From the Select a command drop-down list, choose **Add MAC Filters** to add a MAC Filter, **Delete MAC Filters** to delete the template(s), or **Edit MAC Filter Parameters** to edit the MAC Filters.

**Step 5**
Click **Go**.

### Configuring AAA AP/MSE Authorization

The AP/MSE Authorization page displays the access point policies and the list of authorized access points along with the type of certificate that an access point uses for authorization.

**Note**
You cannot use MAC address in the broadcast range.

To access the AP/MSE Authorization page, follow these steps:

**Step 1**
Choose **Configure > Controllers**.

**Step 2**
Click the IP address of the applicable controller.

**Step 3**
From the left sidebar menu, choose **Security > AAA > AP/MSE Authorization**. The AP/MSE Authorization page displays the following parameters:

- **AP Policies**
  - Authorize APs—Enabled or Disabled.
  - Accept SSC-APs—Enabled or Disabled.
- **AP/MSE Authorization**
  - AP/MSE Base Radio MAC Address—The MAC address of the authorized access point.

**Note**
Click the AP/MSE Base Radio MAC Address to view AP/MSE Authorization details.

- Type
- Certificate Type—MIC or SSC.
- Key Hash—The 40-hex long SHA1 key hash.

**Note**
The key hash is displayed only if the certificate type is SSC.

### Command Buttons

- **Add AP/MSE Auth Entry**—Select this command, and click **Go**. See the “Configuring an Access Point or MSE Authorization Template” section on page 11-58.

- **Delete AP/MSE Auth Entries**—Select one or more access points, select this command, and click **Go** to delete the selected access point from the AP authorization list.
Configuring Devices

Chapter 9 Configuring Devices

Configuring Existing Controllers

• Edit AP Policies—Select this command, and click Go. See the “Editing AP Policies” section on page 9-99.

Editing AP Policies

To edit AP/MSE Authorization access point policies, follow these steps:

**Step 1** Choose Configure > Controllers.

**Step 2** Click the IP address of the applicable controller.

**Step 3** From the left sidebar menu, choose Security > AAA > AP/MSE Authorization.

**Step 4** In Edit AP Policies page, edit the following parameters, if necessary:
- Authorize APs—Select the check box to enable access point authorization.
- Accept SSC-APs—Select the check box to enable the acceptance of SSE access points.

**Step 5** Click Save to confirm the changes, Audit to perform an audit on these device values, or Cancel to close this page with no changes.

Configuring AAA Web Auth Configuration

The Web Auth Configuration page enables the user to configure the web auth configuration type. If the type is configured as customized, the user downloaded web auth replaces the controller-provided internal web auth page.

To access the Web Auth Configuration page, follow these steps:

**Step 1** Choose Configure > Controllers.

**Step 2** Click the IP address of the applicable controller.

**Step 3** From the left sidebar menu, choose Security > AAA > Web Auth Configuration.

**Step 4** In the Web Authentication page, choose the Web Auth Type from the drop-down list. Web auth options include a default internal web page, a customized web authentication page, or an external web page.

**Step 5** Configure the web auth parameters depending on the type chosen:
- Default Internal
  - Logo Display—Enable or disable logo display.
  - Web Auth Page Title—Title displayed on web authentication page.
  - Custom Redirect URL—URL where the user is redirected after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user is directed to the company home page.
- Customized Web Auth
  You have the option of downloading an example login page and customizing the page. If you are using a customized web authentication page, it is necessary to download the example login.tar bundle file from the server, edit the login.html file and save it as either a .tar or .zip file, then download the .tar or .zip file to the controller.
Click the preview image to download this sample login page as a TAR. After editing the HTML you might click here to redirect to the Download Web Auth page. See the “Downloading a Customized WebAuthentication Bundle to a Controller” section on page 9-15 for more information.

- **External**
  - **External Redirect URL**—Location of the login.html on an external server on the network.

    If there are not any external web auth servers configured, you have the option of configuring one.

    No external Web Auth Server(s) configured. Choose this option to configure external web auth servers.

    **Note** To configure an external web server template, see the “Configuring an External Web Auth Server Template” section on page 11-64.

### Command Buttons

- **Save**—Save the current settings to the controller.
- **Audit**—Check the present configuration status of the Prime Infrastructure and controller.

### Configuring AAA Password Policy

This page enables you to determine your password policy.

To make modifications to an existing password policy, follow these steps:

1. **Step 1** Choose **Configure > Controllers**.
2. **Step 2** Click the IP address of the applicable controller.
3. **Step 3** From the left sidebar menu, choose **Security > AAA > Password Policy**.
4. **Step 4** Modify the password policy parameters as appropriate.
5. **Step 5** Click **Save**.

    **Note** If you disable password policy options, you see a “Disabling the strong password check(s) will be a security risk as it allows weak passwords” message.

### Configuring Controllers > IPaddr > Security > Local EAP

Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down.

When you enable local EAP, the controller serves as the authentication server and the local user database, making it independent of an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users.
Configuring Local EAP General Parameters

This page allows you to specify a timeout value for local EAP. You can then add a template with this timeout value or make changes to an existing template.

**Note** If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to then reauthenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP.

To specify a timeout value for local EAP, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click the IP address of the applicable controller.

**Step 3** From the left sidebar menu, choose **Security > Local EAP > General - Local EAP**.

**Step 4** Enter the Local Auth Active Timeout in the Local Auth Active Timeout text box (in seconds).

**Note** Local Auth Active Timeout refers to the timeout period during which Local EAP is always used after all Radius servers are failed.

**Step 5** The following values should be adjusted if you are using EAP-FAST, manual password entry, one-time password, or 7920/7921 phones.

**Note** You must increase the 802.1x timeout values on the controller (default=2 seconds) for the client to obtain the PAC using automatic provisioning. We recommend the default timeout on the Cisco ACS server of 20 seconds.

- Local EAP Identify Request Timeout = 1 (in seconds)
- Local EAP Identity Request Maximum Retries = 20 (in seconds)
- Local EAP Dynamic Wep Key Index = 0
- Local EAP Request Timeout = 20 (in seconds)
- Local EAP Request Maximum Retries = 2
- EAPOL-Key Timeout = 1000 (in milli-seconds)
- EAPOL-Key Max Retries = 2
- Max-Login Ignore Identity Response

**Note** Roaming fails if these values are not set the same across multiple controllers.

**Step 6** Click **Save**.
Command Buttons

- **Save**—Click to save the current template.
- **Apply to Controllers**—Click to apply the current template to controllers. In the Apply to Controllers page, choose the applicable controllers, and click **OK**.
- **Delete**—Click to delete the current template. If the template is currently applied to controllers, click **OK** to confirm that you want to remove the template from the selected controllers to which it is applied.
- **Cancel**—Click to cancel the current template creation or changes to the current template.

Configuring Local EAP Profiles

This page allows you to apply a template for a local EAP profile or make modifications to an existing template.

**Note**
The LDAP backend database supports only these local EAP methods: EAP-TLS and EAP-FAST with certificates. LEAP and EAP-FAST with PACs are not supported for use with the LDAP backend database.

- **Viewing Existing Local EAP Profiles, page 9-102**
- **Adding a Local Net User, page 9-102**

Viewing Existing Local EAP Profiles

To view existing local EAP profiles, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click the IP address of the applicable controller.

**Step 3** From the left sidebar menu, choose **Security > Local EAP > Local EAP Profiles**. The Local EAP Profiles page displays the following parameters:

- **EAP Profile Name**—User-defined identification.
- **LEAP**—Authentication type that leverages Cisco Key Integrity Protocol (CKIP) and MMH message integrity check (MIC) for data protection. A username and password are used to perform mutual authentication with the RADIUS server through the access point.
- **EAP-FAST**—Authentication type (Flexible Authentication via Secure Tunneling) that uses a three-phased tunnel authentication process to provide advanced 802.1x EAP mutual authentication. A username, password, and PAC (protected access credential) are used to perform mutual authentication with the RADIUS server through the access point.
- **TLS**—Authentication type that uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It requires a client certificate for authentication.
- **PEAP**—Protected Extensible Authentication Protocol.

Adding a Local Net User

To add a local EAP profile, follow these steps:
Chapter 9 Configuring Devices

Configuring Existing Controllers

---

Step 1 Choose Configure > Controllers.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Local EAP > Local EAP Profile.

Step 4 From the Select a command drop-down list, choose Add Local EAP Profile to open the Local EAP Profile > Add From Template page.

Step 5 Choose a template from the Select a template to apply to this controller drop-down list.

Step 6 Click Apply.

Note To create a new template for local EAP profiles, choose Configure > Controller Templates > Security > Local EAP Profiles.

---

Configuring Local EAP General EAP-FAST Parameters

This authentication type (Flexible Authentication via Secure Tunneling) uses a three-phased tunnel authentication process to provide advanced 802.1x EAP mutual authentication. A username, password, and PAC are used to perform mutual authentication with the RADIUS server through the access point.

To set EAP-FAST Parameters, follow these steps:

---

Step 1 Choose Configure > Controllers.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Local EAP > EAP-FAST Parameters.

Step 4 Enter the following parameters:

- Time to live for the PAC—The number of days for the PAC to remain viable. The valid range is 1 to 1000 days; the default setting is ten days.
- Authority ID—The authority identifier of the local EAP-FAST server in hexadecimal characters. You can enter up to 32 hexadecimal characters but it must be an even number of characters.
- Authority Info—The authority identifier of the local EAP-FAST server in text format.
- Server Key—The key (in hexadecimal characters) used to encrypt and decrypt PACs.
- Confirm Server Key—Verify the correct Server Key by re-typing it.
- Anonymous Provision—Select the check box to enable anonymous provisioning.

Note This feature allows PACs to be sent automatically to clients that do not have one during PAC provisioning. If this feature is disabled, PACs must be manually provisioned.

Step 5 Click Save.
Configuring Local EAP General Network Users Priority

To specify the order that LDAP and local databases use to retrieve user credential information, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click the IP address of the applicable controller.
Step 3 From the left sidebar menu, choose Security > Local EAP > Network Users Priority.
Step 4 Use the left and right pointing arrows to include or exclude network credentials in the right-most list.
Step 5 Use the up and down buttons to determine the order credentials are attempted.
Step 6 Click Save.

Configuring User Login Policies

To configure the user login policies, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click the IP address of the applicable controller.
Step 3 From the left sidebar menu, choose Security > User Login Policies.
Step 4 Enter the maximum number of concurrent logins allowed for a single username.
Step 5 Click Save.

Managing Manually Disabled Clients

The Disabled Clients page enables you to view excluded (blacklisted) client information. Clients who fail to authenticate three times when attempting to associate are automatically blocked, or excluded, from further association attempts for an operator-defined timeout. After the Excluded timeout, the client is allowed to retry authentication until it associates or fails authentication and is excluded again.

Note You cannot use MAC address in the broadcast range.

To access the Manually Disabled Clients page, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click the IP address of the applicable controller.
Step 3 From the left sidebar menu, choose Security > Manually Disabled Clients. The Manually Disabled Clients page displays the following parameters:
   • MAC Address—Disabled Client MAC addresses. Click a list item to edit the disabled client description.
Manually Disabled Clients Select a command Drop-Down List Options

- **Add Manually Disabled Client**—Choose this option from the drop-down list, and click **Go**. See the “Configuring a Manually Disabled Client Template” section on page 11-58.
- **Delete Manually Disabled Clients**—Select the applicable controller check box, choose this option from the drop-down list, and click **Go**.

Configuring Access Control Lists

The Access Control Lists page displays access control lists (ACLs) available for this controller. It also enables you to add a new rule or edit an existing rule in an applied access control list.

To access the Access Control Lists page, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click the applicable IP address in the IP Address column.

**Step 3** From the left sidebar menu, choose **Security > Access Control Lists**.
- **Check box**—Use the check box to select one or more ACLs for deletion.
- **ACL Name**—User-defined name of this template. Click an ACL item to view its parameters. See the “Configuring IPaddr > Access Control List > listname Rules” section on page 9-105.

Configuring IPaddr > Access Control List > listname Rules

This page displays current access control list (ACL) rules applied to this access control list.

To access the Access Control Lists Rules page, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click the applicable IP address in the IP address column.

**Step 3** From the left sidebar menu, choose **Security > Access Control Lists**.

**Step 4** Click an ACL name.
- **Check box**—Select to delete access control list rules.
- **Seq#**—The operator can define up to 64 Rules for each ACL. The Rules for each ACL are listed in contiguous sequence from 1 to 64. That is, if Rules 1 through 4 are already defined and you add Rule 29, it is added as Rule 5.

**Note** If you add or change a Sequence number, operating system adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have Sequence numbers 1 through 7 defined and change number 7 to 5, operating system automatically reassigns Sequence 6 to 7 and Sequence 5 to 6.
• Action—Permit, Deny.
• Source IP/Mask—Source IP address and mask.
• Destination IP/Mask—Destination IP address and mask.
• Protocol—Protocol to use for this ACL:
  – Any—All protocols
  – TCP—Transmission Control Protocol
  – UDP—User Datagram Protocol
  – ICMP—Internet Control Message Protocol
  – ESP—IP Encapsulating Security Payload
  – AH—Authentication Header
  – GRE—Generic Routing Encapsulation
  – IP—Internet Protocol
  – Eth Over IP—Ethernet over Internet Protocol
  – Other Port OSPF—Open Shortest Path First
  – Other—Any other IANA protocol (http://www.iana.org/)
If TCP or UDP is selected, Source Port and Dest Port parameters appear:
  – Source Port—Source Port. Can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS SS, MS Dir Server, Other and Port Range.
  – Dest Port—Destination port. If TCP or UDP is selected, can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS SS, MS Dir Server, Other and Port Range.
• DSCP (Differentiated Services Code Point)—Any, or 0 through 255.

To add a new ACL rule, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click an applicable IP address.
Step 3 From the left sidebar menu, choose Security > Access Control Lists.
Step 4 Click an ACL name.
Step 5 Click an applicable Seq#, or choose Add New Rule to access this page.

Configuring FlexConnect Access Control Lists

The ACLs on FlexConnect provide a mechanism to cater to the need for access control at the FlexConnect access point for protection and integrity of locally switched data traffic from the access point.
• Adding a FlexConnect Access Control List, page 9-107
Adding a FlexConnect Access Control List

To add an Access Control List for FlexConnect access points, follow these steps:

1. Choose Configure > Controllers.
2. Click a controller IP address.
3. From the left sidebar menu, choose Security > FlexConnect ACLs.
4. From the Select a command drop-down list, choose Add FlexConnect ACLs.
5. Click Go.

Note: You cannot add a FlexConnect ACL if there is no template created. If you try to create an FlexConnect ACL when there are no templates available, you are redirected to the New Controller Templates page where you can create a template for FlexConnect ACL.

The FlexConnect ACLs Details page appears.

6. Choose a template from the drop-down list to apply to the controller, and click Apply.

The FlexConnect ACL that you created appears in Configure > Controllers > IP Address > Security > FlexConnect ACLs.

Deleting a FlexConnect Access Control List

To delete a FlexConnect ACL, follow these steps:

1. Choose Configure > Controllers.
2. Click a controller IP address.
3. From the left sidebar menu, choose Security > FlexConnect ACLs.
4. From the FlexConnect ACLs page, select one or more FlexConnect ACLs to delete.
5. From the Select a command drop-down list, choose Delete FlexConnect ACLs.
6. Click Go.

Configuring CPU Access Control Lists

Access control lists (ACLs) can be applied to the controller CPU to control traffic to the CPU.

The Access Control Lists Rules page displays the name of the CPU access control list template applied to the chosen controller.

To access the Access Control Lists Rules page, follow these steps:

1. Choose Configure > Controllers.
2. Click a controller IP address.
Configuring Existing Controllers

### Configuring Devices

**Step 3** From the left sidebar menu, choose **Security > CPU Access Control Lists**.

**Step 4** Select the **Enable CPU ACL** check box to enable the CPU ACL.

If this check box is selected, the following parameters are available:

- **ACL Name**—Choose the ACL to use from the ACL Name drop-down list.
- **CPU ACL Mode**—Choose which data traffic direction this CPU ACL list controls.

The choices include: **the wired side of the data traffic**, **the wireless side of the data traffic**, or **both wired and wireless**.

---

**Configuring the IDS Sensor List**

When the sensors identify an attack, they alert the controller to shun the offending client. When you add a new IDS (Intrusion Detection System) sensor, you register the controller with that IDS sensor so that the sensor can send shunned client reports to the controller. The controller also polls the sensor periodically.

To view IDS sensors, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click an applicable IP address.

**Step 3** From the left sidebar menu, choose **Security > IDS Sensor Lists**.

The IDS Sensor page lists all IDS sensors that have been configured for this controller. Click an IP address to view details for a specific IDS sensor.

---

**Configuring CA Certificates**

A CA certificate is a digital certificate issued by one certificate authority (CA) for another certification CA.

- **Importing a CA Certificate**, page 9-108
- **Pasting a CA Certificate Directly**, page 9-109

**Importing a CA Certificate**

To import a CA certificate from a file, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click an applicable IP address.

**Step 3** From the left sidebar menu, choose **Security > IP Sec Certificates > CA Certificate**.

**Step 4** Click **Browse** to navigate to the applicable certificate file.

**Step 5** Click **Open**.

**Step 6** Click **Save**.
Pasting a CA Certificate Directly

To paste a CA certificate directly, follow these steps:

**Step 1** Copy the CA certificate to your computer clipboard.
**Step 2** Choose **Configure > Controllers**.
**Step 3** Click an applicable IP address.
**Step 4** From the left sidebar menu, choose **Security > IP Sec Certificates > CA Certificate**.
**Step 5** Select the **Paste** check box.
**Step 6** Paste the certificate directly into the text box.
**Step 7** Click **Save**.

Configuring ID Certificates

This page lists the existing network ID certificates by certificate name. An ID certificate can be used by web server operators to ensure secure server operation.

- Importing an ID Certificate, page 9-109
- Pasting an ID Certificate, page 9-109

Importing an ID Certificate

To import an ID certificate from a file, follow these steps:

**Step 1** Choose **Configure > Controllers**.
**Step 2** Click an applicable IP address.
**Step 3** From the left sidebar menu, choose **Security > IP Sec Certificates > ID Certificate**.
**Step 4** From the Select a command drop-down list, choose **Add Certificate**.
**Step 5** Click **Go**.
**Step 6** Enter the Name and Password.
**Step 7** Click **Browse** to navigate to the applicable certificate file.
**Step 8** Click **Open**.
**Step 9** Click **Save**.

Pasting an ID Certificate

To paste an ID certificate directly, follow these steps:

**Step 1** Copy the ID certificate to your computer clipboard.
**Step 2** Choose **Configure > Controllers**.
**Step 3** Click an applicable IP address.
Configuring Existing Controllers

Step 4 From the left sidebar menu, choose Security > IP Sec Certificates > ID Certificate.

Step 5 From the Select a command drop-down list, choose Add Certificate.

Step 6 Click Go.

Step 7 Enter the Name and Password.

Step 8 Select the Paste check box.

Step 9 Paste the certificate directly into the text box.

Step 10 Click Save.

Note ID certificates are available only if the controller is running Cisco Unified Wireless Network Software Version 3.2 or higher.

Note To delete a certificate, select it, choose Delete Certificates from the Select a command drop-down list, and click Go.

Configuring Controllers > IPaddr > Security > Web Auth Certificate

This page enables you to download a web authorization certificate or regenerate the internally-generated web auth certificate.

To access the Web Auth Certificate page, follow these steps:

Step 1 Choose Configure > Controllers.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose Security > Web Auth Certificate.

Caution Each certificate has a variable-length embedded RSA Key. The RSA key can vary from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a certificate authority (such as the Microsoft CA), make sure the RSA key embedded in the certificate is at least 768 Bits.

- Download Web Auth Certificate—Click to access the Download Web Auth Certificate to Controller page. See the “Downloading Web Auth or Web Admin Certificate to the Controller” section on page 9-158 for additional information.

Command Buttons

- Regenerate Cert—Regenerate the internally-generated web auth certificate.

Configuring Wireless Protection Policies

This section describes the wireless protection policy configurations and contains the following topics:
Configuring Rogue Policies

This page enables you to set up policies for rogue access points.

To access the Rogue Policies page, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click an applicable IP address.

**Step 3** From the left sidebar menu, choose **Security > Wireless Protection Policies > Rogue Policies**. The following parameters appear:

- **Rogue Location Discovery Protocol**—RLDP determines whether or not the rogue is connected to the enterprise wired network. Choose one of the following from the drop-down list:
  - **Disable**—Disables RLDP on all access points. This is the default value.
  - **All APs**—Enables RLDP on all access points.
  - **Monitor Mode APs**—Enables RLDP only on access points in monitor mode.

**Note** Make sure that rogue detection is enabled on the desired access points. Rogue detection is enabled by default for all access points joined to a controller (except for OfficeExtend access points). However, in the Prime Infrastructure software Release 6.0 or later, you can enable or disable rogue detection for individual access points by selecting or unselecting the **Rogue Detection** check box in the Access Point Details page. See the “Configuring Access Points” section on page 9-171 for more information.

**Note** 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 a large number of rogue devices.

- **Rogue APs**
  - **Expiration Timeout for Rogue AP and Rogue Client Entries (seconds)**—Enter the number of seconds after which the rogue access point and client entries expire and are removed from the list.

  The valid range is 240 to 3600 seconds and the default value is 1200 seconds.

**Note** If a rogue access point or client entry times out, it is removed from the controller only if its rogue state is Alert or Threat for any classification type.
- Rogue Detection Report Interval—Enter the time interval in seconds at which the APs should send the rogue detection report to the controller. Valid range is 10 seconds to 300 seconds, and the default value is 10 seconds. This feature is applicable to APs that are in monitor mode only.

- Rogue Detection Minimum RSSI—Enter the minimum RSSI value that a rogue should have for the APs to detect and for the rogue entry to be created in the controller. Valid range is -70 dBm to -128 dBm, and the default value is -128 dBm. This feature is applicable to all the AP modes.

Note: There can be many rogues with very weak RSSI values that do not provide any valuable information in the rogue analysis. Therefore, you can use this option to filter the rogues by specifying the minimum RSSI value at which the APs should detect rogues.

- Rogue Detection Transient Interval—Enter the time interval at which a rogue has to be consistently scanned for by the AP after the first time the rogue is scanned. By entering the transient interval, you can control the time interval at which the AP should scan for rogues. The APs can filter the rogues based on their transient interval values. Valid range is between 120 seconds to 1800 seconds, and the default value is 0. This feature is applicable to APs that are in monitor mode only.

  - Rogue Clients
    - Validate rogue clients against AAA—Select the check box to use the AAA server or local database to validate if rogue clients are valid clients. The default value is unselected.
    - Detect and report Adhoc networks—Select the check box to enable ad-hoc rogue detection and reporting. The default value is selected.

Command Buttons

- Save—Save the changes made to the client exclusion policies and return to the previous page.
- Audit—Compare the Prime Infrastructure values with those used on the controller.

Configuring Rogue AP Rules

This page enables you to view and edit current Rogue AP Rules.

To access the Rogue AP Rules page, follow these steps:

Step 1 Choose Configure > Controllers.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose Security > Wireless Protection Policies > Rogue AP Rules. The Rogue AP Rules displays the Rogue AP Rules, the rule types (Malicious or Friendly), and the rule sequence.

Step 4 Click a Rogue AP Rule to view or edit its details. See the “Configuring a Rogue AP Rules Template” section on page 11-73 for more information.
Configuring Client Exclusion Policies

This page enables you to set, enable, or disable the client exclusion policies applied to the controller.

To access the Client Exclusion Policies page, follow these steps:

**Step 1** Choose Configure > Controllers.

**Step 2** Click an applicable IP address.

**Step 3** From the left sidebar menu, choose Security > Wireless Protection Policies > Client Exclusion Policies. The following parameters appear:

- Excessive 802.11a Association Failures—If enabled, clients are excluded on the sixth 802.11 association attempt, after five consecutive failures.
- Excessive 802.11a Authentication Failures—If enabled, clients are excluded on the sixth 802.11 authentication attempt, after five consecutive failures.
- Excessive 802.11x Authentication Failures—If enabled, clients are excluded on the fourth 802.1X authentication attempt, after three consecutive failures.
- Excessive 802.11 Web Authentication Failures—If enabled, clients are excluded on the fourth web authentication attempt, after three consecutive failures.
- IP Theft Or Reuse—If enabled, clients are excluded if the IP address is already assigned to another device.

**Step 4** Click Save to save the changes made to the client exclusion policies and return to the previous page or click Audit to compare the Prime Infrastructure values with those used on the controller.

Configuring IDS Signatures

You can configure IDS Signatures, or bit-pattern matching rules used to identify various types of attacks in incoming 802.11 packets, on the controller. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller. If an attack is detected, an appropriate mitigation action is initiated.

Cisco supports 17 standard signatures on the controller as shown on the Standard Signatures and Custom Signatures pages. For more information on these IDS Signatures, see the Cisco Prime Prime Infrastructure Configuration Guide.

- Configuring Controller Standard Signature Parameters, page 9-113
- Configuring Custom Signatures, page 9-117
- Configuring AP Authentication and MFP, page 9-118

Configuring Controller Standard Signature Parameters

The Standard Signature Parameters page shows the list of Cisco-supplied signatures that are currently on the controller.

- Downloading Signature Files, page 9-114
- Uploading Signature Files, page 9-115
Configuring Existing Controllers

To access the Standard Signatures page, follow these steps:

**Step 1** Choose **Configure > Controllers**.
**Step 2** Click an applicable IP address.
**Step 3** From the left sidebar menu, choose **Security > Wireless Protection Policies > Standard Signatures**.

This page displays the following parameters:

- Precedence—The order in which the controller performs the signature checks.
- Name—The type of attack the signature is trying to detect.
- Frame Type—Management or data frame type on which the signature is looking for a security attack.
- Action—What the controller is directed to do when the signature detects an attack. For example:
  - None—No action is taken.
  - Report—Report the detection.
- State—Enabled or Disabled.
- Description—A more detailed description of the type of attack the signature is trying to detect.

**Note** Click a signature Name to view individual parameters and to enable or disable the signature.

### Downloading Signature Files

To download a signature file, follow these steps:

**Step 1** Choose **Configure > Controllers**.
**Step 2** Click an applicable IP address.
**Step 3** From the left sidebar menu, choose **Security > Wireless Protection Policies > Standard Signatures** or **Security > Wireless Protection Policies > Custom Signatures**.
**Step 4** From the Select a command drop-down list, choose **Download Signature Files**.

**Note** This function can also be accessed by choosing **System > Commands > Upload/Download Commands > Download IDS Signatures**.

**Step 5** Click **Go**.
**Step 6** Copy the signature file (*.sig) to the default directory on your TFTP server.
**Step 7** Choose **Local Machine** from the File is Located On. If you know the filename and path relative to the server root directory, you can also choose **TFTP server**.
**Step 8** Enter the maximum number of times the controller should attempt to download the signature file in the **Maximum Retries**.
**Step 9** Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the **Timeout**.
Step 10 The signature files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click Browse to navigate to it. A "revision" line in the signature file specifies whether the file is a Cisco-provided standard signature file or a site-tailored custom signature file (custom signature files must always have revision=custom).

Note If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On field, and the server filename is populated for you and retried. The local machine option initiates a two-step operation. First, the local file is copied from the administrator workstation to Prime Infrastructure own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in the Prime Infrastructure server TFTP directory, and the downloaded web page now automatically populates the filename.

Step 11 Click OK.

Uploading Signature Files

To upload a signature file from the controller, follow these steps:

Step 1 Obtain a signature file from Cisco (hereafter called a standard signature file). You can also create your own signature file (hereafter called a custom signature file) by following the “Downloading Signature Files” section on page 9-114.

Step 2 Make sure you have a Trivial File Transfer Protocol (TFTP) server available for the signature download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port cannot be routed.
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port cannot be routed.
- A third-party TFTP server cannot run on the same computer as Prime Infrastructure because the Prime Infrastructure built-in TFTP server and third-party TFTP server use the same communication port.

Step 3 Choose Configure > Controllers.

Step 4 Click an applicable IP address.


Step 6 From the Select a command drop-down list, choose Upload Signature Files from controller.

Note This function can also be accessed by choosing Security > Custom Signatures > Select a command > Upload Signature Files from controller or System > Commands > Upload/Download Commands > Upload File from Controller.

Step 7 Specify the TFTP server name being used for the transfer.

Step 8 If the TFTP server is new, enter the TFTP IP address in the Server IP Address field.

Step 9 Choose Signature Files from the File Type drop-down list.
Step 10  The signature files are uploaded to the root directory which was configured for use by the TFTP server. You can change to a different directory at the Upload to File field (this field only shows if the Server Name is the default server). The controller uses this local filename as a base name and then adds _std.sig as a suffix for standard signature files and _custom.sig as a suffix for custom signature files.

Step 11  Click OK.

Global Settings for Standard and Custom Signatures

This command enables all signatures that were individually selected as enabled. If this text box remains unselected, all files are disabled, even those that were previously enabled. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller.

To enable all standard and custom signatures currently on the controller, follow these steps:

Step 1  From the Select a command drop-down list, choose Edit Signature Parameters.

Step 2  Click Go.

Step 3  Select the Enable Check for All Standard and Custom Signatures check box.

Step 4  Click Save.

To enable or disable an individual signature, follow these steps:

Step 1  Click an applicable Name for the type of attack you want to enable or disable.

The Standard Signature parameters page shows the list of Cisco-supplied signatures that are currently on the controller. The Custom Signatures page shows the list of customer-supplied signatures that are currently on the controller. The following parameters are displayed in both the signature page and the detailed signature page:

- Precedence—The order, or precedence, in which the controller performs the signature checks.
- Name—The type of attack the signature is trying to detect.
- Description—A more detailed description of the type of attack that the signature is trying to detect.
- Frame Type—Management or data frame type on which the signature is looking for a security attack.
- Action—What the controller is directed to do when the signature detects an attack. One possibility is None, where no action is taken, and another is Report, to report the detection.
- Frequency—The signature frequency or the number of matching packets per interval that must be identified at the detecting access point level before an attack is detected. The range is 1 to 32,000 packets per interval and the default value is 50 packets per interval.
- Quiet Time—The length of time (in seconds) after which no attacks have been detected at the individual access point level, and the alarm can stop. This time appears only if the MAC information is all or both. The range is 60 to 32,000 seconds and the default value is 300 seconds.
- MAC Information—Whether the signature is to be tracked per network or per MAC address or both at the detecting access point level.
• MAC Frequency—The signature MAC frequency or the number of matching packets per interval that must be identified at the controller level before an attack is detected. The range is 1 to 32,000 packets per interval and the default value is 30 packets per interval.

• Interval—Enter the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval. The range is 1 to 3600 seconds and the default value is 1 second.

• Enable—Select this check box to enable this signature to detect security attacks or unselect it to disable this signature.

• Signature Patterns—The pattern that is being used to detect a security attack.

**Step 2**
From the Enable drop-down list, choose Yes. Because you are downloading a customized signature, you should enable the files named with the _custom.sgi and disable the standard signature with the same name but differing suffix. For example, if you are customizing broadcast probe flood, you want to disable broadcast probe flood in the standard signatures but enable it in custom signatures.

**Step 3**
Click Save.

---

### Configuring Custom Signatures

The Custom Signature page shows the list of customer-supplied signatures that are currently on the controller.

For more information on Signatures, see the following sections:

- Downloading Signature Files, page 9-114
- Uploading Signature Files, page 9-115
- Global Settings for Standard and Custom Signatures, page 9-116

To access the Custom Signatures page, follow these steps:

**Step 1**
Choose Configure > Controllers.

**Step 2**
Click an applicable IP address.

**Step 3**
From the left sidebar menu, choose Security > Wireless Protection Policies > Custom Signatures. This page displays the following parameters:

- Precedence—The order in which the controller performs the signature checks.
- Name—The type of attack the signature is trying to detect.
- Frame Type—Management or data frame type on which the signature is looking for a security attack.
- Action—What the controller is directed to do when the signature detects an attack. For example:
  - None—No action is taken.
  - Report—Report the detection.
- State—Enabled or Disabled.
- Description—A more detailed description of the type of attack the signature is trying to detect.
Configuring AP Authentication and MFP

This page enables you to set the access point authentication policy.

To access the AP Authentication and MFP (Management Frame Protection) page, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click an applicable IP address.

**Step 3** From the left sidebar menu, choose **Security > Wireless Protection Policies > AP Authentication and MFP**.

This page displays the following fields:

- **RF Network Name**—Not an editable text box. The RF Network Name entered in the General parameters page (See Configure IPaddr > General) is displayed here.

- **Protection Type**—From the drop-down list, choose one of the following authentication policies:
  - **None**—No access point authentication policy.
  - **AP Authentication**—Apply authentication policy.
  - **MFP**—Apply Management Frame Protection. See the “Monitoring Management Frame Protection” section on page 5-19 for more information.

- **Alarm Trigger Threshold**—(Appears only when AP Authentication is selected as the Protection Type). Set the number of hits to be ignored from an alien access point before raising an alarm. The valid range is from 1 to 255. The default value is 255.

**Command Buttons**

- **Save**
- **Audit**

Configuring Cisco Access Points

You can use the Configure > Controllers page to view and configure Cisco access points for a specific controller.

To access the Cisco APs page, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click an applicable IP address.

**Step 3** From the left sidebar menu, choose **Access Points > Cisco APs**. The Cisco APs page opens and displays the following parameters:
Step 4 Click an access point name to view or configure the access point details. The displayed information might vary depending on the access point type.

Note See the “Configuring Access Points” section on page 9-171 for more detailed information.

Command Buttons

- Save—Save the current settings.
- Audit—Discover the present status of this access point.

Sniffer Feature

When the sniffer feature is enabled on an access point, the access point functions as a sniffer and captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek. The packets contain information on timestamp, signal strength, packet size, and so on.

Note The sniffer feature can be enabled only if you are running AiroPeek, which is a third-party network analyzer software that supports decoding of data packets. For more information on AiroPeek, see the following URL: www.wildpackets.com/products/airopeek/overview

Prerequisites for Using the Sniffer Feature

Before using the sniffer feature, you must complete the following:

- Configure an access point in sniffer mode at the remote site. For information on how to configure an access point in sniffer mode, see the “Configuring an AP in Sniffer Mode Using the Web User Interface” section on page 9-120.
- Install AiroPeek Version 2.05 or later on a Windows XP machine.

Note You must be a WildPackets Maintenance Member to download the following dll files. See the following URL:

https://wpdn.wildpackets.com/view_submission.php?id=30

- Copy the following dll files:
  - socket.dll file to the Plugins folder (Example: C:\ProgramFiles\WildPackets\AiroPeek\Plugins)
- socketres.dll file to the PluginRes folder
  (Example:C:\ProgramFiles\WildPackets\AiroPeek\1033\PluginRes)

**Configuring AiroPeek on the Remote Machine**

To configure AiroPeek on the remote machine, follow these steps:

**Step 1**
Start the AiroPeek application and click **Options** on the Tools tab.

**Step 2**
Click **Analysis Module** in the Options page.

**Step 3**
Right-click inside the page and select **Disable All** option.

**Step 4**
Find the Cisco remote module column and enable it. Click **OK** to save the changes.

**Step 5**
Click **New capture** to bring up the capture option page.

**Step 6**
Choose the remote Cisco adapter and from the list of adapter modules.

**Step 7**
Expand it to locate the new remote adapter option. Double-click it to open a new page, enter a name in the text box provided and enter the controller management interface IP in the IP address column.

**Step 8**
Click **OK**. The new adapter is added to the remote Cisco adapter.

**Step 9**
Select the new adapter for remote airopeek capture using the access point.

**Step 10**
Click **start socket capture** in the capture page to start the remote capture process.

**Step 11**
From the controller CLI, bring up an access point, and set it to sniffer mode by entering the `config ap mode sniffer ap-name` command.

The access point reboots and comes up in sniffer mode.

---

**Configuring an AP in Sniffer Mode Using the Web User Interface**

To configure an AP in Sniffer mode using the web user interface, follow these steps:

**Step 1**
Choose **Configure > Access Points**, then click an item in the AP Name column to navigate to this page.

**Step 2**
In the General group box, set the AP mode to Sniffer using the drop-down list, and click **Apply**.

**Step 3**
Click a protocol (802.11a/802.11b/g) in the Protocol column in the Radio Interfaces group box. This opens the configuration page.

**Step 4**
Select the **Sniff** check box to bring up the Sniff parameters. Select the channel to be sniffed and enter the IP address of the server (The remote machine running AiroPeek).

**Step 5**
Click **Save** to save the changes.

---

**Configuring 802.11 Parameters**

- Configuring General Parameters for an 802.11 Controller, page 9-121
- Configuring Security Parameters, page 9-90
- Configuring Aggressive Load Balancing, page 9-122
- Configuring Band Selection, page 9-123
Configuring General Parameters for an 802.11 Controller

This page enables you to edit country selection and timer information on a 802.11 controller. To access this page, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click an applicable IP address.

**Step 3** From the left sidebar menu, choose **802.11 > General**. The page opens and displays the following parameters:

- **Country**
  - **Country**—Countries and the protocols allowed.

  **Note** The maximum number of countries that you can select is 20.

  - **Selected Countries**—Displays countries currently selected.

- **Timers**
  - **Authentication Response Timeout**—Configures 802.11 authentication response timeout in seconds.

Setting Multiple Country Codes

To set multiple country support for a single controller(s) that is not part of a mobility group, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click the controller for which you are adding countries.

**Step 3** Choose **802.11 > General** from the left sidebar menu.

**Step 4** Select the check box to choose which country you want to add. Access points are designed for use in many countries with varying regulatory requirements. You can configure a country code to ensure that it complies with your country regulations.

  **Note** Access points might not operate properly if they are not designed for use in your country of operation. For example, an access point with part number AIR-AP1030-A-K9 (which is included in the Americas regulatory domain) cannot be used in Australia. Always be sure to purchase access points that match your country regulatory domain. For a complete list of country codes supported per product, see the following URL: [http://www.cisco.com/warp/public/779/smbiz/wireless/approvals.html](http://www.cisco.com/warp/public/779/smbiz/wireless/approvals.html)

**Step 5** Enter the time (in seconds) after which the authentication response times out.
Configuring Aggressive Load Balancing

Enabling aggressive load balancing on the controller allows lightweight access points to load balance wireless clients across access points.

### Note
Clients are load balanced between access points on the same controller. Load balancing does not occur between access points on different controllers.

When a wireless client attempts to associate to a lightweight access point, association response packets are sent to the client with an 802.11 response packet including status code 17. This code indicates whether the access point can accept any more associations. If the access point is too busy, the client attempts to associate to a different access point in the area. The system determines if an access point is relatively more busy than its neighbor access points that are also accessible to the client.

For example, if the number of clients on AP1 is more than the number of clients on AP2 plus the load-balancing window, then AP1 is considered to be busier than AP2. When a client attempts to associate to AP1, it 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 controller to deny client associations up to 10 times (if a client attempted to associate 11 times, it is 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).

To configure aggressive load balancing, follow these steps:

**Step 1**  Choose **Configure > Controllers**.

**Step 2**  Choose the controller that you need to configure.

**Step 3**  Choose **802.11 > Load Balancing** from the left sidebar menu. The Load Balancing page appears.

**Step 4**  Enter a value between 1 and 20 for the client window size. The page size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

\[
\text{load-balancing page + client associations on AP with lightest load} = \text{load-balancing threshold}
\]

In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client page size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.

**Step 5**  Enter a value between 0 and 10 for the max denial count. The denial count sets the maximum number of association denials during load balancing.

**Step 6**  Click **Save**.

**Step 7**  To enable or disable aggressive load balancing on specific WLANs, browse to the WLAN Configuration page, and click the **Advanced** tab. For instructions on using the WLAN Configuration page, see the “Configuring Controller WLANs” section on page 9-64.
Band selection enables client radios that are capable of dual-band (2.4- and 5-GHz) operation 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 three non-overlapping channels. To combat these sources of interference and improve overall network performance, you can configure band selection on the controller.

Band selection works by regulating probe responses to clients. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels.

You can enable band selection globally on a controller, or you can enable or disable band selection for a particular WLAN, which is useful if you want to disable it for a select group of clients (such as time-sensitive voice clients).

**Guidelines for Using Band Selection**

Follow these guidelines when using band selection:

- Band selection can be used only with Cisco Aironet 1140 and 1250 series access points.
- Band selection operates only on access points that are connected to a controller. A FlexConnect access point 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 access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.
- You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.

**Configuration Steps**

To configure band selection, follow these steps:

**Step 1** Choose Configure > Controllers.

**Step 2** Choose the controller that you need to configure.

**Step 3** Choose 802.11 > Band Select from the left sidebar menu. The Band Select page appears.

**Step 4** Enter a value between 1 and 10 for the probe cycle count. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.

**Step 5** 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 6** Enter a value between 10 and 200 seconds for the age out suppression field. Age-out suppression sets the expiration time for pruning previously known 802.11b/g clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.
Chapter 9  Configuring Devices

Configuring Existing Controllers

Step 7 Enter a value between 10 and 300 seconds for the age out dual band field. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 60 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 8 Enter a value between –20 and –90 dBm for the acceptable client RSSI field. This field sets the minimum RSSI for a client to respond to a probe. The default value is –80 dBm.

Step 9 Click Save.

Step 10 To enable or disable band selection on specific WLANs, browse to the WLAN Configuration page and click the Advanced tab. For instructions on using the WLAN Configuration page, see the “Configuring Controller WLANs” section on page 9-64.

Configuring Preferred Call

The Preferred Call feature enables you to specify highest priority to SIP calls made to some specific numbers. The high priority is achieved by allocating bandwidth to such preferred SIP Calls even when there is no available voice bandwidth in the configured Voice Pool. This feature is supported only for those clients that use SIP based CAC for bandwidth allocation in WCS or WLC.

Note You can configure up to 6 numbers per controller.

To configure the preferred call support, follow these steps:

Step 1 Choose Configure > Controllers.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose 802.11 > Preferred Call. The following fields appear if there is an existing preferred call:

- Description—Description for the preferred call.
- Number Id—Indicates the unique identifier for the controller and denotes one of the six preferred call numbers assigned to the controller.
- Preferred Number—Indicates the preferred call number.

Step 4 From the Select a command drop-down list, choose Add Number.

Step 5 Select a template to apply to this controller.

Note You need to select a template to apply to the selected controller. To create a New Template for Preferred Call Numbers, see the “Configuring Preferred Call Templates” section on page 11-79.

Step 6 Click Apply.
### Configuring 802.11 Media Parameters

To configure the media parameters for 802.11, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click the applicable IP address.

**Step 3** From the left sidebar menu, choose **802.11 > Media Stream**.

**Step 4** In the Media Stream Configuration section, configure the following parameters:
   - **Media Stream Name**
   - **Multicast Destination Start IP**—Start IP address of the media stream to be multicast
   - **Multicast Destination End IP**—End IP address of the media stream to be multicast
   - **Maximum Expected Bandwidth**—Maximum bandwidth that a media stream can use

**Step 5** In the Resource Reservation Control (RRC) Parameters group box, configure the following parameters:
   - **Average Packet Size**—Average packet size that a media stream can use.
   - **RRC Periodical Update**—Resource Reservation Control calculations that are updated periodically; if disabled, RRC calculations are done only once when a client joins a media stream.
   - **RRC Priority**—Priority of RRC with the highest at 1 and the lowest at 8.
   - **Traffic Profile Violation**—Appears if the stream is dropped or put in the best effort queue if the stream violates the QoS video profile.
   - **Policy**—Appears if the media stream is admitted or denied.

**Step 6** Click **Save**.

### Configuring RF Profiles (802.11)

The RF Profiles page enables you to create or modify RF profiles that get associated to AP Groups.

To configure a RF Profile for a controller, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click **RF Profiles** or choose either **802.11 > RF Profiles** from the left sidebar menu. The RF Profiles page appears. This page lists the existing RF Profile templates.

**Step 3** If you want to add a RF profile, choose **Add RF Profile** from the Select a command drop-down list.

**Step 4** Click **Go**. The New Controller Template page appears.

**Step 5** Configure the following information:
- **General**
  - Template Name—User-defined name for the template.
  - Profile Name—User-defined name for the current profile.
  - Description—Description of the template.
  - Radio Type—The radio type of the access point. This is a drop-down list from which you can choose an RF profile for APs with 802.11a or 802.11b radios.

- **TCP (Transmit Power Control)**
  - Minimum Power Level Assignment (-10 to 30 dBm)—Indicates the minimum power assigned. The range is -10 to 30 dB, and the default value is 30 dB.
  - Maximum Power Level Assignment (-10 to 30 dBm)—Indicates the maximum power assigned. The range is -10 to 30 dB, and the default value is 30 dB.
  - Power Threshold v1(-80 to -50 dBm)—Indicates the transmitted power threshold.
  - Power Threshold v2(-80 to -50 dBm)—Indicates the transmitted power threshold.

- **Data Rates**—Use the Data Rates drop-down lists to specify the rates at which data can be transmitted between the access point and the client. These data rates are available:
  - 802.11a—6, 9, 12, 18, 24, 36, 48, and 54 Mbps.
  - 802.11b/g—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps.
  For each data rate, choose one of these options:
  - Mandatory—Clients must support this data rate to associate to an access point on the controller.
  - Supported—Any associated clients that support this data rate might communicate with the access point using that rate. However, the clients are not required to be able to use this rate to associate.
  - Disabled—The clients specify the data rates used for communication.

---

**Configuring SIP Snooping**

Keep the following guidelines in mind when using SIP Snooping:

- SIPs are available only on the Cisco 5500 Series Controllers and on the 1240, 1130, and 11n access points.
- SIP CAC should only be used for phones that support status code 17 and do not support TSPEC-based admission control.
- SIP CAC will be supported only if SIP snooping is enabled.

To configure SIP Snooping for a controller, follow these steps:

---

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click the IP address of the applicable controller.

**Step 3** From the left sidebar menu, choose **802.11 > SIP Snooping**.

**Step 4** Configure the following fields:

- Port Start
Configuring 802.11a/n Parameters

- Configuring 802.11a/n General Parameters, page 9-127
- Configuring 802.11a/n 802.11h Parameters, page 9-136
- Configuring 802.11a/n RRM Intervals, page 9-129
- Configuring 802.11a/n RRM Transmit Power Control, page 9-130
- Configuring 802.11a/n RRM Dynamic Channel Allocation, page 9-131
- Configuring 802.11a/n RRM Radio Grouping, page 9-132
- Configuring 802.11a/n Media Parameters, page 9-132
- Configuring 802.11a/n EDCA Parameters, page 9-135
- Configuring 802.11a/n Roaming Parameters, page 9-135
- Configuring 802.11a/n 802.11h Parameters, page 9-136
- Configuring 802.11a/n High Throughput (802.11n) Parameters, page 9-137
- Configuring 802.11a/n CleanAir Parameters, page 9-137

Configuring 802.11a/n General Parameters

To view 802.11a/n parameters for a specific controller, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click an applicable IP address.
Step 3 From the left sidebar menu, choose 802.11a/n Parameters to view the following parameters:

- General
  - 802.11a/n Network Status—Select the check box to enable.
  - Beacon Period—The amount of time between beacons. The valid range is from 100 to 600 milliseconds.
  - DTIM Period—The number of beacon intervals that might elapse between transmission of beacon frames containing a traffic indicator message (TIM) element whose delivery count field is 0.
  - Fragmentation Threshold (in bytes)—The size at which packets are fragmented. Use a low setting in areas where communication is poor or where there is a great deal of radio interference.
  - Template Applied
- 802.11a/n Band Status
- Low, Medium, and High Bands (read-only).

- **802.11a/n Power Status**
  - Dynamic Assessment—Automatic, On Demand, or Disabled.
  - Current Tx Level—Range includes: 1 (maximum power allowed per country code setting), 2 (50% power), 3 (25% power), 4 (6.25 to 12.5% power), and 5 (0.195 to 6.25% power).

**Note** The power levels and available channels are defined by the country code setting and are regulated on a country by country basis.

- Control Interval—In seconds (read-only).
- Dynamic Treatment Power Control—Select the check box to enable.

- **802.11a/n Channel Status**
  - Assignment Mode—Automatic, On Demand, or Disabled.
  - Update Interval—In seconds.
  - Avoid Foreign AP Interference—Enable to have RRM consider interference from foreign Cisco access points (those non-Cisco access points outside RF/mobility domain) when assigning channels.
  - Avoid Cisco AP load—Enable to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points.
  - Avoid non 80.11 Noise—Enable to have access points avoid channels that have interference from non-access point sources, such as microwave ovens or Bluetooth devices. Disable this field to have RRM ignore this interference.
  - Signal Strength Contribution—Not configurable.
  - Avoid Persistent Non-WiFi interface

- **Data Rates**
  - Ranges between 6 Mbps and 54 Mbps—Supported, Mandatory, or Disabled.

- **Noise/Interference/Rogue Monitoring Channels.**
  - Channel List—All Channels, Country Channels, DCA Channels.

**Note** Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation from a set of managed devices connected to the controller.

- **CCX Location Measurement**—When enabled, it enhances the location accuracy of clients.
  - Mode—Select the check box to enable.
  - Interval—In seconds.

**Note** The CCX Location Measurement Interval can be changed only when measurement mode is enabled.
Command Buttons

- Save—Save the changes made.
- Audit—Compare the Prime Infrastructure values with those used on the controller.

Configuring 802.11a/n RRM Thresholds

To configure a 802.11a/n RRM threshold controller, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>Configure &gt; Controller</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click an applicable IP address.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the left sidebar menu, choose <strong>802.11a/n &gt; RRM Thresholds</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Make any necessary changes to Coverage Thresholds, Load Thresholds, Other Thresholds, and Noise/Interference/Rogue Monitoring Channels.</td>
</tr>
</tbody>
</table>

**Note** When the Coverage Thresholds Min SNR Level (dB) field is adjusted, the value of the Signal Strength (dB) automatically reflects this change. The Signal Strength (dB) field provides information regarding what the target range of coverage thresholds is when adjusting the SNR value.

| Step 5 | Click **Save**. |

Configuring 802.11a/n RRM Intervals

To configure 802.11a/n or 802.11b/g/n RRM intervals for an individual controller, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>Configure &gt; Controller</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click an applicable IP address.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the left sidebar menu, choose <strong>802.11a/n &gt; RRM Intervals</strong> or <strong>802.11b/g/n &gt; RRM Intervals</strong>.</td>
</tr>
</tbody>
</table>

**Note** The default for the following four RRM interval parameters is 300 seconds.

| Step 4 | Enter at which interval you want strength measurements taken for each access point. |
| Step 5 | Enter at which interval you want noise and interference measurements taken for each access point. |
| Step 6 | Enter at which interval you want load measurements taken for each access point. |
| Step 7 | Enter at which interval you want coverage measurements taken for each access point. |
| Step 8 | Click **Save**. |
Configuring 802.11a/n RRM Transmit Power Control

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the transmit power of the access point according to how the access points are seen by their third strongest neighbor.

The transmit power control (TPC) algorithm both increases and decreases the power of an access point in response to changes in the RF environment. In most instances, TPC seeks to lower the power of an access point 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 surrounding access points. This feature is different from Coverage Hole Detection. Coverage hole detection is primarily concerned with clients, while TPC is tasked with providing enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

Transmit Power Control version 2 (TPCv2) attempts to reduce the co-channel interference from Cisco AP networks. The former version of TPC is designed to provide strong signal coverage with a tendency to use larger Tx Power, and as a result customers were suffering from overheating in densely deployed networks.

To configure 802.11a/n or 802.11b/g/n RRM TPC, follow these steps:

**Step 1** Choose **Configure > Controller**.

**Step 2** Click an applicable IP address.

**Step 3** From the left sidebar menu, choose **802.11a/n-RRM > TPC**.

**Step 4** Configure the following TPC parameters:

- **Template Applied**—The name of the template applied to this controller.
- **Template Version**—Indicates the TPC version.
  
  The TPCv2 option is applicable only for those controllers running 7.2.x release or later.

- **Dynamic Assignment**—At the Dynamic Assignment drop-down list, choose one of three modes:
  - **Automatic** - The transmit power is periodically updated for all access points that permit this operation.
  - **On Demand** - Transmit power is updated when the Assign Now button is selected.
  - **Disabled** - No dynamic transmit power assignments occur, and values are set to their global default.

- **Maximum Power Assignment**—Indicates the maximum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB

- **Minimum Power Assignment**—Indicates the minimum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB

- **Dynamic Tx Power Control**—Determine if you want to enable Dynamic Tx Power Control.
- **Transmitted Power Threshold**—Enter a transmitted power threshold between -50 and -80.
- **Control Interval**—In seconds (read-only).
Configuring 802.11a/n RRM Dynamic Channel Allocation

The Radio Resource Management (RRM) Dynamic Channel Assignment (DCA) page allows you to choose the DCA channels as well as the channel width for this controller.

RRM DCA supports 802.11n 40-MHz channel width in the 5-GHz band. The higher bandwidth allows radios to achieve higher instantaneous data rates.

**Note** Choosing a larger bandwidth reduces the non-overlapping channels which could potentially reduce the overall network throughput for certain deployments.

To configure 802.11a/n RRM DCA channels for an individual controller, follow these steps:

**Step 1** Choose Configure > Controllers.

**Step 2** Click the IP address of the appropriate controller.

**Step 3** From the left sidebar menu, choose 802.11a/n > RRM DCA. The 802.11a/n RRM DCA page appears.

**Note** You can also configure the channel width on the access point page by choosing Configure > Access Points, and clicking the 802.11a/n link in the Radio column. The Current RF Channel Assignment is provided, and you can choose a Global assignment method or choose Custom to specify a channel.

**Step 4** From the Channel Width drop-down list, choose 20 MHz or 40 MHz. Prior to software release 5.1, 40-MHz channels were only statically configurable. Only radios with 20-MHz channels were supported by DCA. With 40 MHz, radios can achieve higher instantaneous data rates; however, larger bandwidths reduce the number of non-overlapping channels so certain deployments could have reduced overall network throughput.

**Note** Be cautious about deploying a mix of 20-MHz and 40-MHz devices. The 40-MHz devices have slightly different channel access rules which might negatively impact the 20-MHz devices.

**Note** To view the channel width for the radio of an access point, go to Monitor > Access Points > name > Interfaces tab. You can also view the channel width and antenna selections by choosing Configure > Access Points and clicking the desired radio in the Radio column.

**Step 5** Select the check boxes for the appropriate DCA channels. The selected channels are listed in the Selected DCA channels list.

**Step 6** Enable or disable event-driven Radio Resource Management (RRM) using the following parameters. Event Driven RRM is used when a CleanAir-enabled access point detects a significant level of interference.

- Event Driven RRM—Enable or Disable spectrum event-driven RRM. By default, Event Driven RRM is enabled.
Configuring Existing Controllers

- Sensitivity Threshold—If Event Driven RRM is enabled, this field displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

Step 7 Click Save.

Configuring 802.11a/n RRM Radio Grouping

To configure 802.11a/n or 802.11b/g/n RRM Radio Grouping for an individual controller, follow these steps:

Step 1 Choose Configure > Controller.
Step 2 Click an applicable IP address.
Step 3 From the left sidebar menu, choose 802.11a/n > RRM > RF Grouping.
Step 4 Choose a grouping mode from the drop-down list. The following parameters appear:
   - Automatic—Allows you to activate the automatic RRM Grouping Algorithm. This is the default mode.
   - Off—Allows you to deactivate the automatic grouping.
   - Leader—Allows you to assign members to the group.
Step 5 Choose a group update interval (secs) from the drop-down list. When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. The grouping algorithm also runs when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. Default value is 600 seconds.
Step 6 In the Group Members group box, click Add >. The selected controller moves from the Available Controllers to the RF Group Members list.

Note The RF Group Members group box appears only when the grouping mode is set to Leader.

Note The maximum number of controllers that can be added to a RF Group is 20.

Step 7 Click Save.

Configuring 802.11a/n Media Parameters

To configure the media parameters for 802.11a/n, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click the applicable IP address.
Step 3  From the left sidebar menu, choose 802.11a/n > Media Parameters.

Step 4  On the Voice tab, configure the following parameters:

- Admission Control (ACM)—Select the check box to enable admission control.

  For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, Call Admission Control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keep the maximum allowed number of calls to an acceptable quantity.

- CAC Method—If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static.

  Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

  In load-based CAC, the access point periodically measures and updates the utilization of the RF channel, channel interference, and the additional calls that the access point can admit. The access point admits a new call only if the channel has enough unused bandwidth to support that call. By doing so, load-based CAC prevents over-subscription of the channel and maintains QoS under all conditions of WLAN loading and interference.

- Maximum Bandwidth Allowed—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled. The valid range is 5 to 85.

- Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled. The valid range is 0 to 25.

- Expedited Bandwidth—Select the check box to enable expedited bandwidth as an extension of CAC for emergency calls.

  You must have an expedited bandwidth that is CCXv5 compliant so that a TSPEC request is given higher priority.

- SIP CAC—Select the check box to enable SIP CAC.

  SIP CAC should be used only for phones that support status code 17 and do not support TSPEC-based admission control.

- SIP Codec—Specify the codec name you want to use on this radio. The available options are G.711, G.729, and User Defined.

- SIP Call Bandwidth—Specify the bandwidth in kilobits per second that you want to assign per SIP call on the network. This field can be configured only when the SIP Codec selected is User Defined.

- SIP Sample Interval—Specify the sample interval in milliseconds that the codec must operate in.

- Max Voice Calls per Radio—Specify the maximum number of voice calls that can be made per Radio.

- Max Roaming Reserved Calls per Radio—Specify the maximum number of roaming calls that can be reserved per Radio.

  **Note**  The Max Voice Calls per Radio and Max Roaming Reserved Calls per Radio options are available only if the CAC Method is specified as Static and SIP CAC is enabled.

- Metric Collection—Select the check box to enable metric collection.
Traffic stream metrics are a series of statistics about VoIP over your wireless LAN which inform you of the QoS of the wireless LAN. For the access point to collect measurement values, traffic stream metrics must be enabled. When this is enabled, the controller begins collecting statistical data every 90 seconds for the 802.11b/g interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.

Step 5  On the Video tab, configure the following parameters:

- Admission Control (ACM)—Select the check box to enable admission control.
- Maximum Bandwidth Allowed—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled. For controller versions 6.0.188.0 and earlier, the valid range is 0 to 100. For controller versions 6.0.188.1 and later, the valid range is 5 to 85.
- Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled. The valid range is 0 to 25, and the default is 0.
- Static CAC method—From the SIP Codec drop-down list, choose one of the following options to set the CAC method. The default value is G.711. The options are as follows:
  - Load-Based
  - Static

  \[\text{Note}\]  Static CAC method is radio based and load-based CAC method is channel based

- SIP CAC—Select the SIP CAC check box to enable Static CAC support. By default, this check box is disabled.

  \[\text{Note}\]  SIP CAC will be supported only if SIP snooping is enabled.

- Unicast Video Redirect—Select the Unicast Video Redirect check box to enable all non-media stream packets in video queue are redirected to the best effort queue. If disabled, all packets with video marking are kept in video queue.
- Client Minimum Phy Rate—Choose the physical data rate required for the client to join a media stream from the Client Minimum Phy Rate drop-down list.
- Multicast Direct Enable—Select the Multicast Direct Enable check box to set the Media Direct for any WLAN with Media Direct enabled on a WLAN on this radio.
- Maximum Number of Streams per Radio—Specify the maximum number of streams per Radio to be allowed.
- Maximum Number of Streams per Client—Specify the maximum number of streams per Client to be allowed.
- Best Effort QOS Admission—Select the Best Effort QOS Admission check box to redirect new client requests to the best effort queue. This happens only if all the video bandwidth has been used.

  \[\text{Note}\]  If disabled and maximum video bandwidth has been used, then any new client request is rejected.

Step 6  On the General tab, configure the following field:

- Maximum Media Bandwidth (0 to 85%)—Specify the percentage of maximum of bandwidth allowed. This option is only available when CAC is enabled.

Step 7  Click Save.
SIPs are available only on the following controllers: 4400, 5500. Also, SIPs are available only for the following access points: 1240, 1130, and 11n.

Command Buttons

- Save—Save the changes made.
- Audit—Compare the Prime Infrastructure values with those used on the controller.

Configuring 802.11a/n EDCA Parameters

The EDCA parameters (EDCA profile and Streaming MAC Enable settings) for 802.11a/n and 802.11b/g/n can be configured either by individual controller or through a controller template to improve voice QoS support.

To configure 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller, follow these steps:

**Step 1** Choose Configure > Controllers.

**Step 2** Click an applicable IP address.

**Step 3** From the left sidebar menu, choose 802.11a/n > EDCA Parameters or 802.11b/g/n > EDCA Parameters.

**Step 4** Choose the EDCA Profile from the drop-down list.

**Note** Profiles include Wi-Fi Multimedia (WMM), Spectralink Voice Priority (SVP), Voice Optimized, and Voice & Video Optimized. WMM is the default EDCA profile.

**Note** You must shut down radio interface before configuring EDCA Parameters.

**Step 5** Select the Enable Streaming MAC check box to enable this feature.

**Note** Only enable Streaming MAC if all clients on the network are WMM compliant.

Configuring 802.11a/n Roaming Parameters

To configure 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller, follow these steps:

**Step 1** Choose Configure > Controllers.

**Step 2** Click an applicable IP address.

**Step 3** From the left sidebar menu, choose 802.11a/n > Roaming Parameters.

**Step 4** From the Mode drop-down list, choose Default values or Custom values.
Configuring Existing Controllers

Chapter 9 Configuring Devices

- Default values—The default values (read-only) are automatically displayed in the text boxes.
- Custom values—Activates the text boxes to enable editing of the roaming parameters.

**Step 5**  
In the Minimum RSSI text box, enter a value for the minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point.
- Range: -80 to -90 dBm
- Default: -85 dBm

**Note**  
If the client average received signal power dips below this threshold, reliable communication is typically impossible; clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.

**Step 6**  
In the Hysteresis text box, enter a value to indicate how strong the signal strength of a neighboring access point must for the client to roam to it.

This field is intended to reduce the amount of “ping ponging” between access points if the client is physically located on or near the border between two access points.
- Range: 2 to 4 dB
- Default: 3 dB

**Step 7**  
In the Adaptive Scan Threshold text box, enter the RSSI value, from a client associated access point, below which the client must be able to roam to a neighboring access point within the specified transition time.

This field provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold.
- Range: -70 to -77 dB
- Default: -72 dB

**Step 8**  
In the Transition Time text box, enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client associated access point is below the scan threshold.

The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.
- Range: 1 to 10 seconds
- Default: 5 seconds

**Step 9**  
Click **Save**.

**Configuring 802.11a/n 802.11h Parameters**

To configure 802.11h parameters for an individual controller, follow these steps:

**Step 1**  
Choose **Configure > Controller**.

**Step 2**  
Click an applicable IP address.
Step 3 From the left sidebar menu, choose 802.11a/n > 802.11h or 802.11b/g/n > 802.11h.

Step 4 Select the power constraint check box to enable TPC.

Step 5 Select the channel announcement check box to enable channel announcement. Channel announcement is a method in which the access point announces when it is switching to a new channel and the new channel number.

Step 6 Click Save.

### Configuring 802.11a/n High Throughput (802.11n) Parameters

To configure 802.11a/n or 802.11b/g/n high throughput parameters, follow these steps:

Step 1 Choose Configure > Controller.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose 802.11a/n > High Throughput or 802.11b/g/n > High Throughput.

Step 4 Select the 802.11n Network Status Enabled check box to enable high throughput.

Step 5 In the MCS (Data Rate) Settings, choose which level of data rate you want supported. MCS is modulation coding schemes which are similar to 802.11a data rate. As a default, 20 MHz and short guard interval is used.

*Note* When you select the Supported check box, the chosen numbers appear in the Selected MCS Indexes page.

Step 6 Click Save.

### Configuring 802.11a/n CleanAir Parameters

To configure 802.11a/n CleanAir parameters, follow these steps:

Step 1 Choose Configure > Controller.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose 802.11a/n > CleanAir to view the following information.

- CleanAir—Select the check box to enable CleanAir functionality on the 802.11 a/n network, or unselect to disable CleanAir functionality. The default value is selected.
- Reporting Configuration—Use the parameters in this section to configure the interferer devices you want to include for your reports.
  - Report—Select the report interferers check box to enable CleanAir system to report and detect sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is selected.
Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect text box and any that do not need to be detected appear in the Interferers to Ignore text box. Use the > and < buttons to move interference sources between these two text boxes. By default, all interference sources are detected.

Select the **Persistent Device Propagation** check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables designating information about interference types and propagating this information to the neighboring access points. Persistent interferers are present at the a location and interfere with the WLAN operations even if they are not detectable at all times.

- **Alarm Configuration**—This section enables you to configure triggering of air quality alarms.
  - **Air Quality Alarm**—Select the **Air Quality Alarm** check box to enable the triggering of air quality alarms, or unselect the box to disable this feature. The default value is selected.
  - **Air Quality Alarm Threshold**—If you selected the Air Quality Alarm check box, enter a value between 1 and 100 (inclusive) in the Air Quality Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.
  - **Air Quality Unclassified category Alarm**—Select the **Air Quality Unclassified category Alarm** check box to enable the alarms to be generated for unclassified interference category. CleanAir can detect and monitor unclassified interferences. Unclassified interference are interference that are detected but do not correspond to any of the known interference types.
    The Unclassified category alarm is generated when the unclassified severity goes above the configured threshold value for unclassified severity or when the air quality index goes below the configured threshold value for Air Quality Index.
  - **Air Quality Unclassified Category Severity Threshold**—If you selected the Air Quality Unclassified category Alarm check box, enter a value between 1 and 99 (inclusive) in the Air Quality Unclassified Severity Threshold text box to specify the threshold at which you want the unclassified category alarm to be triggered. The default is 20.
  - **Interferers For Security Alarm**—Select the **Interferers For Security Alarm** check box to trigger interferer alarms when the controller detects specified device types, or unselect it to disable this feature. The default value is selected.
    - Make sure that any sources of interference that need to trigger interferer alarms appear in the Interferers Selected for Security Alarms text box and any that do not need to trigger interferer alarms appear in the Interferers Ignored for Security Alarms text box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources trigger interferer alarms.

- **Event Driven RRM**—To trigger spectrum event-driven Radio Resource Management (RRM) to run when a CleanAir-enabled access point detects a significant level of interference, follow these steps:
  - **Event Driven RRM**—Displays the current status of spectrum event-driven RRM.
  - **Sensitivity Threshold**—If Event Driven RRM is enabled, this text box displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.
Command Buttons

- Save—Save the changes made.
- Audit—Compare the Prime Infrastructure values with those used on the controller.

Configuring 802.11b/g/n Parameters

- Configuring 802.11b/g/n General Parameters, page 9-139
- Configuring 802.11b/g/n RRM Thresholds, page 9-140
- Configuring 802.11b/g/n RRM Intervals, page 9-141
- Configuring 802.11b/g/n RRM Transmit Power Control, page 9-141
- Configuring 802.11b/g/n RRM DCA, page 9-142
- Configuring 802.11b/g/n RRM Radio Grouping, page 9-142
- Configuring 802.11b/g/n Media Parameters, page 9-143
- Configuring 802.11b/g/n EDCA Parameters, page 9-145
- Configuring 802.11b/g/n Roaming Parameters, page 9-146
- Configuring 802.11b/g/n High Throughput (802.11n) Parameters, page 9-147
- Configuring 802.11b/g/n CleanAir Parameters, page 9-147

Configuring 802.11b/g/n General Parameters

To view 802.11b/g/n parameters for a specific controller, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click an applicable IP address.
Step 3 From the left sidebar menu, choose 802.11b/g/n Parameters to view the following parameters:

- General
  - 802.11b/g Network Status—Select the check box to enable.
  - 802.11g Support—Select the check box to enable.
  - Beacon Period—in milliseconds.
  - DTIM Period—the number of beacon intervals that might elapse between transmission of beacon frames containing a traffic indicator message (TIM) element whose delivery count field is 0.
  - Fragmentation Threshold—in bytes.
  - Short Preamble—Select the check box to enable.
  - Template Applied.
- 802.11a/n Power Status
  - Dynamic Assessment—Automatic, On Demand, or Disabled.
  - Current Tx Level.
- Control Interval—In seconds (Read-only).
- Dynamic Treatment Power Control—Select the check box to enable.

- **802.11a/n Channel Status**
  - Assignment Mode—Automatic, On Demand, or Disabled.
  - Update Interval—In seconds.
  - Avoid Foreign AP Interference—Select the check box to enable.
  - Avoid Cisco AP load—Select the check box to enable.
  - Avoid non 802.11 Noise—Select the check box to enable.
  - Signal Strength Contribution—Select the check box to enable.

- **Data Rates**
  - Ranges between 1 Mbps and 54 Mbps—Supported, Mandatory, or Disabled.

- **Noise/Interference/Rogue Monitoring Channels**
  - Channel List—All Channels, Country Channels, DCA Channels.

- **CCX Location Measurement**
  - Mode—Select the check box to enable.
  - Interval—In seconds.

**Note** The CCX Location Measurement Interval can be changed only when measurement mode is enabled.

---

**Command Buttons**

- **Save**—Save the changes made.
- **Audit**—Compare the Prime Infrastructure values with those used on the controller.

---

**Configuring 802.11b/g/n RRM Thresholds**

To configure a 802.11b/g/n RRM threshold controller, follow these steps:

**Step 1** Choose **Configure > Controller**.

**Step 2** Click an applicable IP address.

**Step 3** From the left sidebar menu, choose **802.11b/g/n > RRM Thresholds**.

**Step 4** Make any necessary changes to Coverage Thresholds, Load Thresholds, Other Thresholds, and Noise/Interference/Rogue Monitoring Channels.

**Note** When the Coverage Thresholds Min SNR Level (dB) field is adjusted, the value of the Signal Strength (dB) automatically reflects this change. The Signal Strength (dB) field provides information regarding what the target range of coverage thresholds is when adjusting the SNR value.
Configuring Existing Controllers

Chapter 9      Configuring Devices

Configuring 802.11b/g/n RRM Intervals

To configure 802.11a/n or 802.11b/g/n RRM intervals for an individual controller, follow these steps:

Step 1 Choose Configure > Controller.
Step 2 Click an applicable IP address.
Step 3 From the left sidebar menu, choose 802.11a/n > RRM Intervals or 802.11b/g/n > RRM Intervals.

Note The default for the following four RRM interval parameters is 300 seconds.

Step 4 Enter at which interval you want strength measurements taken for each access point.
Step 5 Enter at which interval you want noise and interference measurements taken for each access point.
Step 6 Enter at which interval you want load measurements taken for each access point.
Step 7 Enter at which interval you want coverage measurements taken for each access point.
Step 8 Click Save.

Configuring 802.11b/g/n RRM Transmit Power Control

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the transmit power of an access point according to how the access points are seen by their third strongest neighbor.

The transmit power control (TPC) algorithm both increases and decreases the power of an access point in response to changes in the RF environment. In most instances, TPC seeks to lower the power of an access point 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 surrounding access points. This feature is different from Coverage Hole Detection. Coverage hole detection is primarily concerned with clients, while TPC is tasked with providing enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

To configure 802.11b/g/n RRM TPC, follow these steps:

Step 1 Choose Configure > Controller.
Step 2 Click an applicable IP address.
Step 3 From the left sidebar menu, choose 802.11b/g/n-RRM > TPC.
Step 4 Configure the following TPC parameters:
   • Template Applied—The name of the template applied to this controller.
   • Dynamic Assignment—At the Dynamic Assignment drop-down list, choose one of three modes:
     – Automatic—The transmit power is periodically updated for all access points that permit this operation.
Configuring Existing Controllers

Chapter 9 Configuring Devices

Step 5  On Demand—Transmit power is updated when the Assign Now button is selected.

Step 5  Disabled—No dynamic transmit power assignments occur, and values are set to their global default.

- Maximum Power Assignment—Indicates the maximum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB

- Minimum Power Assignment—Indicates the minimum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB

- Dynamic Tx Power Control—Determine if you want to enable Dynamic Tx Power Control.
- Transmitted Power Threshold—Enter a transmitted power threshold between -50 and -80.
- Control Interval—In seconds (read-only).

Step 5  Click Save.

Configuring 802.11b/g/n RRM DCA

To configure 802.11a/n or 802.11b/g/n RRM DCA channels for an individual controller, follow these steps:

Step 1  Choose Configure > Controller.

Step 2  Click an applicable IP address.

Step 3  From the left sidebar menu, choose 802.11b/g/n-RRM > DCA.

Step 4  Select the check box(es) for the applicable DCA channel(s). The selected channels are listed in the Selected DCA channels text box.

Step 5  Enable or disable event-driven Radio Resource Management (RRM). Event Driven RRM is used when a CleanAir-enabled access point detects a significant level of interference, follow these steps:
  - Event Driven RRM—Enable or Disable spectrum event-driven RRM. By default, Event Driven RRM is enabled.
  - Sensitivity Threshold—If Event Driven RRM is enabled, this text box displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

Step 6  Click Save.

Configuring 802.11b/g/n RRM Radio Grouping

To configure 802.11a/n or 802.11b/g/n RRM Radio Grouping for an individual controller, follow these steps:
Chapter 9  Configuring Devices

Configuring Existing Controllers

Step 1  Choose Configure > Controller.

Step 2  Click an applicable IP address.

Step 3  From the left sidebar menu, choose 802.11b/g/n > RRM > RF Grouping.

Step 4  Choose a grouping mode from the drop-down list. The following parameters appear:

- **Automatic**—Allows you to activate the automatic RRM Grouping Algorithm. This is the default mode.
- **Off**—Allows you to deactivate the automatic grouping.
- **Leader**—Allows you to assign members to the group.

Step 5  Choose a group update interval (secs) from the drop-down list. When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. Grouping algorithm also runs when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. The default value is 600 seconds.

Step 6  In the Group Members group box, click Add >. The selected controller moves from the Available Controllers to the RF Group Members list.

Note  The RF Group Members group box appears only when the grouping mode is set to Leader.

Note  The maximum number of controllers that can be added to a RF Group is 20.

Step 7  Click Save.

Configuring 802.11b/g/n Media Parameters

To configure the media parameters for 802.11b/g/n, follow these steps:

Step 1  Choose Configure > Controllers.

Step 2  Click the applicable IP address.

Step 3  From the left sidebar menu, choose 802.11b/g/n > Media Parameters.

Step 4  In the Voice tab, configure the following parameters:

- **Admission Control (ACM)**—Select the check box to enable admission control.
  
  For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, Call Admission Control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keep the maximum allowed number of calls to an acceptable quantity.

- **CAC Method**—If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static.

  Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.
In load-based CAC, the access point periodically measures and updates the utilization of the RF channel, channel interference, and the additional calls that the access point can admit. The access point admits a new call only if the channel has enough unused bandwidth to support that call. By doing so, load-based CAC prevents over-subscription of the channel and maintains QoS under all conditions of WLAN loading and interference.

- **Maximum Bandwidth Allowed**—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled. The valid range is 5 to 85.
- **Reserved Roaming Bandwidth**—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled. The valid range is 0 to 25.
- **Expedited Bandwidth**—Select the check box to enable expedited bandwidth as an extension of CAC for emergency calls.

You must have an expedited bandwidth that is CCXv5 compliant so that a TSPEC request is given higher priority.

- **SIP CAC**—Select the check box to enable SIP CAC.

SIP CAC should be used only for phones that support status code 17 and do not support TSPEC-based admission control.

- **SIP Codec**—Specify the codec name you want to use on this radio. The available options are G.711, G.729, and User Defined.

- **SIP Call Bandwidth**—Specify the bandwidth in kilobits per second that you want to assign per SIP call on the network. This field can be configured only when the SIP Codec selected is User Defined.

- **SIP Sample Interval**—Specify the sample interval in milliseconds that the codec must operate in.

- **Max Voice Calls per Radio**—Indicates the maximum number of voice calls that can be made per radio.

  **Note** You cannot set the value of Max Voice Calls per Radio. This is automatically calculated based on the selected CAC method, Max BW allowed, and Roaming Bandwidth.

- **Max Roaming Reserved Calls per Radio**—Indicates the maximum number roaming calls that can be reserved per radio.

  **Note** The Max Voice Calls per Radio and Max Roaming Reserved Calls per Radio options are available only if the CAC Method is specified as Static and SIP CAC is enabled.

- **Metric Collection**—Select the check box to enable metric collection.

Traffic stream metrics are a series of statistics about VoIP over your wireless LAN which inform you of the QoS of the wireless LAN. For the access point to collect measurement values, traffic stream metrics must be enabled. When this is enabled, the controller begins collecting statistical data every 90 seconds for the 802.11b/g interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.

**Step 5** In the **Video** tab, configure the following parameters:

- **Admission Control (ACM)**—Select the check box to enable admission control.

- **Maximum Bandwidth**—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled. For controller versions 6.0.188.0 and earlier, the valid range is 0 to 100. For controller versions 6.0.188.1 and later, the valid range is 5 to 85.
Chapter 9  Configuring Devices

Configuring Existing Controllers

- Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled. The valid range is 0 to 25.
- Unicast Video Redirect—Select the **Unicast Video Redirect** check box to enable all non-media stream packets in video queue are redirected to the best effort queue. If disabled, all packets with video marking are kept in video queue.
- Client Minimum Phy Rate—Specify the physical data rate required for the client to join a media stream from the **Client Minimum Phy Rate** drop-down list.
- Multicast Direct Enable—Select the **Multicast Direct Enable** check box to set the Media Direct for any WLAN with Media Direct enabled on a WLAN on this radio.
- Maximum Number of Streams per Radio—Specify the maximum number of streams per Radio to be allowed.
- Maximum Number of Streams per Client—Specify the maximum number of streams per Client to be allowed.
- Best Effort QOS Admission—Select the **Best Effort QOS Admission** check box to redirect new client requests to the best effort queue. This happens only if all the video bandwidth has been used.

**Note**

If disabled and maximum video bandwidth has been used, then any new client request is rejected.

**Step 6**

On the **General** tab, configure the following field:

- Maximum Media Bandwidth (0 to 85%)—Specify the percentage of maximum of bandwidth allowed. This option is only available when CAC is enabled.

**Step 7**

Click **Save**.

**Note**

SIPs are available only on the following controllers: 4400, 5500. Also, SIPs are available only for the following access points: 1240, 1130, and 11n.

**Command Buttons**

- **Save**—Save the changes made.
- **Audit**—Compare the Prime Infrastructure values with those used on the controller.

**Configuring 802.11b/g/n EDCA Parameters**

The EDCA parameters (EDCA profile and Streaming MAC Enable settings) for 802.11a/n and 802.11b/g/n can be configured either by individual controller or through a controller template to improve voice QoS support.

To configure 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller, follow these steps:

**Step 1**

Choose **Configure > Controllers**.

**Step 2**

Click an applicable IP address.

**Step 3**

From the left sidebar menu, choose **802.11a/n > EDCA Parameters** or **802.11b/g/n > EDCA Parameters**.
Step 4 Choose the EDCA Profile from the drop-down list.

Note Profiles include Wi-Fi Multimedia (WMM), Spectralink Voice Priority (SVP), Voice Optimized, and Voice & Video Optimized. WMM is the default EDCA profile.

Note You must shut down radio interface before configuring EDCA Parameters.

Step 5 Select the Enable Streaming MAC check box to enable this feature.

Note Only enable Streaming MAC if all clients on the network are WMM compliant.

Configuring 802.11b/g/n Roaming Parameters

To configure 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click an applicable IP address.
Step 3 From the left sidebar menu, choose 802.11a/n > Roaming Parameters or 802.11b/g/n > Roaming Parameters.
Step 4 From the Mode drop-down list, choose Default values or Custom values.
  • Default values—The default values (read-only) are automatically displayed in the text boxes.
  • Custom values—Activates the text boxes to enable editing of the roaming parameters.
Step 5 In the Minimum RSSI text box, enter a value for the minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point.
  • Range: -80 to -90 dBm
  • Default: -85 dBm
  
Note If the client average received signal power dips below this threshold, reliable communication is typically impossible; clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.

Step 6 In the Hysteresis text box, enter a value to indicate how strong the signal strength of a neighboring access point must be in order for the client to roam to it.
  This field is intended to reduce the amount of “ping ponging” between access points if the client is physically located on or near the border between two access points.
  • Range: 2 to 4 dB
  • Default: 3 dB

Step 7 In the Adaptive Scan Threshold text box, enter the RSSI value, from a client associated access point, below which the client must be able to roam to a neighboring access point within the specified transition time.
This field provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold.

- Range: -70 to -77 dB
- Default: -72 dB

**Step 8**

In the Transition Time text box, enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client associated access point is below the scan threshold.

The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

- Range: 1 to 10 seconds
- Default: 5 seconds

**Step 9**

Click **Save**.

### Configuring 802.11b/g/n High Throughput (802.11n) Parameters

To configure 802.11a/n or 802.11b/g/n high throughput parameters, follow these steps:

1. Choose **Configure > Controller**.
2. Click an applicable IP address.
3. From the left sidebar menu, choose **802.11a/n > High Throughput** or **802.11b/g/n > High Throughput**.
4. Select the **802.11n Network Status Enabled** check box to enable high throughput.
5. In the MCS (Data Rate) Settings, choose which level of data rate you want supported. MCS is modulation coding schemes which are similar to 802.11a data rate. As a default, 20 MHz and short guarded interval is used.

   **Note**
   
   When you select the Supported check box, the chosen numbers appear in the Selected MCS Indexes page.

6. Click **Save**.

### Configuring 802.11b/g/n CleanAir Parameters

To configure 802.11b/g/n CleanAir parameters, follow these steps:

1. Choose **Configure > Controller**.
2. Click an applicable IP address.
3. From the left sidebar menu, choose **802.11b/g/n > CleanAir** to view the following information.
• CleanAir—Select the check box to enable CleanAir functionality on the 802.11b/g/n network, or unselect to prevent the controller from detecting spectrum interference. The default value is selected.

• Reporting Configuration—Use the parameters in this section to configure the interferer devices you want to include for your reports.
  – Report—Select the report interferers check box to enable CleanAir system to report and detect sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is selected.
  – Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect text box and any that do not need to be detected appear in the Interferers to Ignore text box. Use the > and < buttons to move interference sources between these two text boxes. By default, all interference sources are detected.
  – Select the Persistent Device Propagation check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables designating information about interference types and propagating this information to the neighboring access points. Persistent interferers are present at a location and interfere with the WLAN operations even if they are not detectable at all times.

• Alarm Configuration—This group box enables you to configure triggering of air quality alarms.
  – Air Quality Alarm—Select the Air Quality Alarm check box to enable the triggering of air quality alarms, or unselect the text box to disable this feature. The default value is selected.
  – Air Quality Alarm Threshold—If you selected the Air Quality Alarm check box, enter a value between 1 and 100 (inclusive) in the Air Quality Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.
  – Air Quality Unclassified category Alarm—Select the Air Quality Unclassified category Alarm check box to enable the alarms to be generated for unclassified interference category. Cisco CleanAir can detect and monitor unclassified interferences. Unclassified interference are interference that are detected but do not correspond to any of the known interference types. The Unclassified category alarm is generated when the unclassified severity goes above the configured threshold value for unclassified severity or when the air quality index goes below the configured threshold value for Air Quality Index.
  – Air Quality Unclassified Category Severity Threshold—If you selected the Air Quality Unclassified category Alarm check box, enter a value between 1 and 99 (inclusive) in the Air Quality Unclassified Severity Threshold text box to specify the threshold at which you want the unclassified severity level to trigger the alarm. The default is 20.
  – Interferers For Security Alarm—Select the Interferers For Security Alarm check box to trigger interferer alarms when the controller detects specified device types, or unselect it to disable this feature. The default value is selected.
  – Make sure that any sources of interference that need to trigger interferer alarms appear in the Interferers Selected for Security Alarms text box and any that do not need to trigger interferer alarms appear in the Interferers Ignored for Security Alarms text box. Use the > and < buttons to move interference sources between these two text boxes. By default, all interference sources trigger interferer alarms.

• Event Driven RRM—To trigger spectrum event-driven Radio Resource Management (RRM) to run when a CleanAir-enabled access point detects a significant level of interference, use the following parameters:
– Event Driven RRM—Displays the current status of spectrum event-driven RRM.
– Sensitivity Threshold—If Event Driven RRM is enabled, this text box displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Allocation (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

Command Buttons

- Save—Save the changes made.
- Audit—Compare the Prime Infrastructure values with those used on the controller.

Configuring Mesh Parameters

To configure Mesh parameters for an individual controller, follow these steps:

Step 1
Choose Configure > Controller.

Step 2
Click an applicable IP address.

Step 3
From the left sidebar menu, choose Mesh > Mesh Settings.

Step 4
View or edit the following mesh parameters:

- RootAP to MeshAP Range (150 - 13200 ft)—By default, this value is 12,000 feet. You can enter a value between 150 and 132,000 feet. Enter the optimum distance (in feet) that should exist between the root access point and the mesh access point. This global field applies to all access points when they join the controller and all existing access points in the network.

- Client Access on Backhaul Link—Enabling this feature lets mesh access points associate with 802.11a wireless clients over the 802.11a backhaul. This client association is in addition to the existing communication on the 802.11a backhaul between the root and mesh access points. This feature is only applicable to access points with two radios. For more information, see the “Client Access on 1524SB Dual Backhaul” section on page 9-150.

  Note
Changing Backhaul Client Access reboots all mesh access points.

- Mesh DCA Channels—Enable or disable. This option is disabled by default. Enable this option to enable backhaul channel deselection on the controller using the DCA channel list. Any change to the channels in the Controller DCA list is pushed to the associated access points. This option is only applicable for 1524SB mesh access points. For more information on this feature, see the “Backhaul Channel Deselection Using the Prime Infrastructure” section on page 9-151.

- Background Scanning—Select the Background Scanning check box to enable background scanning or unselect it to disable the feature. The default value is disabled. Background scanning allows Cisco Aironet 1510 Access Points to actively and continuously monitor neighboring channels for more optimal paths and parents.

- Security Mode—Choose EAP (Extensible Authentication Protocol) or PSK (Pre-Shared Key) from the Security Mode drop-down list.
Chapter 9  Configuring Devices

Configuring Existing Controllers

Note  Changing Security reboots all mesh access points.

Step 5  Click Save.

Client Access on 1524SB Dual Backhaul

The 1524 Serial Backhaul (SB) access point consists of three radio slots. Radio in slot-0 operate in 2.4 GHz frequency band which is used for client access. Radios in slot-1 and slot-2 operate in 5.8 GHz band and are primarily used for backhaul. However, with the Universal Client Access feature, client access is also allowed over slot-1 and slot-2 radios.

The two 802.11a backhaul radios use the same MAC address. There might be instances where the same WLAN maps to the same BSSID in more than one slot.

By default, client access is disabled over both of the backhaul radios.

The following guidelines should be followed for enabling or disabling a radio slot:

- You can enable client access on slot-1 even if client access on slot-2 is disabled.
- You can enable client access on slot-2 only when client access on slot-1 is enabled.
- If you disable client access on slot-1 the client access on slot-2 is automatically disabled.
- All the Mesh Access Points reboot whenever the client access is enabled or disabled.

You can configure client access over backhaul radio from either one of the following:

- The Controller command-line interface (CLI)
- The Controller Graphical User Interface (GUI)
- Prime Infrastructure GUI. For more information, see the “Configuring Client Access Using the Prime Infrastructure - GUI” section on page 9-150.

Note  The procedure for configuring client access using the CLI and GUI is documented in the Controller Configuration Guide.

Configuring Client Access Using the Prime Infrastructure - GUI

To configure client access on the two backhaul radios, follow these steps:

Step 1  Choose Configure > Controllers > Controller IP > Mesh > Mesh Settings.

Step 2  Select the Client Access on Backhaul Link check box.

Step 3  Select the Extended Backhaul Client Access check box if you want to enable extended backhaul client access.

Step 4  Click Save.

A warning message is displayed:

Enabling client access on both backhaul slots will use same BSSIDs on both the slots. Changing Backhaul Client Access will reboot all Mesh APs.

Step 5  Click OK.
The Universal Client access is configured on both the radios.

### Backhaul Channel Deselection Using the Prime Infrastructure

To configure backhaul channel deselection, follow these steps:

**Step 1** You must first configure the Mesh DCA channels flag on the controllers. See the "Configuring Mesh DCA Channel Flag on Controllers Using the Prime Infrastructure" section on page 9-151 for more information.

**Step 2** Then change the channel list using config groups. See the "Changing the Channel List Using Config Groups" section on page 9-151 for more information.

- Configuring Mesh DCA Channel Flag on Controllers Using the Prime Infrastructure, page 9-151
- Changing the Channel List Using Config Groups, page 9-151

### Configuring Mesh DCA Channel Flag on Controllers Using the Prime Infrastructure

You can configure the Mesh DCA Channel flag to push each channel change on one or more controllers to all the associated 1524SB access points. To configure this feature, follow these steps:

**Step 1** Choose Configure > Controllers > ip address of controller > Mesh > Mesh Settings to configure this flag for a specific controller.

Or

Configure > Controller Template Launch Pad > Mesh > Mesh Settings to configure this flag for a list of controllers.

The Mesh Settings page appears.

**Step 2** From the general options select the Mesh DCA Channels option to enable channel selection. This option is unselected by default.

Now the channel changes in the controllers are pushed to the associated 1524SB access points.

### Changing the Channel List Using Config Groups

You can use controller config groups to configure backhaul channel deselection. You can create a config group and add the required controllers into the group and use the Country/DCA tab to select or deselect channels for the controllers in that group.

To configure backhaul channel deselection using config groups, follow these steps:

**Step 1** Choose Configure > Controller Config Groups.

**Step 2** Select a config group to view its config group details.

**Step 3** From the Config Group detail page, click the Country/DCA tab.
Configuring Existing Controllers

Chapter 9 Configuring Devices

Step 4 Select or unselect the channels for the config group.

*Note*
You can also configure backhaul channel deselection from controllers. For more information, see the Controller Online Help or Controller User Guide.

Configuring Port Parameters

To configure Port parameters for an individual controller, follow these steps:

**Step 1** Choose Configure > Controller.
**Step 2** Click an applicable IP address.
**Step 3** From the left sidebar menu, choose Ports > Port Settings.
**Step 4** Click the applicable Port Number to open the Port Settings Details page. The following parameters display:

- **General Parameters:**
  - Port Number—Read-only.
  - Admin Status—Choose Enabled or Disabled from the drop-down list.
  - Physical Mode—Choose Auto Negotiate or Full Duplex 1 Gbps.
  - STP Mode—Choose 802.1D, Fast, or Off.
  - Mirror Mode—Choose Enabled or Disabled.
  - Link Traps—Choose Enabled or Disabled.
  - Power Over Ethernet
  - Multicast Application Mode—Select Enabled or Disabled.

- **Spanning Tree Protocol Parameters:**
  - Priority—The numerical priority number of the ideal switch.
  - Path Cost—A value (typically based on hop count, media bandwidth, or other measures) assigned by a network administrator and used to determine the most favorable through an internetwork environment (the lower the cost, the better the path).

**Step 5** Choose Save or Audit for General or Spanning Tree Protocol settings.

Configuring Controllers Management Parameters

- Configuring Trap Receivers, page 9-153
- Configuring Trap Control Parameters, page 9-154
- Configuring Telnet SSH Parameters, page 9-155
- Configuring a Syslog for an Individual Controller, page 9-156
- Configuring Multiple Syslog Servers, page 9-157
Configuring Trap Receivers

- Configuring Trap Receivers for an Individual Controller, page 9-153
- Adding a New Receiver, page 9-153

Configuring Trap Receivers for an Individual Controller

To configure trap receivers for an individual controller, follow these steps:

**Step 1** Choose Configure > Controller.

**Step 2** Click an applicable IP address.

**Step 3** From the left sidebar menu, choose Management > Trap Receivers.

**Step 4** The following parameters are displayed for current trap receivers:

- Template Name—User-defined name of this template.
- IP Address—The IP address of the server.
- Admin Status—Status must be enabled for the SNMP traps to be sent to the receiver.

**Step 5** Click a receiver Name to access its details.

**Step 6** Select the Admin Status check box to enable the trap receiver. Unselect the check box to disable the trap receiver.

**Step 7** Click Save.

Adding a New Receiver

To add a new receiver, follow these steps:

**Step 1** From the Select a command drop-down list, choose Add Receiver.

**Step 2** Click Go.

**Step 3** From the Select a template to apply to this controller drop-down list, choose the applicable template to apply to this controller.

**Note** To create a new template for Trap Receivers, use the click here link to access the applicable template creation page.

**Step 4** Click Apply.
Configuring Trap Control Parameters

To configure trap control parameters for an individual controller, follow these steps:

**Step 1** Choose **Configure > Controller**.

**Step 2** Click an applicable IP address.

**Step 3** From the left sidebar menu, choose **Management > Trap Control**.

The applied template is identified (if applicable). See the “Configuring Trap Control Templates” section on page 11-111 for more information.

The following traps can be enabled for this controller:

- **Miscellaneous Traps**
  - **SNMP Authentication**—The SNMPv2 entity has received a protocol message that is not properly authenticated.
  
  **Note** When a user who is configured in SNMP V3 mode tries to access the controller with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.
  
  - **Link (Port) Up/Down**—Link changes status from up or down.
  - **Multiple Users**—Two users login with the same login ID.
  - **Spanning Tree**—Spanning Tree traps. See the STP specifications for descriptions of individual parameters.
  - **Rogue AP**—Whenever a rogue access point is detected this trap is sent with its MAC address; When a rogue access point that was detected earlier and it no longer exists this trap is sent.
  - **Config Save**—Notification sent when the controller configuration is modified.

- **Client Related Traps**
  - **802.11 Association**—The associate notification is sent when the client sends an association frame.
  - **802.11 Disassociation**—The disassociate notification is sent when the client sends a disassociation frame.
  - **802.11 Deauthentication**—The deauthenticate notification is sent when the client sends a deauthentication frame.
  - **802.11 Failed Authentication**—The authenticate failure notification is sent when the client sends an authentication frame with a status code other than 'successful'.
  - **802.11 Failed Association**—The associate failure notification is sent when the client sends an association frame with a status code other than 'successful'.
  - **Excluded**—The associate failure notification is sent when a client is excluded.

- **Cisco AP Traps**
  - **AP Register**—Notification sent when an access point associates or disassociates with the controller.
  - **AP Interface Up/Down**—Notification sent when access point interface (802.11a or 802.11b/g) status goes up or down.

- **Auto RF Profile Traps**
• Load Profile—Notification sent when Load Profile state changes between PASS and FAIL.
• Noise Profile—Notification sent when Noise Profile state changes between PASS and FAIL.
• Interference Profile—Notification sent when Interference Profile state changes between PASS and FAIL.
• Coverage Profile—Notification sent when Coverage Profile state changes between PASS and FAIL.
• Auto RF Update Traps
  – Channel Update—Notification sent when access point dynamic channel algorithm is updated.
  – Tx Power Update—Notification sent when access point dynamic transmit power algorithm is updated.
• AAA Traps
  – User Auth Failure—This trap is to inform that a client RADIUS Authentication failure has occurred.
  – RADIUS Server No Response—This trap is to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.
• IP Security Traps
  – ESP Authentication Failure—IPsec packets with invalid hashes were found in an inbound ESP SA.
  – ESP Replay Failure—IPsec packets with invalid sequence numbers were found in an inbound ESP SA.
  – Invalid SPI—A packet with an unknown SPI was detected from the specified peer with the specified SPI using the specified protocol.
  – IKE Negotiation Failure—An attempt to negotiate a phase 1 IKE SA failed. The notification counts are also sent as part of the trap, along with the current value of the total negotiation error counters.
  – IKE Suite Failure—An attempt to negotiate a phase 2 SA suite for the specified selector failed. The current total failure counts are passed as well as the notification type counts for the notify involved in the failure.
  – Invalid Cookie—ISAKMP packets with invalid cookies were detected from the specified source, intended for the specified destination. The initiator and responder cookies are also sent with the trap.
• 802.11 Security Traps
  – WEP Decrypt Error—Notification sent when the controller detects a WEP decrypting error.
• WPS Traps
  – Rogue Auto Containment—Notification sent when a rogue access point is auto-contained.

Step 4 After selecting the applicable parameters, click Save.

Configuring Telnet SSH Parameters

To configure Telnet SSH (Secure Shell) parameters for an individual controller, follow these steps:
Configuring Existing Controllers

Chapter 9  Configuring Devices

Step 1 Choose Configure > Controller.
Step 2 Click an applicable IP address.
Step 3 From the left sidebar menu, choose Management > Telnet SSH.

The applied template is identified (if applicable). See the “Configuring Telnet SSH Templates” section on page 11-113 for more information.

The following parameters can be configured:

- Session Timeout—Indicates the number of minutes a Telnet session is allowed to remain inactive before being logged off. A zero means there is no timeout. Might be specified as a number from 0 to 160. The factory default is 5.
- Maximum Sessions—From the drop-down list, choose a value from 0 to 5. This object indicates the number of simultaneous Telnet sessions allowed.

Note New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the Service port.

- Allow New Telnet Sessions—Indicates that new Telnet sessions are not allowed on the DS Port when set to no. The factory default value is no.

Note New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the Service port.

- Allow New SSH Sessions—Indicates that new Secure Shell Telnet sessions are not allowed when set to no. The factory default value is yes.

Step 4 After configuring the applicable parameters, click Save.

Configuring a Syslog for an Individual Controller

To enable a Syslog for an individual controller, follow these steps:

Step 1 Choose Configure > Controller.
Step 2 Click an applicable IP address.
Step 3 From the left sidebar menu, choose Management > Syslog.

The applied template is identified (if applicable). See the “Configuring Legacy Syslog Templates” section on page 11-114 for more information.

- Syslog Enabled—Select the check box to enable the syslog.

Step 4 Click Save.
Configuring Multiple Syslog Servers

For Release 5.0.148.0 controllers or later, you can configure multiple (up to three) syslog servers on the WLAN controller. With each message logged, the controller sends a copy of the message to each configured syslog host, provided the message has severity greater than or equal to the configured syslog filter severity level.

To enable syslogs for an individual controller, follow these steps:

Step 1  Choose Configure > Controller.
Step 2  Click an applicable IP address.
Step 3  From the left sidebar menu, choose Management > Multiple Syslog.
         The applied template is identified:
         Syslog Server Address—Indicates the server address of the applicable syslog.
Step 4  Click Save.

Configuring WEB Admin

This section provides instructions for enabling the distribution system port as a web port (using HTTP) or as a secure web port (using HTTPS). You can protect communication with the GUI by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Sockets Layer (SSL) protocol. When you enable HTTPS, the controller generates its own local web administration SSL certificate and automatically applies it to the GUI. You also have the option of downloading an externally generated certificate.

To enable WEB admin parameters for an individual controller, follow these steps:

Step 1  Choose Configure > Controller.
Step 2  Click an applicable IP address.
Step 3  From the left sidebar menu, choose Management > Web Admin.
         The following parameters can be configured:
         • Web Mode—Choose Enable or Disable from the drop-down list. When enabled, users can access
           the controller GUI using http://ip-address. The default is Disabled.

           Note  Web mode is not a secure connection.
         • Secure Web Mode—Choose Enable or Disable from the drop-down list. When enabled, users can
           access the controller GUI using https://ip-address. The default is Enabled.

           Note  Secure web mode is a secure connection.
         • Certificate Type
         • Download Web Admin Certificate—Click to access the Download Web Admin Certificate to
           Controller page. See the “Downloading Web Auth or Web Admin Certificate to the Controller”
           section on page 9-158 for additional information.
The controller must be rebooted for the new Web Admin certificate to take effect.

Command Buttons

- Save
- Audit
- Regenerate Cert

Downloading Web Auth or Web Admin Certificate to the Controller

To download a Web Auth or Web Admin Certificate to the controller, follow these steps:

Step 1 Click the Download Web Admin Certificate or Download Web Auth Certificate link.
Step 2 In the File is located on field, specify Local machine or TFTP server.

Note If the certificate is located on the TFTP server, enter the server filename. If it is located on the local machine, click Browse and enter the local filename.

Step 3 Enter the TFTP server name in the Server Name text box. The default is the Prime Infrastructure server.
Step 4 Enter the server IP address.
Step 5 In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.
Step 6 In the Timeout text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.
Step 7 In the Local File Name text box, enter the directory path of the certificate.
Step 8 In the Server File Name text box, enter the name of the certificate.
Step 9 Enter the password in the Password text box.
Step 10 Click OK.

Configuring Local Management Users

This page lists the names and access privileges of the local management users.

To access the Local Management Users page, follow these steps:

Step 1 Choose Configure > Controllers.
Step 2 Click an applicable IP address.
Step 3 From the left sidebar menu, choose Management > Local Management Users.
Step 4 Click a username.
Configuring Authentication Priority

In this page, you can control the order in which authentication servers are used to authenticate a controller management users.

To access the Authentication Priority page, follow these steps:

1. Choose Configure > Controllers.
2. Click an applicable IP address.
3. From the left sidebar menu, choose Management > Authentication Priority.
4. The local database is searched first. Choose either RADIUS or TACACS+ for the next search. If authentication using the local database fails, the controller uses the next type of server.
5. Click Save.

Command Buttons

- Save—Save the changes made to the management user authentication order and return to the previous page.
- Audit—Compare the Prime Infrastructure values with those used on the controller.

Configuring Location Configurations

Currently WiFi clients are moving towards lesser probing to discover an AP. Smartphones do this to conserve battery power. The applications on a smartphone have difficulty generating probe request but can easily generate data packets and hence trigger enhanced location for the application. FastLocate feature enhances the location performance through data packet RSSI reported through the WSSI module in monitor mode. This is accomplished by using the WSSI modules on the AP to monitor all traffic coming from a client. This not only increases the efficiency of monitoring such device packets to improve the location updates from the given client, but also does this with minimal impact on the client’s battery life. Enabling this feature will increase the update rate of location of all associated clients, and will have limited improvement on the update rate of unassociated clients.

In the Location Configuration page, you can configuration location parameters such as expiration times, notification interval, and other advanced configuration options.

You can set the following general and advanced parameters on the location template:

- General parameters—Enable RFID tag collection, set the location path loss for calibrating or normal (non-calibrating) clients, measurement notification for clients, tags, and rogue access points, set the RSSI expiry timeout value for clients, tags, and rogue access points.
- Advanced parameters—Set the RFID tag data timeout value, enable the location path loss configuration for calibrating client multi-band and set the FastLocate configuration.

To configure location configurations for an individual controller, follow these steps:
Step 1  Choose **Configure > Controller**.

Step 2  Click an applicable IP address.

Step 3  From the left sidebar menu, choose **Location Configuration > Location Configuration**.

The Location Configuration page displays two tabs: General and Advanced.

Step 4  Add or modify the General parameters:

- **RFID Tag Data Collection**—Select the check box to enable the collection of data on tags.

  Before the location server can collect asset tag data from controllers, you must enable the detection of active RFID tags using the CLI command **config rfid status enable** on the controllers.

- **Location Path Loss Configuration**–
  - **Calibrating Client**—Select the **Enabled** check box to enable calibration for the client. Controllers send regular S36 or S60 requests (depending on the client capability) by way of the access point to calibrate clients. Packets are transmitted on all channels. All access points gather RSSI data from the client at each location. These additional transmissions and channel changes might degrade contemporaneous voice or video traffic.

  **Note**  
  To use all radios (802.11a/b/g/n) available, you must enable multiband in the Advanced page.

  - **Normal Client**—Select the **Enabled** check box to have a non-calibrating client. No S36 requests are transmitted to the client.

  **Note**  
  S36 and S60 are client drivers compatible with specific Cisco-compatible Extensions. S36 is compatible with CCXv2 or later. S60 is compatible with CCXv4 or later. For details, see the following URL:


- **Measurement Notification Interval (in secs)**
  - **Tags, Clients, and Rogue APs/Clients**—Allows you to set the NMSP measurement notification interval for clients, tags, and rogues. Specify how many seconds should elapse before notification of the found element (tags, clients, and rogue access points/clients).

    Setting this value on the controller generates an out-of-sync notification which you can view in the Synchronize Servers page. When different measurement intervals exist between a controller and the mobility services engine, the largest interval setting of the two is adopted by the mobility services engine.

    Once this controller is synchronized with the mobility services engine, the new value is set on the mobility services engine.

    **Note**  
    Synchronization to the mobility services engine is required if changes are made to measurement notification interval.

- **RSS Expiry Timeout (in secs)**
  - **For Clients**—Enter the number of seconds after which RSSI measurements for normal (non-calibrating) clients should be discarded.
For Calibrating Clients—Enter the number of seconds after which RSSI measurements for calibrating clients should be discarded.

For Tags—Enter the number of seconds after which RSSI measurements for tags should be discarded.

For Rogue APs—Enter the number of seconds after which RSSI measurements for rogue access points should be discarded.

**Step 5**

Add or modify the Advanced parameters:

- **RFID Tag Data Timeout (in secs)**—Enter a value (in seconds) to set the RFID tag data timeout setting.

- **Location Path Loss Configuration**
  - **Calibrating Client Multiband**—Select the **Enable** check box to send S36 and S60 packets (where applicable) on all channels. Calibrating clients must be enable in the general page.

**Note**

To use all radios (802.11a/b/g/n) available, you must enable multiband.

**Reviewers - Please provide the description for the below fields**

- **FastLocate Configuration**
  - **FastLocate**—Select the **Enable** check box to
  - **FastLocate Threshold**—
  - **FastLocate NTP IP Address**—

**Step 6**

Click **Save**.

**Command Buttons**

- **Save**—Save the changes made to the management user authentication order and return to the previous page.

- **Audit**—Compare the Prime Infrastructure values with those used on the controller.

**Configuring IPv6**

- **Configuring Neighbor Binding Timers**, page 9-161
- **Configuring RA Throttle Policy**, page 9-162
- **Configuring RA Guard**, page 9-162

**Configuring Neighbor Binding Timers**

You can configure IPv6 Router Neighbor Binding Timers parameters such as Down Lifetime, Reachable Lifetime, State Lifetime, and corresponding intervals.

To configure Neighbor Binding Timers, follow these steps:

**Step 1**

Choose **Configure > Controllers**.
Configuring Devices

Chapter 9

Configuring Existing Controllers

Step 2  Click an applicable IP address.

Step 3  Choose IPv6 > Neighbor Binding Timers from the left sidebar menu. The IPv6 > Neighbor Binding Timers page appears.

Step 4  If you want to enable the Down Lifetime timer, select the Enable check box. If you have selected this check box, specify the Down Lifetime Interval value. This indicates the maximum time, in seconds. The range is 0 to 86,400 seconds, and the default value is 0.

Step 5  If you want to enable the Reachable Lifetime timer, select the Enable check box. If you have selected this check box, specify the Reachable Lifetime Interval value. This indicates the maximum time, in seconds. The range is 0 to 86,400 seconds, and the default value is 0.

Step 6  If you want to enable the Stale Lifetime timer, select the Enable check box. If you have selected this check box, specify the Stale Lifetime Interval value. This indicates the maximum time, in seconds. The range is 0 to 86,400 seconds, and the default value is 0.

Step 7  Click Save.

Configuring RA Throttle Policy

The RA Throttle Policy allows you to limit the amount of multicast Router Advertisements (RA) circulating on the wireless network. You can configure IPv6 Router Advertisement parameters such as RA Throttle Policy, Throttle Period and other options.

To configure RA Throttle Policy, follow these steps:

Step 1  Choose Configure > Controllers.

Step 2  Click an applicable IP address.

Step 3  Choose IPv6 > RA Throttle Policy from the left sidebar menu. The IPv6 > RA Throttle Policy page appears.

Step 4  If you want to enable the RA Throttle Policy, select the Enable check box and configure the following parameters:

- Throttle Period—Duration of the throttle period in seconds. The range is 10 to 86,400 seconds.
- Max Through—The number of RA that passes through over a period or over an unlimited period.
- Interval Option—Indicates the behavior in case of RA with an interval option.
  - Ignore
  - Passthrough
  - Throttle
- Allow At-least—Indicates the minimum number of RA not throttled per router.
- Allow At-most—Indicates the maximum or unlimited number of RA not throttled per router.

Step 5  Click Save.

Configuring RA Guard

RA Guard is a Unified Wireless solution to drop RA from wireless clients. It is configured globally, and by default it is enabled. You can configure IPv6 Router Advertisement parameters.
To configure RA Guard, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click an applicable IP address.

**Step 3** Choose **IPv6 > RA Guard** from the left sidebar menu. The IPv6 > RA Guard page appears.

**Step 4** If you want to enable the Router Advertisement Guard, select the **Enable** check box.

**Step 5** Click **Save**.

**Configuring Proxy Mobile IPv6**

Proxy Mobile IPv6 is a network-based mobility management protocol that supports a mobile node by acting as the proxy for the mobile node in any IP mobility-related signaling. The mobility entities in the network track the movements of the mobile node and initiate the mobility signaling and set up the required routing state.

The main functional entities are the Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG). The LMA maintains the reachability state of the mobile node and is the topological anchor point for the IP address of the mobile node. The MAG performs the mobility management on behalf of a mobile node. The MAG resides on the access link where the mobile node is anchored. The controller implements the MAG functionality.

**Configuring PMIP Global Configurations**

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click an applicable IP address.

**Step 3** Choose **PMIP > Global Config** from the left sidebar menu.

**Step 4** Configure the following fields:

- **Domain Name**
- **Maximum Bindings Allowed**—Maximum number of binding updates that the controller can send to the MAG. The valid range is between 0 to 40000.
- **Binding Lifetime**—Lifetime of the binding entries in the controller. The valid range is between 10 to 65535 seconds. The default value is 65535. The binding lifetime should be a multiple of 4 seconds.
- **Binding Refresh Time**—Refresh time of the binding entries in the controller. The valid range is between 4 to 65535 seconds. The default value is 300 seconds. The binding refresh time should be a multiple of 4 seconds.
- **Binding Initial Retry Timeout**—Initial timeout between the proxy binding updates (PBU's) when the controller does not receive the proxy binding acknowledgments (PBA). The valid range is between 100 to 65535 seconds. The default value is 1000 second.
- **Binding Maximum Retry Timeout**—Maximum timeout between the proxy binding updates (PBU's) when the controller does not receive the proxy binding acknowledgments (PBA). The valid range is between 100 to 65535 seconds. The default value is 32000 seconds.
• Replay Protection Timestamp—Maximum amount of time difference between the timestamp in the received proxy binding acknowledgment and the current time of the day. The valid range is between 1 to 255 milliseconds. The default value is 7 milliseconds.

• Minimum BRI Retransmit Timeout—Minimum amount of time that the controller waits before retransmitting the BRI message. The valid range is between 500 to 65535 seconds.

• Maximum BRI Retransmit Timeout—Maximum amount of time that the controller waits before retransmitting the Binding Revocation Indication (BRI) message. The valid range is between 500 to 65535 seconds. The default value is 2000 seconds.

**Step 5**  Click **Save**.

---

### Configuring LMA Configurations

**Step 1**  Choose **Configure > Controllers**.

**Step 2**  Click an applicable IP address.

**Step 3**  Choose **PMIP > LMA Config** from the left sidebar menu.

**Step 4**  Configure the following fields:

- LMA Name—Name of the LMA connected to the controller.
- LMA IP Address—IP address of the LMA connected to the controller.

**Step 5**  Click **Save**.

---

### Configuring PMIP Profile

**Step 1**  Choose **Configure > Controllers**.

**Step 2**  Click an applicable IP address.

**Step 3**  Choose **PMIP > PMIP Profile** from the left sidebar menu.

**Step 4**  Enter the profile name.

**Step 5**  Click **Add** and then configure the following fields:

- Network Access Identifier—Name of the Network Access Identifier (NAI) associated with the profile.
- LMA Name—Name of the LMA to which the profile is associated.
- Access Point Node—Name of the access point node connected to the controller.

**Step 6**  Click **Save**.
Configuring mDNS

Multicast DNS (mDNS) service discovery provides a way to announce and discover services on the local network. mDNS perform DNS queries over IP multicast. mDNS supports zero configuration IP networking.

For information about the mDNS templates, guidelines, and limitations, see the “Configuring mDNS Templates” section on page 11-122.

You can configure mDNS so that the controller can learn about the mDNS services and advertise these services to all clients.

There are two tabs—Services and Profiles.

- Services tab—This tab enables you to configure the global mDNS parameters and update the Master Services database.
- Profiles tab—This tab enables to view the mDNS profiles configured on the controller and create new mDNS profiles. After creating a new profile, you must map the profile to an interface group, an interface, or a WLAN. Clients receive service advertisements only for the services associated with the profile. The controller gives the highest priority to the profiles associated to interface groups, followed by the interface profiles, and then the WLAN profiles. Each client is mapped to a profile based on the order of priority. By default, the controller has an mDNS profile, default-mdns-profile. You cannot delete this default profile.

Step 1
Choose Configure > Controllers.

Step 2
Click an applicable IP address.

Step 3
Choose mDNS > mDNS from the left sidebar menu.

Step 4
On the Services tab, configure the following parameters:

- Template Applied—The name of the template applied to this controller.
- mDNS Global Snooping—Check box that you select to enable snooping of mDNS packets.

Note The controller does not support IPv6 mDNS packets even when you enable mDNS snooping.

- Query Interval(10-120)—mDNS query interval, in minutes that you can set. This interval is used by WLC to send periodic mDNS query messages to services which do not send service advertisements automatically after they are started. The range is from 10 to 120 minutes. The default value is 15 minutes.
- Master Services—Click Add Row and then configure the following fields:
  - Master Service Name—Drop-down list from which you can choose the supported services that can be queried. The following services are available:
    - AirTunes
    - AirPrint
    - AppleTV
    - HP Photosmart Printer1
    - HP Photosmart Printer2
    - Apple File Sharing Protocol (AFP)
    - Scanner
- Printer
- FTP
- iTunes Music Sharing
- iTunes Home Sharing
- iTunes Wireless Device Syncing
- Apple Remote Desktop
- Apple CD/DVD Sharing
- Time Capsule Backup

Note: To add a new service, enter or choose the service name, enter the service string, and then choose the service status.

- Service Name—Name of the mDNS service.
- Service String—Unique string associated to an mDNS service. For example, _airplay._tcp.local. is the service string associated to AppleTV.
- Query Status—Check box that you select to enable an mDNS query for a service.

Note: Periodic mDNS query messages will be sent by WLC at configured Query Interval for services only when the query status is enabled; otherwise, service should automatically advertised for other services where the query status is disabled (for example AppleTV).

Step 5 On the Profiles tab, configure the following parameters:

- Profiles—Click Add Profile and then configure the following fields:
  - Profile Name—Name of the mDNS profile. You can create a maximum of 16 profiles.
  - Services—Select the services (using the check boxes) that you want to map to the mDNS profile.

Step 6 Click Save.

Configuring AVC Profiles

Application Visibility and Control (AVC) uses the Network Based Application Recognition (NBAR) deep packet inspection technology to classify applications based on the protocol they use. Using AVC, the controller can detect more than 1400 Layer 4 to Layer 7 protocols. AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades.

AVC is supported only on the Cisco 2500 and 5500 Series Controllers, and Cisco Flex 7500 and Cisco 8500 Series Controllers.

Step 1 Choose Configure > Controllers.
Step 2 Click an applicable IP address.
Step 3 Choose Application Visibility And Control > AVC Profiles from the left sidebar menu.
Step 4  Click the AVC Profile Name that you want to configure.

Step 5  To create AVC rules, click Add Row under the AVC Rule List.

Step 6  Configure the following parameters:

- Application Name—Name of the application.
- Application Group Name—Name of the application group to which the application belongs.
- Action—Drop-down list from which you can choose the following:
  - Drop—Drops the upstream and downstream packets corresponding to the chosen application.
  - Mark—Marks the upstream and downstream packets corresponding to the chosen application with the DSCP value that you specify in the Differentiated Services Code Point (DSCP) drop-down list. The DSCP value helps you provide differentiated services based on the QoS levels.
  - Rate Limit—If you select Rate Limit as an action, you can specify Average Rate Limit per client and Burst data rate limit. The number of rate limit applications is limited to 3. The default action is to permit all applications.

- DSCP—Packet header code that is used to define quality of service across the Internet. The DSCP values are mapped to the following QoS levels:
  - Platinum (Voice)—Assures a high QoS for Voice over Wireless.
  - Gold (Video)—Supports the high-quality video applications.
  - Silver (Best Effort)—Supports the normal bandwidth for clients.
  - Bronze (Background)—Provides lowest bandwidth for guest services.

- DSCP Value—You can also choose Custom and specify the DSCP value. The range is from 0 to 63.

Step 7  Click Save.

Configuring NetFlow

NetFlow is a protocol that provides valuable information about network users and applications, peak usage times, and traffic routing. This protocol collects IP traffic information from network devices to monitor traffic. The NetFlow architecture consists of the following components:

- Collector—An entity that collects all the IP traffic information from various network elements.
- Exporter—A network entity that exports the template with the IP traffic information. The controller acts as an exporter.

Configuring NetFlow Monitor, page 9-167
Configuring NetFlow Exporter, page 9-168

Configuring NetFlow Monitor

Step 1  Choose Configure > Controllers.

Step 2  Click an applicable IP address.

Step 3  Choose NetFlow > Monitor from the left sidebar menu.
Configuring Third-Party Controllers and Access Points

Prime Infrastructure enables you to add third-party controllers and access points. As part of this feature you can perform the following functions:

**Configuring NetFlow Exporter**

**Step 1** Choose Configure > Controllers.

**Step 2** Click an applicable IP address.

**Step 3** Choose NetFlow > Exporter from the left sidebar menu.

**Step 4** Configure the following parameters:
- Exporter Name—Name of the exporter.
- Exporter IP—IP address of the exporter.
- Port Number—The UDP port through which the Netflow record is exported.

**Step 5** Click Save.

**Configuring Third-Party Controllers and Access Points**

**Step 4** Configure the following parameters:
- Monitor Name—Name of the NetFlow monitor. The monitor name can be up to 127 case-sensitive alphanumeric characters. You can configure only one monitor in the controller.
- Record Name—Name of the NetFlow record. A NetFlow record in the controller contains the following information about the traffic in a given flow:
  - Client MAC address
  - Client Source IP address
  - WLAN ID
  - Application ID
  - Incoming bytes of data
  - Outgoing bytes of data
  - Incoming Packets
  - Outgoing Packets
  - Incoming DSCP
  - Outgoing DSCP
  - Name of last AP

**Step 5** Exporter Name—Name of the exporter. You can configure only one monitor in the controller.

**Step 6** Exporter IP—IP address of the collector.

**Step 7** Port—UDP port through which the NetFlow record is exported from the controller.

**Step 8** Click Save.
• Add third-party controllers to the Prime Infrastructure.
• Monitor the state of the third-party controllers.
• Get inventory information for the third-party controllers and their associated access points.
• Use the background tasks to view the operations status third-party controllers and access points.

Adding a Third-Party Controller

To add a third-party controller, follow these steps:

Step 1  Choose Configure > Third Party Controllers.
Step 2  From the Select a command drop-down list, choose Add Controller, and click Go.
Step 3  In the Add Controller page, enter the controller IP address, network mask, and required SNMP settings.
Step 4  Click Add.

Viewing Third-Party Controller Operational Status

To view the Third Party Controller Operational Status page, follow these steps:

Step 1  Choose Administration > Background Tasks.
Step 2  In this page, perform one of the following:

• Execute the task now.
  Select the Third Party Controller Operational Status check box. From the Select a command drop-down list, choose Execute Now, and click Go. You see the status change in the Enabled column.
  or

• Enable the task.
  Select the Third Party Controller Operational Status check box. From the Select a command drop-down list, choose Enable Tasks, and click Go. The task converts from dimmed to available in the Enabled column.
  or

• Disable the task.
  Select the Third Party Controller Operational Status check box. From the Select a command drop-down list, choose Disable Tasks, and click Go. The task is dimmed in the Enabled column after the disabling is complete.
Step 3 To modify the task, click the **Third Party Controller Operational Status** link in the Background Tasks column.

The Third Party Controller Operational Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time (in seconds) of the task.
  - Result—Success or error.
  - Message—Text message regarding this task.

Step 4 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select the check box to enable this task.
- Interval—Indicates the frequency (in minutes) of the task. The default is 3 hours.

Step 5 When finished, click **Save** to confirm task changes.

---

**Viewing the Details of Third-Party Access Points**

The third-party access points are discovered when you add a third-party controller. To view the configurations of a third-party access point, follow these steps:

---

Step 1 Choose **Configure > Third Party Access Points**.

Step 2 Click the AP Name link to display details for that third-party access point. The General tab for that third-party access point appears.

**Note** To add, remove, or reorder columns in the table, click the **Edit View** link.

---

**Removing Third-Party Access Points**

To remove third-party access points, follow these steps:

---

Step 1 Choose **Configure > Third Party Access Points**.

Step 2 Select the check boxes of the access points you want to remove.

Step 3 From the **Select a command** drop-down list, choose **Remove APs**.
Viewing Third-Party Access Point Operational Status

To view the Third Party Access Point Operational Status page, follow these steps:

**Step 1** Choose Administration > Background Tasks.

**Step 2** In this page, perform one of the following:

- Execute the task now.
  
  Select the Third party Access Point Operational Status check box. From the Select a command drop-down list, choose Execute Now, and click Go. You see the status change in the Enabled column.
  
  or
  
  - Enable the task.
  
  Select the Third party Access Point Operational Status check box. From the Select a command drop-down list, choose Enable Tasks, and click Go. The task converts from dimmed to available in the Enabled column.
  
  or
  
  - Disable the task.
  
  Select the Third party Access Point Operational Status check box. From the Select a command drop-down list, choose Disable Tasks, and click Go. The task is dimmed in the Enabled column after the disabling is complete.

**Step 3** To modify the task, click the Third party Access Point Operational Status link in the Background Tasks column.

The Third Party Controller Operational Status page displays the following information:

- Last Execution Information
  
  - Start and end times.
  
  - Elapsed time (in seconds) of the task.
  
  - Result—Success or error.
  
  - Message—Text message regarding this task.

**Step 4** View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.

- Enabled—Select the check box to enable this task.

- Interval—Indicates the frequency (in minutes) of the task. The default is 3 hours.

**Step 5** When finished, click Save to confirm task changes.

Configuring Access Points

This section describes how to configure access points in the Prime Infrastructure database.

- Setting AP Failover Priority, page 9-172

- Configuring Global Credentials for Access Points, page 9-173
Setting AP Failover Priority

When a controller fails, the backup controller configured for the access point suddenly receives a number of discovery and join requests. This might cause the controller to reach a saturation point and reject some of the access points.

By assigning priority to an access point, you have some control over which access points are rejected. In a failover situation when the backup controller is saturated, the higher priority access points are allowed to join the backup controller by disjoining the lower priority access points.

To configure priority settings for access points, you must first enable the AP Priority feature. To enable the AP Priority feature, follow these steps:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click the IP address of the applicable controller.

**Step 3** From the left sidebar menu, choose **System > General**.

**Step 4** From the AP Failover Priority drop-down list, choose **Enable**.

To configure the priority of an access point, see the “Configuring Access Point Details” section on page 9-184.
Configuring Global Credentials for Access Points

Cisco autonomous access points are shipped from the factory with Cisco as the default enable password. This password allows users to log into the non-privileged mode and execute show and debug commands, posing a security threat. The default enable password must be changed to prevent unauthorized access and to enable users to execute configuration commands from the console port of an access point.

In the Prime Infrastructure and controller software releases prior to 5.0, you can set the access point enable password only for access points that are currently connected to the controller. In the Prime Infrastructure and controller software release 5.0, you can set a global username, password, and enable password that all access points inherit as they join a controller. This includes all access points that are currently joined to the controller and any that join in the future. When you are adding an access point, you can also choose to accept this global username and password or override it on a per-access point basis and assign a unique username, password, and enable password. See the “Configuring AP Configuration Templates” section on page 11-126 to see where the global password is displayed and how it can be overridden on a per-access point basis.

Also in controller software release 5.0, after an access point joins the controller, the access point enables console port security, and you are prompted for your username and password whenever you log into the console port of an access point. When you log in, you are in non-privileged mode, and you must enter the enable password to use the privileged mode.

Note

These controller software release 5.0 features are supported on all access points that have been converted to lightweight mode, except the 1100 series. VxWorks access points are not supported.

The global credentials that you configure on the controller are retained across controller and access point reboots. They are overwritten only if the access point joins a new controller that is configured with a global username and password. If the new controller is not configured with global credentials, the access point retains the global username and password configured for the first controller.

Note

You need to keep careful track of the credentials used by the access points. Otherwise, you might not be able to log into the console port of an access point. If necessary, you can clear the access point configuration to return the access point username and password to the default setting.

To establish a global username and password, follow these steps:

1. Choose Configure > Controllers or Configure > Access Points.
2. Choose an IP address of a controller with software release 5.0 or later or choose an access point associated with software release 5.0 or later.
3. Choose System > AP Username Password from the left sidebar menu. The AP Username Password page appears.
4. In the AP Username text box, enter the username that is to be inherited by all access points that join the controller.
5. In the AP Password text box, enter the password that is to be inherited by all access points that join the controller. Reenter the password in the Confirm AP Password text box.
6. For Cisco autonomous access points, you must also enter and confirm an enable password. In the AP Enable Password text box, enter the enable password that is to be inherited by all access points that join the controller. Reenter the password in the Confirm Enable Password text box.
Configuring Ethernet Bridging and Ethernet VLAN Tagging

Ethernet bridging is used in two mesh network scenarios:

1. Point-to-point and point-to-multipoint bridging between MAPs (untagged packets). A typical trunking application might be bridging traffic between buildings within a campus (see Figure 9-3).

   **Note** You do not need to configure VLAN tagging to use Ethernet bridging for point-to-point and point-to-multipoint bridging deployments.

   **Figure 9-3  Point-to-Multipoint Bridging**

2. Ethernet VLAN tagging allows specific application traffic to be segmented within a wireless mesh network and then forwarded (bridged) to a wired LAN (access mode) or bridged to another wireless mesh network (trunk mode).

   A typical public safety access application using Ethernet VLAN tagging is placement of video surveillance cameras at various outdoor locations within a city. Each of these video cameras has a wired connection to a MAP. The video of all these cameras is then streamed across the wireless backhaul to a central command station on a wired network (see Figure 9-4).
Ethernet VLAN Tagging Guidelines

- For security reasons, the Ethernet port on a mesh access point (RAP and MAP) is disabled by default. It is enabled by configuring Ethernet Bridging on the mesh access point port.
- You must enable Ethernet bridging on all the access points in the mesh network to allow Ethernet VLAN Tagging to operate.
- You must set VLAN Mode as non-VLAN transparent (global mesh field). See the “Configuring Ethernet Bridging and Ethernet VLAN Tagging” section on page 9-174.
  - VLAN transparent is enabled by default. To set as non-VLAN transparent, you must unselect the VLAN transparent option in the Global Mesh Parameters page.
- VLAN configuration on a mesh access point is only applied if all the uplink mesh access points are able to support that VLAN.
If uplink access points are not able to support the VLAN, then the configuration is stored rather than applied.

- VLAN tagging can only be configured on Ethernet interfaces.
  - On 152x mesh access points, use three of the four ports as secondary Ethernet interfaces: port 0-PoE in, port 1-PoE out, and port 3-fiber. You cannot configure Port 2-cable as a secondary Ethernet interface.
  - In Ethernet VLAN tagging, port 0-PoE in on the RAP connects the trunk port of the switch of the wired network. Port 1-PoE out on the MAP connects external devices such as video cameras.

- Backhaul interfaces (802.11a radios) act as primary Ethernet interfaces. Backhauls function as trunks in the network and carry all VLAN traffic between the wireless and wired network. You are not required to configure the primary Ethernet interface.

- You must configure the switch port in the wired network that is attached to the RAP (port 0-PoE in) to accept tagged packets on its trunk port. The RAP forwards all tagged packets received from the mesh network to the wired network.

- Configuration to support VLAN tagging on the 802.11a backhaul Ethernet interface is not required within the mesh network.
  - This includes the RAP uplink Ethernet port. The required configuration happens automatically using a registration mechanism.
  - Any configuration changes to an 802.11a Ethernet link acting as a backhaul are ignored, and a warning results. When the Ethernet link no longer functions as a backhaul, the modified configuration is applied.

- You cannot configure VLANs on port-02-cable modem port of a 152x access point. Configure VLANs on ports 0 (PoE-in), 1 (PoE-out), and 3 (fiber).

- If bridging between two MAPs, enter the distance (mesh range) between the two access points that are bridging. (Not applicable to applications in which you are forwarding traffic connected to the MAP to the RAP, access mode.)

- Each sector supports up to 16 VLANs; therefore, the cumulative number of VLANs supported by the children of a RAP (MAPs) cannot exceed 16.

- Ethernet ports on access points function as normal, access, or trunk ports in an Ethernet tagging deployment.
  - Normal mode—In this mode, the Ethernet interface is VLAN-transparent by default and does not accept or send any tagged packets. Tagged frames from clients are dropped. Untagged frames are forwarded to the native VLAN on the RAP trunk port.
  - Access mode—In this mode only untagged packets are accepted. You must tag all packets with a user-configured VLAN called access-VLAN. For this mode to take effect, the global VLAN mode should be non-VLAN transparent.

Use this option for applications in which information is collected from devices connected to the MAP such as cameras or PCs and then forwarded to the RAP. The RAP then applies tags and forwards traffic to a switch on the wired network.

  - Trunk mode—This mode requires the user to configure a native VLAN and an allowed VLAN list (no defaults). In this mode, both tagged and untagged packets are accepted. You can accept untagged packets and tag them with the user-specified native VLAN. You can accept tagged packets if they are tagged with a VLAN in the allowed VLAN list. For this mode to take effect, the global VLAN mode should be non-VLAN transparent.

Use this option for bridging applications such as forwarding traffic between two MAPs resident on separate buildings within a campus.
• The switch port connected to the RAP must be a trunk.
  – The trunk port on the switch and the RAP trunk port must match.
• A configured VLAN on a MAP Ethernet port cannot function as a Management VLAN.
• The RAP must always connect to the native VLAN (ID 1) on a switch.
  – The primary Ethernet interface of the RAP is by default the native VLAN of 1.

### Enabling Ethernet Bridging and VLAN Tagging

To enable Ethernet Bridging and VLAN tagging on a RAP or MAP, follow these steps:

**Step 1** Choose Configure > Access Points.

**Step 2** Click the name of the mesh access point for which you want to enable Ethernet bridging. A configuration page for the access point appears.

**Step 3** In the Bridging Information group box, choose the appropriate backhaul rate from the Data Rate drop-down list. The default value is 24 Mbps for the 802.11a backhaul interface.

**Step 4** In the Bridging Information section, choose Enable from the Ethernet Bridging drop-down list.

**Step 5** Click the appropriate Ethernet interface link (such as FastEthernet or gigabitEthernet1).

**Step 6** In the Ethernet interface page, perform one of the following:

**Note** The configuration options vary for each of the VLAN modes (normal, access, and trunk).

- **a.** If you are configuring a MAP and RAP normal ports and chose FastEthernet0, choose Normal from the VLAN Mode drop-down list.
  
  In this mode, the Ethernet interface is VLAN-transparent by default and does not accept or send any tagged packets. Tagged frames from clients are dropped. Untagged frames are forwarded to the native VLAN on the RAP trunk port.

- **b.** If you are configuring a MAP access port and chose gigabitEthernet1 (port 1-PoE out):
  1. Choose Access from the VLAN Mode drop-down list.
  2. Enter a VLAN ID. The VLAN ID can be any value between 1 and 4095.
  3. Click Save.

  **Note** VLAN ID 1 is not reserved as the default VLAN.

- **c.** If you are configuring a RAP or MAP trunk port and chose gigabitEthernet0 (or FastEthernet0) (port 0-PoE in),
  1. Choose trunk from the VLAN Mode drop-down list.
  2. Enter a native VLAN ID for incoming traffic. The native VLAN ID can be any value between 1 and 4095. Do not assign any value assigned to a user-VLAN (access).
3. Enter a trunk VLAN ID for outgoing traffic, and click Add.
   The added trunk appears in the summary column of allowed VLAN IDs.
   If forwarding untagged packets, do not change the default trunk VLAN ID value of zero (such as MAP-to-MAP bridging, campus environment).
   If forwarding tagged packets, enter a VLAN ID (1 to 4095) that is not already assigned (such as RAP to switch on wired network).

   **Note** To remove a VLAN from the list, click Delete.

4. Click Save.

   **Note** At least one mesh access point must be set to RootAP in the mesh network.

---

**Autonomous to Lightweight Migration Support**

The autonomous to lightweight migration support feature provides a common application from which you can perform basic monitoring of autonomous access points along with current lightweight access points. The following autonomous access points are supported:

- Cisco Aironet 1130 Access Point
- Cisco Aironet 1200 Access Point
- Cisco Aironet 1240 Access Point
- Cisco Aironet 1310 Bridge
- Cisco Aironet 1410 Bridge

You might also choose to convert autonomous access points to lightweight. Once an access point is converted to lightweight, the previous status or configuration of the access point is not retained.

From the Prime Infrastructure, the following functions are available when managing autonomous access points:

- Adding Autonomous Access Points to the Prime Infrastructure, page 9-179
- Viewing Autonomous Access Points in Prime Infrastructure, page 9-183
- Adding and viewing autonomous access points from the Monitor > Maps page (see the “Monitoring Maps” section on page 6-1 for more information)
- Monitoring associated alarms
- Performing an autonomous access point background task
  - Checks the status of autonomous access points managed by the Prime Infrastructure.
  - Generates a critical alarm when an unreachable autonomous access point is detected.
- Running reports on autonomous access points
  - See Reports > Inventory Reports and Reports > Client Reports > Client Count for more information
- Supporting Autonomous Access Points in Work Group Bridge (WGB) mode, page 9-184
• Migrating an Autonomous Access Point to a Lightweight Access Point, page 11-137

Adding Autonomous Access Points to the Prime Infrastructure

From the Prime Infrastructure, the following methods are available for adding autonomous access points:
• Adding Autonomous Access Points by Device Information, page 9-179 (IP addresses and credentials).
• Adding Autonomous Access Points by CSV File, page 9-180.
• Removing Autonomous Access Points, page 9-182

Adding Autonomous Access Points by Device Information

Autonomous access points can be added to the Prime Infrastructure by device information using comma-separated IP addresses and credentials.

To add autonomous access points using device information, follow these steps:

Step 1 Choose Configure > Access Points.
Step 2 From the Select a command drop-down list, choose Add Autonomous APs.
Step 3 Click Go.
Step 4 Choose Device Info from the Add Format Type drop-down list.
Step 5 Enter comma-separated IP addresses of autonomous access points.
Step 6 Enter the SNMP Parameters parameters:
  • Version—Choose from v1, v2, or v3.
  • Retries—Indicates the number of controller discovery attempts.
  • Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The valid range is 2 to 90 seconds. The default is 10 seconds.
  • Community—Public or Private.
Step 7 Enter the Telnet/SSH Parameters:

Note Default values are used if the Telnet/SSH parameters are left blank.

• Protocol—Select the protocol you want to use (either Telnet or SSH).
• User Name—Enter the username. (The default username is admin.)

Note The Telnet/SSH username must have sufficient privileges to execute commands in CLI templates.

• Password/Confirm Password—Enter and confirm the password. (Default password is admin.)
• Enable Password/Confirm Password—Enter and confirm an enable password.
• Telnet Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The default is 60 seconds.
Cisco autonomous access points are shipped from the factory with Cisco as the default enable password. This password allows users to log into the non-privileged mode and execute show and debug commands, posing a security threat. The default enable password must be changed to prevent unauthorized access and to enable users to execute configuration commands from the console port of an access point.

Before you perform the AAP Download Software task, you need to set the maximum Telnet/SSH timeout values.

Step 8
Click Add.

After the AP is added and its inventory collection is completed, it appears in the Access Point list page (Configure > Access Points). If it is not found in the Access Points list, choose Configure > Unknown Device page to check the status. For details, see the “Configuring Unknown Devices” section on page 9-214.

Autonomous access points are not counted towards the total device count for your license.

Adding Autonomous Access Points by CSV File

Autonomous access points can be added to the Prime Infrastructure using a CSV file exported from WLSE.

To add autonomous access points using a CSV file, follow these steps:

Step 1
Choose Configure > Access Points.

Step 2
From the Select a command drop-down list, choose Add Autonomous APs.

Step 3
Click Go.

Step 4
Choose File from the Add Format Type drop-down list.

Step 5
Enter or browse to the applicable CSV file.

The sample CSV files for V2 devices are as follows:

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name, snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries, snmp_timeout, telnet_username, telnet_password, telnet_retries, telnet_timeout
209.165.200.224, 255.255.255.224, v2, public, , , , , , , , , 3, 4
209.165.201.0, 255.255.255.0, v2, public, , , , , , , , , 3, 4
```

The sample CSV files for V3 devices are as follows:

```
ip_address, network_mask, snmp_version, snmpv3_user_name, snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries, snmp_timeout, telnet_username, telnet_password, telnet_retries, telnet_timeout
```

The SNMP, telnet, or SSH credentials are mandatory.
Step 6 Click OK.

Bulk Update of Autonomous Access Points

You can update multiple autonomous access points credentials by importing a CSV file.

To update autonomous access point(s) information in a bulk, follow these steps:

Step 1 Choose Configure > Access Points.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 From the Select a command drop-down list, choose Bulk Update APs. The Bulk Update Autonomous Access Points page appears.

Step 4 Click Choose File to select a CSV file, and then find the location of the CSV file you want to import.

Step 5 Click Update and Sync.

Sample CSV File for the Bulk Update of Autonomous Access Points

The sample CSV files for V2 devices are as follows:
The sample CSV files for V3 devices are as follows:

```
ip_address, network_mask, snmp_version, snmpv3_user_name, snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries, snmp_timeout, telnet_username, telnet_password, telnet_retries, telnet_timeout
209.165.201.0, 255.255.255.255, v3, default, HMAC-MD5, default, DES, default, 3, 4, Cisco, Cisco, 2, 10
```

The CSV files can contain the following fields:

- `ip_address`
- `network_mask`
- `snmp_version`
- `snmp_community`
- `snmpv3_user_name`
- `snmpv3_auth_type`
- `snmpv3_auth_password`
- `snmpv3_privacy_type`
- `snmpv3_privacy_password`
- `snmp_retries`
- `snmp_timeout`
- `telnet_username`
- `telnet_password`
- `enable_password`
- `telnet_retries`
- `telnet_timeout`

### Removing Autonomous Access Points

**Note** If you replace Autonomous Access Points because of some reason, remove the Autonomous Access Points from the Prime Infrastructure before you install the replacement access points on the network.

To remove an autonomous access point from the Prime Infrastructure, follow these steps:

**Step 1** Select the check boxes of the access points you want to remove.
Step 2  Choose Remove APs from the Select a command drop-down list.

Viewing Autonomous Access Points in Prime Infrastructure

Once added, the autonomous access points can be viewed on the Monitor > Access Points page. Click the autonomous access point to view more detailed information such as the following:

- Operational status of the access points
- Key attributes including radio information, channel, power, and number of clients on the radio
- CDP neighbored information

The autonomous access points can also be viewed in Monitor > Maps. They can be added to a floor area by choosing Monitor Maps > floor area and choosing Add Access Points from the Select a command drop-down list.

Downloading Images to Autonomous Access Points (TFTP)

Lightweight access point images are bundled with controller images and managed by the controller. Autonomous access point images must be handled by a NMS system such as WLSE, CiscoWorks, or Prime Infrastructure.

To download images to autonomous access points using TFTP, follow these steps:

Step 1  Choose Configure > Access Points.
Step 2  Select the check box of the autonomous access point to which you want to download an image. The AP Type column displays whether the access point is autonomous or lightweight.
Step 3  From the Select a command drop-down list, choose Download Autonomous AP Image (TFTP). The Download images to Autonomous APs page appears.
Step 4  Configure the following parameters:
   - File is located on—Choose Local machine or TFTP server.
   - Server Name—Choose the default server or add a new server from the Server Name drop-down list.
   - IP address—Specify the TFTP server IP address. This is automatically populated if the default server is selected.
   - Prime Infrastructure Server Files In—Specify where the Prime Infrastructure server files are located. This is automatically populated if the default server is selected.
   - Server File Name—Specify the server filename.
Step 5  Click Download.

Tip  Some TFTP servers might not support files larger than 32 MB.
Downloading Images to Autonomous Access Points (FTP)

To download images to autonomous access points (using FTP), follow these steps:

**Step 1** Choose Configure > Access Points.

**Step 2** Select the check box of the autonomous access point to which you want to download an image. The AP Type column displays whether the access point is autonomous or lightweight.

**Step 3** From the Select a command drop-down list, choose Download Autonomous AP Image (FTP). The Download images to Autonomous APs page appears.

**Step 4** Enter the FTP credentials including username and password.

**Step 5** Configure the following parameters:

- File is located on—Choose Local machine or FTP server.
- Server Name—Choose the default server or add a new server from the Server Name drop-down list.
- IP address—Specify the FTP server IP address. This is automatically populated if the default server is selected.
- Prime Infrastructure Server Files In—Specify where the Prime Infrastructure server files are located. This is automatically populated if the default server is selected.
- Server File Name—Specify the server filename.

**Step 6** Click Download.

Supporting Autonomous Access Points in Work Group Bridge (WGB) mode

Workgroup Bridge (WGB) mode is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The WGB and its wired clients are listed as clients in the Prime Infrastructure if the AP mode is set to Bridge, and the access point is bridge capable.

To view a list of all the Prime Infrastructure clients that are WGBs, choose Monitor > Clients. From the Show drop-down list, choose WGB Clients, and click Go. The Clients (detected as WGBs) page appears. Click a user to view detailed information regarding a specific WGB and its wired clients.

**Note** Prime Infrastructure provides WGB client information for the autonomous access point whether or not it is managed by the Prime Infrastructure. If the WGB access point is also managed by the Prime Infrastructure, Prime Infrastructure provides basic monitoring functions for the access point similar to other autonomous access points.

Configuring Access Point Details

Choose Configure > Access Points to see a summary of all access points in the Prime Infrastructure database. The summary information includes the following:

- Ethernet MAC
- IP Address
- Radio
### Configuring Access Points

- Map Location
- AP Type
- Controller
- Operation Status
- Alarm Status
- Audit Status

**Note** If you hover your mouse cursor over the Audit Status value, the time of the last audit is displayed.

**Note** For details on configuring AP Configuration Templates, see “Configuring AP Configuration Templates” section on page 11-126.

**Note** You can click the **Edit View** link to add, remove or reorder columns such as AP Mode, Channel Width, Client Count, and so on. See the *Configuring the Search Results Display (Edit View)* section in the *Cisco Prime Infrastructure 2.0 User Guide* for more information.

### Step 1

Click the link in the AP Name column to see detailed information about that access point name. The Access Point Detail page appears.

**Note** The operating system software automatically detects and adds an access point to the Prime Infrastructure database as it associates with existing controllers in the Prime Infrastructure database.

**Note** Access point parameters might vary depending on the access point type.

Some of the parameters on the page are automatically populated.

- The General group box displays the Ethernet MAC, the Base Radio MAC, IP Address, and status.
- The Versions group box of the page displays the software and boot version.
- The Inventory Information group box displays the model, AP type, AP certificate type, serial number, and REAP mode support.
- The Ethernet Interfaces group box provides information such as interface name, slot ID, admin status, and CDP state.
- The Radio Interfaces group box provides the current status of the 802.11a/n, 802.11b/g/n radios, and 802.11a/b/g/n such as admin status, channel number, power level, antenna mode, antenna diversity, and antenna type.

To set the configurable parameters, follow these steps:
Chapter 9  Configuring Devices

Configuring Access Points

**Note** Changing access point parameters causes the access point to be temporarily disabled and this might cause some clients to lose connectivity.

**Step 2** Enter the name assigned to the access point.

**Step 3** Use the drop-down list to choose a country code to establish multiple country support. Access points are designed for use in many countries with varying regulatory requirements. You can configure a country code to ensure that the access point complies with the regulations of your country. Consider the following when setting the country code:

- You can configure up to 20 countries per controller.
- Because only one auto-RF engine and one list of available channels exist, configuring multiple countries limits the channels available to auto-RF in the common channels. A common channel is one that is legal in each and every configured country.
- When you configure access points for multiple countries, the auto-RF channels are limited to the highest power level available in every configured country. A particular access point might be set to exceed these limitations (or you might manually set the levels in excess of these limitations), but auto-RF does not automatically choose a non-common channel or raise the power level beyond that available in all countries.

**Note** Access points might not operate properly if they are not designed for use in your country of operation. For example, an (-A) access point with part number AIR-AP1030-A-K9 (which is included in the Americas regulatory domain) cannot be used in Europe (-E). Always be sure to purchase access points that match the regulatory domain of your country. For a complete list of country codes supported per product, see this URL:


**Step 4** If you want to enable the access point for administrative purposes, select the **Enable** check box.

**Step 5** If you click **Enable** at the AP Static IP check box, a static IP address is always assigned to the access point rather than getting an IP address dynamically upon reboot.

**Step 6** Choose the role of the access point from the AP Mode drop-down list. No reboot is required after the mode is changed except when monitor mode is selected. You are notified of the reboot when you click **Save**. The available modes are as follows:

- Local—This is the normal operation of the access point and the default AP Mode choice. With this mode, data clients are serviced while configured channels are scanned for noise and rogues. The access point goes off-channel for 50 ms and listens for rogues. It cycles through each channel for the period specified under the Auto RF configuration.
- AP Sub Mode—When the AP Mode is set to Local, you can set the AP Sub Mode to WIPS.
- FlexConnect—Choose **FlexConnect** from the AP Mode drop-down list to enable FlexConnect for up to six access points. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost.

**Note** To configure Local or FlexConnect access points for Cisco Adaptive wIPS feature, choose Local or FlexConnect, and select the **Enhanced wIPS Engine Enabled** check box.
AP Sub Mode - When the AP Mode is set to FlexConnect, you can set the AP Sub Mode to any one of the following:

- WIPS
- PPPOE—To configure the Point-to-Point Protocol over Ethernet (PPPoE) submode on the access point.
- PPPOE-WIPS—To configure both Point Protocol over Ethernet (PPPoE) and wIPS submodes on the access point.

- Monitor—This is radio receive only mode and allows the access point to scan all configured channels every 12 seconds. Only deauthentication packets are sent in the air with an access point configured this way. A monitor mode access point detects rogues, but it cannot connect to a suspicious rogue as a client to prepare for the sending of RLDP packets.

APE Sub Mode—When the AP Mode is set to Monitor, you can set the AP Sub Mode to WIPS.

**Note**
You can expand the monitor mode for tags to include location calculation by enabling the tracking optimized monitor mode (TOMM) feature. When TOMM is enabled, you can specify which four channels within the 2.4 GHz band (802.11b/g radio) of an access point to use to monitor tags. This allows you to focus channel scans on only those channels for which tags are traditionally found (such as channels 1, 6, and 11) in your network. To enable TOMM, you must also make additional edits on the 802.11b/g radio of the access point. See the “Configuring Access Point Radios for Tracking Optimized Monitor Mode” section on page 9-199 for configuration details.

**Note**
You cannot enable both TOMM and wIPS at the same time. TOMM can be enabled only when wIPS is disabled.

**Note**
To configure access points for Cisco Adaptive wIPS feature, choose Monitor and select the Enhanced wIPS Engine Enabled check box, and select wIPS from the Monitor Mode Optimization drop-down list.

- Rogue Detector—In this mode, the access point radio is turned off, and the access point listens to wired traffic only. The controllers that operate in this mode monitor the rogue access points. The controller sends all the rogue access point and client MAC address lists to the rogue detector, and the rogue detector forwards this information to the WLC. The MAC address list is compared to what the WLC access points expected. If the MAC addresses match, you can determine which rogue access points are connected on the wired network.

- Sniffer—Operating in sniffer mode, the access point captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek. These packets contain information such as timestamp, signal strength, packet size, and so on. This feature can only be enabled if you run AiroPeek, which is a third-party network analyzer software that supports the decoding of data packets. For more information on AiroPeek, see the following URL: [www.wildpackets.com](http://www.wildpackets.com).

- Bridge—Bridge mode is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The bridge and its wired clients are listed as client in the Prime Infrastructure if the AP mode is set to Bridge, and the access point is bridge capable.
SE-Connect—This mode allows a CleanAir-enabled access point to be used extensively for interference detection on all monitored channels. All other functions such as IDS scanning and Wi-Fi are suspended.

**Note**
This option is displayed only if the access point is CleanAir-capable.

**Note**
Changing the AP mode reboots the access point.

### Step 7
Disable any access point radios.

### Step 8
From the AP Failover Priority drop-down list, choose **Low**, **Medium**, **High**, or **Critical** to indicate the failover priority of the access point. The default priority is low. See the “Setting AP Failover Priority” section on page 9-172 for more information.

### Step 9
In the Primary, Secondary, and Tertiary Controller fields, you can define the order in which controllers are accessed.

### Step 10
The AP Group Name drop-down shows all access point group names that have been defined using WLANs > AP Group VLANs, and you can specify whether this access point is tied to any group.

**Note**
An access point group name to 31 characters for WLC versions earlier than 4.2.132.0 and 5.0.159.0.

### Step 11
Enter a description of the physical location where the access point was placed.

### Step 12
In the Stats Collection Period field, enter the time in which the access point sends .11 statistics to the controller. The valid range is 0 to 65535 seconds. A value of 0 means statistics should not be sent.

### Step 13
Choose **Enable** for Mirror Mode if you want to duplicate (to another port) all of the traffic originating from or terminating at a single client device or access point. Mirror mode is useful in diagnosing specific network problems but should only be enabled on an unused port since any connections to this port become unresponsive.

### Step 14
You can globally configure MFP on a controller. When you do, management frame protection and validation are enabled by default for each joined access point, and access point authentication is automatically disabled. After MFP is globally enabled on a controller, you can disable and re-enable it for individual WLANs and access points.

If you click to enable MFP Frame Validation, three main functions are performed:

- **Management frame protection**—When management frame protection is enabled, the access point protects the management frames it transmits by adding a message integrity check information element (MIC IE) to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing those receiving access points which were configured to detect MFP frames to report the discrepancy.

- **Management frame validation**—When management frame validation is enabled, the access point validates every management frame it receives from other access points in the network. When the originator is configured to transmit MFP frames, the access point ensures that the MIC IE is present and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE, it reports the discrepancy to the network management system. To report this discrepancy, the access point must have been configured to transmit MFP frames. Likewise, for the timestamps to operate properly, all controllers must be Network Transfer Protocol (NTP) synchronized.
Event reporting—The access point notifies the controller when it detects an anomaly, and the controller aggregates the received anomaly events and reports the results through SNMP traps to alert the network manager.

**Step 15** Select the **Cisco Discovery Protocol** check box if you want to enable it. CDP is a device discovery protocol that runs on all Cisco-manufactured equipment, such as routers, bridges, and communication servers. Each device sends periodic messages to a multicast address and listens to the messages that others send to learn about neighboring devices. When the device boots, it sends a CDP packet specifying whether the device is inline power enabled so that the requested power can be supplied.

---

**Note** Changing access point parameters temporarily disables an access point and might result in loss of connectivity to some clients.

---

**Step 16** Select the check box to enable rogue detection.

---

**Note** Rogue detection is disabled automatically for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. For more information regarding OfficeExtend access points, see the *Cisco Wireless LAN Controller Configuration Guide*.

---

**Step 17** Select the **Encryption** check box to enable encryption.

---

**Note** Enabling or disabling encryption functionality causes the access point to reboot, which then causes clients to lose connectivity.

---

**Note** DTLS data encryption is enabled automatically for OfficeExtend access points to maintain security, but disabled by default for all other access points.

---

**Note** Cisco 5500 controllers can be loaded with one of the two types of images, AS_5500_LDPE_x_x_x_x.aes or AS_5500_x_x_x_x.aes. For the 5500 controller loaded with former image, you need to have DTLS License to show encryption.

---

**Note** For WiSM2 and 2500 controllers, it is mandatory to have DTLS license to show encryption.

---

**Step 18** If rogue detection is enabled, the access point radio is turned off, and the access point listens to wired traffic only. The controllers that operate in this mode monitor the rogue access points. The controller sends all the rogue access point and client MAC address lists to the rogue detector, and the rogue detector forwards this information to the WLC. The MAC address list is compared to what the WLC access points expected. If the MAC addresses match, you can determine which rogue access points are connected on the wired network.

---

**Step 19** Select the **SSH Access** check box to enable SSH access.

---

**Step 20** Select the **Telnet Access** check box to enable Telnet access.
Note: An OfficeExtend access point might be connected directly to the WAN which allows external access if the default password is used by the access point. Therefore, Telnet and SSH access are disabled automatically for OfficeExtend access points.

Step 21: If you want to override credentials for this access point, select the **Override Global Username** and **Password** check box. You can then enter a new supplicant AP username, AP password, and Enable password that you want to assign for this access point.

Note: In the System > AP Username Password page, you can set global credentials for all access points to inherit as they join a controller. These established credentials appear in the lower right of the AP Parameters tab page.

The information that you enter is retained across controller and access point reboots and if the access point joins a new controller.

Step 22: Select the **Enable Link Latency** check box to enable link latency for this access point or unselect it to prevent the access point from sending the round-trip time to the controller after every echo response is received. See the “Configuring Link Latency Settings for Access Points” section on page 9-218 for more information on link latency.

Step 23: You can now manipulate power injector settings through the Prime Infrastructure without having to go directly to the controllers. In the Power Over Ethernet Settings section, select the check box to enable pre-standard or power injector state.

Pre-standard is chosen if the access point is powered by a high power Cisco switch; otherwise, it is disabled. If power injector state is selected, power injector options appear. The possible values are installed or override. If you choose override, you can either enter a MAC address or leave it empty so that it is supplied by WLC.

Note: To determine which source of power is running the Prime Infrastructure, choose Monitor > Access Points, click Edit View, and then choose and move POE Status to the View Information box. After you click Submit, the POE status appears in the last column. If the device is powered by an injector, the POE status appears as Not Applicable.

Step 24: Select the **Enable** check box to enable the following FlexConnect configurations:

Note: FlexConnect settings cannot be changed when the access point is enabled.

- OfficeExtend AP—The default is Enabled.

Note: Unselecting the check box simply disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point, but it does put the access point at risk because it becomes remotely deployed. If you want to clear the configuration of an access point and return it to factory default settings, click **Clear Config** at the bottom of the access point details page. If you want to clear only the personal SSID of the access point, click **Reset Personal SSID** at the bottom of the access point details page.

When you select Enabled for the OfficeExtend AP, a warning message provides the following information:
• Configuration changes that automatically occur. Encryption and Link Latency are enabled. Rogue Detection, SSH Access, and Telnet Access are disabled.

• A reminder to configure at least one primary, secondary, and tertiary controller (including name and IP address).

Note Typically, an access point first looks for the primary controller to join. After that, the controller tries the secondary and then the tertiary controller. If none of these controllers are configured, the access point switches to a default discovery mode in an attempt to join whatever controller it might find.

An OfficeExtend access point searches only for a primary, secondary, or tertiary controller to join. It does not look any further for a configured controller. Because of this, it is important that you configure at least one primary, secondary, or tertiary controller name and IP address.

– A warning the enabling encryption causes the access point to reboot and causes clients to lose connectivity.

• Least Latency Controller Join—When enabled, the access point switches from a priority order search (primary, secondary, and then tertiary controller) to a search for the controller with the best latency measurement (least latency). The controller with the least latency provides the best performance.

Note The access point only performs this search once when it initially joins the controller. It does not recalculate the primary, secondary, and tertiary controllers latency measurements once joined to see if the measurements have changed.

• VLAN Support—When selected, enter the Native VLAN identifier.

When Enable VLAN is selected, the Prime Infrastructure displays locally switched VLANs. You can only edit a VLAN ID that is mapped to a WLAN ID.

• AP level VLAN ACL Mapping—This group box appears only for FlexConnect mode access points with VLAN support enabled. You can only edit the Ingress and Egress ACLs mapped to a VLAN ID.

Note The AP level VLAN ACL Mapping configuration is pushed to the access point, only when the VLAN IDs entered in the Prime Infrastructure is available in the AP Level VLAN ACL Mapping section of the access point in the associated controller.

• Group level VLAN ACL Mapping—This group box appears only for FlexConnect mode access points with VLAN support enabled. You can view the Group level VLAN ACL mapping that you have specified under the ACL tab of the FlexConnect ACL groups.

• PreAuthentication ACL Mappings

– Web-Authentication and Web-Policy ACLs—Click the External WebAuthentication ACLs link to view the WebAuth and Web Policy ACL mappings at access point level. The ACL Mappings page lists details of the WLAN ACL mappings and web policy ACLs.

Step 25 Select the role of the mesh access point from the Role drop-down list. The default setting is MAP.
Note: An access point in a mesh network functions as either a root access point (RAP) or mesh access point (MAP).

Step 26: Enter the name of the bridge group to which the access point belongs. The name can have up to 10 characters.

Note: Bridge groups are used to logically group the mesh access points to avoid two networks on the same channel from communicating with each other.

Note: For mesh access points to communicate, they must have the same bridge group name.

Note: For configurations with multiple RAPs, make sure that all RAPs have the same bridge group name to allow failover from one RAP to another.

Note: For configurations where separate sectors are required, make sure that each RAP and its associated MAPs have separate bridge group names.

The Type field appears whether the mesh access point is an indoor or outdoor access point, and the Backhaul Interface field displays the access point radio that is being used as the backhaul for the access point.

Step 27: Choose the data rate for the backhaul interface from the drop-down list. Data rates available are dictated by the backhaul interface. The default rate is 18 Mbps.

Note: This data rate is shared between the mesh access points and is fixed for the whole mesh network.

Note: Do NOT change the data rate for a deployed mesh networking solution.

Step 28: Choose Enable from the Ethernet Bridging drop-down list to enable Ethernet bridging for the mesh access point.

Step 29: Click Save to save the configuration.

Step 30: Re-enable the access point radios.

Step 31: If you need to reset this access point, click Reset AP Now.

Step 32: Click Reset Personal SSID to reset the OfficeExtend access point personal SSID to the factory default.

Step 33: If you need to clear the access point configuration and reset all values to the factory default, click Clear Config.
Configuring an Ethernet Interface

Note The 152x mesh access points are configured on any one of these four ports: port 0-PoE in, port 1-PoE out, Port 2 - cable, and port 3- fiber. Other APs (such as 1130,1140,1240,1250) are configured on Port 2 - cable.

To configure an Ethernet interface, follow these steps:

Step 1 Choose Configure > Access Points.

Step 2 Click the link under AP Name to see detailed information about that access point name. The Access Point Detail page appears.

Note The Access Point Details page displays the list of Ethernet interfaces.

Step 3 Click the link under Interface to see detailed information about that interface. The Ethernet Interface page appears.

This page displays the following parameters:
- AP Name—The name of the access point.
- Slot Id—Indicates the slot number.
- Admin Status—Indicates the administration state of the access point.
- CDP State—Select the CDP State check box to enable the CDP state.

Step 4 Click Save.

Viewing the Deleted AP Jobs

In earlier releases of Prime Infrastructure, when you delete a controller, the associated APs are not deleted and remain in the “unassociated” state. When you delete a controller in Prime Infrastructure 2.2, you get a message so that you can delete the associated APs. To view the details of the deleted APs which were associated to a controller, choose Administration > Jobs Dashboard (in the Lifecycle view).

When you delete a controller using the Classic view, the following message appears:
Do you want to delete APs Associated to the selected Devices. To check AP delete status please go to Configure > AccessPoints > View Delete AP Job(s).

To view the details of the deleted APs (which were associated with a controller), choose Configure > Access Points, choose View Delete AP Job(s) from the Select a command drop-down list, and then click Go.

When you delete a controller using the Lifecycle view, the following message appears:
Do you want to delete APs Associated to the selected Devices.

To view the details of the deleted APs which were associated with a controller), choose Administration > Jobs Dashboard.
## Importing AP Configuration

To import a current access point configuration file, follow these steps:

**Step 1** Choose **Configure > Access Points**.

**Step 2** From the **Select a command** drop-down list, choose **Import AP Config**.

A pop-up alert box appears stating All Unified AP(s) are imported from CSV file only. Unified AP(s) from Excel and XML file are not imported.

**Step 3** Click **OK** to close the pop-up alert box.

**Step 4** Click **Go**.

**Step 5** Enter the CSV file path in the text box or click **Browse** to navigate to the CSV file on your computer.

The first row of the CSV file is used to describe the columns included. The AP Ethernet Mac Address column is mandatory. The parameters on this page are used for columns not defined in the CSV file.

Sample File Header:

```
AP Name, Ethernet MAC, Location, Primary Controller, Secondary Controller, Tertiary Controller
ap-1, 00:1c:58:74:8c:22, sjc-14-a, controller-4404-1, controller-4404-2, controller-4404-3
```

The CSV file can contain following fields.

- AP Ethernet MAC Address—Mandatory
- AP Name—Optional
- Location—Optional
- Primary Controller—Optional
- Secondary Controller—Optional
- Tertiary Controller—Optional

Optional fields can remain empty. The AP Config Import ignores empty optional field values. However, if primaryMwar and secondaryMwar entries are empty then a unified access point update is not complete.

- Ethernet MAC—AP Ethernet MAC Address
- AP Name—AP Name
- Location—AP Location
- Primary Controller—Primary Controller Name
- Secondary Controller—Secondary Controller Name
- Tertiary Controller—Tertiary Controller Name

**Note** Optional fields can remain empty. The AP Config Import ignores empty optional field values. However, if primaryMwar and secondaryMwar entries are empty then a unified access point update is not complete.

**Step 6** When the appropriate CSV file path appears in the Select CSV File text box, click **OK**.
Exporting AP Configuration

To export current access point configuration files, follow these steps:

**Step 1** Choose **Configure > Access Points**.

**Step 2** From the Select a command drop-down list, choose **Export AP Config**.

A pop-up alert box appears stating All Unified AP(s) are exported to CSV/EXCEL/XML file.

**Step 3** Click **OK** to close the pop-up alert box.

**Step 4** Click **Go** to view the current AP configurations including:

- AP Name
- Ethernet MAC
- Location
- Primary Controller
- Secondary Controller
- Tertiary Controller

**Step 5** Select the file option (CSV, Excel, XML) to export the access point configurations.

**Step 6** In the File Download window, click **Save** to save the file.

Configuring Access Points 802.11n Antenna

Prime Infrastructure provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

**Note** At least one transmitting and one receiving antenna must be enabled. You cannot disable all transmitting or all receiving antennas at once.

If you choose **Configure > Access Points** and select an **802.11n** item from the Radio column, the following page appears.

This page contains the following fields:

**Note** Changing any of the fields causes the radio to be temporarily disabled and thus might result in loss of connectivity for some clients.

**General**

- AP Name—The operator-defined name of the access point.
- AP Base Radio MAC—MAC address of the base radio of the access point.
- Admin Status—Select the box to enable the administration state of the access point.
- CDP State—Select the CDP State check box to enable CDP.
- Controller—IP address of the controller. Click the IP address of the controller for more details.
- Site Config ID—Site identification number.
- CleanAir Capable—Displays if the access point is CleanAir capable.
- CleanAir—CleanAir Administration status of the spectrum sensor for the access point that you can enable or disable. You can set this field to the following options:
  - Both Enabled—Enables CleanAir for both 2.4-GHz and 5-GHz radios.
  - Both Disabled—Disables CleanAir for both 2.4-GHz and 5-GHz radios.
  - 2.4-GHz Enabled—Enables CleanAir only for 2.4-GHz radio.
  - 5-GHz Enabled—Enables CleanAir only for 5-GHz radio.

**Antenna**

- Antenna Type—Indicates an external or internal antenna.
- Antenna Diversity—Select **Right**, **Left**, or **Enabled**.

| Note | Antenna diversity refers to the Cisco Aironet access point feature where an access point samples the radio signal from two integrated antenna ports and choose the preferred antenna. This diversity option is designed to create robustness in areas with multi-path distortion. |

For external antenna, select one of the following:
- Enabled—Use this setting to enable diversity on both the left and right connectors of the access point.
- Left—Use this setting if your access point has removable antennas and you install a high-gain antenna on the left connector of the access point.
- Right—Use this setting if your access point has removable antennas and you install a high-gain antenna on the right connector of the access point.

For internal antennas, select one of the following:
- Enabled—Use this setting to enable diversity on both Side A and Side B.
- Side A—Use this setting to enable diversity on Side A (front antenna) only.
- Side B—Use this setting to enable diversity on Side B (rear antenna) only.

- External Antenna—Choose the **external antenna** or **Other** from the drop-down list.

| Note | For an 802.11a/b/g/n radio, the antenna type is Internal and the external antenna is Internal-3rdRadio. |

- Antenna Gain—Enter the desired antenna gain in the text box.

| Note | The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBi. An integer value 4 means $4 \times 0.5 = 2$ dBi of gain. |

- Current Gain (dBm)—Indicates the current gain in dBm.

See the Cisco Aironet Antenna Reference Guide for antenna dBi values.
WLAN Override

The following 802.11a WLAN Override field appears:

- WLAN Override—Choose Enable or Disable from the drop-down list.

*Note* When you enable WLAN Override, operating system displays a table showing all current Cisco WLAN Solution WLANs. In the table, select WLANs to enable WLAN operation, and deselect WLANs to disallow WLAN operation for this 802.11a Cisco Radio.

*Note* WLAN override does not apply to access points that support the 512 WLAN feature.

Performance Profile

Click the URL to view or edit performance profile parameters for this access point interface.

- ClientLink—Enable or disable client link for the access point radios per interface. This feature is only supported for legacy (orthogonal frequency-division multiplexing) OFDM rates. The interface must support ClientLink, and OFDM rates must be enabled. Also, two or more antennas must be enabled for transmission, and all three antennas must be enabled for reception.

*Note* The maximum number of clients supported is 15. If the antenna configuration restricts operation to a single transmit antenna or OFDM rates are disabled, ClientLink cannot be used.

RF Channel Assignment

The following 802.11a RF Channel Assignment parameters appear:

- Current Channel—Channel number of the access point.

- Assignment Method—Select one of the following:
  - Global—Use this setting if the channel of the access point is set globally by the controller.
  - Custom—Use this setting if the channel of the access point is set locally. Select a channel from the drop-down list.

  For example, if you select 2(17 dBm) as the custom power, 2 corresponds to the Power Level and 17 is the Absolute Power (dBm).

- Channel width—Select the channel width from the drop-down list. The selections include 20, above 40, and below 40.

  RF Channel assignment supports 802.11n 40 MHz channel width in the 5-GHz band. 40-MHz channelization allows radios to achieve higher instantaneous data rates.

*Note* Selecting a larger bandwidth reduces the non-overlapping channels which could potentially reduce the overall network throughput for certain deployments.

*Note* The power level and channel numbers of an access point are not audited.
Tx Power Level Assignment

- Current Tx Power Level—Indicates the current transmit power level.
- Assignment Method—Select one of the following:
  - Global—Use this setting if the power level is set globally by the controller.
  - Custom—Use this setting if the power level of the access point is set locally. Choose a power level from the drop-down list.

11n Antenna Selection

Prime Infrastructure provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>At least one transmitting and one receiving antenna must be enabled. You cannot disable all transmitting or all receiving antennas at once.</td>
</tr>
</tbody>
</table>

Select any of the 11n Antenna Selection parameters:
- Antenna A
- Antenna B
- Antenna C
- Antenna D

11n Parameters

The following 11n fields appear:
- 11n Supported—Indicates whether or not 802.11n radios are supported.
- Client Link—Use this option to enable or disable client links. Choose Enable, Disable, or Not Applicable from the drop-down list.

Configuring CDP

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP is enabled on the Ethernet and radio ports of the bridge by default.</td>
</tr>
</tbody>
</table>

Configuring CDP on Access Points

To configure CDP on Radio or Ethernet interfaces, follow these steps:

2. Choose an access point associated with software release 5.0 or later.
Step 3  Click the slots of radio or an Ethernet interface for which you want to enable CDP.
Step 4  Select the CDP State check box to enable CDP on the interface.
Step 5  Click Save.

---

**Configuring Access Point Radios for Tracking Optimized Monitor Mode**

To optimize monitoring and location calculation of tags, you can enable Tracking Optimized Monitor Mode (TOMM) on up to four channels within the 2.4-GHz band (802.11b/g radio) of an access point. This allows you to focus channel scans only on those channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

After enabling Monitor mode at the access point level, you must then enable TOMM and assign monitoring channels on the 802.11b/g radio of the access point.

**Note**
For details on enabling Monitor mode on an access point, see Step 6 in the “Configuring Access Point Details” section on page 9-184.

To set enable TOMM and assign monitoring channels on the access point radio, follow these steps:

Step 1  After enabling Monitor mode at the access point level, choose Configure > Access Points.
Step 2  In the Access Points page, click the 802.11 b/g Radio link for the appropriate access point.
Step 3  In the General group box, disable Admin Status by unselecting the check box. This disables the radio.
Step 4  Select the TOMM check box. This check box only appears for Monitor Mode APs. The drop-down lists for each of the four configurable channels are displayed.
Step 5  Choose the four channels on which you want the access point to monitor tags.

**Note**  You can configure fewer than four channels for monitoring. To eliminate a monitoring channel, choose None from the channel drop-down list.

Step 6  Click Save. Channel selection is saved.
Step 7  In the Radio parameters page, reenable the radio by selecting the Admin Status check box.
Step 8  Click Save. The access point is now configured as a TOMM access point.

The AP Mode displays as Monitor/TOMM in the Monitor > Access Points page.

---

**Copying and Replacing Access Points**

The Copy and Replace AP feature is useful if you need to remove an access point from the network and replace it with a new access point. All of the access point information, such as AP mode, name, and map location needs to be copied from the old access point to the new access point.
The Copy and Replace AP feature is supported for same type of APs only.

To access the Copy and Replace AP function, follow these steps:

Step 1  Choose Configure > Access Points.
Step 2  Select the check box for the applicable access point.
Step 3  From the Select a command drop-down list, choose Copy and Replace AP.
Step 4  Click Go.

The old access point needs to be removed from the network first. This access point then becomes unassociated to any controller. When you plug in the new access point, it is associated with the controller and Prime Infrastructure refreshes the information. At that point, select the old unassociated access point and choose to copy and replace the configuration to the new access point.

Note  If a different access point type is used to replace an older access point, only the configuration parameters that apply are copied.

Removing Access Points

To remove access points that are not associated, follow these steps:

Step 1  Choose Configure > Access Points.
Step 2  From the Select a command drop-down list, choose Remove APs.
Step 3  Click Go.
Step 4  Click OK to confirm the removal.

Scheduling and Viewing Radio Status

- Scheduling Radio Status, page 9-200
- Viewing Scheduled Tasks, page 9-201

Scheduling Radio Status

To schedule a radio status change (enable or disable), follow these steps:

Step 1  Choose Configure > Access Points.
Step 2  Select the check box for the applicable access point(s).
Step 3  From the Select a command drop-down list, choose Schedule Radio Status.
Step 4  Click Go.
Step 5  Choose Enable or Disable from the Admin Status drop-down list.
Step 6  Use the Hours and Minutes drop-down lists to determine the scheduled time.
Step 7  Click the calendar icon to select the scheduled date for the status change.
Step 8  If the scheduled task is recurring, choose Daily or Weekly, as applicable. If the scheduled task is a one-time event, choose No Recurrence.
Step 9  Choose Save to confirm the scheduled task.

Viewing Scheduled Tasks

To view currently scheduled radio status tasks, follow these steps:

Step 1  Choose Configure > Access Points.
Step 2  Select the check box for the applicable access point(s).
Step 3  From the Select a command drop-down list, choose View Scheduled Radio Task(s).
Step 4  Click Go.

The Scheduled Task(s) information includes:
- Scheduled Task(s)—Choose the task to view its access points and access point radios.
- Scheduled Radio adminStatus—Indicates the status change (Enable or Disable).
- Schedule Time—Indicates the time the schedule task occurs.
- Execution status—Indicates whether or not the task is scheduled.
- Recurrence—Indicates Daily or Weekly if the scheduled task is recurring.
- Next Execution—Indicates the time and date of the next task occurrence.
- Last Execution—Indicates the time and date of the last task occurrence.
- Unschedule—Click Unschedule to cancel the scheduled task. Click OK to confirm the cancellation.

Viewing Audit Status (for Access Points)

An Audit Status column in the Configure > Access Points page shows an audit status for each of the access points. You can also view the audit report for the selected access points. The report shows the time of the audit, the IP address of the selected access point, and the synchronization status.

To view the audit status, follow these steps:

Step 1  Choose Configure > Access Points.
Step 2  Click the Audit Status column value to go to the latest audit details page for the selected access point. This report is interactive and per access point.
If you hover your mouse cursor over the Audit Status column value, the time of the last audit is displayed.

To run an access point on-demand audit report, select the desired access point for which you want to run the report and choose Audit Now from the Select a command drop-down list. In versions prior to 4.1, the audit only spanned the parameters present in the AP Details and AP Interface Details page. In Release 4.1, this audit report covers complete access point level auditing. The audit results are stored in the database so that you can view the latest audit reports without having to run another audit.

The audit can only be run on an access point that is associated to a controller.

Filtering Alarms for Maintenance Mode Access Points

Prime Infrastructure uses critical alarms to track if the managed access points are down. The controller sends three different alarms when the following occurs:

- The Access point is down
- Radio A of the access point is down
- Radio B/G of the access point is down

In Release 7.0.172.0 and later, these 3 alarms are grouped into a single alarm.

When an access point is under technical maintenance, the critical alarms need to be deprioritized. You can deprioritize the severity of an alarm of an access point using the Configure > Access Points page. When you move an access point to maintenance state, the alarm status for that access point appears in black color.

- Placing an Access Point in Maintenance State, page 9-202
- Removing an Access Point from Maintenance State, page 9-203

Placing an Access Point in Maintenance State

To move an access point to the maintenance state, follow these steps:

**Step 1**
Choose Prime Infrastructure > Configure > Access Points.
The Access Points page appears.

**Step 2**
From the drop-down list, choose Place in Maintenance State, and click Go.
The access point is moved to maintenance state.

Once the access point is moved to maintenance state, the access point down alarms are processed with lower severity instead of critical.
Removing an Access Point from Maintenance State

To remove an access point from the maintenance state, follow these steps:

**Step 1**  Choose Prime Infrastructure > Configure > Access Points.
The Access Points page appears.

**Step 2**  From the drop-down list, choose Remove from Maintenance State, and click Go.
The access point is removed from the maintenance state.

Searching Access Points

Use the search options in the uppermost right corner of the page to create and save custom searches:

- New Search: Enter an IP address, name, SSID, or MAC, and click Search.
- Saved Searches: Click Saved Search to choose a category, a saved custom search, or choose other criteria for a search from the drop-down lists.
- Advanced Search: An advanced search allows you to search for a device based on a variety of categories and filters.

See the Search Methods section in the Cisco Prime Infrastructure 2.0 User Guide for additional information.

After you click Go, the access point search results appear (see Table 9-4).

<table>
<thead>
<tr>
<th>Table 9-4</th>
<th>Access Point Search Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Options</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the access point.</td>
</tr>
<tr>
<td>Ethernet MAC</td>
<td>MAC address of the access point.</td>
</tr>
<tr>
<td>AP Name</td>
<td>Name assigned to the access point. Click the access point name item to display details.</td>
</tr>
<tr>
<td>Radio</td>
<td>Protocol of the access point is either 802.11a/n or 802.11b/g/n.</td>
</tr>
<tr>
<td>Map Location</td>
<td>Campus, building, and floor location.</td>
</tr>
<tr>
<td>Controller</td>
<td>IP address of the controller.</td>
</tr>
<tr>
<td>AP Type</td>
<td>Access point radio frequency type.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Displays the operational status of the Cisco radios (Up or Down).</td>
</tr>
<tr>
<td>Alarm Status</td>
<td>Alarms are color coded as follows:</td>
</tr>
<tr>
<td></td>
<td>• Clear = No Alarm</td>
</tr>
<tr>
<td></td>
<td>• Red = Critical Alarm</td>
</tr>
<tr>
<td></td>
<td>• Orange = Major Alarm</td>
</tr>
<tr>
<td></td>
<td>• Yellow = Minor Alarm</td>
</tr>
<tr>
<td>Audit Status</td>
<td>The audit status of the access point.</td>
</tr>
</tbody>
</table>
Viewing Mesh Link Details

You can access mesh link details in several ways:

- Click the Mesh dashboard in the Prime Infrastructure home page
- Choose Monitor > Access Points, click the Mesh Links tab and then click the Details link
- After you import a KML file from Google Earth, click the AP Mesh link

The current statistics are displayed at the top of the page followed by diagrams for certain statistics.

- SNR Graph—SNR Up and Down graphs are combined into one graph. Each set of data is represented by different colors.
- Link Metrics Graph—The Adjusted Link Metric and Unadjusted Link Metric is combined into one graph. Each set of data is represented by different colors.
- Packet Error Rate Graph—Displays the packet error rates in a graph.
- Link Events—The last five events for the link are displayed.
- Mesh Worst SNR Links—Displays the worst signal-to-noise ratio (SNR) links.
- AP Uptime—These statistics help determine if an access point is rebooting frequently.
- LWAPP Join Taken Time—These statistics determine how long it takes an access point to join.
- Location Links—Allows you to navigate to the Prime Infrastructure map or the Google Earth location.

Viewing or Editing Rogue Access Point Rules

You can view or edit current rogue access point rules on a single WLC. See the “Configuring a Rogue AP Rules Template” section on page 11-73 for more information.

To access the rogue access point rules, follow these steps:

**Step 1** Choose Configure > Controllers.

**Step 2** Click an IP address in the IP Address column.

**Step 3** From the left sidebar menu, choose Security > Rogue AP Rules. The Rogue AP Rules displays the rogue access point rules, the rule types (malicious or friendly), and the rule sequence.

**Step 4** Choose a Rogue AP Rule to view or edit its details.
Configuring Switches

You can add switches to the Prime Infrastructure database to view overall switch health and endpoint monitoring and to perform switchport tracing. While this switch functionality appears on the Configuration menu in the Prime Infrastructure, you are configuring the Prime Infrastructure system and not the switches. You cannot configure switch features using the Prime Infrastructure.

Prime Infrastructure allows you to do the following:

- Add switches in Configure > Switches page and specify CLI and SNMP credentials. See the “Adding Switches” section on page 9-208 for more information.
- Monitor Switches by choosing Monitor > Switches. See the “Monitoring Switches” section on page 5-34 for more information.
- Run switch-related reports using the Reports menu.

**Note**
In the Configure > Switches page, you can also add a location-capable switch for tracking wired clients by mobility services engine and Prime Infrastructure.

- Configuring Switches, page 9-205
- Configuring Spectrum Experts, page 9-215

**Note**
The following switches are supported: 3750, 3560, 3750E, 3560E, and 2960.

Features Available by Switch Type

When you add a switch to the Prime Infrastructure, you specify how the switch is to be managed. Based on how you specify the switch is to be managed, the Prime Infrastructure determines which features are available:

- Monitored switches—You can add switches (choose **Configure > Switches**) and monitor switch operation (choose **Monitor > Switches**). Each switch counts as a single device against the total device count for your license. If you have unused device counts available in your license engine, you can add a switch to the Prime Infrastructure. If you have no remaining device counts available, you cannot add additional switches to the Prime Infrastructure.
- Switch Port Tracing (SPT) only switches—Switches perform switch port tracing only. SPT-only switches appear in the Configure > Switches page and in inventory reports, but SPT-only switches do not appear in the Monitor > Switches page or on the dashboards. Licensing does not apply to SPT switches.

Viewing Switches

Choose **Configure > Switches** to see a summary of all switches in the Prime Infrastructure database. The summary information includes the following:

- Management IP Address—IP address of the switch. Click the IP address of a switch to get more details. See the “Viewing Switch Details” section on page 9-206 for more information.
- Device Name—Name of the switch.
• Device Type—Type of switch.
• Reachability Status—Indicates Reachable if the switch is reachable or Unreachable if the switch is unreachable.
• Inventory Collection Status—Status of the last inventory collection. The possible values are OK, Partial, Failed, NA (for SPT-only switches), or In Progress.
• Inventory Status Detail—Specifies the status of the latest inventory collection. If the inventory collection was not successful, lists the possible reasons for the failure.
• Last Inventory Collection Date—Displays the most recent date in which the inventory was collected.
• Creation Time—Date and time the switch was added to the Prime Infrastructure.
• License Status—Indicates the license status of the switch, which can be Full Support or SPT only. See the “Features Available by Switch Type” section on page 9-205 for more information.

Click any column heading to sort the information by that column. You can switch between ascending and descending sort order by clicking the column heading more than once.

### Viewing Switch Details

Choose Configure > Switches to see a summary of all switches in the Prime Infrastructure database. Click an IP address in the Management IP Address column to see detailed information about that switch. Table 9-5 describes the summary information that is displayed.

| Table 9-5  Configure > Switches Summary Information |
|-----------------------------|-------------------------------------------------|
| **General Parameters**      |                                                 |
| IP Address                  | IP address of the switch.                      |
| Device Name                 | Name of the switch.                            |
| Last Inventory Collection Date | Date and time of the last inventory collection. |
| Inventory Collection Status | Status of the last inventory collection. The possible values are OK, Partial, or Failed. |
| Software Version            | Version of software running on the switch.     |
| Location                    | Location of the switch.                        |
| Contact                     | Contact name for the switch.                   |
| Reachability Status         | Indicates **Reachable** if the switch is reachable or **Unreachable** if the switch is unreachable. |

| **SNMP Parameters**         |                                                 |
| Version                     | SNMP version number, which can be v1, v2c, or v3. |
| Note                        | For switch port tracing to be successful in switches configured with SNMP v3, the context for the corresponding VLAN must be configured in the switch. See the “Configuring SNMPv3 on Switches” section on page 9-209 for more information. |
| Retries                     | Retries (in seconds) allowed before the process stops without success. |
| Timeout                     | Indicate the amount of time (in seconds) allowed before the process time outs. The valid range is 2 to 90 seconds. The default is 10 seconds. |

If you selected v3 in the Version drop-down list, the following fields appear:

| Username                     | Username |
| Auth. Type                   | Authentication type with can be None, HMAC-SHA, or HMAC-HD5. |
Configuring Switches

To modify SNMP parameters for a switch, follow these steps:

Step 1 Choose Configure > Switches, then click the IP address of the switch for which you want to change SNMP credentials.

Step 2 Modify the necessary SNMP Parameters fields, then click the following:

- **Reset** to restore the previously saved parameters.
- **Save** to save and apply the changes you made.
- **Cancel** to exit without saving your changes and return to the previous screen.

To modify Telnet or SSH parameters for a switch, follow these steps:

Step 1 Choose Configure > Switches, then click the IP address of the switch for which you want to change Telnet or SSH credentials.

Step 2 Modify the necessary Telnet/SSH Parameters fields, then click the following:

- **Reset** to restore the previously saved parameters.
- **Save** to save and apply the changes you made.
- **Cancel** to exit without saving your changes and return to the previous screen.

### Table 9-5 Configure > Switches Summary Information (continued)

<table>
<thead>
<tr>
<th>General Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auth. Password</strong></td>
</tr>
<tr>
<td><strong>Privacy Type</strong></td>
</tr>
<tr>
<td><strong>Privacy Password</strong></td>
</tr>
<tr>
<td><strong>Community</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Telnet/SSH Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protocol</strong></td>
</tr>
<tr>
<td><strong>User Name</strong></td>
</tr>
<tr>
<td><strong>Password</strong></td>
</tr>
<tr>
<td><strong>Confirm Password</strong></td>
</tr>
<tr>
<td><strong>Enable Password</strong></td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
</tr>
</tbody>
</table>

### Modifying SNMP Parameters

To modify SNMP parameters for a switch, follow these steps:

Step 1 Choose Configure > Switches, then click the IP address of the switch for which you want to change SNMP credentials.

Step 2 Modify the necessary SNMP Parameters fields, then click the following:

- **Reset** to restore the previously saved parameters.
- **Save** to save and apply the changes you made.
- **Cancel** to exit without saving your changes and return to the previous screen.

### Modifying Telnet/SSH Parameters

To modify Telnet or SSH parameters for a switch, follow these steps:

Step 1 Choose Configure > Switches, then click the IP address of the switch for which you want to change Telnet or SSH credentials.

Step 2 Modify the necessary Telnet/SSH Parameters fields, then click the following:

- **Reset** to restore the previously saved parameters.
- **Save** to save and apply the changes you made.
- **Cancel** to exit without saving your changes and return to the previous screen.
Adding Switches

When you add a switch to the Prime Infrastructure database, by default, the Prime Infrastructure verifies the SNMP credentials of the switch. If the device credentials are not correct, you receive an SNMP failure message but the switch is added to the Prime Infrastructure database.

To add a switch to the Prime Infrastructure, follow these steps:

Step 1  Choose Configure > Switches.
Step 2  From the Select a command drop-down list, choose Add Switches, then click Go.
Step 3  Complete the fields as described in Table 9-6.

Table 9-6 Adding a Switch

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>Add Format Type</td>
<td>Select:</td>
</tr>
<tr>
<td>Device Info</td>
<td>to manually enter comma-separated IP addresses of Ethernet switches.</td>
</tr>
<tr>
<td>CSV File</td>
<td>to import a CSV file that contains IP addresses of multiple switches. Enter the CSV file path in the text box or click Browse to navigate to the CSV file on your computer. See the “Configuring SNMPv3 on Switches” section on page 9-209 for more information.</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>If you selected Device Info, enter comma-separated IP addresses of the Ethernet switches.</td>
</tr>
<tr>
<td>License Level</td>
<td>Select:</td>
</tr>
<tr>
<td>Full</td>
<td></td>
</tr>
<tr>
<td>SPT only</td>
<td>to specify Switch Port Tracing support only.</td>
</tr>
<tr>
<td><strong>SNMP Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>Note Enter SNMP parameters for the write access, if available. If you enter read-only access parameters, the switch is added but the Prime Infrastructure is unable to modify the configuration.</td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td>Enter the SNMP version number, which can be v1, v2c, or v3.</td>
</tr>
<tr>
<td>Note For switch port tracing to be successful in switches configured with SNMP v3, the context for the corresponding VLAN must be configured in the switch. See the “Configuring SNMPv3 on Switches” section on page 9-209 for more information.</td>
<td></td>
</tr>
<tr>
<td>Retries</td>
<td>Enter the retries (in seconds) allowed before the process stops without success.</td>
</tr>
<tr>
<td>SNMP Timeout (in secs)</td>
<td>Enter the SNMP timeout value (in seconds).</td>
</tr>
<tr>
<td>If you selected v1 or v2c in the Version drop-down list, the Community field appears:</td>
<td>Community Enter the SNMP community string.</td>
</tr>
<tr>
<td>If you selected v3 in the Version drop-down list, the following fields appear:</td>
<td>Username Enter the username.</td>
</tr>
<tr>
<td>Auth. Type</td>
<td>Enter the authentication type with can be None, HMAC-SHA, or HMAC-HD5.</td>
</tr>
<tr>
<td>Auth. Password</td>
<td>Enter the authentication password.</td>
</tr>
<tr>
<td>Privacy Type</td>
<td>Enter the privacy type with can be None, CBC-DES, or CFB-AES-128.</td>
</tr>
<tr>
<td>Privacy Password</td>
<td>Enter the privacy password.</td>
</tr>
</tbody>
</table>
Chapter 9      Configuring Devices

Configuring Switches

Table 9-6     Adding a Switch (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet/SSH Parameters</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocol.</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the username.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password by entering it again.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Enter the enable password.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the enable password by entering it again.</td>
</tr>
<tr>
<td>Timeout (in secs)</td>
<td>Enter the timeout value (in seconds).</td>
</tr>
</tbody>
</table>

Step 4  Click Add to add the switch.
Step 5  Click Cancel to cancel the operation and return to the list of switches.

Note  After adding a switch, it is placed temporarily in the Monitor > Unknown Devices page while
the Prime Infrastructure attempts to communicate with the controller that you have added. Once
communication with the switch has been successful, the switch moves from the Monitor >
Unknown Devices page to the Monitor > Switches page. If the Prime Infrastructure is unable to
successfully communicate with a switch, it remains in the Monitor > Unknown Devices and an
error condition an error message is displayed. To access the Unknown Devices page, choose
Configure > Unknown Devices.

Configuring SNMPv3 on Switches

The following is an example for configuring SNMPv3 on the switch:

```
snmp-server view v3default iso included
snmp-server group v3group v3 auth write v3default snmp-server user <username>
   v3 auth <md5 or sha> <authentication password>
```

If the switch has VLANs, you must configure each VLAN, otherwise switch porting tracing fails. The
following is an example if the switch has VLANs 1 and 20.

```
snmp-server group v3group v3 auth context vlan-1 write v3default
snmp-server group v3group v3 auth context vlan-20 write v3default
snmp-server group v3group v3 auth context vlan-20 write v3default
```

Note  When you create SNMP v3 view, make sure you include all of the OIDs.

Sample CSV File for Importing Switches

The first row of the CSV file is used to describe the columns included. The IP Address column is
mandatory. The following example shows a sample CSV file.
Configuring Switch NMSP and Location

Choose Prime Infrastructure > Configure > Switches > Switch IP Address > NMSP & Location to view the NMSP and Location information for switches.

Note: NMSP is supported by the following:
- Cisco Catalyst 3000 and 4000 series switches
- Cisco IOS Release 12.50 and later
You can enable or disable NMSP status and configure switch and switch port location as described in the following sections:

- Enabling and Disabling NMSP for Switches
- Configuring a Switch Location
- Configuring a Switch Port Location

### Enabling and Disabling NMSP for Switches

You can enable or disable NMSP for a switch by choosing **Prime Infrastructure > Configure > Switches > Switch IP Address > NMSP & Location > NMSP Status**.

Table 9-7 lists the options available in the NMSP Status page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NMSP</td>
<td>Select or Unselect this option to enable or disable NMSP for the switch.</td>
</tr>
<tr>
<td>MSE IP Address</td>
<td>Displays the IP address of the MSE if the switch is associated to an MSE. To associate this switch to an MSE, click <strong>Go to Synchronize</strong>. This takes you to the Synchronization page. You can synchronize this switch with an MSE. Alternately, you can choose <strong>Prime Infrastructure &gt; Services &gt; Synchronize Services &gt; Wired Switches</strong> to synchronize switches to an MSE. For more information on Synchronization, see the “Synchronizing Services” section on page 16-12.</td>
</tr>
</tbody>
</table>

### Configuring a Switch Location

You can configure the location for a switch using the Switch Location option.

**Step 1** Choose **Prime Infrastructure > Configure > Switches > Switch IP Address > NMSP & Location > Switch Location**.

**Step 2** In the Map Location pane, choose the following from the drop-down lists:

- Campus
- Building
- Floor

**Step 3** Click **Import Civic** to import the civic information to the switch.

The fields in the Civic Location pane are populated after the civic information is imported.

### Configuring a Switch Port Location

You can configure location for switch ports using the Switch Port Location option.

**Step 1** Choose **Prime Infrastructure > Configure > Switches > Switch IP Address > NMSP & Location > Switch Port Location**.
Step 2 Select one or more ports on which you want to configure location.

Step 3 From the drop-down list, choose Configure Location, then click Go.

The Switch Port Location Configuration page appears.

The Switch Ports pane lists the ports that you have selected to configure location.

Step 4 In the Map Location pane, choose the following from the drop-down lists:
- Campus
- Building
- Floor

Step 5 Click Import Civic to import the civic information to the switch port.

The fields in the Civic Location pane are populated after the civic information is imported.

---

### Removing Switches

When you remove a switch from the Prime Infrastructure database, the following functions are performed:

- Inventory information for that switch is removed from the database.
- Alarms for the switch remain in the database with a status of Clear. By default, cleared alarms are not displayed in the Prime Infrastructure interface.
- Saved reports remain in the database even if the switch on which the report was run is removed.

To remove a switch from the Prime Infrastructure, follow these steps:

Step 1 Choose Configure > Switches.

Step 2 Select the check box(es) of the switch(es) you want to remove.

Step 3 From the Select a command drop-down list, choose Remove Switches.

Step 4 Click Go.

Step 5 Click OK to confirm the deletion.

---

### Refreshing Switch Configuration

By default, inventory information is collected every six hours. If you make configuration changes and want the changes displayed immediately instead of waiting for the next inventory collection, you can refresh the switch as shown in the following steps:

Step 1 Choose Configure > Switches.

Step 2 Select the check box(es) of the switch(es) whose configuration you want to refresh.

Step 3 From the Select a command drop-down list, choose Refresh Config from Switch.
Enabling Traps and Syslogs on Switches for Wired Client Discovery

This section describes how to configure switches to send traps and syslogs to the Prime Infrastructure to discover the clients as they connect/disconnect.

This section contains the following topics:
- MAC Notification for Traps (Used for Non-Identity Client Discovery), page 9-213
- Syslog Configuration, page 9-214

MAC Notification for Traps (Used for Non-Identity Client Discovery)

This Cisco IOS switch feature forwards SNMP traps from the switch to the Prime Infrastructure server for MAC notifications (for non-802.1x clients).

Cisco IOS configuration example:

```plaintext
snmp-server enable traps mac-notification change move threshold
snmp-server host<IP address of Prime Infrastructure server> version 2c <community-string> mac-notification
mac address-table notification change interval 5
mac address-table notification change history-size 10
mac address-table notification change

interface <interface>
description non-identity clients
switchport access vlan <VLAN ID>
switchport mode access
snmp trap mac-notification change added  <- interface level config for MAC Notification
snmp trap mac-notification change removed <- interface level config for MAC Notification
```

Debug Commands

ddebug snmp packets

Show Commands

show mac address-table notification change

References

For more information about configuring MAC Change Notification Traps, see the following URL:
# Syslog Configuration

This feature is used for identity clients discovery.

The syslog configuration forwards syslog messages from a Catalyst switch to the Prime Infrastructure server.

Cisco IOS configuration example:
```
archive
log config
  notify syslog contenttype plaintext
logging facility auth
logging <IP address of Prime Infrastructure server>
```

For more information, see the following URL:

## Configuring Unknown Devices

To configure the unknown devices, follow these steps:

**Step 1**
Choose **Configure > Unknown Devices**. The Unknown Devices page appears. The summary information includes the following:
- IP Address—IP address of the device.
- Device Type—Type of device.
- Reachability Status—Indicates Reachable if the device is reachable or Unreachable if the device is unreachable.
- Inventory Collection Status—Status of the last inventory collection. The possible values are OK, Partial, Failed, NA, or In Progress.
- Inventory Status Detail—Specifies the status of the latest inventory collection. If the inventory collection was not successful, lists the possible reasons for the failure.
- Creation Time—Date and time the device was added to the Prime Infrastructure.

**Step 2**
From the Unknown Devices page, you can perform the following functions:
- Remove Devices—To remove a device from the unknown devices table, select the device(s) and choose **Remove Devices** from the Select a command drop-down list.
- Update Device Credentials—To update the device credentials of a device, select the device and choose **Update Device Credentials** from the Select a command drop-down list. The Update Device Credentials page appears.
- Bulk Update Devices—To update the device credentials in a bulk, select **Bulk Update Devices** from the Select a command drop-down list. The Bulk Update Devices page appears. You can choose a CSV file.
The CSV file contains a list of devices to be updated, one device per line. Each line is a comma separated list of device attributes. The first line describes the attributes included. The IP address attribute is mandatory.

Configuring Spectrum Experts

A Spectrum Expert client acts as a remote interference sensor and sends dynamic interference data to the Prime Infrastructure. This feature allows the Prime Infrastructure to collect, monitor, and archive detailed interferer data from Spectrum Experts in the network.

To configure spectrum experts, choose Configure > Spectrum Experts. This page provides a list of all Spectrum Experts including:

- Hostname—The hostname or IP address of the Spectrum Expert laptop.
- MAC Address—The MAC address of the spectrum sensor card in the laptop.
- Reachability Status—Specifies whether the Spectrum Expert is successfully running and sending information to the Prime Infrastructure. The status appears as reachable or unreachable.

- Adding a Spectrum Expert, page 9-215
- Monitoring Spectrum Experts, page 9-216

Adding a Spectrum Expert

To add a Spectrum Expert, follow these steps:

**Step 1** Choose Configure > Spectrum Experts.

**Step 2** From the Select a command drop-down list, choose Add Spectrum Expert.

**Note** This link only appears when no spectrum experts are added. You can also access the Add Spectrum Expert page by choosing Add Spectrum Expert from the Select a command drop-down list.

**Step 3** Enter the hostname or IP address of the Spectrum Expert. If you use hostname, your spectrum expert must be registered with DNS to be added to the Prime Infrastructure.

**Note** To be correctly added as a spectrum expert, the spectrum expert client must be running and configured to communicate to the Prime Infrastructure.
Monitoring Spectrum Experts

You also have the option to monitor spectrum experts.

To monitor spectrum expert, follow these steps:

Step 1
Choose Monitor > Spectrum Experts.

Step 2
From the left sidebar menu, you can access the Spectrum Experts page and the Interferers-SEs page.

Viewing Spectrum Experts Summary

The Spectrum Experts page provides a table of the Spectrum Experts added to the system. The table provides the following Spectrum Expert information:

Hostname—Displays the host name or IP address.

Active Interferers—Indicates the current number of interferes being detected by the Spectrum Experts.

Alarms APs—The number of access points seen by the Spectrum Experts that are potentially affected by detected interferers.

Alarms—The number of active interference traps sent by the Spectrum Expert. Click to access the Alarm page that is filtered to the active alarms for this Spectrum Expert.

Reachability Status—Indicates “Reachable” in green if the Spectrum Expert is running and sending data to the Prime Infrastructure. Otherwise, indicates “unreachable” in red.

Location—When the Spectrum Expert is a wireless client, a link for location is available. It shows the location of the Spectrum Expert with a red box that shows the effective range.

Viewing Interferers Summary

The Interferers-SEs page displays a list of all the interferers detected over a 30-day interval. The table provides the following interferer information:

- Interferer ID—An identifier that is unique across different spectrum experts. This is a pseudo-randomly generated ID. Though it is similar to a MAC address, it is not a real address, which you can use to find the interfering device.

- Category—Indicates the category of the interferer. Categories include: Bluetooth, cordless phones, microwave ovens, 802.11 FH, generic: fixed-frequency, jammers, generic: frequency-hopped, generic:continuous, and analog video.

- Type—Active indicates that the interferer is currently being detected by a spectrum expert. Inactive indicates that the interferer is no longer detected by a spectrum expert or the spectrum expert saw that the interferer is no longer reachable by the Prime Infrastructure.

- Discover Time—Indicates when the interferer was discovered.

- Affected Channels—Identifies affected channels.

- Number of APs Affected—The number of access points managed by the Prime Infrastructure that the spectrum expert detects or the interferers that the spectrum expert detected on the channels of the access point. Only active interferers are shown. If all of the following conditions are met, the access point is labelled as affected:
  - If the access point is managed by the Prime Infrastructure.
– If the spectrum expects detects the access point.
– If the spectrum expert detects an interferer on the serving channel of the access point.

- Power—Indicated in dBm.
- Duty Cycle—Indicated in percentage. 100% is the worst value.
- Severity—Indicates the severity ranking of the interferer. 100 is the worst case whereas 0 is no interference.

### Viewing Spectrum Experts Details

The Spectrum Expert page provides all interference details from a single Spectrum Expert. This page updates every 20 seconds and gives a real-time look at the remote spectrum expert. This page includes the following items:

- Total Interferer Count—Given from the specific spectrum expert.
- Active Interferers Count Chart—Displays a pie chart that groups interferers by category.
- Active Interferer Count Per Channel—Displays the number of interferers grouped by category on different channels.
- AP List—Provides a list of access points detected by the spectrum expert. These access points are on channels that have active interferers detected.
- Affected Clients List—Provides a list of clients that are currently authenticated to an access point. You can select specific RADIUS or LDAP servers to provide external authentication in the Security > AAA page.

### OfficeExtend Access Point

An OfficeExtend access point provides secure communications from a controller to an access point at a remote location, seamlessly extending the corporate WLAN over the Internet to the residence of an employee. The experience of a teleworker at the home office is exactly the same as it is at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the access point and the controller ensures that all communications have the highest level of security.

**Figure 9-5** illustrates a typical OfficeExtend access point setup.

![Typical OfficeExtend Access Point Setup](image-url)
Configuring Spectrum Experts

Note OfficeExtend access points are designed to work behind a router or other gateway device that is using network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a personal network (private), thereby enabling an entire group of computers to be represented by a single IP address. In controller release 6.0, only one OfficeExtend access point can be deployed behind a single NAT device.

Currently, only Cisco Aironet 1130 series and 1140 series access points that are joined to a Cisco 5500 series controller with a WPlus license can be configured to operate as OfficeExtend access points.

Note Your firewall must be configured to allow traffic from access points using CAPWAP. Make sure that UDP ports 5246 and 5247 are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.

Licensing for an OfficeExtend Access Point

Make sure that the WPlus license is installed on the 5500 series controller. After the license is installed, you can enable the OfficeExtend mode on an 1130 series or 1140 series access point.

Note The operating system software automatically detects and adds an access point to the Prime Infrastructure database as it associates with existing controllers in the Prime Infrastructure database.

Configuring Link Latency Settings for Access Points

You can configure link latency on the controller to measure the link between an access point and the controller. This feature can be used with all access points joined to a controller but is especially useful for FlexConnect access points, for which the link could be a slow or unreliable WAN connection.

Note Link latency is supported for use only with FlexConnect access points in connected mode. FlexConnect access points in standalone mode are not supported.

Link latency monitors the round-trip time of the CAPWAP heartbeat packets (echo request and response) from the access point to the controller and back. This time can vary due to network link speed and controller processing loads. The access point timestamps the outgoing echo requests to the controller and the echo requests received from the controller. The access point sends this delta time to the controller as the system round-trip time. The access point sends heartbeat packets to the controller at a default interval of 30 seconds.

Note Link latency calculates the CAPWAP response time between the access point and the controller. It does not measure network latency or ping responses.

The controller displays the current round-trip time as well as a running minimum and maximum round-trip time. The minimum and maximum times continue to run as long as the controller is up or can be cleared and allowed to restart.

To configure link latency, follow these steps:
In the Configure > Access Point details page, select the **Enable Link Latency** check box to enable link latency for this access point or unselect it to prevent the access point from sending the round-trip time to the controller after every echo response is received. The default value is unselected.

Click **Save** to save your changes.

The link latency results appear below the Enable Link Latency check box:

- **Current**—The current round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
- **Minimum**—Because link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
- **Maximum**—Because the link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.

To clear the current, minimum, and maximum link latency statistics on the controller for this access point, click **Reset Link Latency**. The updated statistics appear in the Minimum and Maximum fields.

### Configuring Chokepoints

Chokepoints are low frequency transmitting devices. When a tag passes within range of placed chokepoint, the low-frequency field awakens the tag that in turn sends a message over the Cisco Unified Wireless Network including the chokepoint device ID. The transmitted message includes sensor information (such as temperature and pressure). A chokepoint location system provides room level accuracy (ranging from few inches to 2 feet depending on the vendor).

Chokepoints are installed and configured as recommended by the Chokepoint vendor. After the chokepoint installation is complete and operational, the chokepoint can be entered into the location database and plotted on a the Prime Infrastructure map.

- Configuring New Chokepoints, page 9-219
- Editing Current Chokepoints, page 9-222

### Configuring New Chokepoints

- Adding a Chokepoint to Prime Infrastructure Database, page 9-219
- Adding a Chokepoint to an Prime Infrastructure Map, page 9-220
- Removing a Chokepoint from an Prime Infrastructure Map, page 9-221
- Removing a Chokepoint from Prime Infrastructure, page 9-221

### Adding a Chokepoint to Prime Infrastructure Database

To add a chokepoint to the Prime Infrastructure database, follow these steps:

**Step 1** Choose **Configure > Chokepoints**.

**Step 2** From the Select a command drop-down list, choose **Add Chokepoints**.

**Step 3** Click **Go**.
Step 4  Enter the MAC address and name for the chokepoint.

Step 5  Select the check box to indicate that it is an Entry/Exit Chokepoint.

Step 6  Enter the coverage range for the chokepoint.

Note  Chokepoint range is a visual representation only. It is product-specific. The actual range must be configured separately using the applicable chokepoint vendor software.

Step 7  Click OK.

Note  After the chokepoint is added to the database, it can be placed on the appropriate the Prime Infrastructure floor map.

Adding a Chokepoint to an Prime Infrastructure Map

To add the chokepoint to a map, follow these steps:

Step 1  Choose Monitor > Maps.

Step 2  In the Maps page, click the link that corresponds to the floor location of the chokepoint.

Step 3  From the Select a command drop-down list, choose Add Chokepoints.

Step 4  Click Go.

Note  The Add Chokepoints summary page lists all recently-added chokepoints that are in the database but not yet mapped.

Step 5  Select the check box next to the chokepoint that you want to place on the map.

Step 6  Click OK.

A map appears with a chokepoint icon located in the top-left hand corner. You are now ready to place the chokepoint on the map.

Step 7  Left-click the chokepoint icon and drag and place it in the proper location.

Note  The MAC address, name, and coverage range of the chokepoint appear in the selected chokepoints detail page when you click the chokepoint icon for placement.

Step 8  Click Save.

You are returned to the floor map and the added chokepoint appears on the map.

Note  The newly created chokepoint icon might or might not appear on the map depending on the display settings for that floor.
Note: The rings around the chokepoint icon indicate the coverage area. When a CCX tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.

Note: MAC address, name, entry/exit chokepoint, static IP address, and range of the chokepoint display when you pass a mouse over its map icon.

Step 9: If the chokepoint does not appear on the map, select the Chokepoints check box located in the Floor Settings menu.

Note: Do not select the Save Settings check box unless you want to save this display criteria for all maps.

Note: You must synchronize network design to the mobility services engine or location server to push chokepoint information.

Removing a Chokepoint from an Prime Infrastructure Map

To remove an chokepoint from the map, follow these steps:

Step 1: Choose Monitor > Maps.
Step 2: In the Maps page, choose the link that corresponds to the floor location of the chokepoint.
Step 3: From the Select a command drop-down list, choose Remove Chokepoints.
Step 4: Click Go.
Step 5: Click OK to confirm the deletion.

Removing a Chokepoint from Prime Infrastructure

To remove an chokepoint from the Prime Infrastructure, follow these steps:

Step 1: Choose Configure > Chokepoints.
Step 2: Select the check box of the chokepoint that you want to delete.
Step 3: From the Select a command drop-down list, choose Remove Chokepoints.
Step 4: Click Go.
Step 5: Click OK to confirm the deletion.
Editing Current Chokepoints

To edit a current chokepoint in the Prime Infrastructure database and appropriate map, follow these steps:

**Step 1** Choose **Configure > Chokepoints**. The Configure > Chokepoints page displays the following information for each current chokepoint: MAC address, chokepoint name, entry/exit chokepoint, range, static IP address, and map location for the chokepoint.

**Step 2** Click the chokepoint you want to edit in the MAC Address column.

**Step 3** Edit the following parameters, as necessary:

- **Name**
- **Entry/Exit Chokepoint**—Click to enable.
- **Range**—Coverage range for the chokepoint.

Note: The chokepoint range is product-specific and is supplied by the chokepoint vendor.

- **Static IP Address**

**Step 4** Click **Save**.

Configuring Spectrum Experts

A spectrum expert client acts as a remote interference sensor and sends dynamic interference data to Prime Infrastructure. This feature allows Prime Infrastructure to collect, monitor, and archive detailed interferer data from spectrum experts in the network.

To configure spectrum experts (from the Converged Theme), choose **Monitor > Wireless Technologies > Spectrum Experts**. This page provides a list of all spectrum experts including:

- **Hostname**—The hostname or IP address of the spectrum expert laptop.
- **MAC Address**—The MAC address of the spectrum sensor card in the laptop.
- **Reachability Status**—Specifies whether the spectrum expert is successfully running and sending information to Prime Infrastructure. The status appears as reachable or unreachable.

Adding a Spectrum Expert

To add a spectrum expert:

**Step 1** Choose **Monitor > Wireless Technologies > Spectrum Experts**.

**Step 2** Choose **Select a command > Add Spectrum Expert**. (This link appears only if no spectrum experts already exist.)
Step 3  Enter the hostname or IP address of the spectrum expert. If you use the hostname, your spectrum expert must be registered with DNS to be added to Prime Infrastructure.

**Note**  To be correctly added as a spectrum expert, the spectrum expert client must be running and configured to communicate with Prime Infrastructure.

---

**Spectrum Experts Details**

The Spectrum Expert Details page provides interference details for a single spectrum expert. This page is updated every 20 seconds, providing a real-time look at what is happening on the remote spectrum expert. This page displays the following:

- **Total Interferer Count**—As seen by the specific spectrum expert.
- **Active Interferers Count Chart**—Displays a pie chart that groups interferers by category.
- **Active Interferer Count Per Channel**—Displays the number of interferers, grouped by category, on different channels.
- **AP List**—Provides a list of access points detected by the spectrum expert that are on channels that have active interferers detected by the spectrum expert on those channels.
- **Affected Clients List**—Provides a list of clients that are authenticated and associated with the radio of one of the access points listed in the access point list.

---

**Configuring Wi-Fi TDOA Receivers**

- Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting, page 9-223
- Adding Wi-Fi TDOA Receivers to Prime Infrastructure and Maps, page 9-224
- Viewing or Editing Current Wi-Fi TDOA Receivers, page 9-226
- Removing Wi-Fi TDOA Receivers from Prime Infrastructure and Maps, page 9-226

---

**Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting**

The Wi-Fi TDOA receiver is an external system designed to receive signals transmitted from a tagged, tracked asset. These signals are then forwarded to the mobility services engine to aid in the location calculation of the asset. TDOA receivers use the method of Time Difference of Arrival (TDOA) to calculate tag location. This method uses data from a minimum of three TDOA receivers to generate a tagged asset location.
Note

- If a TDOA receiver is not in use and the partner engine software is resident on the mobility service engine, then the location calculations for tags are generated using RSSI readings from access points.
- The Cisco Tag engine can calculate the tag location using the RSSI readings from access points.

Before using a TDOA receiver within the Cisco Unified Wireless Network, you must perform the following steps:

1. Have a mobility services engine active in the network.
   See the “Adding a Mobility Services Engine” section on page 16-6 for details on adding a mobility services engine.
2. Add the TDOA receiver to the Prime Infrastructure database and map.
   See the “Adding Wi-Fi TDOA Receivers to Prime Infrastructure and Maps” section on page 9-224 for details on adding the TDOA receiver to the Prime Infrastructure.
3. Activate or start the partner engine service on the MSE using the Prime Infrastructure.
4. Synchronize the Prime Infrastructure and mobility services engines.
   See the “Synchronizing Services” section on page 16-12 for details on synchronization.
5. Set up the TDOA receiver using the AeroScout System Manager.

Note

See the AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User’s Guide for configuration details at the following URL:

Adding Wi-Fi TDOA Receivers to Prime Infrastructure and Maps

After the Wi-Fi TDOA receiver is installed and configured by the AeroScout System Manager and the partner software is downloaded on the mobility services engine, you are ready to add the TDOA receiver to the mobility services engine database and position it on a Prime Infrastructure map.

After adding TDOA receivers to the Prime Infrastructure maps, you continue to make configuration changes to the TDOA receivers using the AeroScout System Manager application rather than the Prime Infrastructure.

Note

For more details on configuration options, see the AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User Guide at the following URL:

To add a TDOA receiver to the Prime Infrastructure database and appropriate map, follow these steps:

Step 1
Choose Configure > WiFi TDOA Receivers to open the All WiFi TDOA Receivers summary page.

Note
To view or edit current WiFi TDOA receiver details, click the MAC Address link to open the details page.
Step 2  From the Select a command drop-down list, choose **Add WiFi TDOA Receivers**.

Step 3  Click **Go**.

Step 4  Enter the MAC address, name and static IP address of the TDOA receiver.

Step 5  Click **OK** to save the TDOA receiver entry to the database.

---

**Note**  After you add the TDOA receiver to the database, you can place the TDOA receiver on the appropriate Prime Infrastructure floor map. To do so, continue with **Step 6**.

---

**Note**  A WiFi TDOA Receiver must be configured separately using the receiver vendor software.

Step 6  To add the TDOA receiver to a map, choose **Monitor > Maps**.

Step 7  In the Maps page, select the link that corresponds to the floor location of the TDOA receiver.

Step 8  From the Select a command drop-down list, choose **Add WiFi TDOA receivers**.

Step 9  Click **Go**.

---

**Note**  The All WiFi TDOA Receivers summary page lists all recently-added TDOA receivers that are in the database but not yet mapped.

Step 10  Select the check box next to each TDOA receiver to add it to the map.

Step 11  Click **OK**. A map appears with a TDOA receiver icon located in the top-left hand corner. You are now ready to place the TDOA receiver on the map.

Step 12  Left-click the TDOA receiver icon and drag and place it in the proper location on the floor map.

---

**Note**  The MAC address and name of the TDOA receiver appear in the left pane when you click the TDOA receiver icon for placement.

Step 13  Click **Save** when the icon is placed correctly on the map. The added TDOA receiver appears on the floor heat map.

---

**Note**  The icon for the newly added TDOA receiver might or might not appear on the map depending on the display settings for that floor. If the icon did not appear, proceed with **Step 14**.

Step 14  If the TDOA receiver does not appear on the map, click **Layers** to collapse a selection menu of possible elements to display on the map.

Step 15  Select the **WiFi TDOA Receivers** check box. The TDOA receiver appears on the map.

---

**Note**  When you place your cursor over a TDOA receiver on a map, configuration details display for that receiver.

Step 16  Click **X** to close the Layers page.
Configuring Wi-Fi TDOA Receivers

**Note** Do not choose **Save Settings** from the Layers menu unless you want to save this display criteria for all maps.

**Step 17** You can now download the partner engine software to the mobility services engine.

---

**Viewing or Editing Current Wi-Fi TDOA Receivers**

To view a current TDOA receiver to the Prime Infrastructure database, follow these steps:

**Step 1** Choose **Configure > WiFi TDOA Receivers** to open the All WiFi TDOA Receivers summary page.

**Step 2** Click the MAC Address link to view the TDOA receiver details including MAC address, name, and static IP address.

**Step 3** If you make any changes to the receiver name or IP address, click **Save** to confirm these changes.

**Note** A WiFi TDOA Receiver must be configured separately using the receiver vendor software.

---

**Removing Wi-Fi TDOA Receivers from Prime Infrastructure and Maps**

You can remove one or multiple WiFi TDOA receivers at a time. If you remove a TDOA receiver from a map it remains in Prime Infrastructure database but is labeled as unassigned.

To delete a TDOA receiver from the Prime Infrastructure, follow these steps:

**Step 1** Choose **Configure > WiFi TDOA Receivers** to open the All WiFi TDOA Receivers summary page.

**Step 2** Select the check box next to each TDOA receiver to be deleted.

**Step 3** From the Select a command drop-down list, choose **Remove WiFi TDOA Receivers**.

**Step 4** Click **Go**.

**Step 5** To confirm TDOA receiver deletion, click **OK** in the dialog box.

In the All WiFi TDOA Receivers page, a message confirms the deletion. The deleted TDOA receiver is no longer listed in the page.
Configuring Scheduled Configuration Tasks

The Scheduled Configuration Tasks page allows you to navigate to any configuration task that has been scheduled. It provides a filtered view of the templates or software download tasks, which have been scheduled. This page displays the summary information about a task such as the template name, last time the task was run, next time the task is scheduled to run, and a link to view the results of previous runs. You can also edit the template, modify the schedule, enable, disable, or delete a scheduled task.

Once you create and schedule a configuration template, configuration group, or a software download task, the scheduled task or template is listed in the Scheduled Configuration Tasks page.

Note
You cannot create any new scheduled task or template in this page. You can only edit the scheduled task or template that is already created.

For more information about the tasks that you can perform in the Scheduled Configuration Tasks page, see the Managing Scheduled Configuration Task Templates section in the Cisco Prime Infrastructure 2.0 User Guide.

Configuring Auto Provisioning for Controllers

Auto provisioning allows the Prime Infrastructure to automatically configure a new or replace a current wireless LAN controller (WLC). Prime Infrastructure auto provisioning feature can simplify deployments for customers with a large number of controllers.

Note
For Auto Provisioning privileges, you must have Admin, Root, or SuperUser status.

Note
To allow or disallow a user Auto Provisioning privileges, edit the permitted tasks using Administration > AAA > User Groups > group name > List of Tasks Permitted in the Prime Infrastructure. Select or unselect the check box to allow or disallow these privileges.

Note
A controller radio and b/g networks are initially disabled by the Prime Infrastructure downloaded startup configuration file. If desired, you might turn on those radio networks by using a template, which should be included as one of the automated templates.

Note
To specify the Auto Provision filter contents, you can directly enter the details in the application or import the details from a CSV file. The auto provisioning feature supports the 5500 and non-5500 series controllers. The non-5500 series controllers have AP manager interface configuration information defined, whereas 5500 series controllers do not have this information.

To access the Auto Provisioning feature, choose Configure > Controller Auto Provisioning. For more information about this feature and the tasks that you can perform, see the Configuring Controller Deployments section in the Cisco Prime Infrastructure 2.0 User Guide.
Configuring Redundancy on Controllers

The term Redundancy in the Prime Infrastructure refers to the High Availability (HA) framework in Controllers. Redundancy in wireless networks allows you to reduce the downtime of the networks. In a redundancy architecture, one controller is in the Active state and a second controller is in the Standby state, which continuously monitors the health of the controller in the Active state through a redundant port. Both controllers share the same configurations including the IP address of the management interface.

The Standby or Active state of a controller is based on the redundancy stock keeping unit (SKU), which is a manufacturing ordered unique device identification (UDI). A controller with redundancy SKU UDI is in the Standby state for the first time when it boots and pairs with a controller that runs a permanent count license. For controllers that have permanent count licenses, you can manually configure whether the controller is in the Active state or the Standby state.

In this release, a stateful switchover of access points (AP SSO) is supported. An AP SSO ensures that the AP sessions are intact even after a switchover.

For more information about the Redundancy feature, see the Configuring Redundancy section in the Cisco Prime Infrastructure 2.0 Administrator Guide.

Configuring wIPS Profiles

Prime Infrastructure provides several pre-defined profiles from which to choose. These profiles (based on customer types, building types, industry types, and so on) allow you to quickly activate the additional wireless threat protection available through Cisco Adaptive wIPS. You can use a profile ‘as is’ or customize it to better meet your needs.

To learn more about Cisco Adaptive wIPS features and functionality, go to Cisco.com to watch a multimedia presentation. Here you find learning modules for a variety of the Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

Pre-defined profiles include the following:

- Education
- EnterpriseBest
- EnterpriseRogue
- Financial
- HealthCare
- HotSpotOpen
- Hotspot8021x
- Military
- Retail
- Tradeshow
- Warehouse

The wIPS Profiles page provides access to the wIPS profile list and the SSID group list. To access the wIPS Profile page, choose Configure > wIPS Profiles.
The current wIPS profile list and the SSID group list can be accessed from the left sidebar menu. The wIPS Profiles page defaults to the Profile List. The SSID Group List page is accessible from the left sidebar menu.

**Profile List**

The wIPS Profiles > Profile List page allows you to view, edit, apply, or delete current wIPS profiles and to add new profiles.

The profile editor allows you to create new or modify current profiles. See the “Profile Editor” section on page 9-230 for more information.

**Adding a Profile**

A new wIPS profile can be created using the default or a pre-configured profile.

To learn more about Cisco Adaptive wIPS features and functionality, go to Cisco.com to watch a multimedia presentation. Here you also find learning modules for a variety of Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

**Note**

Adaptive wIPS does not support the Prime Infrastructure partitioning feature.
To add a wIPS profile, follow these steps:

**Step 1**  Select **Configure > wIPS Profiles**. The page defaults to the wIPS Profiles > Profile List.

**Step 2**  From the Select a command drop-down list, choose **Add Profile**.

**Step 3**  Click **Go**.

**Step 4**  Type a profile name in the Profile Name text box of the Profile Parameters page.

**Step 5**  Select the applicable pre-defined profile, or choose **Default** from the drop-down list. Pre-defined profiles include the following:
- Education
- EnterpriseBest
- EnterpriseRogue
- Financial
- HealthCare
- HotSpotOpen
- Hotspot8021x
- Military
- Retail
- Tradeshows
- Warehouse

**Step 6**  Select one of the following:
- **Save**—Saves the profiles to the Prime Infrastructure database with no changes and no mobility services engine or controller assignments. The profile appears in the profile list.
- **Save and Edit**—Saves the profile and allows you to edit the profile.
- **Cancel**—Closes the Profile Parameters page without creating a profile.

---

### Profile Editor

**Tip**  To learn more about Cisco Adaptive wIPS features and functionality, access the following URL: [http://www.cisco.com/en/US/products/ps6305/tsd_products_support_onlinel_earning_modules_list.html](http://www.cisco.com/en/US/products/ps6305/tsd_products_support_onlinel_earning_modules_list.html)

Here you also find learning modules for a variety of the Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

The profile editor allows you to configure profile details including the following:
- **SSID groups**—Add, edit, or delete SSID groups.
- **Policy inclusion**—Determine which policies are included in the profile.
- **Policy level settings**—Configure settings for each policy such as threshold, severity, notification type, and ACL/SSID groups.
Configuring wIPS Profiles

- MSE/controller applications—Select the mobility services engine(s) or controller(s) to which you want to apply the profile.

To configure profile details, follow these steps:

**Step 1**
Access the profile editor. This can be done in two ways:
- When creating a new profile, click **Save and Edit** in the Profile Parameters page.
- Click the profile name from the Profile List page.

**Step 2**
From the SSID Groups page, you can edit and delete current groups or add a new group. For more information on adding, editing, or deleting SSID groups, see the “Configure > wIPS > SSID Group List” section on page 9-233 for more information.

**Step 3**
When SSID groups have been added or edited as needed, select one of the following:
- Save—Saves the changes made to the SSID groups.
- Cancel—Returns to the profile list with no changes made.
- Next—Proceeds to the Profile Configuration page.

**Step 4**
From the Profile Configuration page, you can determine which policies are included in the current profile. The check boxes in the policy tree (located in the left Select Policy pane) indicate which policies are enabled or disabled in the current profile. You can enable or disable an entire branch or an individual policy as needed by selecting the check box for the applicable branch or policy.

*Note*  
By default, all policies are selected.

*Note*  
For detailed information regarding each of the wIPS policies, see the “wIPS Policy Alarm Encyclopedia” section on page 18-1.

**Step 5**
In the Profile Configuration page, click an individual policy to display the policy description and to view or modify current policy rule settings.

The following options are available for each policy:
- Add—Click **Add** to access the Policy Rule Configuration page to create a new rule for this policy.
- Edit—Select the check box of the applicable rule, and click **Edit** to access the Policy Rule Configuration page to edit the settings for this rule.
- Delete—Select the check box of the rule you want to delete, and click **Delete**. Click **OK** to confirm the deletion.

*Note*  
There must be at least one policy rule in place. You cannot delete a policy rule if it is the only one in the list.

- Move Up—Select the check box of the rule you want to move up in the list. Click **Move Up**.
- Move Down—Select the check box of the rule you want to move down in the list. Click **Move Down**.

The following settings can be configured at the policy level:
- Threshold (not applicable to all policies)—Indicates the threshold or upper limit associated with the selected policy. When the threshold is reached for a policy, an alarm is triggered.
Configuring Devices

Chapter 9

Step 6

When the profile configuration is complete, select one of the following:

- **Save**—Saves the changes made to the current profile.
- **Cancel**—Returns to the profile list with no changes made.
- **Back**—Returns to the SSID Groups page.
- **Next**—Proceeds to the MSE/Controller(s) page.

Step 7

In the Apply Profile page, select the check box(es) of the mobility services engine and controller(s) to which you want to apply the current profile.

Step 8

When the applicable mobility services engine(s) and controller(s) are selected, choose one of the following:

- **Apply**—Applies the current profile to the selected mobility services engine/controller(s).
- **Cancel**—Returns to the profile list with no changes made.

Deleting a Profile

To delete a wIPS profile, follow these steps:

Step 1

Choose **Configure > wIPS Profiles**. The page defaults to the wIPS Profiles > Profile List.
Step 2 Select the check box of the wIPS profile(s) you want to delete.

Step 3 From the Select a command drop-down list, choose Delete Profile.

Step 4 Click Go.

Step 5 Click OK to confirm the deletion.

Note If the profile is already applied to a controller, it cannot be deleted.

Applying a Current Profile

Tip To learn more about Cisco Adaptive wIPS features and functionality, access the following URL: http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html

Here you also find learning modules for a variety of Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

To apply a wIPS profile, follow these steps:

Step 1 Choose Configure > wIPS Profiles. The page defaults to the wIPS Profiles > Profile List.

Step 2 Select the check box of the wIPS profile(s) you want to apply.

Step 3 From the Select a command drop-down list, choose Apply Profile.

Step 4 Click Go.

Step 5 Select the mobility services engine(s) and controller(s) to which the profile is applied.

Note If the new assignment is different than the current assignment, you are prompted to save the profile with a different name.

Step 6 When the applicable mobility services engine(s) and controller(s) are selected, choose one of the following:

- Apply—Applies the current profile to the selected mobility services engine/controller(s).
- Cancel—Returns to the profile list with no changes made.

Configure > wIPS > SSID Group List

The SSID (Service Set IDentifier) is a token or key which identifies an 802.11 (Wi-Fi) network. You must know the SSID to join an 802.11 network. SSIDs can be associated with a wIPS profile as a group using the SSID group list feature.

An SSID group can be added to a profile by importing it from the Global SSID Group List page (Configure > wIPS Profiles > SSID Group List) or by adding one directly from the SSID Groups page.
Tip
To learn more about Cisco Adaptive wIPS features and functionality, access the following URL:
Here you also find learning modules for a variety of Prime Infrastructure topics. Over future releases,
we will add more overview and technical presentations to enhance your learning.

Global SSID Group List

The SSID Group List page allows you to add or configure global SSID groups that you might later import
into an applicable wIPS profile.

Tip
To learn more about Cisco Adaptive wIPS features and functionality, access the following URL:
Here you also find learning modules for a variety of Prime Infrastructure topics. Over future releases,
we will add more overview and technical presentations to enhance your learning.

To access the SSID Group List page, choose Configure > wIPS Profiles. From the left sidebar menu,
choose SSID Group List. The SSID Group List page display current SSID groups and their associated
SSIDs.

• Adding a Group, page 9-234
• Editing a Group, page 9-235
• Deleting a Group, page 9-235

Adding a Group

To add an SSID Group, follow these steps:

Step 1 Choose Configure > wIPS Profiles.
Step 2 From the left sidebar menu, choose SSID Group List.
Step 3 From the Select a command drop-down list, choose Add Group.
Step 4 Click Go.
Step 5 In the SSID configuration page, type an SSID group name in the available text box.
Step 6 Enter the SSIDs in the SSID List text box. Separate multiple SSIDs with carriage return.
Step 7 When finished, select one of the following:
  • Save—Saves the SSID group and adds it to the SSID Group List.
  • Cancel—Closes the SSID configuration page without saving the new SSID group.
To import the SSID groups to a profile, choose **Configure > wIPS Profile**. Click the profile name for the applicable profile to open the SSID Groups page. From the Select a command drop-down list, choose **Add Groups from Global List**. Select the check box(es) for the SSID group(s) you want to import and click **Save**.

**Note**

**Editing a Group**

To edit a current SSID Group, follow these steps:

**Step 1** Choose **Configure > wIPS Profiles**.
**Step 2** From the left sidebar menu, choose **SSID Group List**.
**Step 3** Select the check box of the SSID group that you want to edit.
**Step 4** From the Select a command drop-down list, choose **Edit Group**.
**Step 5** Click **Go**.
**Step 6** In the SSID configuration page, make the necessary changes to the SSID group name or the SSID list.
**Step 7** When finished, select one of the following:
   - **Save**—Saves the current changes and closes the SSID configuration page.
   - **Cancel**—Closes the SSID configuration page without saving the changes.

**Deleting a Group**

To delete a current SSID Group, follow these steps:

**Step 1** Choose **Configure > wIPS Profiles**.
**Step 2** From the left sidebar menu, choose **SSID Group List**.
**Step 3** Select the check box of the SSID group(s) that you want to delete.
**Step 4** From the Select a command drop-down list, choose **Delete Group**.
**Step 5** Click **Go**.
**Step 6** Click **OK** to confirm the deletion.

**SSID Groups**

The SSID Groups page is the first page displayed when you access the profile editor. This page displays SSID groups that are included for the current wIPS profile. From this page, you can add, import, edit, or delete an SSID group for the current profile.
Adding a Group

To add an SSID Group to the current wIPS profile, follow these steps:

Step 1 Choose Configure > wIPS Profiles.
Step 2 From the left sidebar menu, choose Profile List.
Step 3 Click the profile name of the applicable wIPS profile.
Step 4 From the Select a command drop-down list, choose Add Group.
Step 5 Click Go.
Step 6 In the SSID configuration page, type an SSID group name in the available text box.
Step 7 Enter the SSIDs in the SSID List text box. Separate multiple SSIDs with a comma.
Step 8 When finished, select one of the following:
   - Save—Saves the SSID group and adds it to the SSID Group List.
   - Cancel—Closes the SSID configuration page without saving the new SSID group.

Adding Groups from Your Global List

SSID groups can also be added by importing them from your Global SSID Groups list. See the “Global SSID Group List” section on page 9-234 for more information on creating a global SSID groups list.

To import SSID groups into a profile, follow these steps:

Step 1 Select Configure > wIPS Profile.
Step 2 Click the profile name for the applicable profile to open the SSID Groups page.
Step 3 From the Select a command drop-down list, choose Add Groups from Global List.
Step 4 Select the check box(es) for the SSID group(s) you want to import.
Step 5 Click Save.
Editing a Group

To edit a current SSID Group, follow these steps:

Step 1 Choose Configure > wIPS Profiles.
Step 2 From the left sidebar menu, choose Profile List.
Step 3 Click the profile name of the applicable wIPS profile.
Step 4 Select the check box of the SSID group that you want to edit.
Step 5 From the Select a command drop-down list, choose Edit Group.
Step 6 Click Go.
Step 7 In the SSID configuration page, make the necessary changes to the SSID group name or the SSID list.
Step 8 When finished, select one of the following:
   • Save—Saves the current changes and closes the SSID configuration page.
   • Cancel—Closes the SSID configuration page without saving the changes.

Deleting a Group

To delete a current SSID Group, follow these steps:

Step 1 Choose Configure > wIPS Profiles.
Step 2 From the left sidebar menu, choose Profile List.
Step 3 Click the profile name of the applicable wIPS profile.
Step 4 Select the check box of the SSID group that you want to delete.
Step 5 From the Select a command drop-down list, choose Delete Group.
Step 6 Click Go.
Step 7 Click OK to confirm the deletion.

Configuring ACS View Servers

To facilitate communication between the Prime Infrastructure and the ACS View Server and to access the ACS View Server tab, you must add a view server with credentials.

Note
Prime Infrastructure only supports ACS View Server 5.1 or later.

To configure the ACS View Server Credentials, follow these steps:

Step 1 Choose Configure > ACS View Server.
Step 2 Select Add ACS View Server from the Select a command drop down list at the top right of the page, and then click Go.
Step 3 Enter the IP address or hostname of the ACS View Server.
Step 4 Enter the port number of the ACS View Server you are adding. (Some ACS View Servers do not allow you to change the port on which HTTPS runs.)
Step 5 Enter the username.
Step 6 Enter the password that was established on the ACS View Server. Confirm the password.
Step 7 Specify the number of retries to be attempted.
Step 8 Click Submit.

You must enable the web interface on ACS before Prime Infrastructure interacts with the ACS View web services. To enable the web interface, login to the CLI of the ACS server as admin user and enter “acs config web-interface view enable” command.

For more details, see http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/sdk/mrvapis.html

Configuring ACS View Server Credentials

To facilitate communication between the Prime Infrastructure and the ACS View Server and to access the ACS View Server tab, you must add a view server with credentials.

To configure the ACS View Server Credentials, follow these steps:

Note Prime Infrastructure only supports ACS View Server 5.1 or later.

Step 1 Choose Configure > ACS View Server.
Step 2 Enter the port number of the ACS View Server you are adding. (Some ACS View Servers do not allow you to change the port on which HTTPS runs.)
Step 3 Enter the password that was established on the ACS View Server. Confirm the password.
Step 4 Specify the number of retries to be attempted.
Step 5 Click Submit.

Configuring TFTP or FTP Servers

Choose Configure > TFTP/FTP Servers to add or delete TFTP or FTP servers from the Prime Infrastructure.

Note Prime Infrastructure uses an integral TFTP/FTP server. This means that third-party TFTP or FTP servers cannot run on the same workstation as Prime Infrastructure, because the Prime Infrastructure and the third-party TFTP or FTP servers use the same communication port.
Adding a TFTP or FTP Server

To add a TFTP or FTP server, follow these steps:

**Step 1** Choose Configure > TFTP/FTP Servers.

**Step 2** From the Select a command drop-down list, choose Add TFTP/FTP Server.

**Step 3** From the Server Type drop-down list, choose TFTP, FTP, or Both.

**Step 4** Enter a TFTP/FTP server name. This is a user-defined name for the server.

**Step 5** Enter the IP address of the TFTP/FTP server.

**Step 6** Click Save.

Deleting TFTP or FTP Servers

To delete a TFTP or FTP server, select the check box for the applicable server, and choose Delete TFTP/FTP Servers from the Select a command drop-down list. Click Go and then click OK to confirm the deletion.

Interactive Graphs

- Interactive Graphs Overview, page 9-239
- Interactive Graph Features, page 9-240

Interactive Graphs Overview

Interactive graph features are based on Adobe Flex technology that uses flash to render the graphs on the browser and provide interactivity to the user.

Minimum Requirements include the following:

- Windows—Flash Player version 9.0.115.0.
- Linux—Flash Player version 9.0.115.0.

**Note** If you do not have a flash player or your version is not recent enough, an error page prompts you with this information. Click the Get Latest Flash Player link to access Adobe website. From this site, you can download the latest version of the flash player. You only need to download the flash player once. Remember to restart the browser following the download.

Prime Infrastructure Interactive Graphs include line, area, pie, and stacked bar graphs.
Interactive Graph Features

Interactive graph features include the following:

- Two distinct types of graphs:
  - Time-based Graphs
  - Non-Time based

- Support for automatic refresh—The graphs refresh automatically within a predetermined interval of time.

- Two graph views:
  - Graph (Chart) view (default)
  - Table (Grid) view

**Note**

Use the two toggle buttons located at the bottom left side of the graph page to switch between the two graph views. To view the button type, hover your mouse cursor over the applicable button for a tool tip identifying View in Chart or View in Grid. Click View in Chart to view the data in a graph. Click View in Grid to view the data in a table.

- Enlarged View—Click the button located at the bottom right side of the graph to enlarge the graph in a separate page. The Chart View and Grid View buttons are available in the new page to change the type of graph displayed.

Time-based Graphs

For graphs that are time-based, there is a link bar at the top of the graph page that displays 6h, 1d, 1w, 2w, 4w, 3m, 6m, 1y, and Custom. When selected, the data for that time frame is retrieved and the corresponding graph is displayed. The time-frame options include the following:

- 6h—Denotes the last six hours of data from the current time. The data is gathered from the current database table.
- 1d—Denotes the last day (24 hours) of data from the current time. The data is gathered from the current database table.
- 1w—Denotes the last week (seven days) of data from the current time. The data is gathered from the hourly aggregated table.
- 2w—Denotes the last two weeks of data from the current time. The data is gathered from the hourly aggregated table.
- 4w—Denotes the last four weeks of data from the current time. The data is gathered from the hourly aggregated table.
- 3m—Denotes the last three months of data from the current time. The data is gathered from the daily aggregated table.
- 6m—Denotes the last six months of data from the current time. The data is gathered from the weekly aggregated table.
- 1y—Denotes the past year (12 months) of data from the current time. The data is gathered from the weekly aggregated table.
• Custom—User-selected time period. Both days and hours can be set for the start and end dates. The use of a current or hourly, daily, or weekly aggregated source for data depends upon the selected start date.

**Note**
The data management settings for aggregated tables are located in the “Performing Administrative Tasks” section on page 15-1 on the Administration menu. The default settings have a value of 31 days for Daily Aggregated Data and ten weeks for Weekly Aggregated Data.

For more information on Interactive Graphs, see the “Interactive Graphs” section on page 9-239.
Managing Clients

A client is a device that is connected to an access point or a switch. Cisco Prime Infrastructure supports both wired and wireless clients. After you add controllers and switches to Prime Infrastructure, the client discovery process starts. Wireless clients are discovered from managed controllers or autonomous access points. The wireless client count includes autonomous clients as well. Only in the case of switches, Prime Infrastructure polls for clients immediately after the device is added. In the case of controllers, these are polled during regular client status poll. Prime Infrastructure gets the client information from the switch and updates this information in the database. For wired clients, the client status polling to discover client associations occurs every two hours (by default). A complete polling happens twice every day to poll complete information of all wired clients connected to all switches.

Prime Infrastructure uses background tasks to perform the data polling operations. There are three tasks associated with clients:

1. Autonomous AP Client Status
2. Lightweight Client Status
3. Wired Client Status

Prime Infrastructure do not poll end hosts connected through VLAN 1000-1024.

**Note**

You can refresh the data collection tasks (such as polling interval) from the Administration > Background Tasks page. For details, see the “Performing Administrative Tasks” section on page 15-1.

**Note**

Prime Infrastructure enables you to track clients and be notified when these clients connect to the network. For details, see the “Tracking Clients” section on page 10-30.

**Note**

For more information about enabling traps and syslogs on switches for wired client discovery, see the “Tracking Clients” section on page 10-30.

Not all users or devices are authenticated via 802.1x (for example, printers). In such a case, a network administrator can assign a username to a device. For details, see the “Configuring Unknown Devices” section on page 9-214.

If a client device is authenticated to the network through web auth, Prime Infrastructure might not have username information for the client (applicable only for wired clients).

Client status (applicable only for wired clients) is noted as connected, disconnected, or unknown:
Connected clients—Clients that are active and connected to a wired switch.
Disconnected clients—Clients that are disconnected from the wired switch.
Unknown clients—Clients that are marked as unknown when the SNMP connection to the wired switch is lost.

**Note**  See the “Configuring Unknown Devices” section on page 9-214 for more information about tracking clients.

For the clients of autonomous access point managed by Prime Infrastructure, the username is not registered and is displayed as unknown.

Prime Infrastructure supports both identity and non-identity wired clients. The support for wired clients is based on the identity service. The identity service provides secure network access to users and devices and it also enables the network administrators to provision services and resources to the users based on their job functions.

- Client Dashlets on the General Dashboard, page 10-3
- Client Dashboard, page 10-3
- Monitoring Clients and Users, page 10-9
- Client Troubleshooting, page 10-21
- Tracking Clients, page 10-30
- Enabling Automatic Client Troubleshooting, page 10-32
- Viewing Client Details in the Access Point Page, page 10-33
- Viewing Currently Associated Clients, page 10-33
- Running Client Reports, page 10-33
- Running ISE Reports, page 10-33
- Specifying Client Settings, page 10-33
- Receiving Radio Measurements for a Client, page 10-33
- Viewing Client V5 Statistics, page 10-35
- Viewing Client Operational Parameters, page 10-36
- Viewing Client Profiles, page 10-38
- Disabling a Current Client, page 10-38
- Removing a Current Client, page 10-39
- Enabling Mirror Mode, page 10-39
- Viewing a Map (High Resolution) of a Client Recent Location, page 10-39
- Viewing a Map (High Resolution) of a Client Current Location, page 10-39
- Running a Client Sessions Report for the Client, page 10-40
- Viewing a Roam Reason Report for the Client, page 10-40
- Viewing Detecting Access Point Details, page 10-41
- Viewing Client Location History, page 10-41
- Viewing Voice Metrics for a Client, page 10-41
Client Dashlets on the General Dashboard

The dashlets that you see on the dashboard are presented in the form of interactive graphs. See the “Interactive Graphs” section on page 9-239 for more information.

When you log into Prime Infrastructure, the General dashboard displays a few client-related dashlets.

- Client Count By Association/Authentication—Displays the total number of clients by Association and authentication in Prime Infrastructure over the selected period of time.
  - Associated client—All clients connected regardless of whether it is authenticated or not.
  - Authenticated client—All clients connected and passed authentication, authorization and other policies, and ready to use the network.
- Client Count By Wireless/Wired—Displays the total number of wired and wireless clients in Prime Infrastructure over the selected period of time.

Client Dashboard

The dashlets that you see on the dashboard are presented in the form of interactive graphs. See the “Interactive Graphs” section on page 9-239 for more information.

The Client dashboard in the Prime Infrastructure home page displays the client-related dashlets. These dashlets enable you to monitor the clients on the network. The data for graphs is also polled/updated periodically and stored in Prime Infrastructure database. On the other hand, most of the information in the Client Details page are polled directly from the controller/switch.

Click the Edit Content link to choose the dashlets you want to have appear on the Client dashboard. You can choose the dashlet from the Available dashlets list and then click to add it to the left or right column. For example, if you want to see the client count in both the General and Client dashboards, you can add the same dashlet to both.

To return to the original Client dashboard before customization, click Edit Tabs, and click Reset to Factory Default.

This section describes the Client dashboard dashlets and contains the following topics:

- Client Troubleshooting Dashlet, page 10-4
- Client Distribution Dashlet, page 10-4
- Client Alarms and Events Summary Dashlet, page 10-5
- Client Traffic Dashlet, page 10-6
- Wired Client Speed Distribution Dashlet, page 10-6
- Top 5 SSIDs by Client Count, page 10-6
- Top 5 Switches by Switch Count, page 10-7
- Client Posture Status Dashlet, page 10-7
- Client Count By IP Address Type, page 10-7
- IPv6 Assignment Distribution, page 10-7
Client Troubleshooting Dashlet

To troubleshoot a client, enter a client MAC address, and then click **Troubleshoot**. The properties information appears.

---

**Note**

If the client is not currently associated, most of the information does not appear.

For details about client troubleshooting see the “Client Troubleshooting” section on page 10-21.

Client Distribution Dashlet

This dashlet shows how many clients are on your network presently. You can see how clients are distributed by protocol, EAP type, and authentication type.

- Protocol
  - 802.11—wireless client protocol
  - 802.3—wired client protocol.

---

**Note**

You can click a protocol to access the list of users belonging to that protocol. For example, if you click the 802.3 protocol, you can directly access the list of the wired clients and users in the Clients and Users page.
**EAP-Type**—Represents Extensible Authentication Protocol (EAP) types such as EAP-FAST, PEAP, and so on

**Authentication Type**—Represents types such as WPA (TKIP), WPA2 (AES), open, and so on

You can choose to display this information in table form or in a pie chart. The pie charts are clickable. If you hover your mouse cursor over a particular portion of the pie chart, a heading and percentage appears, and you can then click the pie chart piece to open a filtered list. When you click the number (next to the header ‘Client Distribution’) represented by Client Distribution, you get a list of clients represented by this number (the same page that you see when you choose Monitor > Clients and Users). You can filter the data that is displayed in client distribution by clicking the Dashlet Options icon and choosing either controller IP, SSID, or floor area.

---

**Note**  
The *Edited* label next to the Client Distribution count indicates that the dashlet has been customized. If you reset to the default page, the *Edited* label is cleared.

---

### Client Authentication Type Distribution

This Client Authentication Type graph shows the number of clients for each authentication type. You can choose to display this information in table form or in a pie chart. When you click the number represented by Total Clients, you get a list of clients represented by this number (the same page that you see when you choose Monitor > Clients and Users). You can filter the data that is displayed in client authentication type distribution by clicking the Dashlet Options icon and choosing either controller IP, SSID, or floor area.

### Client Alarms and Events Summary Dashlet

This dashlet shows the most recent client alarms of both wired and wireless clients.

- Client Association Failure
- Client Authentication Failure
- Client WEP Key Decryption Error
- Client WPA MIC Error Counter Activated
- Client Excluded
- Autonomous AP Client Authentication Failure
- Wired Client Authentication Failure
- Wired Client Authorization Failure
- Wired Client Critical VLAN Assigned
- Wired Client Auth fail VLAN Assigned
- Wired Client Guest VLAN Assigned
- Wired Client Security Violation

---

**Note**  
For more information about the alarms and events, see the “Alarm and Event Dictionary” section on page 13-1.
Click the number in the Total column to open the Events page (the same page that you see when you choose Monitor > Events).

### Client Traffic Dashlet

Controllers keep counters for the number of bytes transferred and received for each client. Prime Infrastructure reads the number every 15 minutes and then calculates the difference, comparing the prior polling. This client traffic data is then aggregated every hour, every day, and every week. It shows the average and maximum values in megabytes per second for both downstream and upstream traffic. You can display the information in table form or in an area chart. When generating the chart based on the floor, Prime Infrastructure adds up all client traffic on this floor. You can filter the data that is displayed in client traffic by clicking the Dashlet Options icon and choosing either controller IP, SSID, or floor area.

For wireless clients, client traffic information comes from controller. For wired clients, the client traffic information comes form ISE, and therefore you need to enable accounting information and other necessary functions on switches.

If you click **View History**, the Client Traffic Historical Charts dashlet appears for the various time frames. The Client Traffic Historical Charts dashlet shows the client traffic over the last 6 hours, last day, last week, last month, and last year. The blue line shows the authenticated client count and the orange line shows the associated client count. The upper right-hand corner shows when the chart was last updated.

### Wired Client Speed Distribution Dashlet

This dashlet displays the wired client speeds and the client count for each speed. There are three different speeds on which clients run:

- 10 Mbps
- 100 Mbps
- 1 Gbps

**Note**

The ports are in the Auto Negotiate mode by default. For example, you get 100 Mbps speed for a client that runs in 100 Mbps speed.

### Top 5 SSIDs by Client Count

This dashlet shows the count of currently associated and authenticated clients. You can choose to display the information in table form or in an area chart.

**Note**

In Prime Infrastructure 1.0, the WGB, Wired Guest, and OEAP 600 (Office Extended Access Point 600) are tracked as wireless clients.
Top 5 Switches by Switch Count

This dashlet displays the five switches that have the most clients as well as the number of clients associated to the switch.

Client Posture Status Dashlet

Prime Infrastructure collects the posture status information from the Identity Services Engine (ISE). You need to add an ISE for authorization and authentication purpose. For information about adding an ISE, see the “Adding an Identity Services Engine” section on page 16-103. After you enable necessary functions in ISE, Prime Infrastructure shows the data in the Client Posture Status dashlet.

This dashlet displays the client posture status and the number of clients in each of the following status categories:

- Compliant
- Non-compliant
- Unknown
- Pending
- Not Applicable
- Error

Client Count By IP Address Type

This dashlet displays a chart which shows client count trend over time by different IP addresses types. The types include IPv4, IPv6, Dual-Stack and Unknown.

IPv6 Assignment Distribution

This dashlet displays a pie chart which shows distribution of all clients based on how their IPv6 addresses get assigned. The type include Unknown, DHCPv6, Self-Assigned, and SLACC or Static.

User Auth Failure Count

This dashlet displays a chart which shows user authentication failure count trend over time.

Client Protocol Distribution

This dashlet displays the current client count distribution by protocols.

Client EAP Type Distribution

This dashlet displays the count based on the EAP type.
Guest Users Count

This dashlet displays Guest client count over a specified time.

Client CCX Distribution

This dashlet displays a pie chart which shows client distribution among different CCX versions.

Top N Client Count

This dashlet displays a bar chart which shows top N elements based on client count. The elements include SSID, APs, Controller, Endpoint Type, Vendor, Switches, and Anchor Controllers. It is a generic top N chart to replace different individual top N charts.

The Top N Client Count shows the anchor clients count on each anchor controller.

Client Mobility Status Distribution

This dashlet displays a pie chart which shows client distribution between local (not anchored) and anchored.

Client 11u Distribution

This dashlet displays a pie chart which shows 11u clients over non-11u clients.

11u Client Count

This dashlet displays a chart which shows 11u client count trend over time.

11u Client Traffic

This dashlet displays a chart which shows 11u client traffic trend over time.

PMIP Clients Distribution

This dashlet displays a pie chart which shows PMIP client over non-PMIP clients.

PMIP Client Count

This dashlet displays a chart which shows PMIP client count trend over time.
Top APs By Client Count

This dashlet displays the Top APs by client count.

Most Recent Client Alarms

This dashlet displays the most recent client alarms.

Recent 5 Guest User Accounts

This dashlet displays the most recent guest user accounts created or modified.

Latest 5 logged in Guest Users

This dashlet displays the most recent guest users to log in.

Clients Detected by Context Aware Service

This dashlet displays the client count detected by the context aware service within the previous 15 minutes.

Monitoring Clients and Users

Using the Monitor Clients and Users feature, you can view all the clients in your network—both wired and wireless. In addition, you can view the client association history and statistical information. These tools are useful when users complain of network performance as they move throughout a building with their laptop computers. The information might help you assess what areas experience inconsistent coverage and which areas have the potential to drop coverage.

The Client Detail page shows the association history graph to represent the time-based data. The information helps you identify, diagnose, and resolve client issues.

Note

Some of the features mentioned in this chapter are not applicable for wired clients (for example, disabling or removing).

Choose Monitor > Clients and Users to view both wired and wireless clients information. The Clients and Users page appears. In the Clients and Users page, you see the clients in tabular format with different tools available at the top of the table.

- Filtering Clients and Users, page 10-10
- Viewing Clients and Users, page 10-12
- Configuring the Search Results Display, page 10-32
Filtering Clients and Users

In the Clients and Users list page, all associated clients are displayed by default. There are 17 preset filters that allow you to view a subset of clients (see Table 10-1).

Note

The WGB, Wired Guest, and OEAP 600 (Office Extended Access Point 600) are tracked as wireless clients.

Note

Sorting on non-indexed column causes serious performance issue when loading the client list page. Prime Infrastructure only remembers sorting column which is indexed including MAC Address, IP Address, Username, AP MAC Address and SSID. You can still sort the table by any column. But after you leave this page, Prime Infrastructure will not remember the last used sorting column if it is not indexed.

Table 10-1 lists the preset filters that are available in the Clients and Users page. Choose the filter you want to show from the Show drop-down list.

Table 10-1 Client List Filters

<table>
<thead>
<tr>
<th>Filter</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>All clients including inactive clients.</td>
</tr>
<tr>
<td></td>
<td>Note: Generally, &quot;All&quot; filter means no filters.</td>
</tr>
<tr>
<td></td>
<td>All SSID returns all clients connected to all controllers such as PMIP, WGB, or wired guest clients.</td>
</tr>
<tr>
<td>2.4 GHz Clients</td>
<td>All clients using 2.4 GHz radio band.</td>
</tr>
<tr>
<td>5 GHz Clients</td>
<td>All clients using 5.0 GHz radio band.</td>
</tr>
<tr>
<td>All Lightweight Clients</td>
<td>All clients connected to lightweight APs.</td>
</tr>
<tr>
<td>All Autonomous Clients</td>
<td>All clients connected to autonomous APs.</td>
</tr>
<tr>
<td>All Wired Clients</td>
<td>All clients directly connected to a switch managed by Prime Infrastructure.</td>
</tr>
<tr>
<td>Associated Clients</td>
<td>All clients connected to the network regardless of whether they are authenticated or not.</td>
</tr>
<tr>
<td>Clients detected by MSE</td>
<td>All clients detected by MSE including wired and wireless clients.</td>
</tr>
<tr>
<td>Clients detected in last 24 hours</td>
<td>All clients detected in the last 24 hours.</td>
</tr>
<tr>
<td>Clients Known by ISE</td>
<td>Shows all the clients that are authenticated by ISE.</td>
</tr>
<tr>
<td>Clients with Problems</td>
<td>Clients that are associated, but have not yet completed policy.</td>
</tr>
<tr>
<td>Excluded Clients</td>
<td>All lightweight wireless clients excluded by the controller.</td>
</tr>
<tr>
<td>FlexConnect Locally Authenticated</td>
<td>Clients connected to FlexConnect APs and authenticated locally.</td>
</tr>
</tbody>
</table>
In addition, you can use the filter icon ( ) to filter the records that match the filter rules. If you want to specify a filter rule, choose All from the Show drop-down list before you click .

When you select a preset filter and click the filter icon, the filter criteria is dimmed. You can only see the filter criteria but cannot change it. When the All option is selected to view all the entries, clicking the filter icon shows the quick filter options, where you can filter the data using the filterable fields. You can also enter text in the free form text box for table filtering.

When you perform advanced client filtering on IPv6 addresses, each octet that you specify must be a complete octet. If you specify a partial octet, the filtering might not show correct results. The following example shows how the advanced client filtering works on IPv6 addresses.

This example assumes that you have the following IP addresses in the system:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Clients detected in last 24 hours</td>
<td>New Clients detected in the last 24 hours.</td>
</tr>
<tr>
<td>On Network Clients</td>
<td>Clients that have gone through authentication/authorization and are able to send and receive data. This means the clients that have completed all set policies and are on the network. The clients are not Identity clients and are always appear as ‘On Network’.</td>
</tr>
<tr>
<td>WGB Clients</td>
<td>All WGB clients.</td>
</tr>
<tr>
<td>Note</td>
<td>If an access point is bridge capable, and the AP mode is set to Bridge, you can view clients identified as WGBs. WGB clients bridge wireless to wired. Any Cisco IOS access point can take on the role of a WGB, acting as a wireless client with a wired client connected to it. The information about this WGB is propagated to the controller and appears as a client in both Prime Infrastructure and WLC.</td>
</tr>
<tr>
<td>All IPv4 Address Clients</td>
<td>Clients which have IPv4 addresses (wired and wireless).</td>
</tr>
<tr>
<td>All IPv6 Address Clients</td>
<td>Clients which have IPv6 addresses (wired and wireless).</td>
</tr>
<tr>
<td>All Dual-Stack Clients</td>
<td>Clients which have both IPv4 and IPv6 address (wired and wireless).</td>
</tr>
</tbody>
</table>
If you search for all IP addresses containing 40, you get the following result:

10.10.40.1
10.10.40.2
10.10.40.3
Fec0::40:20

The IP addresses that contain 240 are not filtered because the filtering feature expects you to enter a complete octet.

Viewing Clients and Users

**Note**
You can use the advanced search feature to narrow the client list based on specific categories and filters. See the Search Methods section in the Cisco Prime Infrastructure 2.0 User Guide for additional information. You can also filter the current list using the Show drop-down list. See the “Filtering Clients and Users” section on page 10-10 for more information.

**Note**
See the “Configuring the Search Results Display” section on page 10-32 for other available client parameters. See the “Filtering Clients and Users” section on page 10-10 for information on filtering this client list.

**Note**
To view complete details in the Monitor > Client and Users page and to perform operations such as Radio Measurement, users in User Defined groups require permission before they access the Monitor Clients, View Alerts & Events, Configure Controllers, and Client Location pages.

To view clients and users, follow these steps:

**Step 1** Choose Monitor > Clients and Users to view both wired and wireless clients information. The Clients and Users page appears.

The Clients and Users table displays a few columns by default. If you want display the additional columns that are available, click ☰ +, and then click Columns. The available columns appear. Select the columns that you want to show in the Clients and Users table. When you click anywhere in a row, the row is selected and the client details are shown.

The following columns are available in the Clients and Users table:

- **MAC Address**—Client MAC address.
- **IP Address**—Client IP address.

The IP address that appears in the IP Address column is determined by a predefined priority order. The first IP address available in the following order appears in the IP address field:

- IPv4 address.
IPv6 unique global address. If there are multiple addresses of this type, most recent IPv6 address the client received are shown, because a user can have two global IPv6 addresses but one might be from an older router advertisement that is being aged out.

IPv6 unique local address. If there are multiple IPv6 unique local addresses, the most recent one is used.

IPv6 link-local address. The IPv6 clients always have at least one link-local address.

The following are the different IPv6 address types:

- Link-local Unicast—The link-local addresses are designed to be used for addressing on a single link for purposes such as auto-address configuration, neighbor discovery, or when no routers are present.

- Site-local Unicast—The site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix.

- Global Unicast—The global unicast address uniquely identifies the client in the global network and is equivalent to a public IPv4 address. A client can have multiple global unicast addresses.

Note When there is more than one IP address of the same type, only the most recent IP address of that type appears, and the rest appear in the QuickView page when you hover your mouse cursor over the QuickView (+) icon.

- IP Address Type—The IP address type such as IPv4 and IPv6.
- Global Unique—The aggregate global unicast address of an IPv6 address. This field is populated only if a client is assigned a global unique IPv6 address.
- Unique Local—The local unicast address of an IPv6 address. This field is populated only if a client is assigned a local unique IPv6 address.
- Link Local—The link-local unicast address of an IPv6 address. This field is populated only if a client is assigned a link-local IPv6 address.
- User Name—Username based on 802.1x authentication or Web authentication. Unknown is displayed for a client connected without a username.
- Type—Indicates the client type.
  - Indicates a lightweight client
  - Indicates a wired client
  - Indicates an autonomous client
- Vendor—Device vendor derived from OUI.
- AP Name—Wireless only
- Device Name—Network authentication device name, for example, WLC, switch.
- Location—Map location of connected device.
- ISE—Yes/No. This column represents whether the client is authenticated using the ISE, which is added to Prime Infrastructure.
- Endpoint Type—Endpoint type as reported by the ISE, available only when the ISE is added (for example, iPhone, iPad, Windows workstation).
- Posture—Latest client posture status
- SSID—Wireless only
- Profile Name—Wireless only
- VLAN——Indicates the access VLAN ID for this client.
- Status—Current client status
  - Idle—Normal operation; no rejections of client association requests.
  - Auth Pending—Completing a AAA transaction.
  - Authenticated—802.11 authentication complete.
  - Associated—802.11 association complete. This is also used by wired clients to represent that a client is currently connected to the network.
  - Power Save—Client is in power save mode.
  - Disassociated—802.11 disassociation complete. This is also used by wired clients to represent that a client is currently not on the network.
  - To Be Deleted—The client that is deleted after disassociation.
  - Excluded—Automatically disabled by the system due to perceived security threat.
- Interface—Controller interface (wireless) or switch interface (wired) that the client is connected to.
- Protocol
  - 802.11—wireless
  - 802.3—wired
- Speed—Ethernet port speed (wired only). Displays “N/A” for wireless.
- Association Time—Last association start time (for wireless client). For a wired client, this is the time when the client is connected to a switch port. This column remains blank when the clients are not successfully authenticated.
- Session Length—Session length.
- First Seen—Indicates the date and time when the client was first detected.
- Authentication Type—WPA, WPA2, 802.1x, MAC Auth Bypass, or Web Auth.
- Authorization Profile Names—Authorization profiles applied to this client by the ISE. This contains data only when the ISE is added and the client is authenticated by the ISE.
- Traffic (MB)—Traffic (transmitted/received) in this session in MB.
- Average Session Throughput (kbps)—Average session throughput in kbps.
- Automated Test Run—Indicates whether the client is in auto test mode. This is applicable for wireless clients only.
- AP MAC Address—Wireless only.
- AP IP Address—Wireless only.
- Anchor Controller—Lightweight wireless only.
- On Network—Shows Yes for the clients that are associated and have successfully finished authentication, if required.
- CCX—Lightweight wireless only.
- Client Host Name—Wired and wireless. Result of DNS reverse lookup.
- Device IP Address—IP address of the connected device (WLC, switch, or autonomous AP).
- Port—Switch port on WLC.
- E2E—Lightweight wireless only.
• Encryption Cipher—Wireless only.
• MSE—MSE server managing this client.
• RSSI—Wireless only.
• SNR—Wireless only.
• Router Advertisements Dropped—The router advertisements that are dropped for each client for a particular session.
• Session ID—Audit-session-ID used in the ISE and on the switch.
• FlexConnect Local Authentication—Indicates if the FlexConnect Local Authentication is enabled for this client.
• WGB Status—Indicates the status of the work group bridge mode.
• Mobility Status—Indicates the mobility status of the wireless client.
• SNMP NAC State—Indicates the state of the NAC appliance in out-of-band mode.

Step 2
Select a client or user. The following information appears:

- Client Attributes, page 10-15
- Client Statistics, page 10-17

**Note** Client Statistics shows statistical information after the client details are shown.

- Client Association History, page 10-17
- Client Event Information, page 10-18
- Client Location Information, page 10-18
- Wired Location History, page 10-19
- Client CCXv5 Information, page 10-19

The following attributes are populated only when the ISE is added to Prime Infrastructure:

- ISE
- Endpoint Type
- Posture
- Authorization Profile Names

**Note** Prime Infrastructure queries the ISE for client authentication records for the last 24 hours to populate this data. If the client is connected to the network 24 hours before it is discovered in Prime Infrastructure, you might not see the ISE-related data in the table. You might see the data in client details page. To work around this, reconnect the client to the network. The ISE information is shown in the table after the next client background task run.

**Client Attributes**

When you select a client from the Clients and Users list, the client attributes appear in the Clients and Users list. Clients are identified using the MAC address.
The details that appear in the Client Attributes group box are from the device, whereas the details that appear in the Clients and Users list are from the database. Therefore, there can be some discrepancy between the details that appear in the Clients and Users list and the Client Attributes group box.

For wired clients, the information comes from the switch. Also, the data that appears in the details page is live data collected on demand from the controller/switch/ISE.

These details include the following client details:

- General—Lists the generation information such as User Name, MAC address, and so on.
  
  **Note** Click the © icon next to the username to access the correlated users of a user.

- Session—Lists the client session information.

- Security (wireless and Identity wired clients only)—Lists Security policy, authentication information, and EAP type.
  
  **Note** The identity clients are the clients whose authentication types are 802.1x, MAC Auth Bypass or Web Auth. For non-identity clients, the authentication type is N/A.

- Statistics (wireless only)

- Traffic—Shows the client traffic information.
  
  **Note** For wireless clients, client traffic information comes from controller. For wired clients, the client traffic information comes form the ISE, therefore you must enable accounting information and other necessary functions on the switches.

**Client IPv6 Addresses**

When you select an IPv6 client from the Clients and Users list, the client IPv6 address details appear. These details come from the controller directly.

For the wired clients that have IPv6 addresses, Prime Infrastructure discovers the client addresses from the IPv6 neighbors table on the switch.

These details include the following information:

- IP Address—Client IPv6 address.

- Scope

- Address Type
• Discovery Time

Client Statistics

The Client Statistics includes the following information for the selected client:

• Client AP Association History
• Client RSSI History (dBm)—History of RSSI (Received Signal Strength Indicator) as detected by the access point with which the client is associated.
• Client SNR History—History of SNR (signal-to-noise ratio of the client RF session) as detected by the access point with which the client is associated.
• Bytes Sent and Received (Kbps)—Bytes sent and received with the associated access point.
• Packets Sent and Received (per second)—Packets sent and received with the associated access point.
• Data rate over time

**Note** Hover your mouse cursor over points on the graph for additional statistical information.

**Note** This information is presented in interactive graphs. See the “Interactive Graphs” section on page 9-239 for more information.

Client Association History

The Association History dashlet displays information regarding the last ten association times for the selected client. This information can help in troubleshooting the client. This section remains blank when the clients are not successfully authenticated.

• Client Association History (for wireless clients) includes the following information:
  – Date and time of association
  – Duration of association
  – Username
  – IP address
  – Access point name
  – Controller name
  – SSID
  – Protocol
  – Amount of traffic (MB)
  – Hostname
  – Roam reason (such as No longer seen from controller or New association detected)

• Client Association History (for wired clients) includes the following information:
  – Date and time of association
  – Duration of association
  – Username
- IP address
- Access point and controller name
- Map location
- SSID
- Protocol
- Amount of traffic (MB)
- Hostname
- Roam reason (such as No longer seen from controller or New association detected)

**Note**
Click the **Edit View** link to add, remove or reorder columns in the Current Associated Clients table. See the “Configuring the List of Access Points Display” section on page 5-47 for adding new parameters than can be added through Edit View.

Prime Infrastructure reports the reassociations of an access point as separate sessions. This is because of the following reasons:
- Session timeout on WLAN
- Low power level because of interference in setup
- Client is roaming
- Client driver implementation
- Data decrypt errors on the client driver

**Client Event Information**

The Client Event dashlet of the Client Details page displays all events for this client including the event type as well as the date and time of the event.

Click an event type to view its details. See the “Monitoring Failure Objects” section on page 5-143 for more information.

**Client Location Information**

The following location parameters appear (if available) for the selected client:

- **Map Area**—The map area in which the client was last located.
- **ELIN**—The Emergency Location Identification Number. This is applicable only to the wired clients that are located by MSE.
- **Civic Address**—The fields on the Civic Address tab are populated if a civic address is imported for a client. This is applicable only to the wired clients that are located by MSE.
- **Advanced**—Detailed information about the client. The fields on this tab are populated if a civic address is imported for a client.

For more information on importing Civic information for the client, see the “Configuring a Switch Location” section on page 9-211.
Wired Location History

You can view the Location History for wired clients.

Note

The wired clients must be located by MSE and the history for wired clients must be enabled on the MSE.

The following Location History information is displayed for a client:

- Timestamp
- State
- Port Type
- Slot
- Module
- Port
- User Name
- IP Address
- Switch IP
- Server Name
- Map Location
- Civic Location

Wireless Location History

You can view the Location History for wireless clients.

Note

The wireless clients must be located by MSE and the history for wired clients must be enabled on the MSE.

Client CCXv5 Information

CCXv5 clients are client devices that support Cisco-compatible Extensions Version 5 (CCXv5). Reports specific to CCXv5 clients provide client details that enhance client diagnostics and troubleshooting.

Note

The CCXv5 manufacturing information is displayed for CCXv5 clients only.

To view specific client details, perform a client search using the applicable search parameters. For more information on performing a client search, see the “Client CCXv5 Information” section on page 10-19.

CCXv5 information is displayed in the Monitor Clients > Client Details page. CCXv5 information includes the following:

CCXv5 Manufacturing Information:

- Organizationally Unique Identifier—The IEEE assigned organizational unique identifier, for example, the first 3 bytes of the MAC address of the wireless network connected device.
• ID—The manufacturer identifier of the wireless network adapter.
• Model—Model of the wireless network adapter.
• Serial Number—Serial number of the wireless network adapter.
• Radio—Radio type of the client.
• MAC Address—MAC address assigned to the client.
• Antenna Type—Type of antenna connected to the wireless network adapter.
• Antenna Gain—The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means 4 x 0.5 = 2 dBm of gain.

**Note** Click *More* to view the following additional CCXv5 parameters.

Automated Troubleshooting Report—If the automated test runs, this report displays the location of automated troubleshooting log AUTO_TS_LOG<ClientMac>.txt. If no automated test runs, Not Exists appears.

• Click *Export* to save the .zip file. The file contains three logs: automated troubleshoot report, frame log, and watch list log.

**Note** The *Settings > Client* page allows you to enable automatic client troubleshooting on a diagnostic channel. This feature is only available for Cisco-compatible Extension clients version 5.

Radio Receiver Sensitivity—Displays receiver sensitivity of the wireless network adapter including the following:
- Radio
- Data Rate
- Minimum and Maximum RSSI

CCXV5 Capability Information—Displays the Capability Information parameters for CCXv5 clients only.
- Radio
- Client Status—Success or failure.
- Service Capability—Service capabilities such as voice, streaming (uni-directional) video, interactive (bi-directional) video.

Radio Channels—Identifies the channels for each applicable radio.

Transmit Data Rates—Identifies the transmission data rates (Mbps) for each radio.

Transmit Power Values—Identifies the transmission power values including:
- Power mode
- Radio
- Power (dBm)
Exporting Clients and Users

You can quickly export your clients and users list into a CSV file (spreadsheet format with comma-separated values).

Note: The columns that are shown in the Clients and Users table are only exported to the CSV file.

To export the clients and users list, follow these steps:

Step 1. Choose Monitor > Clients and Users.

Step 2. Click the icon on the toolbar. A dialog box appears.

Step 3. In the File Download dialog box, click Save.

Client Troubleshooting

You can begin troubleshooting several ways: by entering a MAC address on the Client dashboard, by using the search function, or by selecting a row in the Monitor > Clients and Users page. Any of these methods provides all the information necessary to troubleshoot historical client issues. You can monitor the status of the connection, verify the current and past locations of a user, and troubleshoot client connectivity problems. You might want to use the client troubleshooting option if a user experiences repeated connectivity issues. The Client Details page shows SNR over time, RSSI over time, client reassociations, client re authentications, and any RRM events. An administrator can correlate reassociations and reauthorizations and determine if the problem was with the network or client.

Note: You can troubleshoot current client issues only. You cannot troubleshoot the historic client issues. However, for location assisted clients, you can find the location history.

Note: The client troubleshooting feature is available for identity wired clients only. This feature is not available for non-identity wired clients.

Prime Infrastructure provides integrated management for wired and wireless devices or clients. You can monitor and troubleshoot both wired and wireless clients. SNMP is used to discover clients and collect client data. The ISE is polled periodically to collect client statistics and other attributes to populate related dashboard dashlets and reports. If the ISE is added to the systems and devices are authenticating to it, the Client Details page displays security information.

To launch the Client Troubleshooting tool, select a client, and then click the icon indicated above the IP address that you want to troubleshoot. The Troubleshooting Client page appears.

The troubleshooting page displays the following states for wired clients:

- Link Connectivity
- 802.1X Authentication
- MAC Authentication
- Web Authentication
- IP Connectivity
- Authorization
- Successful Connection

Note: The exact states displayed depend on the level of security used by the client.

The following are the security mechanisms used by clients:
- 802.1X
- MAC Authentication
- Web Authentication

Table 10-2 summarizes the validity of states against the security types. The states are arranged in the order the client goes through.

<table>
<thead>
<tr>
<th>Security/Client State</th>
<th>Link Connectivity</th>
<th>802.1X Authentication</th>
<th>MAC Authentication</th>
<th>Web Authentication</th>
<th>IP Connectivity</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td>–</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>MAC Authentication</td>
<td>X</td>
<td>–</td>
<td>X</td>
<td>–</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Web Authentication</td>
<td>X</td>
<td>–</td>
<td>–</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Table 10-3 provides the list of problems and suggested actions depending on the state in which a client failed:

<table>
<thead>
<tr>
<th>Client State</th>
<th>Problem</th>
<th>Suggested Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Connectivity</td>
<td>Cannot find the client in network</td>
<td>• Check whether the client cable is plugged into the network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the client is using the proper cable to connect to the network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Make sure that the port to which client is connected is not disabled administratively.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Make sure that the port to which client is connected is not error disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the speed and duplex are set to Auto on the port to which the client is connected.</td>
</tr>
<tr>
<td>Authentication in progress</td>
<td>If the client has been in this state for a long time, check the following:</td>
<td>• If the client has been in this state for a long time, check the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Check whether the supplicant on the client is configured properly as required.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Modify the timers related to authentication method and try again.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– If you are not sure which authentication method works with the client, use the fall back authentication feature.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Try disconnecting and reconnecting.</td>
</tr>
<tr>
<td>802.1X Authentication</td>
<td>802.1X Authentication Failure</td>
<td>• Check whether the RADIUS server(s) is reachable from the switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the client choice of EAP is supported by RADIUS server(s).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the username/password/certificate of the client is valid.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• See whether the certificates used by RADIUS server are accepted by the client.</td>
</tr>
<tr>
<td>MAC Authentication</td>
<td>MAC Authentication Failure</td>
<td>• Check whether the RADIUS server(s) is reachable from the switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the MAC address of the client is in the list of known clients on the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the MAC address of the client is not in the list of excluded clients.</td>
</tr>
</tbody>
</table>
Using the Search Feature to Troubleshoot Clients

Client search is the primary method used to locate clients. For a detailed description of the search feature, see the Search Methods section in the Cisco Prime Infrastructure 2.0 User Guide.

To troubleshoot a client using the Search feature, follow these steps:

Step 1 Choose Monitor > Clients and Users.
Step 2 Type the full or partial client MAC address in the Advanced Search text box, and click Search. The Search Results page appears.

Step 3 Click View List to see the clients that match the search criteria in the Clients page. The Monitor > Clients and Users page appears.

**Note** You can click the Reset link to set the table to the default display so that the search criteria is no longer applied.

Step 4 Select a client, and then click the icon indicated above the IP address that you want to troubleshoot. The Troubleshooting Client page appears. If you are troubleshooting a Cisco-compatible Extension v5 client (wireless), your Troubleshooting Client page has additional tabs.

**Note** If you receive a message that the client does not seem to be connected to any access point, you must reconnect the client and click Refresh.

**Note** You can use the detach/clone icon located in the top right corner of the page to detach the current page into a new window/tab.

**Note** Click Go back to return to the page from where you launched client troubleshooting. For example, if you have launched client troubleshooting from the list page, you can return to the list page.

The summary page briefly describes the problem and recommends a course of action.

**Note** Some Cisco-compatible Extension features do not function properly when you use a web browser other than Mozilla Firefox 11.0 or later or Internet Explorer 8 or later on a Windows workstation.

Step 5 To view log messages logged against the client, click the Log Analysis tab.

Step 6 To begin capturing log messages about the client from the controller, click Start. To stop log message capture, click Stop. To clear all log messages, click Clear.

**Note** Log messages are captured for ten minutes and then stopped automatically. You must click Start to continue.

Step 7 To select log messages to display, click one of the links under Select Log Messages (the number between parentheses indicates the number of messages). The messages appear in the group box. The message includes the following information:

- A status message
- The controller time
- A severity level of info or error (errors are displayed in red)
- The controller to which the client is connected

Step 8 To display the event history of a client, click the Event History tab.
Event History provides messages related to connectivity events for this client. In this example, the client failed to successfully authenticate. The date/time information is provided to assist the network administrator in troubleshooting this client.

**Step 9**

To view the event log, click the **Event Log** tab. Click **Start** to begin capturing log messages from the client. When a sufficient number of messages have been collected, click **Stop**.

**Note**
The Client Troubleshooting Event log and Messaging features are available to CCX Version 6 clients only if the Management Service version is 2 and later.

**Step 10**

If you click the ACS View Server tab, you can interact with the Cisco Access Control (ACS) System View Server. This tab displays the latest authentication records received either from an ACS View server or Identity Services Engine (ISE), whichever is configured in Prime Infrastructure. You must have View Server credentials established before you can access this tab. (The tab shows the server list as empty if no view servers are configured.) See the “Configuring ACS View Server Credentials” section on page 9-238 for steps on establishing credentials.

If the ACS View Server is already configured, you can select a time range and click **Submit** to retrieve the authentication records from the ACS View Server. Prime Infrastructure uses the ACS View NS API to retrieve the records.

**Step 11**

You can click the Identity Services Engine tab to view information about the ISE authentication. Enter the date and time ranges to retrieve the historical authentication and authorization information, and click **Submit**. The results of the query are displayed in the Authentication Records portion of the page.

**Step 12**

You can click the CleanAir tab to view information about the air quality parameters and the active interferers for the CleanAir-enabled access point. This tab provides the following information about the air quality detected by the CleanAir-enabled access point.

- **AP Name**—Click to view the access point details. See the “Monitoring Access Points Details” section on page 5-58 for more information.
- **AP MAC Address**
- **Radio**
- **CleanAir Capable**—Indicates if the access point is CleanAir Capable.
- **CleanAir Enabled**—Indicates if CleanAir is enabled on this access point.
- **Admin Status**—Enabled or disabled.
- **Operational Status**—Displays the operational status of the Cisco Radio(s) (Up or Down).
- **Channel**—The channel upon which the Cisco Radio is broadcasting.
- **Extension Channel**—Indicates the secondary channel on which the Cisco Radio is broadcasting.
- **Channel Width**—Indicates the channel bandwidth for this radio interface. See the “Configuring 802.11a/n RRM Dynamic Channel Allocation” section on page 9-131 for more information on configuring channel bandwidth.
- **Power Level**—Access Point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.
- The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis.
- **Average AQ Index**—Average air quality index.
- **Minimum AQ Index**—Minimum air quality index.

The following information about the active interferers is displayed:
- Interferer Name—The name of the interfering device.
- Affected Channels—The channel the interfering device is affecting.
- Detected Time—The time at which the interference was detected.
- Severity—The severity index of the interfering device.
- Duty Cycle(%)—The duty cycle (in percentage) of the interfering device.
- RSSI(dBm)—The Received Signal Strength Indicator of the interfering device.
- Click **CleanAir Details** to know more about the air quality index.

**Step 13**
(Continuous) If Cisco-compatible Extension Version 5 or Version 6 clients are available, you can click the Test Analysis tab.

**Note**
The Client Troubleshooting Test Analysis feature is available to CCX Version 6 clients only if Management Service version is 2 and later.

The Test Analysis tab allows you to run a variety of diagnostic tests on the client. Select the check box for the applicable diagnostic test, enter any appropriate input information, and click **Start**. The following diagnostic tests are available:

- DHCP—Executes a complete DHCP Discover/Offer/Request/ACK exchange to determine that the DHCP is operating properly between the controller and the client.
- IP Connectivity—Causes the client to execute a ping test of the default gateway obtained in the DHCP test to verify that IP connectivity exists on the local subnet.
- DNS Ping—Causes the client to execute a ping test of the DNS server obtained in the DHCP test to verify that IP connectivity exists to the DNS server.
- DNS Resolution—Causes the DNS client to attempt to resolve a network name known to be resolvable to verify that name resolution is functioning correctly.
- 802.11 Association—Directs an association to be completed with a specific access point to verify that the client is able to associate properly with a designated WLAN.
- 802.1X Authentication—Directs an association and 802.1X authentication to be completed with a specific access point to verify that the client is able to properly complete an 802.1x authentication.
- Profile Redirect—At any time, the diagnostic system might direct the client to activate one of the configured WLAN profiles and to continue operation under that profile.

**Note**
To run the profile diagnostic test, the client must be on the diagnostic channel. This test uses the profile number as an input. To indicate a wildcard redirect, enter 0. With this redirect, the client is asked to disassociate from the diagnostic channel and to associate with any profile. You can also enter a valid profile ID. Because the client is on the diagnostic channel when the test is run, only one profile is returned in the profile list. You should use this profile ID in the profile redirect test (when wildcard redirecting is not desired).

**Step 14**
(Optional) If Cisco-compatible Extension Version 5 or Version 6 clients are available, a Messaging tab appears. Use this tab to send an instant text message to the user of this client. From the Message Category drop-down list, choose a message, and click **Send**.

**Note**
The Client Troubleshooting Event log and Messaging features are available to CCX Version 6 clients only if the Management Service version is 2 and later.
Step 15 You can click the **Identity Services Engine** tab to view information about the identity services parameters. You must have an Identity Services Engine (ISE) configured before you can access this tab. (The tab shows the server list as empty if no ISEs are configured.)

**Note** If the ISE is not configured it provides a link to add an ISE to Prime Infrastructure.

The ISE provides authentication records to Prime Infrastructure via REST API. The network administrator can choose a time period for retrieving authentication records from the ISE.

Step 16 To view the client location history, click the **Context Aware History** tab.

Step 17 To view the Real Time Troubleshooting (RTTS) details, click the **RTTS** tab.

   a. Select the **modules to debug** and **debug level**.

   b. Click **Run**. The RTTS manager executes a set of commands in the controllers connected to the client based on the selected debug modules and debug level and displays the RTTS details. For more details, refer **Debug Commands for RTTS**.

   c. Click the **Filter** tab to filter the RTTS details based on debug time, controller name, controller IP, severity and debug message.

   d. Click the **Export** tab to export the debug details as a .csv file.

**Note** You can also debug other controllers based on the selected debug modules and debug levels using **Choose different controllers** option.

**Note** The RTTS Manager supports 5 concurrent RTTS debug sessions and each debug session is limited to 5 devices.

Step 18 Close the Troubleshooting Client page.

**Debug Commands for RTTS**

Table 10-4 contains the list of debug commands for Legacy controllers and NGWC controllers.

<table>
<thead>
<tr>
<th>Controller</th>
<th>Modules to Debug</th>
<th>Debug Level</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy</td>
<td>All</td>
<td></td>
<td>• debug capwap info enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• debug dot1x all enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• debug mobility directory enable</td>
</tr>
<tr>
<td>Dot1.x</td>
<td>Detail</td>
<td>debug dot1x all enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Error</td>
<td>debug dot1x events enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High Level</td>
<td>debug dot1x states enable</td>
<td></td>
</tr>
<tr>
<td>Controller</td>
<td>Modules to Debug</td>
<td>Debug Level</td>
<td>Commands</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------</td>
<td>-------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Legacy</td>
<td>Mobility</td>
<td>Detail</td>
<td>• debug mobility packet enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• debug mobility keepalive enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Error</td>
<td>• debug mobility directory enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• debug mobility config enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Level</td>
<td>debug mobility handoff enable</td>
</tr>
<tr>
<td>Wireless Client Join</td>
<td>Detail</td>
<td></td>
<td>• debug client &lt;macAddress&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• debug aaa all enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• debug dot1x all enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Error</td>
<td>debug client &lt;macAddress&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Level</td>
<td>debug client &lt;macAddress&gt;</td>
</tr>
<tr>
<td>NGWC</td>
<td>All</td>
<td>Detail</td>
<td>• debug capwap ap error</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• debug dot1x events</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• debug capwap ios detail</td>
</tr>
<tr>
<td>Dot1.x</td>
<td>Detail</td>
<td></td>
<td>• debug wcm-dot1x detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• debug wcm-dot1x all</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• debug dot1x all</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Error</td>
<td>• debug wcm-dot1x errors</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• debug dot1x errors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Level</td>
<td>• debug wcm-dot1x trace</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• debug wcm-dot1x event</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• debug wcm-dot1x error</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• debug client mac-address &lt;macAddress&gt;</td>
</tr>
<tr>
<td>Mobility</td>
<td>Detail</td>
<td></td>
<td>debug mobility all</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Error</td>
<td>debug mobility error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Level</td>
<td>debug mobility handoff</td>
</tr>
<tr>
<td>Wireless Client Join</td>
<td>Detail</td>
<td></td>
<td>debug wcdb error</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug wcdb event</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug wcdb db</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug ip dhcp snooping events</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug ip dhcp server events</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug client mac &lt;macAddress&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Error</td>
<td>debug client mac &lt;macAddress&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Level</td>
<td>debug client mac &lt;macAddress&gt;</td>
</tr>
</tbody>
</table>
Tracking Clients

This feature enables you to track clients and be notified when these clients connect to the network.

To track clients, follow these steps:

Step 1 Choose Monitor > Clients and Users.
Step 2 Click Track Clients. The Track Clients dialog box appears listing the currently tracked clients.

Tip This table supports a maximum of 2000 rows. To add or import new rows, you must first remove some older entries.

Step 3 To track a single client, click Add, and then enter the following parameters:

- Client MAC address
- Expiration—Choose Never or enter a date.

Step 4 To track multiple clients, click Import. This allows you to import a client list from a CSV file. Enter MAC Address and username.

A sample CSV file can be downloaded that provides data format:

```
# MACAddress, Expiration: Never/Date in MM/DD/YYYY format
00:40:96:b6:02:cc,10/07/2010
00:02:8a:a2:2e:60,Never
```

Notification Settings

To specify notification settings for the tracked clients, follow these steps:

Step 1 Choose Monitor > Clients and Users.
Step 2 Click Track Clients. The Track Clients dialog box appears listing the currently tracked clients.
Step 3 Select the tracked client(s) for which you want to specify notification settings.
Step 4 Specify the notification settings. There are three options for notifications:

a. Purged Expired Entries—You can set the duration to keep tracked clients in Prime Infrastructure database. Clients can be purged as follows:
   - after 1 week
   - after 2 weeks
   - after 1 month
   - after 2 months
   - after 6 months
   - kept indefinitely

b. Notification Frequency—You can specify when Prime Infrastructure sends a notification of a tracked client:
   - on first detection
Identifying Unknown Users

Not all users or devices are authenticated via 802.1x (for example, printers). In such a case, a network administrator can assign a username to a device.

If a client device is authenticated to the network through web auth, Prime Infrastructure might not have username information for the client (applicable only for wired clients).

Clients are marked as unknown when the NMSP connection to the wired switch is lost. A client status (applicable only for wired client) is noted as connected, disconnected, or unknown:

- Connected clients—Clients that are active and connected to a wired switch.
- Disconnected clients—Clients that are disconnected from the wired switch.
- Unknown clients—Clients that are marked as unknown when the NMSP connection to the wired switch is lost.

To view the unknown devices, follow these steps:

**Step 1** Choose Monitor > Clients and Users.

**Step 2** Click Identify Unknown Users.

**Step 3** Click Add to assign client MAC addresses to username.

**Step 4** Enter the MAC address and username.

**Note** Once a client and MAC address have been added, Prime Infrastructure uses this data for client lookup based on the matching MAC address.

**Step 5** Click Add.

**Step 6** Repeat Step 3 to Step 5 to enter a MAC Address and its corresponding username for each client.

**Step 7** Click Save.

**Note** The username is updated only when the next association of the client occurs.

**Note** This table supports a maximum of 10,000 rows. To add or import new rows, you must first remove some older entries.
Enabling Automatic Client Troubleshooting

In the Settings > Client page, you can enable automatic client troubleshooting on a diagnostic channel. This feature is available only for Cisco-compatible Extension clients Version 5.

To enable automatic client troubleshooting, follow these steps:

Step 1 Choose Administration > Settings.
Step 2 From the left sidebar menu, choose Client.
Step 3 Select the Automatically troubleshoot client on diagnostic channel check box.

Note When the check box is selected, Prime Infrastructure processes the diagnostic association trap. When it is not selected, Prime Infrastructure raises the trap, but automated troubleshooting is not initiated.

Step 4 Click Save.
Viewing Client Details in the Access Point Page

You can also view the client information from the access point page. Choose **Monitor > Access Points**. Click an access point URL from the column to see details about that access point. Click the **Current Associated Clients** tab.

Viewing Currently Associated Clients

You can also view the currently associated clients (wired) from the switch details page. Choose **Monitor > Controllers**, select an IP address, and choose **Clients > Current Associated Clients** from the left sidebar menu.

Running Client Reports

You can run client reports such as busiest clients, client count, client sessions, client summary, throughput, unique clients and v5 clients statistics from the Report Launch pad. See the “Reports” section on page 14-1.

Running ISE Reports

You can also launch ISE reports from the Report Launch pad. See the “Reports” section on page 14-1. For more information about running the ISE reports, see the ISE online help.

Specifying Client Settings

The Administration > Settings > Client page allows you to specify various client settings. For details, see “Performing Administrative Tasks” section on page 15-1.

Receiving Radio Measurements for a Client

In the client page, you can receive radio measurements only if the client is Cisco-compatible Extensions v2 (or higher) and is in the associated state (with a valid IP address). If the client is busy when asked to do the measurement, it determines whether to honor the measurement or not. If it declines to make the measurement, it shows no data from the client.

**Note**

This feature is available to CCX Version 6 clients only if the Foundation service version is 1 or later.

To receive radio measurements, follow these steps:

**Step 1** Choose **Monitor > Clients and Users**.

**Step 2** Choose a client from the Client Username column.
Received Radio Measurements for a Client

Note You can also perform a search for a specific client using Prime Infrastructure Search feature. See the Search Methods section in the *Cisco Prime Infrastructure 2.0 User Guide* for additional information.

Step 3 From the **Test** drop-down list, choose **Radio Measurement**.

Note The Radio Measurement option only appears if the client is Cisco-compatible Extensions v2 (or higher) and is in the associated state (with a valid IP address).

Step 4 Select the check box to indicate if you want to specify beacon measurement, frame measurement, channel load, or noise histogram.

Step 5 Click **Initiate**. The different measurements produce differing results. See the “Radio Measurement Results for a Client” section on page 10-34 for more information.

Note The measurements take about 5 milliseconds to perform. A message from Prime Infrastructure indicates the progress. If the client chooses not to perform the measurement, that is communicated.

**Radio Measurement Results for a Client**

Depending on the measurement type requested, the following information might appear:

- **Beacon Response**
  - Channel—The channel number for this measurement
  - BSSID—6-byte BSSID of the station that sent the beacon or probe response
  - PHY—Physical Medium Type (FH, DSS, OFDM, high rate DSS or ERP)
  - Received Signal Power—The strength of the beacon or probe response frame in dBm
  - Parent TSF—The lower 4 bytes of serving access point TSF value
  - Target TSF—The 8-byte TSF value contained in the beacon or probe response
  - Beacon Interval—The 2-byte beacon interval in the received beacon or probe response
  - Capability information—As found in the beacon or probe response
- **Frame Measurement**
  - Channel—Channel number for this measurement
  - BSSID—BSSID contained in the MAC header of the data frames received
  - Number of frames—Number of frames received from the transmit address
  - Received Signal Power—The signal strength of 802.11 frames in dBm
- **Channel Load**
  - Channel—The channel number for this measurement
Viewing Client V5 Statistics

To access the Statistics request page, follow these steps:

Step 1  Choose **Monitor > Clients and Users**.
Step 2  Choose a client from the Client Username column.
Step 3  From the **Test** drop-down list, choose **V5 Statistics**.

**Note**  This menu is shown only for CCX v5 and later clients.

Step 4  Click **Go**.
Step 5  Select the desired type of stats (Dot11 Measurement or Security Measurement).
Step 6  Click **Initiate** to initiate the measurements.

**Note**  The duration of measurement is five seconds.

Step 7  Depending on the V5 Statistics request type, the following counters are displayed in the results page:

- **Dot11 Measurement**
  - Transmitted Fragment Count
  - Multicast Transmitted Frame Count
  - Failed Count
  - Retry Count
  - Multiple Retry Count
  - Frame Duplicate Count
  - Rts Success Count
  - Rts Failure Count
  - Ack Failure Count
  - Received Fragment Count
  - Multicast Received Frame Count
  - FCS Error Count—This counter increments when an FCS error is detected in a received MPDU.
  - Transmitted Frame Count
- **Security**
Viewing Client Operational Parameters

To view specific client operational parameters, follow these steps:

**Step 1** Choose Monitor > Clients and Users.

**Step 2** Choose a client from the Client Username column.

**Step 3** From the Test drop-down list, choose Operational Parameters.

The following information is displayed:

**Operational Parameters:**

- **Device Name**—User-defined name for device.
- **Client Type**—Client type can be any of the following:
  - laptop(0)
  - pc(1)
  - pda(2)
  - dot11mobilephone(3)
  - dualmodephone(4)
  - wgb(5)
  - scanner(6)
  - tabletpc(7)
  - printer(8)
- projector(9)
- videoconfsystem(10)
- camera(11)
- gamingsystem(12)
- dot11deskphone(13)
- cashregister(14)
- radiotag(15)
- rfidsensor(16)
- server(17)

- SSID—SSID being used by the client.
- IP Address Mode—The IP address mode such as static configuration or DHCP.
- IPv4 Address—IPv4 address assigned to the client.
- IPv4 Subnet Address—IPv4 subnet address assigned to the client.
- IPv6 Address—IPv6 address assigned to the client.
- IPv6 Subnet Address—IPv6 address assigned to the client.
- Default Gateway—The default gateway chosen for the client.
- Operating System—Identifies the operating system that is using the wireless network adaptor.
- Operating System Version—Identifies the version of the operating system that is using the wireless network adaptor.
- WNA Firmware Version—Version of the firmware currently installed on the client.
- Driver Version—
- Enterprise Phone Number—Enterprise phone number for the client.
- Cell Phone Number—Cell phone number for the client.
- Power Save Mode—Displays any of the following power save modes: awake, normal, or maxPower.
- System Name—
- Localization—

Radio Information:
- Radio Type—The following radio types are available:
  - unused(0)
  - fhss(1)
  - dsss(2)
  - irbaseband(3)
  - ofdm(4)
  - hrdss(5)
  - erp(6)
- Radio Channel—Radio channel in use.

DNS/WNS Information:
- DNS Servers—IP address for DNS server.
• WNS Servers—IP address for WNS server.

Security Information:
• Credential Type—Indicates how the credentials are configured for the client.
• Authentication Method—Method of authentication used by the client.
• EAP Method—Method of Extensible Authentication Protocol (EAP) used by the client.
• Encryption Method—Encryption method used by the client.
• Key Management Method—Key management method used by the client.

---

**Viewing Client Profiles**

To view specific client profile information, follow these steps:

**Step 1** Choose Monitor > Clients and Users.
**Step 2** Choose a client from the Client Username column.
**Step 3** From the More drop-down list, choose Profiles.

The following information is displayed:
• Profile Name—List of profile names as hyperlinks. Click to display the profile details.
• SSID—SSID of the WLAN to which the client is associated.

---

**Disabling a Current Client**

To disable a current client, follow these steps:

**Step 1** Choose Monitor > Clients and Users.
**Step 2** Choose a client that you want to disable.
**Step 3** Click Disable. The Disable Client page appears.
**Step 4** Enter a description in the Description text box.
**Step 5** Click OK.

**Note**
Once a client is disabled, it cannot join any network/ssid on controller(s). To reenable the client, choose Configure > Controllers > IP Address > Security > Manually Disabled Clients, and remove the client entry.
Removalg a Current Client

To remove a current client, follow these steps:

**Step 1** Choose Monitor > Clients and Users.
**Step 2** Choose a client that you want to remove.
**Step 3** Choose Remove.
**Step 4** Click Remove to confirm the deletion.

Enabling Mirror Mode

When enabled, mirror mode enables you to duplicate (to another port) all of the traffic originating from or terminating at a single client device or access point.

**Note**

Mirror mode is useful in diagnosing specific network problems but should only be enabled on an unused port as any connections to this port become unresponsive.

To enable mirror mode, follow these steps:

**Step 1** Choose Monitor > Clients and Users.
**Step 2** Choose a client from the Client Username column.
**Step 3** From the More drop-down list, choose Enable Mirror Mode.
**Step 4** Click Go.

Viewing a Map (High Resolution) of a Client Recent Location

To display a high-resolution map of the client recent location, follow these steps:

**Step 1** Choose Monitor > Clients and Users.
**Step 2** Choose a client from the Client Username column.
**Step 3** From the More drop-down list, choose Recent Map (High Resolution).
**Step 4** Click Go.

Viewing a Map (High Resolution) of a Client Current Location

To display a high-resolution map of the client present location, follow these steps:
Running a Client Sessions Report for the Client

To view the most recent client session report results for this client, follow these steps:

Step 1 Choose Monitor > Clients and Users.
Step 2 Choose a client from the Client Username column.
Step 3 From the More drop-down list, choose Present Map (High Resolution).
Step 4 Click Go. The Client Session report details display. See the “Reports” section on page 14-1 for more information.

Viewing a Roam Reason Report for the Client

To view the most recent roam report for this client, follow these steps:

Step 1 Choose Monitor > Clients and Users.
Step 2 Choose a client from the Client Username column.
Step 3 From the More drop-down list, choose Roam Reason.
Step 4 Click Go.

This page displays the most recent roam report for the client. Each roam report has the following information:

- New AP MAC address
- Old (previous) AP MAC address
- Previous AP SSID
- Previous AP channel
- Transition time—Time that it took the client to associate to a new access point.
- Roam reason—Reason for the client roam.
Viewing Detecting Access Point Details

To display details of access points that can hear the client including at which signal strength/SNR, follow these steps:

Step 1 Choose Monitor > Clients and Users.
Step 2 Choose a client from the Client Username column.
Step 3 From the More drop-down list, choose Detecting APs.
Step 4 Click Go.

Viewing Client Location History

To display the history of the client location based on RF fingerprinting, follow these steps:

Step 1 Choose Monitor > Clients and Users.
Step 2 Choose a client from the Client Username column.
Step 3 From the More drop-down list, choose Location History.
Step 4 Click Go.

Viewing Voice Metrics for a Client

To view traffic stream metrics for this client, follow these steps:

Step 1 Choose Monitor > Clients and Users.
Step 2 Choose a client from the Client Username column.
Step 3 From the More drop-down list, choose Voice Metrics.
Step 4 Click Go.

The following information appears:

- Time—Time that the statistics were gathered from the access point(s).
- QoS
- AP Ethernet MAC
- Radio
- % PLR (Downlink)—Percentage of packets lost on the downlink (access point to client) during the 90 second interval.
- % PLR (Uplink)—Percentage of packets lost on the uplink (client to access point) during the 90 second interval.
- Avg Queuing Delay (ms) (Uplink)—Average queuing delay in milliseconds for the uplink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.

- % Packets > 40 ms Queuing Delay (Downlink)—Percentage of queuing delay packets greater than 40 ms.

- % Packets 20ms—40ms Queuing Delay (Downlink)—Percentage of queuing delay packets greater than 20 ms.

- Roaming Delay—Roaming delay in milliseconds. Roaming delay, which is measured by clients, is measured beginning when the last packet is received from the old access point and ending when the first packet is received from the new access point after a successful roam.
Using Templates

This chapter describes how to add and apply templates. Templates allow you to set fields that you can then apply to multiple devices without having to reenter the common information.

- Information About Templates, page 11-1
- Accessing the Controller Template Launch Pad, page 11-1
- Adding Controller Templates, page 11-2
- Deleting Controller Templates, page 11-2
- Applying Controller Templates, page 11-2
- Configuring Controller Templates, page 11-4
- Configuring AP Configuration Templates, page 11-126
- Configuring Switch Location Configuration Templates, page 11-136
- Configuring Autonomous AP Migration Templates, page 11-137

Information About Templates

The Controller Template Launch Pad is a hub for all controller templates. From this Template Launch Pad you can add and apply controller templates, view templates, or make modifications to existing templates. This chapter also includes steps for applying and deleting controller templates and creating or changing access point templates.

Note

Template information can be overridden on individual devices.

Accessing the Controller Template Launch Pad

To access the Controller Template Launch Pad, choose Configure > Controller Template Launch Pad. The controller template launch pad provides access to all Cisco Prime Infrastructure templates from a single page. From this page, you can view current controller templates or create and save new templates.

Tip

Hover your mouse cursor over the tool tip next to the template type to view more details regarding the template.
Adding Controller Templates

To add a new controller template, follow these steps:

**Step 1** Choose Configure > Controller Template Launch Pad.

**Step 2** Click New beside the template you want to add.

**Step 3** Enter the template name.

**Note** Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

**Step 4** Provide a description of the template.

**Step 5** Click Save.

Deleting Controller Templates

To delete a controller template, follow these steps:

**Step 1** Choose Configure > Controller Template Launch Pad.

**Step 2** Click the template type to open its template list page.

**Step 3** Select the check box(es) of the template(s) you want to delete.

**Step 4** From the Select a command drop-down list, choose Delete Templates.

**Step 5** Click Go.

**Step 6** Click OK to confirm the deletion. If this template is applied to controllers, the Remove Template Confirmation page opens and lists all controllers to which this template is currently applied.

**Step 7** Select the check box of each controller from which you want to remove the template.

**Step 8** Click OK to confirm the deletion or Cancel to close this page without deleting the template.

Applying Controller Templates

You can apply a controller template directly to a controller or to controllers in a selected configuration group.

To apply a controller template, follow these steps:

**Step 1** Choose Configure > Controller Template Launch Pad.

**Step 2** From the left sidebar menu, choose the category of templates to apply.

**Step 3** Click the template name for the template that you want to apply to the controller.
Step 4  Click **Apply to Controllers** to open the Apply to Controllers page.

Step 5  Select the check box for each controller to which you want to apply the template.

**Note**  To select all controllers, select the check box that appears at the left most corner of the controllers table.

**Note**  Select the **Ignore errors on Apply template to Controllers** check box to ignore errors and apply all commands in the template to the controller. If this check box is not selected, any errors encountered while applying a command in the template to a controller causes the rest of the commands to be not applied.

Step 6  Choose between applying the template directly to a controller or to all controllers in a selected configuration group.

To apply the template directly to a controller (or controllers), follow these steps:

a. Select the **Apply to controllers selected directly** radio button. The Apply to Controllers page lists the IP address for each available controller along with the controller name and the configuration group name (if applicable).

b. Select the check box for each controller to which you want to apply the template.

**Note**  Select the **Ignore errors on Apply template to Controllers** check box to ignore errors and apply all commands in the template to the controller. If this check box is not selected, any errors encountered while applying a command in the template to a controller causes the rest of the commands to be not applied.

To apply the template to all controllers in a selected configuration group, follow these steps:

a. Select the **Apply to controllers in the selected Config Groups** radio button. The Apply to Controllers page lists the name of each configuration group along with the mobility group name and the number of controllers included.

b. Select the check box for each configuration group to which you want to apply the template.

**Note**  Configuration groups which have no controllers cannot be selected to apply the templates.

Step 7  You can perform the following additional operations:

- If you select the Save Config to Flash after apply check box, the save config to Flash command is executed after the template is applied successfully.
- If you select the Reboot Controller after apply check box, the controller reboots after the template is successfully applied.

**Note**  This configuration results can be viewed in the Template Results page by enabling the View Save Config / Reboot Results option.

Step 8  Click **Save**.
You can apply some templates directly from the Template List page. Select the check box(es) of the template(s) that you want to apply, choose **Apply Templates** from the Select a command drop-down list, and click **Go** to open the Apply to Controllers page. Select the check box(es) of the controllers to which you want to apply this template, and click **OK**.

### Configuring Controller Templates

- Configuring System Templates, page 11-4
- Configuring WLAN Templates, page 11-18
- Configuring FlexConnect Templates, page 11-40
- Configuring Security Templates, page 11-44
- Configuring Security - Access Control Templates, page 11-64
- Configuring Security - CPU Access Control List Templates, page 11-71
- Configuring Security - Rogue Templates, page 11-72
- Configuring 802.11 Templates, page 11-78
- Configuring Radio Templates (802.11a/n), page 11-83
- Configuring Radio Templates (802.11b/g/n), page 11-96
- Configuring Mesh Templates, page 11-110
- Configuring Management Templates, page 11-111
- Configuring CLI Templates, page 11-116
- Configuring Location Configuration Templates, page 11-117
- Configuring IPv6 Templates, page 11-118
- Configuring Proxy Mobile IPv6 Templates, page 11-120
- Configuring mDNS Templates, page 11-122
- Configuring AVC Profiles Templates, page 11-124
- Configuring NetFlow Templates, page 11-125

### Configuring System Templates

- Configuring General Templates, page 11-5
- Configuring SNMP Community Controller Templates, page 11-7
- Configuring an NTP Server Template, page 11-9
- Configuring User Roles Controller Templates, page 11-9
- Configuring AP Username Password Controller Templates, page 11-10
- Configuring AP 802.1X Supplicant Credentials, page 11-11
- Configuring a Global CDP Configuration Template, page 11-11
Chapter 11  Using Templates

Configuring General Templates

To add a general template or make changes to an existing general template, follow these steps:

Step 1  Choose Configure > Controller Template Launch Pad.

Click General or choose System > General from the left sidebar menu. The System > General Template page appears, and the number of controllers and virtual domains the template is applied to automatically populates. The last column shows when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page that displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 2  If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The General template page appears.

Step 3  Use the 802.3x Flow Control Mode drop-down list to enable or disable flow control mode.

Step 4  Use the 802.3x Bridging drop-down list to enable or disable 802.3 bridging.

Note  This 802.3 bridging option is not available for 5500 and 2106 series controllers.

Step 5  Use the Web RADIUS Authentication drop-down list to choose the desired Web RADIUS authentication. You can choose to use PAP, CHAP, or MD5-CHAP for authentication between the controller and the client during the user credential exchange.

Step 6  Specify the number of seconds for the AP Primary Discovery Timeout. The default is 120 seconds, and the valid range is 30 to 3600.

Step 7  Specify the number of seconds for the AP Primed Discovery Timeout. This configuration enables the APs to join only the primary/secondary/tertiary WLCs configured on the AP. The AP keeps waiting for one of the primary/secondary/tertiary WLCs to come up for the configured interval. Enter a value between 120 and 43200 seconds. This option is applicable for Cisco WLC Release 8.0.

Step 8  Specify the back-up primary and secondary controller details (controller IP address and controller name).

Step 9  Specify Layer 2 or Layer 3 transport mode. When set to Layer 3, the lightweight access point uses IP addresses to communicate with the access points; these IP addresses are collected from a mandatory DHCP server. When set to Layer 2, the lightweight access point uses proprietary code to communicate with the access points.

Note  Controllers through Release 5.2 use LWAPP and the new controller release uses CAPWAP.
Step 10  Choose to enable or disable broadcast forwarding. The default is disabled.

Step 11  Choose **Enable** or **Disable** from the LAG Mode drop-down list. Link aggregation allows you to reduce the number of IP addresses needed to configure the ports on your controller by grouping all the physical ports and creating a link aggregation group (LAG).

If LAG is enabled on a controller, any dynamic interfaces that you have created are deleted to prevent configuration inconsistencies in the interface database. When you make changes to the LAG configuration, the controller has to be rebooted for the changes to take effect.

**Note** Interfaces cannot be created with the Dynamic AP Manager flag set. Also, you cannot create more than one LAG on a controller.

Step 12  Choose to enable or disable peer-to-peer blocking mode. If you choose Disable, any same-subnet clients communicate through the controller. If you choose Enable, any same-subnet clients communicate through a higher-level router.

Step 13  From the Over Air AP Provision Mode drop-down list, choose **enable** or **disable**.

Step 14  From the AP Fallback drop-down list, choose **enable** or **disable**. Enabling fallback causes an access point that lost a primary controller connection to automatically return to service when the primary controller returns.

Step 15  When a controller fails, the backup controller configured for the access point suddenly receives a number of discovery and join requests. This might cause the controller to reach a saturation point and reject some of the access points. By assigning priority to an access point, you have some control over which access points are rejected. In a failover situation when the backup controller is saturated, the higher priority access points can join the backup controller if the lower priority access points are disjoined. Choose **enable** from the AP Failover Priority drop-down list if you want to allow this capability.

Step 16  Choose to enable or disable AppleTalk bridging.

**Note** This AppleTalk bridging option is not available on 5500 series controllers.

Step 17  Choose to enable or disable the Fast SSID Change option. If the option is enabled, the client connects instantly to the controller between SSIDs without having much loss of connectivity. Normally, each client is connected to a particular WLAN identified by the SSID. If the client moves out of reach of the connected access point, the client has to reconnect to the controller using a different access point. This normal process consumes some time as the DHCP (Dynamic Host Configuration Protocol) server has to assign an IP address to the client.

Step 18  Because the master controller is normally not used in a deployed network, the master controller setting is automatically disabled upon reboot or operating system code upgrade. You might want to enable the controller as the master controller from the Master Controller Mode drop-down list.

Step 19  Choose to enable or disable access to the controller management interface from wireless clients. Because of IPsec operation, management via wireless is only available to operators logging in across WPA or Static WEP. Wireless management is not available to clients attempting to log in via an IPsec WLAN.

Step 20  Choose to enable or disable symmetric tunneling mode. With symmetric mobility tunneling, the controller provides inter-subnet mobility for clients roaming from one access point to another within a wireless LAN. The client traffic on the wired network is directly routed by the foreign controller. If a router has Reverse Path Forwarding (RPF) enabled (which provides additional checks on incoming packets), the communication is blocked. Symmetric mobility tunneling allows the client traffic to reach the controller designated as the anchor, even with RPF enabled.
Chapter 11      Using Templates

Configuring Controller Templates

Note
All controllers in a mobility group should have the same symmetric tunneling mode.

Note
For symmetric tunneling to take effect, you must reboot.

Step 21 Use the ACL Counters drop-down list to enable or disable ACL counters. The values per ACL rule can be viewed for each controller.

Step 22 Enter the operator-defined RF mobility group name in the Default Mobility Domain Name text box.

Step 23 At the Mobility Anchor Group Keep Alive Interval, determine the delay between tries for clients attempting to join another access point. With this guest tunneling N+1 redundancy feature, the time it takes for a client to join another access point following a controller failure is decreased because a failure is quickly identified, the clients are moved away from the problem controller, and the clients are anchored to another controller.

Note When you hover your mouse cursor over the field, the valid range of values appear.

Step 24 At the Mobility Anchor Group Keep Alive Retries, specify the number of queries to anchor before the client declares it unreachable.

Step 25 Enter the RF network group name between 8 and 19 characters. Radio Resource Management (RRM) neighbor packets are distributed among access points within an RF network group. The Cisco access points only accept RRM neighbor packets sent with this RF network name. The RRM neighbor packets sent with different RF network names are dropped.

Step 26 Specify the time out for idle clients. The factory default is 300 seconds. When the timeout expires, the client loses authentication, briefly disassociates from the access point, reassociates, and re-authenticates.

Step 27 Specify the timeout in seconds for the address resolution protocol. The factory default is 300 seconds.

Step 28 Select the Global TCP Adjust MMS check box to start checking the TCP packets originating from the client, for the TCP SYN/ TCP ACK packets and MSS value and reset it to the configured value on the upstream and downstream side.

Step 29 Choose enable or disable Web Auth Proxy Redirect Mode if a manual proxy configuration is configured on the browser of the client; all web traffic going out from the client is destined for the PROXY IP and PORT configured on the browser.

Step 30 Enter the Web Auth Proxy Redirect Port. The default ports are 8080 and 3128. The range is 0 to 65535.

Step 31 Enter the AP Retransmit Count and Intervals. The AP Retransmit Count default value is 5 and the range is from 3 to 8. The AP Retransmit Interval default value is 3. The range is 2 to 5.

Step 32 Click Save.

Configuring SNMP Community Controller Templates

Create or modify a template for configuring SNMP communities on controllers. Communities can have read-only or read-write privileges using SNMP v1, v2, or v3.
When setting up SNMP communities on the WLC (Wireless LAN Controller), you are given an option to specify IP address and subnet. The default is 0.0.0.0 for both, which allows open SNMP access to any host using the specified community string. If you specify something other than the default of 0.0.0.0, the SNMP access is limited to the settings specified for IP address and Subnet Mask. A subnet of 255.255.255.255 limits to the specific host ID specified in the IP address.

To add a new template with SNMP community information for a controller, follow these steps:

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **New** beside the template you want to add.

**Step 3** Configure the following fields:

- **Template Name**
  
  **Note** Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- **Community Name**

- **Confirm Community Name**—Retype the community name.

- **IP Address**—The IP address of the server.

- **Netmask**

- **Access Mode**—Choose **Read Only** or **Read Write** from the drop-down list.
  - **Read Only**—Cannot be edited.
  - **Read Write**—Can be edited.

- **Admin Status**—Select the check box to enable this template and also to enable the Update Discover Community option.

- **Update Discover Community**—Select the check box to update the SNMP version as v2. This updates the Read/Write Community as the template community name for the applied controllers.

  **Note** If the Access Mode option is configured as Read Only, then Prime Infrastructure has only read access to the controller after applying this template.

**Step 4** Click **Save**. Once saved, the template appears in the Template List page. In the Template List page, you can apply this template to controllers. See the “Applying Controller Templates” section on page 11-2 for more information.

**Note** If a template is applied successfully and the Update Discover Community option is enabled, then the applied community name is updated in Prime Infrastructure database for that applied controller. Also, Prime Infrastructure uses that community name for further communication with that controller.
Configuring Controller Templates

Configuring an NTP Server Template

Note
NTP is used to synchronize computer clocks on the Internet.

To add an NTP template or make modifications to an existing NTP template, follow these steps:

Step 1
Choose Configure > Controller Template Launch Pad.

Step 2
Click Network Time Protocol or choose System > Network Time Protocol from the left sidebar menu. The System > NTP Server Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens the Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens to an Applied to Virtual Domains page that shows all partition names.

Step 3
If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Network Time Protocol template page appears.

Step 4
Enter the NTP server IP address.

Step 5
Click Save.

Configuring User Roles Controller Templates

This section describes how to create or modify a template for configuring user roles. User roles determine how much bandwidth the network can use. Four QoS levels (Platinum, Bronze, Gold, and Silver) are available for the bandwidth distribution to Guest Users. Guest Users are associated with predefined roles (Contractor, Customer, Partner, Vendor, Visitor, Other) with respective bandwidth configured by the Admin. These roles can be applied when adding a new Guest User. See the “Configuring a Guest User Template” section on page 11-55 for more information on adding Guest Users.

To add a new template with User Roles information for a controller, follow these steps:

Step 1
Choose Configure > Controller Template Launch Pad.

Step 2
Click New beside the template you want to add.

Step 3
Configure the following fields:

- Role Name
- Average Data Rate—The average data rate for non-UDP (User Datagram Protocol) traffic.
- Burst Data Rate—The peak data rate for non-UDP traffic.
- Average Real-time Rate—The average data rate for UDP traffic.
- Burst Real-time Rate—The peak data rate for UDP traffic.
Configuring AP Username Password Controller Templates

Create or modify a template for setting an access point username and password. All access points inherit the password as they join the controller and these credentials are used to log into the access point via the console or Telnet/SSH.

### Note
See the “Configuring a Global Access Point Password” section on page 9-59 for more information regarding global passwords.

The AP Username Password page enables you to set a global password that all access points inherit as they join a controller. When you are adding an access point, you can also choose to accept this global username and password or override it on a per-access point basis. See the “Configuring AP Configuration Templates” section on page 11-126 to see where the global password is displayed and how it can be overridden on a per-access point basis.

Also, in controller software Release 5.0, after an access point joins the controller, the access point enables console port security and you are prompted for your username and password whenever you log into the access point console port. When you log in, you are in non-privileged mode and you must enter the enable password to use the privileged mode.

To add a new template with AP Username Password information for a controller, follow these steps:

### Step 1
Choose **Configure > Controller Template Launch Pad**.

### Step 2
Click **New** beside the template you want to add.

### Step 3
Configure the following fields:
- **AP Username**—Type the username that you want to be inherited by all access point that join the controller.
- **AP Password**—Type the password that you want to be inherited by all access point that join the controller.
- **Confirm Password**—Retype the access point password.
- **Enable Password**

#### Note
For Cisco IOS access points, you must also enter and confirm an enable password.

- **Confirm Enable Password**

### Step 4
Click **Save**. Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the “Applying Controller Templates” section on page 11-2 for more information.
Chapter 11 Using Templates

Configuring Controller Templates

Note
See the “Configuring a Global Access Point Password” section on page 9-59 for more information regarding global passwords.

Configuring AP 802.1X Supplicant Credentials

You can configure 802.1X authentication between lightweight access points and the switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning. You can set global authentication settings that all access points inherit as they join the controller. All access points that are currently joined to the controller and any that join in the future are included.

To add or modify an existing AP 802.1X Supplicant Credentials template, follow these steps:

Note
If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point. See the “Configuring Access Points” section on page 9-171 for more information.

Step 1
Choose Configure > Controller Templates Launch Pad.

Step 2
Click AP 802.1X Supplicant Credentials or choose System > AP 802.1X Supplicant Credentials from the left sidebar menu. The AP 802.1X Supplicant Credentials Templates page displays all currently saved AP 802.1X Supplicant Credentials templates. It also displays the number of controllers and virtual domains to which each template is applied.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3
Click a template name to open the Controller Template list page. From there, you can edit the current template fields.

Step 4
Click Save.

Configuring a Global CDP Configuration Template

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices.

Note
CDP is enabled on the Ethernet and radio ports of the bridge by default.

To configure a Global CDP Configuration template, follow these steps:

Step 1
Choose Configure > Controller Template Launch Pad.
Configuring Controller Templates

Step 2 Click Global CDP Configuration or choose System > Global CDP Configuration from the left sidebar menu. The Global CDP Configuration Templates page displays all currently saved Global CDP Configuration templates.

Step 3 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Global CDP Configuration template page appears.

Step 4 Enter the new CDP template name.

Step 5 In the Global CDP group box of the page, configure the following fields:

- CDP on controller—Choose enable or disable CDP on the controller.
  
  Note This configuration cannot be applied on WiSM2 controllers.

- Global CDP on APs—Choose to enable or disable CDP on the access points.

- Refresh-time Interval (seconds)—At the Refresh Time Interval field, enter the time in seconds at which CDP messages are generated. The default is 60.

- Holdtime (seconds)—Enter the time in seconds before the CDP neighbor entry expires. The default is 180.

- CDP Advertisement Version—Enter which version of the CDP protocol to use. The default is v1.

Step 6 In the CDP for Ethernet Interfaces group box of the page, select the slots of Ethernet interfaces for which you want to enable CDP.

Note CDP for Ethernet Interfaces fields are supported for Controller Release 7.0.110.2 and later.

Step 7 In the CDP for Radio Interfaces group box of the page, select the slots of Radio interfaces for which you want to enable CDP.

Note CDP for Radio Interfaces fields are supported for Controller Release 7.0.110.2 and later.

Step 8 Click Save.

Note The Global Interface CDP configuration is applied only to the APs for which the CDP is enabled at AP level.

Configuring DHCP Templates

To add a DHCP template or make modifications to an existing DHCP template, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.

Step 2 Click DHCP or choose System > DHCP from the left sidebar menu. The System > DHCP Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.
Chapter 11  Using Templates

Configuring Controller Templates

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3  If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The DHCP template page appears.

Step 4  You can enable or disable DHCP proxy on a global basis rather than on a WLAN basis. When DHCP proxy is enabled on the controller, the controller unicasts DHCP requests from the client to the configured servers. At least one DHCP server must be configured on either the interface associated with the WLAN or on the WLAN itself. DHCP proxy is enabled by default.

Step 5  Enter the DHCP Timeout in seconds, after which the DHCP request times out. The default setting is 5. Allowed values range from 5 to 120 seconds.

Note  DHCP Timeout is applicable for Controller Release 7.0.114.74 and later.

Step 6  Click Save.

Configuring Dynamic Interface Templates

To add a dynamic interface template or make modifications to an existing interface configuration, follow these steps:

Step 1  Choose Configure > Controller Template Launch Pad.

Step 2  Click Dynamic Interface or choose System > Dynamic Interface from the left sidebar menu. The System > Dynamic Interface Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3  If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Dynamic Interface template page appears.

Step 4  Select the Guest LAN check box to mark the interface as wired.

Step 5  Enter the net mask address of the interface.

Step 6  Enter the port currently used by the interface.

Step 7  Enter a secondary port to be used by the interface when the primary port is down. When the primary port is reactivated, the Cisco 4400 Series Wireless LAN controller transfers the interfaces back to the primary port.

Note  Primary and secondary port numbers are present only in the Cisco 4400 Series Wireless LAN controllers.
Step 8  Enter the IP address of the primary DHCP server.
Step 9  Enter the IP address of the secondary DHCP server.
Step 10 From the ACL Name drop-down list, choose a name from the list of defined names.
Step 11 From the mDNS Profile drop-down list, choose the mDNS profile. The default option is none.
Step 12 From the Add Format Type drop-down list in the Add Interface Format Type group box, choose either Device Info or File. If you choose device info, you must configure the device-specific fields for each controller. If you choose File, you must configure CSV device-specific fields (Interface Name, VLAN Identifier, Quarantine VLAN Identifier, IP Address, and Gateway) for all the managed controllers specified in the CSV file (see Table 11-1). If you choose Device Info, continue to Step 12.

The sample CSV files are as follows.

<table>
<thead>
<tr>
<th>ip_address</th>
<th>interface_name</th>
<th>vlan_id</th>
<th>quarantine_vlan_id</th>
<th>interface_ip_address</th>
<th>gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>209.165.200.224</td>
<td>dyn-1</td>
<td>1</td>
<td>2</td>
<td>209.165.200.228</td>
<td>209.165.200.229</td>
</tr>
<tr>
<td>209.165.200.225</td>
<td>interface-1</td>
<td>4</td>
<td>2</td>
<td>209.165.200.230</td>
<td>209.165.200.231</td>
</tr>
<tr>
<td>209.165.200.227</td>
<td>dyna-2</td>
<td>2</td>
<td>3</td>
<td>209.165.200.234</td>
<td>209.165.200.235</td>
</tr>
</tbody>
</table>

The first row of the CSV file is used to describe the columns included. The CSV files can contain the following fields:

- ip_address
- interface_name
- vlan_id
- quarantine_vlan_id
- interface_ip_address
- gateway

Step 13 If you choose Apply to Controllers, you advance to the Apply To page where you can configure device-specific fields for each controller.

Step 14 Use the Add and Remove options to configure device specific fields for each controllers. If you click Edit, a dialog box appears with the current parameter input.

Step 15 Make the necessary changes in the dialog box, and click OK.

Note  If you change the interface fields, the WLANs are temporarily disabled, therefore you might lose connectivity for some clients. Any changes to the interface fields are saved only after you successfully apply them to the controller(s).
Applying a Dynamic Interface Template to Controllers

To apply a Dynamic Interface template to a controller, follow these steps:

**Step 1** In the Dynamic Interface controller template page, click **Apply to Controllers**.

**Step 2** Use the Manage Interfaces options to configure device-specific fields:
- **Add**—Click **Add** to open the Add Interface dialog box. Enter an interface name, VLAN identifier, IP address, and gateway. When all fields are entered, click **Done**.
- **Edit**—Click **Edit** to make changes to current interfaces.
- **Remove**—Click **Remove** to delete a current interface.

**Step 3** Select a check box for each controller to which you want to apply this template.

**Step 4** Click **Apply**.

**Note** Changing the Interface fields causes the WLANs to be temporarily disabled and might result in loss of connectivity for some clients.

**Note** Interface field changes or configurations made on this page are saved only when applied successfully to the controller(s).

**Note** Interfaces removed from this page are removed only from this template and not from controllers.

**Note** See the “Configuring Dynamic Interface Templates” section on page 11-13 for more information on Dynamic Interface controller templates.

Configuring QoS Templates

To modify the quality of service (QoS) profiles, follow these steps:

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **QoS Profiles** or choose **System > QoS Profiles** from the left sidebar menu. The System > QoS Profiles page appears. The number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.
The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to edit the bronze, gold, platinum, or silver QoS profile, click in the Name column for the profile you want to edit. The Edit QoS Profile Template page appears.

**Step 4** Set the following values in the Per-User Bandwidth Contracts group box. All have a default of 0 or Off.

- **Average Data Rate**—The average data rate for non-UDP traffic.
- **Burst Data Rate**—The peak data rate for non-UDP traffic.
- **Average Real-time Rate**—The average data rate for UDP traffic.
- **Burst Real-time Rate**—The peak data rate for UDP traffic.

**Step 5** Set the following values in the Over-the-Air QoS group box.

- **Maximum QoS RF Usage per AP** - The maximum air bandwidth available to clients. The default is 100%.
- **QoS Queue Depth** - The depth of queue for a class of client. The packets with a greater value are dropped at the access point.

*Note* The Air QoS configurations are applicable for controller Release 7.0 and earlier.

**Step 6** Set the following values in the Wired QoS Protocol group box.

- **Wired QoS Protocol** - Choose 802.1P to activate 802.1P priority tags or None to deactivate 802.1P priority flags.
- **802.1P Tag** - Choose 802.1P priority tag for a wired connection from 0 to 7. This tag is used for traffic and CAPWAP packets.

**Step 7** Click **Save**.

---

### Configuring AP Timers Templates

Some advanced timer configuration for FlexConnect and local mode is available for the controller on Prime Infrastructure.

To configure a template for AP timers, follow these steps:

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **AP Timers** or choose **System > AP Timers** from the left sidebar menu. The System > AP Timers page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The values in the Access Point Mode column are links. When you click a link, the Controller Template *access point mode* page appears. The Access Point Mode is automatically populated.

**Step 3** Select the **AP Fast Heartbeat Timer State** check box to enable AP Fast Heartbeat Timeout.

**Step 4** Enter an AP Fast Heartbeat Timeout value. The valid range is 1 to 15 seconds. The default is 10 seconds. The recommended timeout values are:

- 10 to 15 seconds for 7500 series controllers.
Step 5 Click Save.

Configuring an Interface Group Template

The interface group template page allows you to select list of interfaces and form a group. You cannot create interfaces using this page.

Note

The Interface Groups feature is supported by controller software release 7.0.116.0 and later.

To configure an interface group template, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.

Step 2 Click Interface Groups or choose System > Interface Groups from the left sidebar menu. The System > Interface Groups page appears.

Step 3 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The New Controller template page appears.

Step 4 Specify the following details:

- Name—Interface Group name.
- Description(optional)—A more detailed description of the interface group.
- Quarantine—Indicates the type of interfaces that can be added to an interface group. If this option is enabled, you can add interfaces with quarantine VLAN ID set. If this options is disabled, you can add interfaces with quarantine VLAN ID not set.
- mDNS Profile—Drop-down list from which you can choose the mDNS profile. The default option is none.

Step 5 Selected Controllers/Interfaces that you want to add to the group.

Step 6 Click Save.

Configuring a Traffic Stream Metrics QoS Template

Traffic stream metrics are a series of statistics about VoIP over your wireless LAN and informs you of the QoS of the wireless LAN. These statistics are different than the end-to-end statistics provided by VoIP systems. End-to-end statistics provide information on packet loss and latency covering all the links comprising the call path. However, traffic stream metrics are statistics for only the WLAN segment of the call. Because of this, system administrators can quickly determine whether audio problems are being caused by the WLAN or by other network elements participating in a call. By observing which access points have impaired QoS, system administrators can quickly determine the physical area where the problem is occurring. This is important when lack of radio coverage or excessive interference is the root problem.
Four QoS values (packet latency, packet jitter, packet loss, and roaming time), which can affect the audio quality of voice calls, are monitored. All the wireless LAN components participate in this process. Access points and clients measure the metrics, access points collect the measurements and then send them to the controller. The access points update the controller with traffic stream metric information every 90 seconds, and 10 minutes of data is stored at one time. Prime Infrastructure queries the controller for the metrics and displays them in the Traffic Stream Metrics QoS Status. These metrics are compared to threshold values to determine their status level and if any of the statistics are displaying a status level of fair (yellow) or degraded (red), the administrator investigates the QoS of the wireless LAN.

For the access points to collect measurement values, traffic stream metrics must be enabled on the controller.

To configure a Traffic Stream Metrics QoS template, follow these steps:

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Traffic Stream Metrics QoS** or choose **System > Traffic Stream Metrics QoS** from the left sidebar menu. The Traffic Stream Metrics QoS Controller Templates page appears.

The Traffic Stream Metrics QoS Controller Configuration page shows several QoS values. An administrator can monitor voice and video quality of the following:

- Upstream delay
- Upstream packet loss rate
- Roaming time
- Downstream packet loss rate
- Downstream delay

Packet Loss Rate (PLR) affects the intelligibility of voice. Packet delay can affect both the intelligibility and conversational quality of the connection. Excessive roaming time produces undesired gaps in audio.

There are three levels of measurement:

- Normal: Normal QoS (green)
- Fair: Fair QoS (yellow)
- Degraded: Degraded QoS (red)

System administrators should employ some judgment when setting the green, yellow, and red alarm levels. Some factors to consider are:

- Environmental factors including interference and radio coverage which can affect PLR.
- End-user expectations and system administrator requirements for audio quality on mobile devices (lower audio quality can permit greater PLR).
- Different codec types used by the phones have different tolerance for packet loss.
- Not all calls are mobile-to-mobile; therefore, some have less stringent PLR requirements for the wireless LAN.

---

**Configuring WLAN Templates**

- Configuring WLAN Templates, page 11-19
- Configuring WLAN AP Groups Templates, page 11-37
Chapter 11 Using Templates

Configuring WLAN Templates

WLAN templates allow you to define various WLAN profiles for application to different controllers. You can configure multiple WLANs with the same SSID. This feature enables you to assign different Layer 2 security policies within the same wireless LAN. Unlike previous release where profile name was used as the unique identifier, the template name is now the unique identifier with software release 5.1.

These restrictions apply when configuring multiple WLANs with the same SSID:

- WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on information advertised in the beacons and probes. These are the available Layer 2 security policies:
  - None (open WLAN)
  - Static WEP or 802.1
  - CKIP
  - WPA/WPA2
- Broadcast SSID must be enabled on the WLANs that share an SSID so that the access points can generate probe responses for these WLANs.
- FlexConnect access points do not support multiple SSIDs.

To add a WLAN template or make modifications to an existing WLAN template, follow these steps:

---

**Step 1** Choose Configure > Controller Template Launch Pad.

**Step 2** Click WLAN or choose WLANs > WLAN Configuration from the left sidebar menu. The WLAN template page appears with a summary of all existing defined WLANs. The following information headings are used to define the WLANs listed in the WLAN Template General page:

- Template Name—The user-defined name of the template. Clicking the name displays fields for this template.
- Profile Name—User-defined profile name used to distinguish WLANs with the same SSID.
- SSID—Displays the name of the WLAN.
- WLAN/Guest LAN—Determines if guest LAN or WLAN.
- Security Policies—Indicates what security policy is chosen. None indicates no 802.1X.
- WLAN Status—Determines whether the WLAN is enabled or not.
- Applied to Controllers—The number of controllers the WLAN template is applied to. The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status.
- Applied to Virtual Domains—The number of virtual domains the WLAN template is applied to. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.
- Last Saved At—Indicates when the template was last saved.

**Step 3** If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The WLAN template page appears.

**Step 4** Select the Wired LAN check box to indicate whether or not this WLAN is a wired LAN.
**Note** Specify if you want guest users to have wired guest access from an Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or specific ports in a conference room and accounts are added to the network using the Lobby Ambassador portal. (See the “Creating Guest User Accounts” section on page 7-8).

**Note** The Egress or Ingress interface configurations are applicable for Wired LAN only.

**Step 5** Use the **Type** drop-down list to select the type of the wired LAN.

- Guest LAN—Indicates that this wired LAN is a Guest LAN.

**Note** If you selected the Guest LAN option, you need to select an Ingress interface which has not already been assigned to any Guest LAN.

- Remote LAN—Indicates that this wired LAN is a Remote LAN.

**Step 6** Enter a name in the Profile Name text box that identifies the WLAN or the guest LAN. Do not use any spaces in the name entered.

**Step 7** Enter the name of the WLAN SSID. An SSID is not required for a guest LAN. WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on information advertised in the beacons and probes.

**Step 8** Select the **Enable** check box for the Status field.

**Step 9** Use the Radio Policy drop-down list to set the WLAN policy to apply to All (802.11a/b/g/n), 802.11a only, 802.11g only, 802.11b/g only, or 802.11a/g only.

**Step 10** Use the Interface/Interface Group drop-down list to choose the available names of interfaces created by the Controller > Interfaces module.

**Step 11** From the Egress Interface drop-down list, choose the Egress interface that you created in the “Creating an Egress Interface” section on page 9-49. This provides a path out of the controller for wired guest client traffic.

**Step 12** From the Ingress Interface drop-down list, choose the Ingress interface that you created in the “Creating an Ingress Interface” section on page 9-49. The provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

**Step 13** Select the **Enable** check box to enable the multicast VLAN feature.

**Step 14** From the Multicast VLAN Interface drop-down list, choose the appropriate interface name. This list is automatically populated when you enable the multicast VLAN feature.

**Step 15** Click **Broadcast SSID** to activate SSID broadcasts for this WLAN.

**Step 16** Click **Save**.

**Step 17** To further configure the WLAN template, choose from the following:

- Click the **Security** tab to establish which AAA can override the default servers on this WLAN and to establish the security mode for Layer 2 and 3. Continue to the “Security Tab” section on page 11-21.

- Click the **QoS** tab to establish which quality of service is expected for this WLAN. Continue to the “QoS Tab” section on page 11-27.
Click the Advanced tab to configure any other details about the WLAN, such as DHCP assignments and management frame protection. Continue to the “Advanced Tab” section on page 11-28.

Security Tab

After choosing Security, you have an additional three tabs: Layer 2, Layer 3, and AAA Servers.

Layer 2 Tab

When you click the Layer 2 tab, the Layer 2 tab appears.

Note: The tab contains different views depending on what option is chosen in the Layer 2 Security drop-down list.

To configure the Layer 2 tab, follow these steps:

Step 1 Use the Layer 2 Security drop-down list to choose None, 802.1X, Static WEP, Static WEP-802.1X, WPA + WPA2, or CKIP as described in Table 11-2.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No Layer 2 security selected.</td>
</tr>
<tr>
<td></td>
<td>• FT Enable—Select the check box to enable Fast Transition (FT) between access points.</td>
</tr>
<tr>
<td>Note</td>
<td>Fast transition is not supported with FlexConnect mode.</td>
</tr>
<tr>
<td></td>
<td>• Over the DS—Select the check box to enable or disable the fast transition over a distributed system.</td>
</tr>
<tr>
<td></td>
<td>• Reassociation Timeout—Time in seconds after which fast transition reassociation times out. The default is 20 seconds, and the valid range is 1 to 100.</td>
</tr>
<tr>
<td></td>
<td>Note: To enable Over the DS or Reassociation Timeout, you must enable fast transition.</td>
</tr>
<tr>
<td>802.1X</td>
<td>WEP 802.1X data encryption type (Note 1): 40/64 bit key. 104 bit key. 152 bit key.</td>
</tr>
</tbody>
</table>
### Configuring Controller Templates

#### Table 11-2  
Layer 2 Security Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Static WEP             | Static WEP encryption fields:  
|                        | Key sizes: Not set, 40/64, 104, and 152 bit key sizes.  
|                        | Key Index: 1 to 4 (Note 2).  
|                        | Encryption Key: Encryption key required.  
|                        | Key Format: ASCII or HEX.  
|                        | Allowed Shared Key Authentication—Select the check box to enable shared key authentication.  
|                        | **Note** Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device. |
| Static WEP-802.1X      | Use this setting to enable both Static WEP and 802.1X policies. If this option is selected, static WEP and 802.1X fields are displayed at the bottom of the page.  
|                        | Static WEP encryption fields:  
|                        | Key sizes: Not set, 40/64, 104, and 152 bit key sizes.  
|                        | Key Index: 1 to 4 (Note 2).  
|                        | Encryption Key: Enter encryption key.  
|                        | Key Format: ASCII or HEX.  
|                        | Allowed Shared Key Authentication—Select the check box to enable.  
|                        | 802.1 Data Encryption: 40/64 bit key, 104 bit key, 152 bit key. |
WPA+WPA2 Use this setting to enable WPA, WPA2, or both. WPA enables Wi-Fi Protected Access with TKIP-MIC Data Encryption or AES. When WPA+WPA2 is selected, you can use Cisco Centralized Key Management (CCKM) authentication key management, which allows fast exchange when a client roams from one access point to another.

When WPA+WPA2 is selected as the Layer 2 security policy and preshared key is enabled, neither CCKM nor 802.1X can be enabled; although, both CCKM and 802.1X can be enabled at the same time.

- Mac Filtering—Enables MAC address filtering.

**Note** Mac Filtering and Max-Clients are not supported with FlexConnect local authentication.

- FT Enable—Select the check box to enable fast transition between access points.

**Note** Fast transition is not supported with FlexConnect mode.

  - Over the DS—Select the check box to enable the fast transition over a distributed system.
  - Reassociation Timeout—Time in seconds after which fast transition reassociation times out. The default is 20 seconds, and the valid range is 1 to 100.

**Note** To enable Over the DS or Reassociation Timeout, enable fast transition.

WPA+WPA2 parameters:

- WPA1—Select the check box to enable WPA1.
- WPA2—Select the check box to enable WPA2.

Authentication Key Management:

- FT802.1X—Select the check box to enable FT802.1X.
- 802.1X—Select the check box to enable 802.1X.
- CCKM—Select the check box to enable CCKM.
- PSK—Select the check box to enable PSK.
- FTPSK—Select the check box to enable FTPSK.

**Note** Enable WPA2 and fast transition to set FT802.1X or FTPSK.
Table 11-2  Layer 2 Security Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CKIP</td>
<td>Cisco Key Integrity Protocol (CKIP). A Cisco access point advertises support for CKIP in beacon and probe response packets. CKIP can be configured only when Aironet IE is enabled on the WLAN.</td>
</tr>
<tr>
<td>Note</td>
<td>CKIP is not supported on 10xx APs.</td>
</tr>
<tr>
<td></td>
<td>When selected, these CKIP fields are displayed.</td>
</tr>
<tr>
<td></td>
<td>Key size: Not set, 40, or 104.</td>
</tr>
<tr>
<td></td>
<td>Key Index: 1 to 4</td>
</tr>
<tr>
<td></td>
<td>Encryption Key: Specify encryption key.</td>
</tr>
<tr>
<td></td>
<td>Key Format: ASCII or HEX.</td>
</tr>
<tr>
<td>Note</td>
<td>Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.</td>
</tr>
<tr>
<td>MMH Mode: Select the check box to enable.</td>
<td></td>
</tr>
<tr>
<td>Key Permutation: Select the check box to enable.</td>
<td></td>
</tr>
</tbody>
</table>

Step 2  Select the MAC Filtering check box if you want to filter clients by MAC address.

Note  The ability to join a controller without specification within a MAC filter list is only supported on mesh access points.

Note  For releases prior to 4.1.82.0, mesh access points do not join the controller unless they are defined in the MAC filter list.

You might want to disable the MAC filter list to allow newly added access points to join the controller. Before enabling the MAC filter list again, you should enter the MAC addresses of the new access points.

Step 3  Choose the desired type of authentication key management. The choices are 802.1X, CCKM, or PSK.

Note  If you choose PSK, you must enter the shared key and type (ASCII or hexadecimal).

Note  Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.
Step 4  Click Save.

Layer 3 Tab

When you click the Layer 3 tab, the Layer 3 tab appears.

Note  The tab contains different views depending on the option you chose from the Layer 3 Security drop-down list.

To configure the Layer 3 tab, follow these steps:

Step 1  Use the Layer 3 security drop-down list to choose between None and VPN Pass Through. The page fields change according to the selection you make. If you choose VPN pass through, you must enter the VPN gateway address.

Note  The VPN passthrough option is not available for the 2106 or 5500 series controllers.

Step 2  You can modify the default static WEP (web authentication) or assign specific web authentication (login, logout, login failure) pages and the server source.

a. To change the static WEP to passthrough, select the Web Policy check box and choose the Passthrough option from the drop-down list. This option allows users to access the network without entering a username or password.

An Email Input check box appears. Select this check box if you want users to be prompted for their e-mail address when attempting to connect to the network.

b. Choose the WebAuth on MAC Filter Failure option so that when clients fail on MAC filter, they are automatically switched to webAuth.

Note  The WebAuth on Mac Filter Failure option works only when the Layer 2 Mac Filtering option is enabled.

c. To specify custom web authentication pages, unselect the Global WebAuth Configuration Enable check box.

1. When the Web Auth Type drop-down list appears, choose one of the following options to define the web login page for the wireless guest users:

   Default Internal—Displays the default web login page for the controller. This is the default value.

   Customized Web Auth—Displays custom web login, login failure, and logout pages. When the customized option is selected, three separate drop-down lists for login, login failure, and logout page selection appear. You do not need to define a customized page for all three of the options. Choose None from the appropriate drop-down list if you do not want to display a customized page for that option.

   These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files.
**Configuring Controller Templates**

**Chapter 11**

**Using Templates**

---

**External**—Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.

**Note**

External web auth is not supported for 2106 and 5500 series controllers.

You can select specific RADIUS or LDAP servers to provide external authentication in the Security > AAA page. To do so, continue with Step 4.

**Note**

The RADIUS and LDAP servers must be already configured to have selectable options in the Security > AAA page. You can configure these servers in the RADIUS Authentication Servers page and TACACS+ Authentication Servers page.

---

**Step 3**

If you selected External as the Web Authentication Type in Step 2, choose **Security > AAA**, and choose up to three RADIUS and LDAP servers using the drop-down lists.

**Step 4**

Click **Save**.

**Step 5**

Repeat this process if a second (anchor) controller is being used in the network.

---

**AAA Servers**

When you click the AAA Servers tab, the AAA Servers tab appears.

To configure the AAA Servers tab, follow these steps:

---

**Step 1**

Select the **Radius Server Overwrite Interface** check box to send the client authentication request through the dynamic interface which is set on the WLAN. When you enable the Radius Server Overwrite Interface option, the WLC sources all radius traffic for a WLAN using the dynamic interface configured on that WLAN.

**Note**

You cannot enable Radius Server Overwrite Interface when Diagnostic Channel is enabled.

**Note**

The Radius Server Overwrite Interface option is supported in controller Release 7.0.x and later.

---

**Step 2**

Select the **Enable** check boxes, then use the drop-down lists in the RADIUS and LDAP servers section to choose authentication and accounting servers. This selects the default RADIUS server for the specified WLAN and overrides the RADIUS server that is configured for the network. If all three RADIUS servers are configured for a particular WLAN, server 1 has the highest priority, and so on.

If no LDAP servers are chosen here, Prime Infrastructure uses the default LDAP server order from the database.

**Step 3**

Select the **Interim Update** check box if you want to enable interim update for RADIUS Server Accounting. If you have selected this check box, specify the Interim Interval value. The range is 180 to 3600 seconds, and the default value is 0.

**Note**

The Interim Interval can be entered only when Interim Update is enabled.
Step 4  Select the **Local EAP Authentication** check box if you have an EAP profile already configured that you want to enable. Local EAP is an authentication method that allows users and wireless clients to locally authenticate. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down.

Step 5  When AAA Override is enabled, and a client has conflicting AAA and controller WLAN authentication fields, client authentication is performed by the AAA server. As part of this authentication, the operating system moves clients from the default Cisco WLAN Solution to a VLAN returned by the AAA server and predefined in the controller interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the operating system also uses QoS and ACL provided by the AAA server, as long as they are predefined in the controller interface configuration. (This VLAN switching by AAA override is also referred to as identity networking.)

For instance, if the corporate WLAN primarily uses a management interface assigned to VLAN 2, and if AAA override returns a redirect to VLAN 100, the operating system redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.

When AAA override is disabled, all client authentication defaults to the controller authentication parameter settings, and authentication is only performed by the AAA server if the controller WLANs do not contain any client-specific authentication parameters.

The AAA override values might come from a RADIUS server, for example.

Step 6  Click **Save**.

---

**QoS Tab**

When you click the QoS tab in the WLAN Template page, the QoS tab appears.

The WLAN template for the CUWN-IOS devices lists only default metal policies such as Platinum, Gold, Silver, and Bronze.

To configure the QoS fields, follow these steps:

---

**Step 1**  From the QoS drop-down list, choose **Platinum** (voice), **Gold** (video), **Silver** (best effort), or **Bronze** (background). Services such as VoIP should be set to gold while non-discriminating services such as text messaging can be set to bronze.

**Step 2**  Select the NBAR Visibility check box to view the classification of applications based on the Network Based Application Recognition (NBAR) deep packet inspection technology.

**Step 3**  From the AVC Profile drop-down list from which you can choose an Application Visibility and Control (AVC) profile for the WLAN.

**Step 4**  From the NetFlow Monitor drop-down list from which you can choose a NetFlow monitor for the WLAN.

**Step 5**  Under the Override Per-User Rate Limits group box, configure the following fields:

**Note**  The wireless rate limits can be defined on both upstream and downstream traffic.

- Average Data Rate—Define the average data rate for TCP traffic per user or per SSID by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile.
- **Burst Data Rate**—Define the peak data rate for TCP traffic per user or per SSID by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile. The Burst Data Rate should be greater than or equal to the Average Data Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

- **Average Real-Time Rate**—Define the average real-time rate for UDP traffic per user or per SSID by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile.

- **Burst Real-Time Rate**—Define the peak real-time rate for UDP traffic per user or per SSID by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile. The Burst Real-Time Rate should be greater than or equal to the Average Real-Time Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

**Step 6** Under the Override Per-SSID Rate Limits group box, configure the following fields:

- **Average Data Rate**—Define the average data rate TCP traffic per user or per SSID by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile.

- **Burst Data Rate**—Define the peak data rate for TCP traffic per user or per SSID by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile. The Burst Data Rate should be greater than or equal to the Average Data Rate. Otherwise, the QoS policy may block traffic to and from the WLANs.

- **Average Real-Time Rate**—Define the average real-time rate for UDP traffic per user or per SSID by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile.

- **Burst Real-Time Rate**—Define the peak real-time rate for UDP traffic per user or per SSID by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile. The Burst Real-Time Rate should be greater than or equal to the Average Real-Time Rate. Otherwise, the QoS policy may block traffic to and from the WLANs.

**Step 7** From the WMM Policy drop-down list, choose **Disabled**, **Allowed** (so clients can communicate with the WLAN), or **Required** to make it mandatory for clients to have WMM enabled for communication.

**Step 8** Select the **7920 AP CAC** check box if you want to enable support on Cisco 7920 phones.

**Step 9** If you want WLAN to support older versions of the software on 7920 phones, select the **7920 Client CAC** check box to enable it. The CAC limit is set on the access point for newer versions of software.

**Step 10** Click **Save**.

---

**Advanced Tab**

**Step 1** Select the **FlexConnect local switching** check box if you want to enable FlexConnect local switching. For more information on FlexConnect, see the “Configuring FlexConnect” section on page 12-4. If you enable it, the FlexConnect access point handles client authentication and switches client data packets locally.

FlexConnect local switching is only applicable to the Cisco 1130/1240/1250 series access points. It is not supported with L2TP or PPTP authentications, and it is not applicable to WLAN IDs 9-16.

**Step 2** Select the **FlexConnect Local Auth** check box if you want to enable FlexConnect local authentication.
Local authentication is useful where you cannot maintain the criteria a remote office setup of minimum bandwidth of 128 kbps with the roundtrip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes. In local switching, the authentication capabilities are present in the access point itself. Thus local authentication reduces the latency requirements of the branch office.

**Note** Local authentication can only be enabled on the WLAN of a FlexConnect AP that is in local switching mode.

Local authentication is not supported in the following scenarios:

- Guest Authentication cannot be performed on a FlexConnect local authentication enabled WLAN.
- RRM information is not available at the controller for the FlexConnect local authentication enabled WLAN.
- Local radius is not supported.
- Once the client has been authenticated, roaming is supported after the WLC and the other FlexConnects in the group are updated with the client information.

**Step 3** When you enable hybrid-REAP local switching, the Learn Client IP Address check box is enabled by default. However, if the client is configured with Fortress Layer 2 encryption, the controller cannot learn the client IP address, and the controller periodically drops the client. Disable this option so that the controller maintains the client connection without waiting to learn the client IP address. The ability to disable this option is supported only with hybrid-REAP local switching; it is not supported with hybrid-REAP central switching.

**Step 4** Select or unselect the VLAN based Central Switching check box to enable or disable central switching on a locally switched WLAN based on AAA overridden VLAN. The following are the features and limitations of this feature.

- Multicast on overridden interfaces is not supported.
- This feature is available only on a per-WLAN basis, where the WLAN is locally switched.
- IPv6 ACLs, CAC, NAC, and IPv6 are not supported.
- IPv4 ACLs are supported only with VLAN-based central switching enabled and applicable only to central switching clients on the WLAN.
- This feature is applicable to APs in FlexConnect mode in locally switched WLANs.
- This feature is not applicable to APs in Local mode.
- This feature is not supported on APs in FlexConnect mode in centrally switched WLANs.
- This feature is supported on central authentication only.
- This features is not supported on web authentication security clients.
- Layer 3 roaming for local switching clients is not supported.

**Step 5** Select or unselect the Central DHCP Processing check box to enable or disable the feature. When you enable this feature, 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.

**Step 6** Select or unselect the Override DNS check box to enable or disable the overriding of the DNS server address on the interface assigned to the locally switched WLAN. When you override DNS in centrally switched WLANs, the clients get their DNS server IP address from the AP, not from the controller.
Step 7  Select or unselect the NAT-PAT check box to enable or disable Network Address Translation (NAT) and Port Address Translation (PAT) on locally switched WLANs. You must enable Central DHCP Processing to enable NAT and PAT.

Step 8  Choose to enable the diagnostic channel feature or leave it disabled. The diagnostic channel feature allows you to troubleshoot problems regarding client communication with a WLAN. When initiated by a client having difficulties, the diagnostic channel provides the most robust communication methods with the fewest obstacles to communication.

Step 9  Select the Aironet IE check box if you want to enable support for Aironet information elements (IEs) for this WLAN. 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 controller sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the controller and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

Step 10  Select the IPv6 check box. You can configure IPv6 bridging and IPv4 web auth on the same WLAN.

Step 11  Select the Session Timeout check box to set the maximum time a client session can continue before requiring reauthorization.

Step 12  Choose to enable or disable coverage hold detection (CHD) on this WLAN. By default, CHD is enabled on all WLANs on the controller. If you disable CHD on a WLAN, a coverage hole alert is still sent to the controller, but no other processing is done to mitigate the coverage hole. This feature is useful for guest WLANs where highly mobile guests are connected to your network for short periods of time.

Step 13  The Override Interface drop-down list provides a list of defined access control lists (ACLs). (See the “Configuring an Access Control List Template” section on page 11-65 for steps on defining ACLs.) Upon choosing an ACL from the list, the WLAN associates the ACL to the WLAN. Selecting an ACL is optional, and the default for this field is None.

Step 14  You can configure peer-to-peer blocking per WLAN rather than applying the status to all WLANs. From the Peer to Peer Blocking drop-down list, choose one of the following:

- Disable—Peer-to-peer blocking is disabled, and traffic is bridged locally whenever possible.
- Drop—The packet is discarded.
- Forward Up Stream—The packet is forwarded on the upstream VLAN, and the decision is made about what to do with the packet.

**Note**  For controller Release 7.2.x and later, the Forward Up Stream is same as Drop for locally switched clients.

If FlexConnect local switching is enabled for the WLAN, which prevents traffic from passing through the controller, this drop-down list is dimmed.

**Note**  Peer-to-peer blocking does not apply to multicast traffic.

Step 15  From the Wi-Fi Direct Clients Policy drop-down list, choose one of the following options:

- **Disabled**—Disables the Wi-Fi Direct Clients Policy for the WLAN and deauthenticates all Wi-Fi Direct capable clients. The default is Disabled.
- **Allow**—Allows the Wi-Fi Direct clients to associate with an infrastructure WLAN.
- **Not-Allow**—Disallows the Wi-Fi Direct clients from associating with an infrastructure WLAN.
The Wi-Fi Direct Clients Policy is applicable to WLANs that have APs in local mode only.

The Wi-Fi Direct Clients Policy is applicable for controller Release 7.2.x. and later.

Step 16
Select the check box if you want to enable automatic client exclusion.

Step 17
If you enable client exclusion, you must also set the Timeout Value in seconds for disabled client machines. Client machines are excluded by MAC address, and their status can be observed. A timeout setting of 0 indicates that administrative control is required to reenable the client.

Note
When session timeout is not set, it implies that an excluded client remains and does not timeout from the excluded state. It does not imply that the exclusion feature is disabled.

Step 18
Enter the maximum number of clients to be associated in a WLAN in the Maximum Clients text box. The valid range is from 0 to 7000. The default value is 0.

Note
A value of 0 allows unlimited number of clients to be associated with a WLAN.

Step 19
Enable dynamic anchoring of static IP clients by selecting the Static IP Tunneling check box.

Step 20
Select the Media Session Snooping check box. This feature enables access points to detect the establishment, termination, and failure of voice calls and then report them to the controller and Prime Infrastructure. It can be enabled or disabled per WLAN.

When media session snooping is enabled, the access point radios that advertise this WLAN snoop for Session Initiation Protocol (SIP) voice packets. Any packets destined to or originating from port number 5060 are considered for further inspection. The access point tracks whether Wi-Fi Multimedia (WMM) and non-WMM clients are establishing a call, already on an active call, or in the process of ending a call and then notify the controller of any major call events.

Step 21
Select the KTS based CAC check box to enable KTS based CAC support per WLAN.

WLC supports TSPEC based CAC and SIP based CAC. But there are certain phones that work with different protocols for CAC, which are based on the KTS (Key Telephone System). For supporting CAC with KTS-based SIP clients, WLC should understand and process the bandwidth request message from those clients to allocate the required bandwidth on the AP radio, in addition to handling and sending certain other messages, as part of this protocol.

Note
The KTS CAC configuration is only supported by Cisco 5508, 7500, WISM2, and 2500 controllers that run controller software Release 7.2.x. This feature is not supported by Cisco 4400 series controllers.

Step 22
NAC State—From the NAC State drop-down list, choose SNMP NAC or Radius NAC. SIP errors that are discovered generate traps that appear on the client troubleshooting and alarms screens. The controller can integrate with the NAC appliance in out-of-band mode, where the NAC appliance remains in the data path only until clients have been analyzed and cleaned. Out-of-band mode reduces the traffic load on the NAC appliance and enables centralized NAC processing. See the “NAC Integration” section on page 9-44 for more information.
Step 23  Off-Channel Scanning Defer is essential to the operation of RRM, which gathers information about alternate channel choices such as noise and interference. Additionally, Off-Channel Scanning Defer is responsible for rogue detection. Devices that need to defer Off-Channel Scanning Defer should use the same WLAN as often as possible. If there are many of these devices (and the possibility exists that Off-Channel Defer scanning could be completely disabled by the use of this feature), you should implement an alternative to local AP Off-Channel Scanning Defer, such as monitor access points, or other access points in the same location that do not have this WLAN assigned.

Assignment of a QoS policy (bronze, silver, gold, and platinum) to a WLAN affects how packets are marked on the downlink connection from the access point regardless of how they were received on the uplink from the client. UP=1,2 is the lowest priority, and UP=0,3 is the next higher priority. The marking results of each QoS policy are as follows:

- Bronze marks all downlink traffic to UP=1.
- Silver marks all downlink traffic to UP=0.
- Gold marks all downlink traffic to UP=4.
- Platinum marks all downlink traffic to UP=6.

Set the Scan Defer Priority by clicking the priority argument and Set the time in milliseconds in the Scan Defer Interval text box. Valid values are 0 through 60000. The default value is 100 milliseconds.

Step 24  In 802.11a/n and 802.11b/g/n 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.

Normally, the DTIM value is set to 1 (transmit broadcast and multicast frames after every beacon) or 2 (transmit after every other beacon). For instance, if the beacon period of the 802.11a/n or 802.11b/g/n network is 100 ms and the DTIM value is set to 1, the access point transmits buffered broadcast and multicast frames 10 times per 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 5 times per second. Either of these settings might be suitable for applications, including VoIP, that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (transmit broadcast and multicast frames after every 255th beacon) if all 802.11a/n or 802.11b/g/n clients have power save enabled. Because the clients have to listen only when the DTIM period is reached, they can be set to listen for broadcasts and multicasts less frequently, resulting in longer battery life. For instance, if the beacon period is 100 ms and the DTIM value is set to 100, the access point transmits buffered broadcast and multicast frames once every 10 seconds, allowing the power-saving clients to sleep longer before they have to wake up and listen for broadcasts and multicasts, resulting in longer battery life.

Many applications cannot tolerate a long time between broadcast and multicast messages, resulting in poor protocol and application performance. We recommend a low DTIM value for 802.11a/n and 802.11b/g/n networks that support such clients.

Under DTIM Period, enter a value between 1 and 255 (inclusive) in the 802.11a/n and 802.11b/g/n fields. The default value is 1 (transmit broadcast and multicast frames after every beacon).

Step 25  When you select the check box to override DHCP server, another field appears where you can enter the IP address of your DHCP server. For some WLAN configurations, this is required. Three valid configurations are as follows:

- DHCP Required and a valid DHCP server IP address - All WLAN clients obtain an IP address from the DHCP server.
Configuring Controller Templates

- DHCP is not required and a valid DHCP server IP address - All WLAN clients obtain an IP address from the DHCP server or use a static IP address.
- DHCP not required and DHCP server IP address 0.0.0.0 - All WLAN clients are forced to use a static IP address. All DHCP requests are dropped.

You cannot choose to require a DHCP address assignment and then enter a DHCP server IP address.

**Step 26** If the MFP Signature Generation check box is selected, it enables signature generation for the 802.11 management frames transmitted by an access point associated with this WLAN. Signature generation makes sure that changes to the transmitted management frames by an intruder are detected and reported.

**Step 27** From the MFP Client Protection drop-down list, choose **Enabled, Disabled, or Required** for configuration of individual WLANs of a controller. If infrastructure MFP is not enabled, this drop-down list is unavailable.

**Note** The Enabled parameter is the same as the Optional parameter that you choose from the MFP Client Protection drop-down list in the WLC graphical user interface.

**Note** Client-side MFP is only available for those WLANs configured to support Cisco-compatible Extensions (version 5 or later) clients, and WPA2 must first be configured.

**Step 28** Enter a value between 1 and 255 beacon intervals in the 802.11a/n DTIM Period group box of the page. The controller sends a DTIM packet on the 802.11a/n radio for this WLAN based on what is entered as an interval.

**Step 29** Enter a value between 1 and 255 beacon intervals in the 802.11b/g/n DTIM Period group box of the page. The controller sends a DTIM packet on the 802.11b/g/n radio for this WLAN based on what is entered as an interval.

**Note** The DTIM configuration is not appropriate for guest LANs.

**Step 30** From the PMIP Mobility Type drop-down list, choose the mobility type from the following options:
- None—Configures the WLAN with Simple IP.
- Mixed—Configures the WLAN with Simple IP and PMIPv6.
- PMIPv6—Configures the WLAN with only PMIPv6.

**Step 31** Select the mDNS Snooping check box to enable mDNS snooping on the WLAN. By default, this option is enabled.

**Step 32** From the mDNS Profile drop-down list from which you can choose the mDNS profile for the WLAN. The default value is default-mdns-profile.

**Step 33** Click **Save**.

---

**Policy Configuration Tab**

**Step 1** On the Policy Configuration tab, configure the following fields:
- Policy Name—Name of the policy.
- Policy Priority—Configure policy priority between 1 and 16. No two policies can have same priority.

**Note** Only 16 Policy mappings are allowed per WLAN. Selected policy template for the mapping will be applied first if it does not exist on the controller.

### Configuring Client Profiling

When a client tries to associate with a WLAN, it is possible to determine the client type from the information received in the process. The controller acts as the collector of the information and sends the ISE with the required data in an optimal form.

Follow these guidelines when configuring client profiling:

By default, client profiling will be disabled on all WLANs.

- Client profiling is supported on access points that are in Local mode and FlexConnect mode.
- Profiling is not supported for clients in the following scenarios:
  - Clients associating with FlexConnect mode APs in Standalone mode.
  - Clients associating with FlexConnect mode APs when local authentication is done with local switching is enabled.
- Both DHCP Proxy and DHCP Bridging mode on the controller are supported.
- Accounting Server configuration on the WLAN must be pointing at an ISE running 1.1 MnR or later releases. Cisco ACS does not support client profiling.
- The type of DHCP server used does not affect client profiling.
- If the DHCP_REQUEST packet contains a string that is found in the Profiled Devices list of the ISE, then the client will be profiled automatically.
- The client is identified based on the MAC address sent in the Accounting request packet.
- Only MAC address should be sent as calling station ID in accounting packets when profiling is enabled.
- With profiling enabled for local switching FlexConnect mode APs, only VLAN override is supported as an AAA override attribute.

To configure client profiling, follow these steps:

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **WLAN** or choose **WLANs > WLAN Configuration** from the left sidebar menu.

**Step 3** Click the **Advanced** tab.

**Step 4** Select the **DHCP Profiling** check box to enable DHCP profiling.

**Step 5** Select the **HTTP Profiling** check box to enable HTTP profiling.

**Note** HTTP client profiling is supported since controller Version 7.3.1.31.
Configuring Mobile Concierge (802.11u)

Mobile Concierge is a solution that enables 802.1X capable clients to interwork with external networks. The Mobile Concierge feature provides service availability information to clients and can help them to associate available networks.

The services offered by the network can be broadly classified into two protocols:

- 802.11u MSAP
- 802.11u HotSpot 2.0

The following guidelines and limitations apply to Mobile Concierge:

- Mobile Concierge is not supported on FlexConnect Access Points.
- 802.11u configuration upload is not supported. If you perform a configuration upgrade and upload a configuration on the controller, the HotSpot configuration on the WLANs is lost.

To configure Mobile Concierge (802.11u) Groups, follow these steps:

**Step 1** Choose Configure > Controller Template Launch Pad.

**Step 2** Click WLAN or choose WLANs > WLAN Configuration from the left sidebar menu.

**Step 3** Click the Hot Spot tab.

**Step 4** On the General tab, configure the following fields:

- Select the 802.11u Status check box to enable 802.11u on the WLAN.
- Select the Internet Access check box to enable this WLAN to provide Internet services.
- From the Network Type drop-down list, choose the network type that best describes the 802.11u you want to configure on this WLAN. The following options are available:
  - Private Network
  - Private Network with Guest Access
  - Chargeable Public Network
  - Free Public Network
  - Emergency Services Only Network
  - Personal Device Network
  - Test or Experimental
  - Wildcard
- Choose the authentication type that you want to configure for the 802.11u parameters on this network:
  - Not configured
  - Acceptance of Terms and Conditions
  - Online Enrollment
  - HTTP/HTTPS Redirection
In the HESSID field, enter the Homogenous Extended Service Set Identifier value. The HESSID is a 6-octet MAC address that identifies the homogeneous ESS.

**Step 5**

On the Others tab, configure the following fields:

- In the OUI List group box, enter the following details:
  - OUI name
  - Is Beacon
  - OUI Index

Click Add to add the OUI (Organizationally Unique Identifier) entry to this WLAN.

- In the Domain List group box, enter the following details:
  - Domain Name—The domain name operating in the 802.11 access network.
  - Domain Index—Choose the domain index from the drop-down list.

Click Add to add the domain entry to this WLAN.

**Step 6**

On the Realm tab, configure the following fields:

- In the OUI List section, enter the following details:
  - Realm Name—The realm name.
  - Realm Index—The realm index.

Click Add to add the domain entry to this WLAN.

**Step 7**

On the Service Advertisement tab, configure the following fields:

- Select the MSAP Enable check box to enable service advertisements.
- If you enabled MSAP in the previous step, you must provide a server index. Enter the server index for this WLAN. The server index field uniquely identifies an MSAP server instance serving a venue that is reachable through the BSSID.

**Note**

MSAP (Mobility Services Advertisement Protocol) is designed to be used primarily by mobile devices that are configured with a set of policies for establishing network services. These services are available for devices that offer higher-layer services, or network services that are enabled through service providers. Service advertisements use MSAP to provide services to mobile devices prior to association to a Wi-Fi access network. This information is conveyed in a service advertisement. A single-mode or dual-mode mobile device queries the network for service advertisements before association. The device's network discovery and the selection function may use the service advertisements in its decision to join the network.

**Step 8**

On the HotSpot 2.0 tab, configure the following fields:

- Choose the Enable option from the HotSpot2 Enable drop-down list.
- In the WAM Metrics group box, specify the following:
  - WAN Link Status—The link status. The valid range is 1 to 3.
  - WAN SIM Link Status—The symmetric link status. For example, you can configure the uplink and downlink to have different speeds or same speeds.
  - Down Link Speed—The downlink speed. The maximum value is 4,194,304 kbps.
  - Up Link Speed—The uplink speed. The maximum value is 4,194,304 kbps.
- In the Operator Name List group box, specify the following:
Chapter 11 Using Templates

Configuring Controller Templates

- Operator Name—Specify the name of the 802.11 operator.
- Operator Index—Select an operator index. The range is from 1 to 32.
- Language Code—An ISO-14962-1997 encoded string defining the language. This string is a three character language code.

Click Add to add the operator details. The operator details are displayed in a tabular form.

- In the Port Config List, specify the following:
  - IP Protocol—The IP protocol that you want to enable. The following options are ESP, FTP, ICMP, and IKEV2.
  - Port No—The port number that is enabled on this WLAN.
  - Status—The status of the port.

Step 9 Click Save.

Configuring WLAN AP Groups Templates

Site-specific VLANs or AP groups limit the broadcast domains to a minimum by segmenting a WLAN into different broadcast domains. Benefits include more effective management of load balancing and bandwidth allocation.

To configure WLAN AP Groups, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.

Step 2 Click AP Groups or choose WLAN > AP Groups from the left sidebar menu. The WLAN > AP Groups page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The AP Groups template page appears.

This page displays a summary of the AP groups configured on your network. In this page, you can add, remove, edit, or view details of an AP group. Click in the Edit column to edit its access point(s). Select the check box in the WLAN Profile Name column, and click Remove to delete WLAN profiles.

Note The maximum characters that you can enter in the Description text box is 256.

Adding Access Point Groups

You can create or modify a template for dividing the WLAN profiles into AP groups.

To add a new access point group, follow these steps:
Step 1 Choose Configure > Controller Template Launch Pad.

Step 2 Click AP Group VLANs or choose WLAN > AP Group VLANs from the left sidebar menu.

Note AP Groups (for controllers Release 5.2 and later) are referred to as AP Group VLANs for controllers prior to 5.2.

Step 3 Choose Add Template from the Select a command drop-down list, and click Go.

Step 4 Enter a name and group description for the access point group.

Note The group description is optional.

Step 5 If you want to add a WLAN profile, click the WLAN Profiles tab and configure the following fields:

a. Click Add.

Note To display all available WLAN profile names, delete the current WLAN profile name from the text box. When the current WLAN profile name is deleted from the text box, all available WLAN profiles appear in the drop-down list.

Note Each access point is limited to 16 WLAN profiles. Each access point broadcasts all WLAN profiles unless the WLAN override feature is enabled. The WLAN override feature allows you to disable any of the 16 WLAN profiles per access point.

Note The WLAN override feature applies only to older controllers that do not support the 512 WLAN feature (can support up to 512 WLAN profiles).

b. Type a WLAN profile name or choose one from the WLAN Profile Name drop-down list.

c. Enter an interface/interface group or choose one from the Interface/Interface Group drop-down list.

Note To display all available interfaces, delete the current interface from the Interface text box. When the current interface is deleted from the Interface text box, all available interfaces appear in the drop-down list.

d. Select the NAC Override check box, if applicable. The NAC override feature is disabled by default.

e. Specify the policy configuration parameters by clicking the Add/Edit link.

- Policy Name—Name of the policy.

- Policy Priority—Configure policy priority between 1 and 16. No two policies can have same priority.

Note Only 16 Policy mappings are allowed per WLAN. Selected policy template for the mapping will be applied first if it does not exist on the controller.
When access points and WLAN profiles are added, click **Save**.

**Step 6**

If you want to add a RF profile, click the **RF Profiles** tab, and configure the following fields:

- 802.11a—Drop-down list from which you can choose an RF profile for APs with 802.11a radios.
- 802.11b—Drop-down list from which you can choose an RF profile for APs with 802.11b radios.
- When RF profiles are added, click **Save**.

---

**Note**

Click the **Click here** link to add a new RF profile. See the “Configuring RF Profiles Templates (802.11)” section on page 11-81 for more information.

---

### Deleting Access Point Groups

To delete an access point group, follow these steps:

**Step 1**

Choose **Configure > Controller Template Launch Pad**.

**Step 2**

Click **AP Groups** or choose **WLAN > AP Groups** from the left sidebar menu.

**Step 3**

Click **Remove**.

---

### Configuring Policy Configuration Templates

The Policy Configuration Templates page enables you to configure the device-based policies on the controller. You can configure policies for a user or a device on the network. The maximum number of policies that you can configure is 64.

**Note**

Policies are not applied on WLANs and AP groups if AAA override is configured on the controller.

To configure Policy Configuration templates, follow these steps:

**Step 1**

Choose **Configure > Controller Template Launch Pad**.

**Step 2**

Click **Policy Configuration** or choose **WLANs > Policy Configuration** from the left sidebar menu.

**Step 3**

If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**.

**Step 4**

Configure the following fields:

- **Policy Name**—Name of the policy.
- **Policy Role**—Specifies the user type or the user group the user belongs to. For example, student, employee.
- **EAP Type**—EAP authentication method used by the client. The available methods are as follows:
  - LEAP
  - EAP-FAST
Chapter 11      Using Templates

Configuring Controller Templates

- EAP-TLS
- PEAP

- Device Type—Drop-down list from which you can choose a type of device.
- VLAN—VLAN associated with the policy.
- ACL—Drop-down list from which you can choose an IPv4 ACL for the policy.
- QoS—Drop-down list from which you can choose the QoS policy that can be one of the follows:
  - Platinum (Voice)—Assures a high QoS for Voice over Wireless.
  - Gold (Video)—Supports the high-quality video applications.
  - Silver (Best Effort)—Supports the normal bandwidth for clients.
  - Bronze (Background)—Provides the lowest bandwidth for guest services.
- Session Timeout—Maximum amount of time, in seconds, before a client is forced to reauthenticate. The default value is 0 seconds.
- Sleeping Client Timeout—Maximum amount of time, in hours, before a guest client is forced to reauthenticate. The default value is 12 hours. The range is from 1 to 720 hours.

Configuring FlexConnect Templates

- Configuring FlexConnect AP Groups Templates, page 11-40
- Configuring FlexConnect Users, page 11-43

Configuring FlexConnect AP Groups Templates

FlexConnect enables you 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 a controller in each office. There is no deployment restriction on the number of FlexConnect access points per location, but you can organize and group the access points per floor and limit them to 25 or so per building, because it is likely the branch offices share the same configuration.

To set up an FlexConnect AP group, follow these steps:

Step 1  Choose Configure > Controller Template Launch Pad.

Step 2  Click FlexConnect AP Groups or choose FlexConnect > FlexConnect AP Groups from the left sidebar menu. The FlexConnect > FlexConnect AP Groups page appears. It displays the primary and secondary RADIUS, as well as the number of controllers and virtual domains that the template is applied to, which automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3  If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The General tab of the FlexConnect AP Groups page appears.

Step 4  The Template Name field shows the group name assigned to the FlexConnect access point group.
Step 5  Choose the primary RADIUS authentication servers for each group. You can also configure local RADIUS servers on the flexconnect group (at a site-level) which are not present on the controller. The FlexConnect groups support up to 100 RADIUS servers per group.

Step 6  Choose the secondary RADIUS authentication servers for each group. You can also configure local RADIUS servers on the flexconnect group (at a site-level) which are not present on the controller. The FlexConnect groups support up to 100 RADIUS servers per group.

Step 7  If you want to add an access point to the group, click the FlexConnect AP tab.

Step 8  An access point Ethernet MAC address cannot exist in more than one FlexConnect group on the same controller. If more than one group is applied to the same controller, select the Ethernet MAC check box to unselect an access point from one of the groups. You should save this change or apply it to controllers.

Step 9  Click Add AP. The FlexConnect AP Group page appears.

Step 10  Click the FlexConnect Configuration tab to enable local authentication for a FlexConnect group.

---

**Note**  Make sure that the Primary RADIUS Server and Secondary RADIUS Server fields are set to None on the General tab.

---

Step 11  Select the FlexConnect Local Authentication check box to enable local authentication for this FlexConnect group. The default value is unselected.

---

**Note**  When you attempt to use this feature, a warning message indicates that it is a licensed feature.

---

**Note**  You can click the Users configured in the group link that appears at the bottom of the page to view the list of FlexConnect users. You can create FlexConnect users only after you save the FlexConnect AP Group.

---

Step 12  To allow a FlexConnect access point to authenticate clients using LEAP, select the LEAP check box. Otherwise, to allow a FlexConnect access point to authenticate clients using EAP-FAST, select the EAP-FAST check box.

Step 13  Perform one of the following, depending on how you want Protected Access Credentials (PACs) to be provisioned:

- To use manual PAC provisioning, enter the key used to encrypt and decrypt PACs in the EAP-FAST Key and Confirm EAP-FAST Key text boxes. The key must be 32 hexadecimal characters.
- To allow PACs to be sent automatically to clients that do not have one during PAC provisioning, select the Auto key generation check box.

Step 14  In the EAP-FAST Key text box, enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.

Step 15  In the EAP-FAST Authority ID text box, enter the authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.

Step 16  In the EAP-FAST Authority Info text box, enter the authority information of the EAP-FAST server.

Step 17  In the EAP-FAST Pac Timeout text box, specify a PAC timeout value by entering the number of seconds for the PAC to remain viable in the edit box. The valid range is 2 to 4095 seconds.

---

**Note**  The EAP-FAST options are available only if you select the EAP-FAST check box in Step 12.
Step 18 Click the **Image Upgrade** tab and configure the following:

- FlexConnect AP Upgrade—Select the check box if you want to upgrade the FlexConnect access points.
- Slave Maximum Retry Count—Enter the maximum retries for the slave to undertake to start the download from the master in the FlexConnect group. This option is available only if you select the FlexConnect AP Upgrade check box.

**Note** You are allowed to add an access point as a master access point only if the FlexConnect AP Upgrade check box is enabled on the General tab.

Step 19 Click the **VLAN-ACL Mapping** tab to view, add, edit, or remove a VLAN ACL mapping.

a. Click **Add Row**.

b. Enter a VLAN ID. The valid VLAN ID range is 1—4094.

c. From the Ingress ACL drop-down list, choose an Ingress ACL.

d. From the Egress AC drop-down list, choose an Egress ACL.

e. Click **Save**.

Step 20 Click the **WLAN-ACL Mapping** tab to view, add, edit, or remove a WLAN ACL mapping.

a. Click **Add Row**.

b. From the WLAN Profile Name drop-down list, choose a WLAN profile.

c. From the WebAuth ACL drop-down list, choose a WebAuth ACL.

d. Click **Save**.

**Note** You can add up to a maximum of 16 WebAuth ACLs.

Step 21 Click the **WebPolicy ACL** tab to view, add, edit, or remove a WebPolicy ACL mapping.

a. Click **Add Row**.

b. From the Web-Policy ACL drop-down list, choose a WebPolicy ACL.

c. Click **Save**.

**Note** You can add up to a maximum of 16 Web-Policy ACLs.

Step 22 Click the **Local Split** tab to view, add, edit, or remove a Local Split ACL mapping.

a. Click **Add Row**.

b. From the WLAN Profile Name drop-down list, choose a WLAN profile.

**Note** Only the FlexConnect central switching WLANs are displayed in the WLAN Profile Name drop-down list.

c. From the Local-Split ACL drop-down list, choose a FlexConnect ACL.

d. Click **Save**.
Step 23  Click the Central DHCP tab to view, add, edit, or remove a Central DHCP processing.
   a.  Click Add Row.
   b.  From the WLAN Profile Name drop-down list, choose a WLAN profile.
   
   | Note | Only the FlexConnect local switching WLANs are displayed in the WLAN Profile Name drop-down list. |

c.  From the Central DHCP drop-down list, choose Enable or Disable. When you enable this feature, 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.
d.  From the Override DNS drop-down list, choose Enable or Disable. You can enable or disable the overriding of the DNS server address on the interface assigned to the locally switched WLAN. When you override DNS in centrally switched WLANs, the clients get their DNS server IP address from the AP, not from the controller.
e.  From the NAT-PAT drop-down list, choose Enable or Disable. You can enable or disable Network Address Translation (NAT) and Port Address Translation (PAT) on locally switched WLANs. You must enable Central DHCP Processing to enable NAT and PAT.
f.  Click Save.

Step 24  Click Save.

Configuring FlexConnect Users

| Note | You can create FlexConnect users only after you save the FlexConnect AP Group. |

| Note | Maximum 100 FlexConnect users are supported in controller Release 5.2.x.x and later. If controller Release 5.2.0.0, and earlier supports only 20 FlexConnect users. |

To configure a FlexConnect user, follow these steps:

Step 1  Choose Configure > Controller Template Launch Pad.
Step 2  Click FlexConnect AP Groups or choose FlexConnect > FlexConnect AP Groups from the left sidebar menu. The FlexConnect > FlexConnect AP Groups page appears.
Step 3  Click the FlexConnect Configuration tab to enable local authentication for a FlexConnect group.
Step 4  Select the FlexConnect Local Authentication check box to enable local authentication for this FlexConnect group.
Step 5  Click the Users configured in the group link. The FlexConnect Users page appears.
Step 6  If you want to add a new user, choose Add User from the Select a command drop-down list, and click Go. The Add User page appears.
Step 7  In the User Name text box, enter the FlexConnect username.
Step 8  In the Password text box, enter the password.
Configuring Controller Templates

Step 9  Reenter the password in the Confirm Password text box.
Step 10  Click **Save**.

---

**Note**  To delete a FlexConnect User, choose a user from the FlexConnect Users list, and then click **Delete**.

---

**Configuring Security Templates**

- Configuring a General Security Controller Template, page 11-44
- Configuring a File Encryption Template, page 11-45
- Configuring a RADIUS Authentication Template, page 11-45
- Configuring a RADIUS Accounting Template, page 11-47
- Configuring a RADIUS Fallback Template, page 11-48
- Configuring an LDAP Server Template, page 11-49
- Configuring a TACACS+ Server Template, page 11-50
- Configuring a Local EAP General Template, page 11-51
- Configuring a Local EAP Profile Template, page 11-52
- Configuring an EAP-FAST Template, page 11-53
- Configuring a Network User Priority Template, page 11-54
- Configuring a Local Network Users Template, page 11-54
- Configuring a Guest User Template, page 11-55
- Configuring a User Login Policies Template, page 11-56
- Configuring a MAC Filter Template, page 11-57
- Configuring an Access Point or MSE Authorization Template, page 11-58
- Configuring a Manually Disabled Client Template, page 11-58
- Configuring a Client Exclusion Policies Template, page 11-59
- Configuring an Access Point Authentication and MFP Template, page 11-60
- Configuring a Web Authentication Template, page 11-61
- Configuring an External Web Auth Server Template, page 11-64

---

**Configuring a General Security Controller Template**

To add a new template with general security information for a controller, follow these steps:

**Step 1**  Choose **Configure > Controller Template Launch Pad**.
**Step 2**  Click **New** beside the template you want to add.
**Step 3**  Configure the following fields:
• Template Name

Note  Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

• Maximum Local Database Entries (on next reboot)—Enter the maximum number of allowed database entries. This amount becomes effective on the next reboot.

Step 4  Click **Save**. Once saved, the template appears in the Template List page. In the Template List page, you can apply this template to controllers. See the “Applying Controller Templates” section on page 11-2 for more information.

### Configuring a File Encryption Template

This page enables you to add a file encryption template or make modifications to an existing file encryption template.

To configure a File Encryption template, follow these steps:

Step 1  Choose **Configure > Controller Template Launch Pad**.

Step 2  Click **File Encryption** or choose **Security > File Encryption** from the left sidebar menu. The Security > File Encryption page appears. The number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved. The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3  If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The File Encryption template page appears.

Step 4  Check if you want to enable file encryption.

Step 5  Enter an encryption key text string of exactly 16 ASCII characters.

Step 6  Retype the encryption key.

Step 7  Click **Save**.

### Configuring a RADIUS Authentication Template

This page allows you to add a RADIUS authentication template or make modifications to an existing template. After these server templates are configured, controller users who log into the controller through the CLI or GUI are authenticated.

To configure a RADIUS Authentication template, follow these steps:

Step 1  Choose **Configure > Controller Template Launch Pad**.
Step 2  Click **RADIUS Auth Servers** or choose **Security > RADIUS Auth Servers** from the left sidebar menu. The Security > RADIUS Auth Servers page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The IP address of the RADIUS server and the port number and admin status for the interface protocol is also displayed. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3  If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The RADIUS Auth Servers template page appears.

Step 4  From the Shared Secret Format drop-down list, choose either **ASCII** or **hex**.

**Note**  Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.

Step 5  Enter the RADIUS shared secret used by your specified server.

Step 6  Select the check box if you want to enable key wrap. If this check box is enabled, the authentication request is sent to RADIUS servers that have following key encryption key (KEK) and message authenticator code keys (MACK) configured. When enabled, the following fields appear:

- **Shared Secret Format**: Enter ASCII or hexadecimal.

**Note**  Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.

- **KEK Shared Secret**: Enter the KEK shared secret.
- **MACK Shared Secret**: Enter the MACK shared secret.

**Note**  Each time the controller is notified with the shared secret, the existing shared secret is overwritten with the new shared secret.

Step 7  Click if you want to enable administration privileges.

Step 8  Click if you want to enable support for RFC 3576. RFC 3576 is an extension to the Remote Authentication Dial In User Service (RADIUS) protocol. It allows dynamic changes to a user session and includes support for disconnecting users and changing authorizations applicable to a user session. With these authorizations, support is provided for Disconnect and Change-of-Authorization (CoA) messages. Disconnect messages immediately terminate a user session, whereas CoA messages modify session authorization attributes such as data filters.

Step 9  Click if you want to enable network user authentication. If this option is enabled, this entry is considered as the RADIUS authenticating server for the network user.
Step 10 Click if you want to enable management authentication. If this option is enabled, this entry is considered as the RADIUS authenticating server for the management user.

Step 11 Specify the time in seconds after which the RADIUS authentication request times out and a retransmission is attempted by the controller. You can specify a value between 2 and 30 seconds.

Step 12 If you click to enable the IP security mechanism, additional IP security fields are added to the page, and Steps 13 to 19 are required. If you disable it, click Save and skip Steps 13 to 19.

Step 13 Use the drop-down list to choose which IP security authentication protocol to use. The options are HMAC-SHA1, HMAC-MD5, and None.

Message Authentication Codes (MAC) are used between two parties that share a secret key to validate information transmitted between them. HMAC (Hash MAC) is a mechanism based on cryptographic hash functions and can be used in combination with any iterated cryptographic hash function. HMAC-MD5 and HMAC-SHA1 are two constructs of the HMAC using the MD5 hash function and the SHA1 hash function. HMAC also uses a secret key for calculation and verification of the message authentication values.

Step 14 Set the IP security encryption mechanism to use. The options are as follows:

- DES—Data Encryption Standard is a method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.
- Triple DES—Data Encryption Standard that applies three keys in succession.
- AES 128 CBC—Advanced Encryption Standard uses keys with a length of 128, 192, or 256 bits to encrypt blocks with a length of 128, 192, or 256 bits. AES 128 CBC uses a 128-bit data path in Cipher Clock Chaining (CBC) mode.
- None—No IP security encryption mechanism.

Step 15 The Internet Key Exchange (IKE) authentication is not an editable text box. Internet Key Exchange protocol (IKE) is used as a method of distributing the session keys (encryption and authentication), as well as providing a way for the VPN endpoints to agree on how data should be protected. IKE keeps track of connections by assigning a bundle of security associations (SAs) to each connection.

Step 16 Use the IKE phase 1 drop-down list to choose either aggressive or main. This sets the IKE protocol. IKE phase 1 is used to negotiate how IKE is protected. Aggressive mode passes more information in fewer packets, with the benefit of a slightly faster connection, at the cost of transmitting the identities of the security gateways in the clear.

Step 17 At the Lifetime field, set the timeout interval (in seconds) when the session expires.

Step 18 Set the IKE Diffie Hellman group. The options are group 1 (768 bits), group 2 (1024 bits), or group 5 (1536 bits). Diffie-Hellman techniques are used by two devices to generate a symmetric key where you can publicly exchange values and generate the same symmetric key.

Although all three groups provide security from conventional attacks, Group 5 is considered more secure because of its larger key size. However, computations involving Group 1 and Group 2 based keys might occur slightly faster because of their smaller prime number size.

Step 19 Click Save.

### Configuring a RADIUS Accounting Template

This page allows you to add a RADIUS accounting template or make modifications to an existing RADIUS accounting template.

To configure a RADIUS Accounting template, follow these steps:
Chapter 11 Using Templates

Configuring Controller Templates

Step 1: Choose Configure > Controller Template Launch Pad.

Step 2: Click RADIUS Acct Servers or choose Security > RADIUS Acct Servers from the left sidebar menu. The Security > RADIUS Acct Servers page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The IP address of the RADIUS server and the port number and admin status for the interface protocols are also displayed. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3: If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The RADIUS Accounting Server template page appears.

Step 4: Use the Shared Secret Format drop-down list to choose either ASCII or hexadecimal.

Note: Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.

Step 5: Enter the RADIUS shared secret used by your specified server.

Step 6: Retype the shared secret.

Step 7: Click if you want to establish administrative privileges for the server.

Step 8: Click if you want to enable the network user authentication. If this option is enabled, this entry is considered as the RADIUS authenticating server for the network user.

Step 9: Specify the time in seconds after which the RADIUS authentication request times out and a retransmission by the controller occurs. You can specify a value between 2 and 30 seconds.

Step 10: Click Save.

Configuring a RADIUS Fallback Template

This page allows you to add a RADIUS fallback template or make modifications to an existing RADIUS fallback template.

To configuring a RADIUS Fallback template, follow these steps:

Step 1: Choose Configure > Controller Template Launch Pad.

Step 2: Click RADIUS Fallback or choose Security > RADIUS Fallback from the left sidebar menu. The Security > RADIUS Fallback page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.
Chapter 11 - Using Templates

Configuring Controller Templates

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3**
If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The RADIUS Fallback template page appears.

**Step 4**
From the RADIUS Fallback Mode drop-down list, choose **Off**, **Passive**, or **Active**.
- **Off**—Disables fallback.
- **Passive**—You must enter a time interval.
- **Active**—You must enter a username and time interval.

**Step 5**
Click **Save**.

Configuring an LDAP Server Template

This section explains how to configure a Lightweight Directory Access Protocol (LDAP) server as a backend database, similar to a RADIUS or local user database. An LDAP backend database allows the controller to query an LDAP server for the credentials (username and password) of a particular user. These credentials are then used to authenticate the user. For example, local EAP might use an LDAP server as its backend database to retrieve user credentials.

To add an LDAP server template or make modifications to an existing LDAP server template, follow these steps:

**Step 1**
Choose **Configure > Controller Template Launch Pad**.

**Step 2**
Click **LDAP Servers** or choose **Security > LDAP Servers** from the left sidebar menu. The Security > LDAP Servers page appears. The IP address of the LDAP server and the port number for the interface protocols are displayed. Also, the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3**
If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The LDAP Server template page appears.

**Step 4**
The port number of the controller to which the access point is connected.

**Step 5**
From the Bind Type drop-down list, choose **Authenticated** or **Anonymous**. If you choose Authenticated, you must enter a bind username and password as well. A bind is a socket opening that performs a lookup. Anonymous bind requests are rejected.

**Step 6**
In the Server User Base DN text box, enter the distinguished name of the subtree in the LDAP server that contains a list of all the users.

**Step 7**
In the Server User Attribute text box, enter the attribute that contains the username in the LDAP server.

**Step 8**
In the Server User Type text box, enter the ObjectType attribute that identifies the user.
Configuring Controller Templates

Chapter 11      Using Templates

Configuring a TACACS+ Server Template

This page allows you to add a TACACS+ server or make modifications to an existing TACACS+ server template. After these server templates are configured, controller users who log into the controller through the CLI or GUI are authenticated.

To configure a TACACS+ Server template, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.
Step 2 Click TACACS+ Server or choose Security > TACACS+ Server from the left sidebar menu. The Security > TACACS+ Servers page appears. The IP address and the port number and admin of the TACACS+ template are displayed. Also, the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The TACACS+ Servers template page appears.

Step 4 Select one or more server types by selecting their respective check boxes. The following server types are available:
- **authentication**—Server for user authentication/authorization.
- **authorization**—Server for user authorization only.
- **accounting**—Server for RADIUS user accounting.

Step 5 Enter the IP address of the server.
Step 6 Enter the port number of the server. The default is 49.
Step 7 From the drop-down list, choose either **ASCII** or **hex**.

**Note** Regardless of which format you choose, for security reasons, only ASCII is visible on the WLC (and Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. Set the key format again in the template in the event a discovered template is applied to another device.

Step 8 Enter the TACACS+ shared secret used by your specified server in the Shared Secret text box.
Step 9 Reenter the shared secret in the Confirm Shared Secret text box.
Step 10 Select the **Admin Status** check box if you want the TACACS+ server to have administrative privileges.
**Step 11**  In the Retransmit Timeout text box, enter the time, in seconds, after which the TACACS+ authentication request times out and a retransmission is attempted by the controller.

**Step 12**  Click Save.

---

**Configuring a Local EAP General Template**

This page allows you to specify a timeout value for local EAP. You can then add or make changes to an existing local EAP general template.

**Note**  If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to then reauthenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP.

**Step 1**  Choose Configure > Controller Template Launch Pad.

**Step 2**  Click Local EAP General or choose Security > Local EAP General from the left sidebar menu. The Security > Local EAP General page appears. The number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3**  If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Local EAP General controller template page appears.

**Step 4**  In the Local Auth Active Timeout text box, enter the amount of time (in seconds) that the controller attempts to authenticate wireless clients using local EAP after any pair of configured RADIUS servers fail. The valid range is 1 to 3600 seconds, and the default setting is 1000 seconds.

**Step 5**  The following values should be adjusted if you are using EAP-FAST, manual password entry, one-time password, or 7920/7921 phones. You must increase the 802.1x timeout values on the controller (default=2 seconds) for the client to obtain the PAC using automatic provisioning. The recommended and default timeout on the Cisco ACS server is 20 seconds.

**Note**  Roaming fails if these values are not set the same across multiple controllers.

- Local EAP Identify Request Timeout = 1
- Local EAP Identity Request Maximum Retries = 20
- Local EAP Dynamic WEP Key Index = 0
- Local EAP Request Timeout = 20
- Local EAP Request Maximum Retries = 2
Step 6  Click Save.

Configuring a Local EAP Profile Template

This page allows you to add a local EAP profile template or make modifications to an existing template. Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down. When you enable local EAP, the controller serves as the authentication server and the local user database, thereby removing dependence on an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users.

Note  The LDAP backend database supports only these local EAP methods: EAP-TLS and EAP-FAST with certificates. LEAP and EAP-FAST with PACs are not supported for use with the LDAP backend database.

Step 1  Choose Configure > Controller Template Launch Pad.

Step 2  Click Local EAP Profiles or choose Security > Local EAP Profiles from the left sidebar menu. The Security > Local EAP Profiles page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. It also shows the EAP profile name and indicates whether LEAP, EAP-FAST, TLS, or PEAP is used. The last column indicates when the template was last saved. The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3  If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Local EAP Profiles template page appears.

Step 4  Each EAP profile must be associated with an authentication type(s). Choose the desired authentication type:

- LEAP—This authentication type leverages Cisco Key Integrity Protocol (CKIP) and MMH message integrity check (MIC) for data protection. A username and password are used to perform mutual authentication with the RADIUS server through the access point.
- EAP-FAST—This authentication type (Flexible Authentication via Secure Tunneling) uses a three-phased tunnel authentication process to provide advanced 802.1X EAP mutual authentication. A username, password, and PAC (protected access credential) are used to perform mutual authentication with the RADIUS server through the access point.
- TLS—This authentication type uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It requires a client certificate for authentication.
- PEAP—This authentication type is based on EAP-TLS authentication but uses a password instead of a client certificate for authentication. PEAP uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data.

Step 5  Use the Certificate Issuer drop-down list to determine whether Cisco or another vendor issued the certificate for authentication. Only EAP-FAST and TLS require a certificate.
Step 6 If you want the incoming certificate from the client to be validated against the certificate authority (CA) certificates on the controller, select the **Check Against CA Certificates** check box.

Step 7 If you want the (CN) in the incoming certificate to be validated against the common name of the CA certificate, select the **Verify Certificate CN Identity** check box.

Step 8 If you want the controller to verify that the incoming device certificate is still valid and has not expired, select the **Check Against Date Validity** check box.

Step 9 If a local certificate is required, select the check box.

Step 10 If a client certificate is required, select the check box.

Step 11 Click **Save**.

Step 12 To enable local EAP, follow these steps:
   a. Choose **WLAN > WLAN Configuration** from the left sidebar menu.
   b. Click the profile name of the desired WLAN.
   c. Choose the **Security > AAA Servers** tab to access the AAA Servers page.
   d. Select the **Local EAP Authentication** check box to enable local EAP for this WLAN.

Step 13 Click **Save**.

### Configuring an EAP-FAST Template

This authentication type (Flexible Authentication via Secure Tunneling) uses a three-phased tunnel authentication process to provide advanced 802.1X EAP mutual authentication. A username, password, and PAC are used to perform mutual authentication with the RADIUS server through the access point. This page allows you to add an EAP-FAST template or make modifications to an existing EAP-FAST template.

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **EAP-FAST Parameters** or choose **Security > EAP-FAST Parameters** from the left sidebar menu. The Security > EAP-FAST Parameters page appears. The number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

   The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The EAP-FAST Parameters template page appears.

Step 4 In the **Time to Live for the PAC** text box, enter the number of days for the PAC to remain viable. The valid range is 1 to 1000 days, and the default setting is 10 days.

Step 5 In the **Authority ID** text box, enter the authority identifier of the local EAP-FAST server in hexadecimal characters. You can enter up to 32 hexadecimal characters, but you must enter an even number of characters.

Step 6 In the **Authority Info** text box, enter the authority identifier of the local EAP-FAST server in text format.
Configuring Controller Templates

Step 7 In the Server Key and Confirm Server Key text boxes, enter the key (in hexadecimal characters) used to encrypt and decrypt PACs.

Step 8 If you want to enable anonymous provisioning, select the Anonymous Provision check box. This feature allows PACs to be sent automatically to clients that do not have one during PAC provisioning. If you disable this feature, PACs must be manually provisioned.

Step 9 Click Save.

Configuring a Network User Priority Template

You can specify the order that LDAP and local databases use to retrieve user credential information. This page allows you to add or make modifications to an existing network user credential retrieval priority template.

Step 1 Choose Configure > Controller Template Launch Pad.

Step 2 Click Network Users Priority or choose Security > Network Users Priority from the left sidebar menu. The Security > Network User Credential Retrieval Priority page appears. The network retrieval order and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Network Users Priority template page appears.

Step 4 Use the left and right pointing arrows to include or exclude network user credentials in the right page.

Step 5 Use the up and down buttons to determine the order credentials are tried.

Step 6 Click Save.

Configuring a Local Network Users Template

With this template, you can store the credentials (username and password) of all the local network users. These credentials are then used to authenticate the users. For example, local EAP might use the local user database as its backend database to retrieve user credentials. This page allows you to add or make modifications to an existing local network user template. You must create a local net user and define a password when logging in as a web authentication client.

To configure a Local Network Users template, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.

Step 2 Click Local Net Users or choose Security > Local Net Users from the left sidebar menu. The Security > Local Net Users page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.
The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Local Net Users template page appears.

**Step 4** If you keep Import from File enabled, you need to enter a file path or click **Browse** to navigate to the file path. Then continue to Step 11. If you disable the import, continue to Step 5.

**Note** You can only import a .csv file. Any other file formats are not supported.

The first row in the file is the header. The data in the header is not read by Prime Infrastructure. The header can either be blank or filled. Prime Infrastructure reads data from the second row onwards.

**Step 5** Enter a username and password. It is mandatory to fill the Username and Password fields in all the rows.

**Step 6** Enter a profile. The Profile column if left blank (or filled in with *any profile*) means a client on any profile can use this account.

**Step 7** Enter a description of the profile.

**Step 8** Use the drop-down list to choose the SSID which this local user is applied to or choose the any SSID option.

**Step 9** Enter a user-defined description of this interface. Skip to Step 11.

**Step 10** If you want to override the existing template, select the **Override existing templates** check box.

**Step 11** Click **Save**.

---

**Guest User Templates**

Choose **Configure > Controller Template Launch Pad > Security > Guest Users** to access the Guest Users list page.

**Note** To reduce clutter, Prime Infrastructure does not show expired templates by default. You can specify which guest users to filter based on their status (active, scheduled, expired, not active, or none). Use the Select a Status Filter drop-down list to determine the filter criteria.

**Note** Click the **Edit View** link to add, remove, or reorder columns in the Guest Users table.

---

**Configuring a Guest User Template**

This page allows you to add a guest user template or make modifications to an existing guest user template. The purpose of a guest user account is to provide a user account for a limited amount of time. A Lobby Ambassador is able to configure a specific time frame for the guest user account to be active. After the specified time period, the guest user account automatically expires. See the “Creating Guest User Accounts” section on page 7-8 for further information on guest access.
Configuring Controller Templates

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Guest Users** or choose **Security > Guest Users** from the left sidebar menu. The Security > Guest User page appears.

**Note** To reduce clutter, Prime Infrastructure does not show expired templates by default. You can specify which guest users to filter based on their status (active, scheduled, expired, not active, or none). Use the Select a Status Filter drop-down list to determine the filter criteria.

**Step 3** If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Guest Users template page appears.

**Step 4** Enter a guest username in the User Name text box. The maximum size is 24 characters.

**Step 5** Enter a password for this username in the Password text box.

**Step 6** Click the **Advanced** tab.

**Step 7** Use the Profile drop-down list to choose the guest user to connect to.

**Step 8** Choose a user role for the guest user from the drop-down list. User roles are predefined by the administrator and are associated with the access of the guest (such as contractor, customer, partner, vendor, visitor, and so on).

User Role is used to manage the amount of bandwidth allocated to specific users within the network.

**Step 9** Define how long the guest user account remains active by choosing either the Limited or Unlimited Lifetime option.

- For the limited option, you choose the period of time that the guest user account is active using the hours and minutes drop-down lists. The default value for Limited is one day (8 hours).
- When Unlimited is chosen, there is no expiration date for the guest account.

**Step 10** Choose the area (indoor, outdoor), controller list, or config group to which the guest user traffic is limited from the Apply to drop-down list.

If you choose the controller list option, a list of controller IP addresses appears.

**Step 11** (Optional) Modify the default guest user description on the General tab if necessary.

**Step 12** (Optional) Modify the Disclaimer text on the General tab, if necessary. If you want the supplied text to be the default, select the **Make this Disclaimer default** check box.

**Step 13** Click **Save**.

---

**Configuring a User Login Policies Template**

This page allows you to add a user login template or make modifications to an existing user login policies template. On this template you set the maximum number of concurrent logins that each single user can have.

**Step 1** Choose **Configure > Controller Template Launch Pad**.
Step 2 Click **User Login Policies** or choose **Security > User Login Policies** from the left sidebar menu. The Security > User Login Policies page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The User Login Policies template page appears.

Step 4 You can adjust the maximum number of concurrent logins each single user can have.

Step 5 Click **Save** to keep this template.

---

**Configuring a MAC Filter Template**

This page allows you to add a MAC filter template or make modifications to an existing MAC filter template.

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **MAC Filtering** or choose **Security > MAC Filtering** from the left sidebar menu. The Security > MAC Filtering page appears.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The MAC Filtering template page appears.

Step 4 If you keep Import From File enabled, you must enter a file path or click **Browse** to navigate to the file path. The import file must be a CSV file with MAC address, profile name, interface, and description (such as 00:11:22:33:44:55, Profile1, management, test filter). If you unselect the Import from File check box, continue to Step 5. Otherwise, skip to Step 8.

The client MAC address appears.

Step 5 Choose the profile name to which this MAC filter is applied or choose the **any Profile** option.

Step 6 Use the drop-down list to choose from the available interface names.

Step 7 Enter a user-defined description of this interface. Skip to Step 9.

Step 8 If you want to override the existing template, select the **Override existing templates** check box.

Step 9 Click **Save**.

**Note** You cannot use MAC address in the broadcast range.
Chapter 11 Using Templates

Configuring Controller Templates

Configuring an Access Point or MSE Authorization Template

To add an MSE authorization or make changes to an existing access point or MSE authorization template, follow these steps:

**Note** These templates are devised for Cisco 11xx/12xx series access points converted from Cisco IOS to lightweight access points or for 1030 access points connecting in bridge mode. See the Cisco Mobility Services Engine Configuration Guide for further information.

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **AP/MSE Authorization** or choose **Security > AP/MSE Authorization** from the left sidebar menu. The Security > AP/LBS Authorization Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also shows the Base Radio MAC and the certificate type and key. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The AP/MSE Authorization template page appears.

**Step 4** Select the **Import From File** check box if you want to import a file containing access point MAC addresses.

**Note** You can only import a .csv file. The .csv file format parallels the fields in the GUI and therefore includes access point base radio MAC, Type, Certificate Type (MIC or SSC), and key hash (such as 00:00:00:00:00:00, AP, SSC, xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx). Any other file formats are not supported.

**Step 5** Enter the desired file path or click **Browse** to import the file.

**Step 6** Click **Save**.

**Note** You cannot use MAC address in the broadcast range.

Configuring a Manually Disabled Client Template

This page allows you to add a manually disable client template or make modifications to an existing disabled client template.

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Disable Clients** or choose **Security > Disabled Clients** from the left sidebar menu. The Security > Disabled Clients page appears.
Step 3 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Manually Disabled template page appears.

Step 4 Enter the MAC address of the client you want to disable.

Step 5 Enter a description of the client you are setting to disabled.

Step 6 Click Save.

Note You cannot use a MAC address in the broadcast range.

Configuring a Client Exclusion Policies Template

To add a client exclusion policies template or modify an existing client exclusion policies template, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.

Step 2 Click Client Exclusion Policies or choose Security > Client Exclusion Policies from the left sidebar menu. The Security > Client Exclusion Policies page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Client Exclusion Policies template page appears.

Step 4 Edit a client exclusion policies template by configuring its field (see Table 11-3).

**Table 11-3 Policies Template Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Name</td>
<td>Enter a name for the client exclusion policy.</td>
</tr>
<tr>
<td>Excessive 802.11 Association Failures</td>
<td>Enable to exclude clients with excessive 802.11 association failures.</td>
</tr>
<tr>
<td>Excessive 802.11 Authentication Failures</td>
<td>Enable to exclude clients with excessive 802.11 authentication failures.</td>
</tr>
<tr>
<td>Excessive 802.1X Authentication Failures</td>
<td>Enable to exclude clients with excessive 802.1X authentication failures.</td>
</tr>
<tr>
<td>Excessive 802.11 Web Authentication Failures</td>
<td>Enable to exclude clients with excessive 802.11 web authentication failures.</td>
</tr>
<tr>
<td>IP Theft or Reuse</td>
<td>Enable to exclude clients exhibiting IP theft or reuse symptoms.</td>
</tr>
</tbody>
</table>
Configuring an Access Point Authentication and MFP Template

Management Frame Protection (MFP) provides for the authentication of 802.11 management frames by the wireless network infrastructure. Management frames can be protected to detect adversaries who are invoking denial of service attacks, flooding the network with associations and probes, interjecting as rogue access points, and affecting the network performance by attacking the QoS and radio measurement frames.

When enabled, the access point protects the management frames it transmits by adding a message integrity check information element (MIC IE) to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing any receiving access point configured to detect MFP frames to report the discrepancy. An access point must be a member of a WDS to transmit MFP frames.

When MFP detection is enabled, the access point validates every management frame that it receives from other access points in the network. It ensures that the MIC IE is present (when the originator is configured to transmit MFP frames) and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE from a BSSID belonging to an access point that is configured to transmit MFP frames, it reports the discrepancy to the network management system.

To add or make modifications for the access point authentication and management frame protection (MFP) template, follow these steps:

Step 1  Choose Configure > Controller Template Launch Pad.

Step 2  Click AP Authentication and MFP or choose Security > AP Authentication and MFP from the left sidebar menu. The Security > AP Authentication Policy Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3  If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The AP Authentication and MFP template page appears.

Step 4  From the Protection Type drop-down list, choose one of the following authentication policies:

- **None**—No access point authentication policy.
- **AP Authentication**—Apply authentication policy.
- **MFP**—Apply management frame protection.

Alarm trigger threshold appears only when AP authentication is selected as a protection type. Set the number of hits from an alien access point to ignore before raising an alarm.

The valid range is from 1 to 255. The default value is 255.

Step 5  Click Save.
### Configuring a Web Authentication Template

With web authentication, guests are automatically redirected to a web authentication page when they launch their browsers. Guests gain access to the WLAN through this web portal. Wireless LAN administrators using this authentication mechanism should have the option of providing unencrypted or encrypted guest access. Guest users can then log into the wireless network using a valid username and password, which is encrypted with SSL. Web authentication accounts might be created locally or managed by a RADIUS server. The Cisco Wireless LAN controllers can be configured to support a web authentication client. You can use this template to replace the Web authentication page provided on the controller.

To add or make modifications to an existing web authentication template, follow these steps:

**Step 1** Choose Configure > Controller Template Launch Pad.

**Step 2** Click Web Auth Configuration or choose Security > Web Auth Configuration from the left sidebar menu. The Security > Web Authentication page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Web Authentication template page appears.

**Step 4** Choose the appropriate web authentication type from the drop-down list. The choices are default internal, customized web authentication, or external.

- If you choose default internal, you can still alter the page title, message, and redirect URL, as well as whether the logo appears. Continue to Step 5.

- If you choose customized web authentication, click Save and apply this template to the controller. You are prompted to download the web authentication bundle.

**Note** Before you can choose customized web authentication, you must first download the bundle by going to Config > Controller and choose Download Customized Web Authentication from the Select a command drop-down list, and click Go.

- If you choose external, you need to enter the URL you want to redirect to after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user is directed to the company home page.

**Step 5** Select the Logo Display check box if you want your company logo displayed.

**Step 6** Enter the title you want displayed on the Web Authentication page.

**Step 7** Enter the message you want displayed on the Web Authentication page.

**Step 8** Provide the URL where the user is redirected after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user would be directed to the company home page.
Configuring Controller Templates

Chapter 11      Using Templates

Step 9  Click Save.

Downloading a Customized Web Authentication Page

You can download a customized Web Authentication page to the controller. With a customized web page, you can establish a username and password for user web access.

When downloading customized web authentication, you must follow these strict guidelines:

- Provide a username.
- Provide a password.
- Retain a redirect URL as a hidden input item after extracting from the original URL.
- Extract the action URL and set aside from the original URL.
- Include scripts to decode the return status code.

Before downloading, follow these steps:

Step 1  Download the sample login.html bundle file from the server. The .html file is shown in Figure 11-1. The login page is presented to web users the first time they access the WLAN if web authentication is turned on.

Figure 11-1    Login.html

Web Authentication

User Name
Password
Submit

Step 2  Edit the login.html file and save it as a .tar or .zip file.

Note  You can change the text of the Submit button to read Accept terms and conditions and Submit.

Step 3  Make sure you have a Trivial File Transfer Protocol (TFTP) server available for the download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable. However, if you want to put the TFTP server on a different network while the management port is down, add a static route if the subnet where the service port resides has a gateway (config route add IP address of TFTP server).
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
• A third-party TFTP server cannot run on the same computer as Prime Infrastructure because the built-in TFTP server of Prime Infrastructure and third-party TFTP server use the same communication port.

**Step 4**  
Download the .tar or .zip file to the controller(s).

**Note**  
The controller allows you to download up to 1 MB of a .tar file containing the pages and image files required for the Web authentication display. The 1 MB limit includes the total size of uncompressed files in the bundle.

You can now continue with the download.

**Step 5**  
Copy the file to the default directory on your TFTP server.

**Step 6**  
Choose **Configure > Controllers**.

**Step 7**  
Choose a controller by clicking the URL for the corresponding IP address. If you select more than one IP address, the customized Web authentication page is downloaded to multiple controllers.

**Step 8**  
From the left sidebar menu, choose **System > Commands**.

**Step 9**  
From the Upload/Download Commands drop-down list, choose **Download Customized Web Auth**, and click **Go**.

**Step 10**  
The IP address of the controller to receive the bundle and the current status are displayed.

**Step 11**  
Choose **local machine** from the File is Located On field. If you know the filename and path relative to the root directory of the server, you can also select TFTP server.

**Note**  
For a local machine download, either .zip or .tar file options exists, but Prime Infrastructure does the conversion of .zip to .tar automatically. If you chose a TFTP server download, only .tar files would be specified.

**Step 12**  
Enter the maximum number of times the controller should attempt to download the file in the Maximum Retries field.

**Step 13**  
Enter the maximum amount of time in seconds before the controller times out while attempting to download the file in the Timeout field.

**Step 14**  
The files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click **Browse** to navigate to it.

**Step 15**  
Click **OK**.

If the transfer times out, you can simply choose the TFTP server option in the File Is Located On field, and the server filename is populated for you. The local machine option initiates a two-step operation. First, the local file is copied from the workstation of the administrator to the built-in TFTP server of Prime Infrastructure. Then the controller retrieves that file. For later operations, the file is already in the TFTP directory of Prime Infrastructure server, and the download web page now automatically populates the filename.

**Step 16**  
Click the **Click here to download a sample tar file** link to get an option to open or save the login.tar file.

**Step 17**  
After completing the download, you are directed to the new page and able to authenticate.
Configuring an External Web Auth Server Template

To create or modify an External Web Auth Server template, follow these steps:

Step 1: Choose Configure > Controller Templates Launch Pad.
Step 2: Click External Web Auth Server or choose Security > External Web Auth Server from the left sidebar menu. The External Web Auth Server Controller Templates page displays all currently saved External Web Auth Server templates. It also displays the number of controllers and virtual domains to which each template is applied.
Step 3: Click a template name to open the Controller Template list page. In this page, you can edit the current template fields.

Configuring a Security Password Policy Template

This page enables you to determine your security password policy.

To add or make modifications to an existing password policy template, follow these steps:

Step 1: Choose Configure > Controller Template Launch Pad.
Step 2: Click Password Policy or choose Security > Password Policy from the left sidebar menu. The Security > Password Policy page appears.
Step 3: If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Password Policy template page appears.
Step 4: Enter the template name.
Step 5: You can enable or disable the following settings:
- Password must contain characters from at least 3 different classes such as uppercase letters, lowercase letters, digits, and special characters.
- No character can be repeated more than 3 times consecutively.
- Password cannot be the default words like cisco, admin.

Note: Password cannot be “cisco”, “ocsic”, “admin”, “nimda’ or any variant obtained by changing the capitalization of letters, or by substituting ‘1’ “!” or “!” for i, or substituting “0” for “o”, or substituting “$” for “s”.
- Password cannot contain username or reverse of username.
Step 6: Click Save.

Configuring Security - Access Control Templates

- Configuring an Access Control List Template, page 11-65
- Configuring a FlexConnect Access Control List Template, page 11-67
Chapter 11 Using Templates

Configuring Controller Templates

- Configuring an ACL IP Groups Template, page 11-69
- Configuring an ACL Protocol Groups Template, page 11-70

Configuring an Access Control List Template

You can create or modify an ACL template for configuring the type of traffic that is allowed, by protocol, direction, and the source or destination of the traffic.

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 controller). ACLs can be applied to data traffic to and from wireless clients or to all traffic destined for the controller Central Processing Unit (CPU) and can now support reusable grouped IP addresses and reusable protocols. After ACLs are configured in the template, they can be applied to the management interface, the AP-manager interface, or any of the dynamic interfaces for client data traffic; to the Network Processing Unit (NPU) interface for traffic to the controller CPU; or to a WAN.

This release of Prime Infrastructure provides support to IPv6 ACLs.

To add or modify an existing ACL template, follow these steps:

**Step 1** Choose Configure > Controller Template Launch Pad.

**Step 2** Click Access Control Lists or choose Security > Access Control > Access Control Lists in the left sidebar menu. The Security > Access Control List page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new Access Control List template, choose Add Template from the Select a command drop-down list, and click Go. The New Controller Template page appears. In this page, specify the following fields:

- Access Control List Name—User-defined name of the template.
- ACL Type—Choose either IPv4 or IPv6.

**Note** IPv6 ACL is supported from controller Release 7.2.x.

**Step 4** To create reusable grouped IP addresses and protocols, choose Access Control > IP Groups from the left sidebar menu.

**Step 5** All the IP address groups are listed. One IP address group can have a maximum of 128 IP address and netmask combinations. To define a new IP address group, choose Add IP Group from the Select a command drop-down list, and click Go. To view or modify an existing IP address group, click the URL of the IP address group. The IP address group page opens.

**Note** For the IP address of any, an any group is predefined.

**Step 6** In the ACL IP Groups details page you can edit the current IP group fields.

- IP Group Name
Chapter 11      Using Templates

Configuring Controller Templates

- IP Address
- Netmask OR CIDR Notation—Enter the Netmask or CIDR Notation and then click Add. The list of IP addresses or Netmasks appears in the List of IP Address/Netmasks text box.

CIDR notation allows you to add a large number of clients that exist in a subnet range by configuring a single client object.

Netmask allows you to set the subnet mask in dotted-decimal notation rather than the CIDR notation for the IP address property.

- Netmask—A range of IP addresses defined so that only machines with IP addresses within the range are allowed to access an Internet service.
- CIDR—Classless InterDomain Routing. A protocol which allows the assignment of Class C IP addresses in multiple contiguous blocks.

- Broadcast/Network
- List of IP Addresses/Netmasks—Use the Move Up and Move Down buttons to rearrange the order of the list items. Use the Delete button to delete any IP address or Netmask.

**Step 7** To define an additional protocol that is not a standard predefined one, choose Access Control > Protocol Groups from the left sidebar menu. The protocol groups with their source and destination port and DSCP are displayed.

**Step 8** To create a new protocol group, choose Add Protocol Group from the Select a command drop-down list, and click Go. To view or modify an existing protocol group, click the URL of the group. The Protocol Groups page appears.

**Step 9** The rule name is provided for the existing rules, or you can now enter a name for a new rule. ACLs are not required to have rules defined. When a packet matches all the parameters of a rule, the action for this rule is exercised.

**Step 10** Choose a protocol from the drop-down list:

- Any—All protocols
- TCP—Transmission Control Protocol
- UDP—User Datagram Protocol
- ICMP—Internet Control Message Protocol
- ESP—IP Encapsulating Security Payload
- AH—Authentication Header
- GRE—Generic Routing Encapsulation
- IP—Internet Protocol
- Eth Over IP—Ethernet over Internet Protocol
- Other Port OSPF—Open Shortest Path First
- Other—Any other IANA protocol (http://www.iana.org/)

**Step 11** Some protocol choices (such as TCP or UDP) cause additional Source Port and Dest Port GUI elements to appear.

- Source Port—Specify the source of the packets to which this ACL applies. The choices are Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other, and Port Range.
Dest Port—Specify the destination of the packets to which this ACL applies. The choices are Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other, and Port Range.

Step 12 From the DSCP (Differentiated Services Code Point) drop-down list, choose any or specific. If you choose specific, enter the DSCP (range of 0 to 255).

Note DSCP is a packet header code that can be used to define the quality of service across the Internet.

Step 13 Click Save.

Step 14 You can now create new mappings from the defined IP address groups and protocol groups. To define a new mapping, choose the ACL template to which you want to map the new groups. All ACL mappings appear on the top of the page, and all ACL rules appear on the bottom.

Step 15 To define a new mapping, choose Add Rule Mappings from the Select a command drop-down list. The Add Rule Mapping page appears.

Step 16 Configure the following fields:

- Source IP Group—Predefined groups for IPv4 and IPv6.
- Destination IP Group—Predefined groups for IPv4 and IPv6.
- Protocol Group—Protocol group to use for the ACL.
- Direction—Any, Inbound (from client) or Outbound (to client).
- Action—Deny or Permit. The default filter is to deny all access unless a rule explicitly permits it.

Step 17 Click Add. The new mappings populate the bottom table.

Step 18 Click Save.

Step 19 You can now automatically generate rules from the rule mappings you created. Choose the mappings for which you want to generate rules, and click Generate. This automatically creates the rules. These rules are generated with contiguous sequence. That is, if rules 1 through 4 are already defined and you add rule 29, it is added as rule 5.

Existing ACL templates are duplicated into a new ACL template. This duplication clones all the ACL rules and mappings defined in the source ACL template.

Configuring a FlexConnect Access Control List Template

You can create or modify a FlexConnect ACL template for configuring the type of traffic that is allowed by protocol, and the source or destination of the traffic.

Note The FlexConnect ACLs do not support IPv6 addresses.

- Configuring and Applying a FlexConnect Access Control List, page 11-67
- Deleting a FlexConnect Access Control List, page 11-69

Configuring and Applying a FlexConnect Access Control List

To configure and apply an Access Control List template to a Controller, follow these steps:
Step 1  Choose **Configure > Controller Template Launch Pad**.

Step 2  Click a controller IP address.

Step 3  From the left sidebar menu, choose **Security > Access Control > FlexConnect ACLs**.

Step 4  From the Select a command drop-down list, choose **Add a Template**.

Step 5  Click **Go**.

The New Controller Template page appears.

Step 6  Enter a name for the new FlexConnect ACL in the **FlexConnect ACL Name** text box.

Step 7  Click **Save**.

A FlexConnect ACL template is created. You can now create new mappings from the defined IP address groups and protocol groups. To define a new mapping, choose the ACL template to which you want to map the new groups. All FlexConnect ACL mappings appear on the top of the page, and all FlexConnect ACL rules appear in the bottom.

Step 8  From the Select a command drop-down list, choose **Add Rule Mappings**, and click **Go**.

Step 9  The FlexConnect ACL IP Protocol Map page appears.

Step 10 Configure the following fields:

- **Source IP Group**—Predefined groups for IPv4 and IPv6.
- **Destination IP Group**—Predefined groups for IPv4 and IPv6.
- **Protocol Group**—Protocol group to use for the ACL.
- **Action**—Deny or Permit. The default filter is to deny all access unless a rule explicitly permits it.

Step 11 Click **Add**. The new mappings populate the bottom table.

Step 12 Click **Save**.

Step 13 You can now automatically generate rules from the rule mappings you created. Choose the mappings for which you want to generate rules, and click **Generate**. This automatically creates the rules. These rules are generated with contiguous sequence. That is, if rules 1 through 4 are already defined and you add rule 29, it is added as rule 5.

Existing FlexConnect ACL templates are duplicated into a new FlexConnect ACL template. This duplication clones all the FlexConnect ACL rules and mappings defined in the source FlexConnect ACL template.

Step 14 From the Select a command drop-down list in the FlexConnect ACL page, choose **Apply Templates**.

The Apply to Controllers page appears.

Step 15 Select **Save Config to Flash after apply** check box to save the configuration to Flash after applying the FlexConnect ACL to the controller.

Step 16 Select **Reboot Controller after apply** to reboot the controller once the FlexConnect ACL is applied. This check box is available only when you select the Save Config to Flash after apply check box.

Step 17 Select one or more controllers and click **OK** to apply the FlexConnect ACL template.

The FlexConnect ACL that you created appears in **Configure > Controller Template Launch Pad > IP Address > Security > Access Control > FlexConnect ACLs**.
Deleting a FlexConnect Access Control List

To delete a FlexConnect ACL, follow these steps:

**Step 1** Choose Configure > Controllers.

**Step 2** Click a controller IP address.

**Step 3** From the left sidebar menu, choose Security > FlexConnect ACLs.

**Step 4** From the FlexConnect ACLs page, select one or more FlexConnect ACLs to delete.

**Step 5** From the Select a command drop-down list, choose Delete FlexConnect ACLs.

**Step 6** Click Go.

Configuring an ACL IP Groups Template

To create reusable grouped IP addresses, follow these steps:

**Step 1** Choose Configure > Controller Template Launch Pad.

**Step 2** Choose Security > Access Control > IP Groups from the left sidebar menu.

**Step 3** All the IP address including IPv4 and IPv6 groups are listed. One IP address group can have a maximum of 128 IP address and netmask combinations. To define a new IP address group, choose Add IP Group or Add IPv6 Group from the Select a command drop-down list, and click Go.

| **Note** | For the IP address of any, an any group is predefined. |

| **Note** | For the IPv6 address of any, an any group is predefined with an IP address type as IPv6. |

**Step 4** Configure the following fields:

- IP Group Name
- IP Address—For IP Group, enter an IPv4 address format. For IPv6 groups, enter an IPv6 address format.
- Netmask OR CIDR Notation—Enter the Netmask or CIDR Notation and then click Add. The list of IP addresses or Netmasks appears in the List of IP Addresses/Netmasks text box.

| **Note** | These fields are not applicable for IPv6 groups. |

CIDR notation allows the user to add a large number of clients that exist in a subnet range by configuring a single client object.

Netmask allows the user to set the subnet mask in dotted-decimal notation rather than the CIDR notation for the IP address property.

- Netmask—A range of IP addresses defined so that only machines with IP addresses within the range are allowed to access an Internet service.
- CIDR—Classless InterDomain Routing. A protocol which allows the assignment of Class C IP addresses in multiple contiguous blocks.

- Broadcast/Network

  **Note** These fields are not applicable for IPv6 groups.

- Prefix Length—Prefix for IPv6 addresses, ranging from 0 to 128.

- List of IP Addresses/Netmasks—Use the Move Up and Move Down buttons to rearrange the order of the list items. Use the Delete button to delete an IP address or Netmask.

**Step 5** Click **Save**. Once saved, the IP Group appears in the Template List page.

You can create new mappings from the defined IP address groups and protocol groups. To define a new mapping, choose the ACL template to which you want to map the new groups. All ACL mappings appear in the top of the page, and all ACL rules appear in the bottom. See the “Configuring an Access Control List Template” section on page 11-65 for more information.

See the “Configuring an ACL Protocol Groups Template” section on page 11-70 for information on defining Protocol Groups.

---

### Configuring an ACL Protocol Groups Template

To define an additional protocol that is not a standard predefined one, follow these steps:

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Choose **Access Control > Protocol Groups** from the left sidebar menu.

**Step 3** Configure the following fields:

- **Rule Name**—The rule name is provided for the existing rules, or you can now enter a name for a new rule. ACLs are not required to have rules defined. When a packet matches all the fields of a rule, the action for this rule is exercised.

  **Note** See the “Configuring an Access Control List Template” section on page 11-65 for more information on ACLs.

- **Protocol**—Choose a protocol from the drop-down list:
  - Any—All protocols
  - TCP—Transmission Control Protocol
  - UDP—User Datagram Protocol
  - ICMP—Internet Control Message Protocol
  - ESP—IP Encapsulating Security Payload
  - AH—Authentication Header
  - GRE—Generic Routing Encapsulation
  - IP—Internet Protocol
  - Eth Over IP—Ethernet over Internet Protocol
Chapter 11 Using Templates

Configuring Controller Templates

- Other Port OSPF—Open Shortest Path First
- Other—Any other IANA protocol (http://www.iana.org/)

- Source Port—Can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.

- Dest Port—Destination port. If TCP or UDP is selected, can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.

- DSCP (Differentiated Services Code Point)—Choose Any or Specific from the drop-down list. If Specific is selected, enter the DSCP (range of 0 through 255).

### Note

DSCP is a packet header code that can be used to define the quality of service across the Internet.

**Step 4**

Click **Save**. Once saved, the IP Group displays in the Template List page.

You can create new mappings from the defined IP address groups and protocol groups. To define a new mapping, choose the ACL template to which you want to map the new groups. All ACL mappings appear in the top of the page, and all ACL rules appear in the bottom. See the “Configuring an Access Control List Template” section on page 11-65 for more information.

See the “Configuring an ACL IP Groups Template” section on page 11-69 for information on defining IP Groups.

---

**Configuring Security - CPU Access Control List Templates**

**Note**

CPU ACL configuration with IPv6 is not supported in this release because all IP addresses of controllers on interfaces use IPv4 except the virtual interface.

**Configuring a CPU Access Control List (ACL) Template**

The existing ACLs established in the “Configuring an Access Control List Template” section on page 11-65 is used to set traffic controls between the Central Processing Unit (CPU) and Network Processing Unit (NPU).

To add or modify an existing CPU ACL template, follow these steps:

**Step 1**

Choose **Configure > Controller Template Launch Pad**.

**Step 2**

Click **CPU Access Control Lists** or choose **Security > CPU Access Control > CPU Access Control List** from the left sidebar menu. The Security > CPU Access Control List page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.
The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The CPU Access Control List template page appears.

**Step 4** If you select the check box to enable CPU ACL, two more fields appear. When CPU ACL is enabled and applied on the controller, Prime Infrastructure displays the details of the CPU ACL against that controller.

**Step 5** From the ACL Name drop-down list, choose a name from the list of defined names.

**Step 6** From the CPU ACL Mode drop-down list, choose which data traffic direction this CPU ACL list controls. The choices are the wired side of the data traffic, the wireless side of the data traffic, or both wired and wireless.

**Step 7** Click Save.

---

**Configuring Security - Rogue Templates**

- Configuring a Rogue Policies Template, page 11-72
- Configuring a Rogue AP Rules Template, page 11-73
- Configuring a Rogue AP Rule Groups Template, page 11-75
- Configuring a Friendly Access Point Template, page 11-76

**Configuring a Rogue Policies Template**

This page enables you to configure the rogue policy (for access points and clients) applied to the controller.

To add or modify an existing template, follow these steps:

**Step 1** Choose Configure > Controller Template Launch Pad.

**Step 2** Click Rogue Policies or choose Security > Rogue > Rogue Policies from the left sidebar menu. The Security > Rogue Policy Setup page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Rogue Policies template page appears.

**Step 4** Determine whether or not the Rogue Location Discovery Protocol (RLDP) is connected to the enterprise wired network. Choose one of the following from the drop-down list:
### Configuring Controller Templates

- **Disable**—Disables RLDP on all access points.
- **All APs**—Enables RLDP on all access points.
- **Monitor Mode APs**—Enables RLDP only on access points in monitor mode.

**Note**

With RLDP, the controller instructs a managed access point to associate with the rogue access point and sends a special packet to the controller. If the controller receives the packet, the rogue access point is connected to the enterprise network. This method works for rogue access points that do not have encryption enabled.

**Step 5**
Set the expiration timeout (in seconds) for rogue access point entries.

**Step 6**
In the Rogue Detection Report Interval text box, enter the time interval in seconds at which the APs should send the rogue detection report to the controller. A valid range is 10 seconds to 300 seconds, and the default value is 10 seconds. This feature is applicable to APs that are in monitor mode only.

**Step 7**
In the Rogue Detection Minimum RSSI text box, enter the minimum RSSI value that a rogue should have for the APs to detect and for the rogue entry to be created in the controller. A valid range is -70 dBm to -128 dBm, and the default value is -128 dBm. This feature is applicable to all the AP modes.

**Note**

There can be many rogues with very weak RSSI values that do not provide any valuable information in the rogue analysis. Therefore, you can use this option to filter the rogues by specifying the minimum RSSI value at which the APs should detect rogues.

**Step 8**
In the Rogue Detection Transient Interval text box, enter the time interval at which a rogue has to be consistently scanned for by the AP after the first time the rogue is scanned. By entering the transient interval, you can control the time interval at which the AP should scan for rogues. The APs can filter the rogues based on their transient interval values. Valid range is between 120 seconds to 1800 seconds, and the default value is 0. This feature is applicable to APs that are in monitor mode only.

**Step 9**
Select the **Validate rogue clients against AAA** check box to enable the AAA validation of rogue clients.

**Step 10**
Select the **Detect and report Adhoc networks** check box to enable detection and reporting of rogue clients participating in ad hoc networking.

**Step 11**
Click **Save**.

---

### Configuring a Rogue AP Rules Template

Rogue access point rules allow you to define rules to automatically classify rogue access points. Prime Infrastructure applies the rogue access point classification rules to the controllers. These rules can limit the appearance of a rogue on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time). Rogue access point rules also help reduce false alarms.

**Note**

The new enhancements to the role classification rule are applicable for Cisco WLC 7.4 and later. These enhancements are not applicable to Catalyst 3850, Catalyst 3650, Catalyst 4500 switches, and Cisco 5760 WLAN Controllers (WLC).
To view current classification rule templates, rule type, and the number of controllers to which they are applied, choose **Configure > Controller Template Launch Pad > Security > Rogue > Rogue AP Rules**. If you want to view rogue access point rules, see the “**Viewing or Editing Rogue Access Point Rules**” section on page 9-204.

**Note**

Rogue classes include the following types:
- **Malicious Rogue**—A detected access point that matches the user-defined malicious rules or has been manually moved from the Friendly AP category.
- **Friendly Rogue**—Known, acknowledged, or trusted access point or a detected access point that matches user-defined friendly rules.
- **Unclassified Rogue**—A detected access point that does not match the malicious or friendly rules.

To add or create a new classification rule template for rogue access points, follow these steps:

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** From the left sidebar menu, choose **Security > Rogue > Rogue AP Rules**. The Rogue AP Rules Controller template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** From the Select a command drop-down list, choose **Add Classification Rule**, and click **Go**. The Rogue AP Rules > New Template page appears. To modify an existing rogue access point rules template or to apply a current template to the controllers, choose **Configure > Controller Template Launch Pad > Security > Rogue > Rogue AP Rules**, and click a template name.

**Step 4** In the General group box, configure the following fields:

- **Rule Name**—Enter a name for the rule in the text box.
- **Rule Type**—Choose **Malicious**, **Friendly**, or **Custom** from the drop-down list. A rogue is considered malicious if a detected access point matches the user-defined malicious rules or has been manually moved from the Friendly AP category. A rogue is considered friendly if it is a known, acknowledged, or trusted access point or a detected access point that matches the user-defined friendly rules. To define a user-defined classification type, choose Custom from the drop-down list.
- **Notify**—Choose **Global**, **Local**, **None**, or **All** from the drop-down list.
  - **Global**—Trap information is sent only to Prime Infrastructure.
  - **Local**—Trap information is sent only to controller.
  - **None**—Trap information is not sent.
  - **All**—Trap information is sent to Prime Infrastructure and controller.
- **State**—Use the drop-down list to choose from **Contain**, **Alert**, or **Delete**.
- **Match Type**—Choose **Match All Conditions** or **Match Any Condition** from the drop-down list.
- **Severity Score** (for Custom rule type only)—Specify the severity score. The Custom Rogue AP severity is based on Severity Score Value.
- **Classification Name** (for Custom rule type only)—Specify the classification name for the custom classification rule.
Step 5 In the Rogue Classification Rule group box of the page, configure the following fields.

- Open Authentication—Select the check box to enable open authentication.
- Match Managed AP SSID—Select the check box to enable the matching of a Managed AP SSID.

**Note** Managed SSIDs are the SSIDs configured for the WLAN and known to the system.

- Match User Configured SSID—Select the check box to enable the matching of User Configured SSIDs.

**Note** User Configured SSIDs are the SSIDs that are manually added. Enter the User Configured SSIDs (one per line) in the Match User Configured SSID text box.

- Match Wildcard Configured SSID—Select the check box to enable the matching of Wildcard Configured SSIDs. You can use wildcards (*).

- Minimum RSSI—Select the check box to enable the Minimum RSSI threshold limit.

**Note** Enter the minimum RSSI threshold level (dB) in the text box. The detected access point is classified as malicious if it is detected above the indicated RSSI threshold.

- Time Duration—Select the check box to enable the Time Duration limit.

**Note** Enter the time duration limit (in seconds) in the text box. The detected access point is classified as malicious if it is viewed for a longer period of time than the indicated time limit.

- Minimum Number Rogue Clients—Select the check box to enable the Minimum Number Rogue Clients limit. Enter the minimum number of rogue clients allowed. The detected access point is classified as malicious if the number of clients associated to the detected access point is greater than or equal to the indicated value.

Step 6 Click Save.

---

**Configuring a Rogue AP Rule Groups Template**

A rogue access point rule group template allows you to combine more than one rogue access point rule to controllers.

To view current rogue access point rule group templates or create a new rule group, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Rogue AP Rule Groups** or choose **Security > Rogue > Rogue AP Rule Groups** from the left sidebar menu.

Step 3 From the Select a command drop-down list, click **Add Rogue Rule Group**.

Step 4 Click Go. The Rogue AP Rule Groups > New Template page appears.
Configuring Controller Templates

To modify an existing rogue policy template or to apply a current template to controllers, choose Configure > Controller Template Launch Pad > Security > Rogue > Rogue AP Rule Groups and click a template name. Make the necessary changes to the template, and click Save or Apply to Controllers.

**Step 5** Enter a name for the rule group in the General group box of the page.

**Step 6** To add a Rogue AP rule, click to highlight the rule in the left column. Click Add to move the rule to the right column.

**Note** Rogue access point rules can be added from the Rogue Access Point Rules section. See the “Configuring a Rogue AP Rules Template” section on page 11-73 for more information.

**Step 7** To remove a rogue access point rule, click to highlight the rule in the right column. Click Remove to move the rule to the left column.

**Step 8** Use the Move Up/Move Down buttons to specify the order in which the rules apply. Highlight the desired rule and click Move Up or Move Down to move it higher or lower in the current list.

**Step 9** Click Save to confirm the rogue access point rule list.

**Step 10** Click Cancel to close the page without making any changes to the current list.

**Note** To view and edit the rules applied to a controller, choose Configure > Controller, and click the controller name.

Configuring a Friendly Access Point Template

This template allows you to import friendly internal access points. Importing these friendly access points prevents non-lightweight access points from being falsely identified as rogues.

**Note** Friendly Internal access points were previously referred to as Known APs.

**Note** The Friendly AP page identifies the MAC address of an access point, status, any comments, and whether or not the alarm is suppressed for this access point.

To view or edit the current list of friendly access points, follow these steps:

**Step 1** Choose Configure > Controller Template Launch Pad.

**Step 2** Click Friendly AP or choose Security > Rogue > Friendly AP from the left sidebar menu.

**Step 3** From the Select a command drop-down list, choose Add Friendly.

**Step 4** Click Go. The Friendly AP page appears.
Note To modify an existing friendly access point, choose Configure > Controller Template Launch Pad > Security > Rogue > Friendly Internal, and click the MAC address of an access point. Make the necessary changes to the access point, and click Save.

Step 5 Friendly access points can be added by either importing the access point or manually entering the access point information:

- To import an access point using the Import feature do the following:
  - Select the Import from File check box.
  - Enter the file path or click Browse to navigate to the correct file.

Note Use a line break to separate MAC addresses. For example, enter the MAC addresses as follows:

```
00:00:11:22:33:44
00:00:11:22:33:45
00:00:11:22:33:46
```

- To manually add an access point, do the following:
  - Unselect the Import from File check box.
  - Enter the MAC address for the access point.
  - Choose Internal access point from the Status drop-down list.
  - Enter a comment regarding this access point, if necessary.
  - Select the Suppress Alarms check box to suppress all alarms for this access point.
- Click Save to confirm this access point or Cancel to close the page without adding the access point to the list.

Configuring Ignored Rogue AP Templates

The Ignored Rogue AP Template page allows you to create or modify a template for importing ignored access points. Access points in the Ignored AP list are not identified as rogues.

Note An Ignored Rogue AP template does not get applied to any controller. It suppresses the Rogue AP/Adhoc alarm if Ignored Rogue AP Template has the Rogue MAC Address when the controller reports the Rogue AP to Prime Infrastructure and this MAC address is added to the Rogue AP Ignore-List on the controller.

To add or edit the Ignored Rogue access points, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.
Step 2 Click Ignored Rogue AP or choose Security > Rogue > Ignored Rogue AP from the left sidebar menu.
Step 3 From the Select a command drop-down list, choose Add Ignored Rogue AP.
Step 4 Click Go. The Ignored Rogue AP page appears.
Step 5 The Ignored Rogue access points can be added by either importing the access point or manually entering the access point information:

- To import an ignored rogue access point using the Import feature:
  - Select the Import from File check box.
  - Enter the file path or use the Browse button to navigate to the correct file. The import file must be a CSV file with MAC address (one MAC Address per line).

  **Note** For example, enter the MAC addresses as follows:
  00:00:11:22:33:44
  00:00:11:22:33:45
  00:00:11:22:33:46

- To manually add an ignored rogue access point:
  - Unselect the Import from File check box.
  - Enter the MAC address and comment for the rogue access point.

- Click Save to confirm this access point or Cancel to close the page without adding the ignored rogue access point to the list.

  **Note** To modify an existing friendly access point, choose Configure > Controller Template Launch Pad > Security > Rogue > Ignored Rogue AP, and click the MAC address of the ignored rogue access point. Make the necessary changes, and click Save.

  **Note** If you remove the MAC address from the Ignored AP list, the MAC address is removed from the Rogue AP Ignore-List on the controller.

Configuring 802.11 Templates

- Configuring Load Balancing Templates, page 11-78
- Configuring Band Selection Templates, page 11-79
- Configuring Media Parameters Controller Templates (802.11a/n), page 11-85

### Configuring Load Balancing Templates

To configure load balancing templates, follow these steps:

**Step 1** Choose Configure > Controller Template Launch Pad.

**Step 2** Click Load Balancing or choose 802.11 > Load Balancing from the left sidebar menu. The Load Balancing page appears.

**Step 3** Enter a value between 1 and 20 for the client window size. The page size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:
load-balancing page + client associations on AP with lightest load = load-balancing threshold

In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client page size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.

**Step 4** Enter a value between 0 and 10 for the max denial count. The denial count sets the maximum number of association denials during load balancing.

**Step 5** Click **Save**.

---

**Configuring Band Selection Templates**

To configure band selection templates, follow these steps:

**Step 1** Choose Configure > Controller Template Launch Pad.

**Step 2** Click **Band Select** or choose **802.11 > Band Select** from the left sidebar menu. The Band Select page appears.

**Step 3** Enter a value between 1 and 10 for the probe cycle count. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.

**Step 4** 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 5** Enter a value between 10 and 200 seconds for the age out suppression field. Age-out suppression sets the expiration time for pruning previously known 802.11b/g clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.

**Step 6** Enter a value between 10 and 300 seconds for the age out dual band field. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 60 seconds. After this time elapses, clients become new and are subject to probe response suppression.

**Step 7** Enter a value between –20 and –90 dBm for the acceptable client RSSI field. This field sets the minimum RSSI for a client to respond to a probe. The default value is –80 dBm.

**Step 8** Click **Save**.

---

**Configuring Preferred Call Templates**

This page enables you to create or modify a template for configuring Preferred Call.

To add or modify preferred call templates, follow these steps:

**Step 1** Choose Configure > Controller Template Launch Pad.

**Step 2** Click **Preferred Call** or choose **802.11 > Preferred Call** from the left sidebar menu. The Preferred Call Controller Templates page appears.
Step 3  If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The New Controller Template page appears.

Step 4  Configure the following Preferred Call parameters:

- **Template Name**
  
  | Note | Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes. |

- **Number Id**—Enter a value to identify the preferred number. You can have a maximum of six preferred call numbers. The valid range is from 1 to 6. The default value is 1.
- **Preferred Number**—Enter the preferred call number.

Step 5  Click **Save**.

### Configuring Media Stream for Controller Templates (802.11)

To configure the media stream for a controller template for an 802.11 Radio, follow these steps:

Step 1  Choose **Configure > Controller Template Launch Pad**.

Step 2  In the **802.11** group box, click **New** beside Media Stream. The New Controller Template page appears.

Step 3  In the General group box, specify an appropriate name for the template.

| Note | Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes. |

Step 4  In the Media Stream Configuration group box, specify the following fields:

- **Media Stream Name**
- **Multicast Destination Start IP**—Start IP address of the media stream to be multicast.
- **Multicast Destination End IP**—End IP address of the media stream to be multicast.

| Note | Start IP and End IP can be IPv4 or IPv6 multicast address from controller Release 7.2.x. |

- **Maximum Expected Bandwidth**—Maximum bandwidth that a media stream can use.

Step 5  In the Resource Reservation Control (RRC) Parameters group box, specify the following fields:

- **Average Packet Size**—Average packet size that a media stream can use.
- **RRC Periodical Update**—Resource Reservation Control calculations that are updated periodically; if disabled, RRC calculations are done only once when a client joins a media stream.
- **RRC Priority**—Priority of RRC with the highest at 1 and the lowest at 8.
- **Traffic Profile Violation**—Appears if the stream is dropped or put in the best effort queue if the stream violates the QoS video profile.
- **Policy**—Appears if the media stream is admitted or denied.
Step 6  Click Save.

Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the “Applying Controller Templates” section on page 11-2 for more information.

### Configuring RF Profiles Templates (802.11)

The RF Profiles page enables you to create or modify RF profiles that get associated to AP Groups.

To configure a RF Profile for a controller template for an 802.11 Radio, follow these steps:

**Step 1** Choose Configure > Controller Template Launch Pad.

**Step 2** Click RF Profiles or choose either 802.11 > RF Profiles from the left sidebar menu. The RF Profiles page appears.

**Step 3** From the Select a command drop-down list, choose Add Template.

**Step 4** Click Go. The New Controller template page appears.

**Step 5** Configure the following information:

- General
  - Template Name—User-defined name for the template.
  - Profile Name—User-defined name for the current profile.
  - Description—Description of the template.
  - Radio Type—The radio type of the access point. This is a drop-down list from which you can choose an RF profile for APs with 802.11a or 802.11b radios.

- TPC (Transmit Power Control)
  - Minimum Power Level Assignment (-10 to 30 dBm)—Indicates the minimum power assigned. Range: -10 to 30 dBm Default: -10 dBm.
  - Maximum Power Level Assignment (-10 to 30 dBm)—Indicates the maximum power assigned. Range: -10 to 30 dBm Default: 30 dBm.
  - Power Threshold v1(-80 to -50 dBm)—Indicates the transmitted power threshold.
  - Power Threshold v2(-80 to -50 dBm)—Indicates the transmitted power threshold.

- Data Rates—Use the Data Rates drop-down lists to specify the rates at which data can be transmitted between the access point and the client. These data rates are available:
  - 802.11a—6, 9, 12, 18, 24, 36, 48, and 54 Mbps.
  - 802.11b/g—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps

For each data rate, choose one of these options:

- Mandatory—Clients must support this data rate to associate to an access point on the controller.
- Supported—Any associated clients that support this data rate might communicate with the access point using that rate. However, the clients are not required to be able to use this rate to associate.
- Disabled—The clients specify the data rates used for communication.
• Band Select—The Band Select feature enables you to balance client distribution among both serving radios when APs are serving hundreds of clients in a dense auditorium or stadium sites. Band Select discovers the client capabilities to verify whether client can associate on both 2.4 GHz and 5Ghz spectrum. Enabling band select on a WLAN, forces AP to do a probe suppression on 2.4GHz that ultimately moves dual band clients to 5Ghz spectrum. In the Band Select group box, specify the following:
  - Probe Response
  - Cycle Count(1 to 10 Cycles)
  - Cycle Threshold(1 to 1000 msecs)
  - Suppression Expire(10 to 200 secs)
  - Dual Band Expire(10 to 300 secs)
  - Client RSSI(-90 to -20 dBm)

• High Density Configurations
  - Maximum Clients—Specify the maximum number of clients

• Multicast Configurations
  - Multicast Data Rate—From the Multicast Data Rate drop-down list, choose the data rate. The value “auto” indicates that the AP automatically adjusts data rate with client.

• Coverage Hole Detection
  - Data RSSI(-90 to -60 dBm)—Enter the minimum receive signal strength indication (RSSI) value for data packets received by the access point. The value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. If the access point receives a packet in the data queue with an RSSI value below the value that you enter here, a potential coverage hole has been detected. The valid range is –90 to –60 dBm, and the default value is –80 dBm. The access point takes data RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.
  - Voice RSSI(-90 to -60 dBm)—Enter the minimum receive signal strength indication (RSSI) value for voice packets received by the access point. The value that you enter is used to identify coverage holes within your network. If the access point receives a packet in the voice queue with an RSSI value below the value that you enter here, a potential coverage hole has been detected. The valid range is –90 to –60 dBm, and the default value is –75 dBm. The access point takes voice RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.
  - Coverage Exception(1 to 75 Clients)—Enter the minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold. The valid range is 1 to 75, and the default value is 3.
  - Coverage Level(0 to 100 %)—In the Coverage Exception Level per AP text box, enter the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point. The valid range is 0 to 100%, and the default value is 25%.

• Load Balancing
  - Window(0 to 20 Clients)—Enter a value between 1 and 20. The window size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations.
  - Denial(1 to 10)—Enter a value between 0 and 10. The denial count sets the maximum number of association denials during load balancing.
Configuring Controller Templates

Configuring SIP Snooping

Keep the following guidelines in mind when using SIP Snooping:

- SIPs are available only on the Cisco 5500 Series Controllers and on the 1240, 1130, and 11n access points.
- SIP CAC should only be used for phones that support status code 17 and do not support TSPEC-based admission control.
- SIP CAC will be supported only if SIP snooping is enabled.

To configure SIP Snooping for a controller, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.
Step 2 Click SIP Snooping or choose either 802.11 > SIP Snooping from the left sidebar menu.
Step 3 From the Select a command drop-down list, choose Add Template.
Step 4 Click Go. The New Controller template page appears.
Step 5 Configure the following fields:
  - Port Start
  - Port End
Step 6 Click Save.

Note If single port is to be used, configure both start and end port fields with same number.

Configuring Radio Templates (802.11a/n)

- Configuring 802.11a/n Parameters Templates, page 11-83
- Configuring Media Parameters Controller Templates (802.11a/n), page 11-85
- Configuring EDCA Parameters Through a Controller Template (802.11a/n), page 11-88
- Configuring a Roaming Parameters Template (802.11a/n), page 11-88
- Configuring an 802.11h Template, page 11-90
- Configuring a High Throughput Template (802.11a/n), page 11-90
- Configuring CleanAir Controller Templates (802.11a/n), page 11-91

Configuring 802.11a/n Parameters Templates

To add or modify radio templates, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.
Step 2  Click **Parameters** or choose either *802.11a/n > Parameters* from the left sidebar menu. The 802.11a/n Parameters template page appears and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the 802.11 network status and the channel and power mode. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3  If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n Parameters template page appears.

Step 4  Select the check box if you want to enable 802.11a/n network status.

Step 5  Use the ClientLink drop-down list to enable Clientlink on all access point 802.11a/n radios that support ClientLink. Otherwise, choose **Disable**.

Step 6  Enter a transmitted power threshold between -50 and -80.

Step 7  Enter the amount of time between beacons in kilomicroseconds. The valid range is from 20 to 1000 milliseconds.

Step 8  Enter the number of beacon intervals that might elapse between transmission of beacon frames containing a traffic indicator message (TIM) element whose delivery count text box is 0. This value is transmitted in the DTIM period field of beacon frames. When client devices receive a beacon that contains a DTIM, they normally wake up to check for pending packets. Longer intervals between DTIMS let clients sleep longer and preserve power. Conversely, shorter DTIM periods reduce the delay in receiving packets but use more battery power because clients wake up more often.

Step 9  In the Fragmentation Threshold field, determine the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference.

Step 10 Enter the percentage for 802.11e maximum bandwidth.

Step 11 Click if you want short preamble enabled.

Step 12 From the Dynamic Assignment drop-down list, choose one of three modes:

- **Automatic**—The transmit power is periodically updated for all access points that permit this operation.
- **On Demand**—Transmit power is updated when the Assign Now button is selected.
- **Disabled**—No dynamic transmit power assignments occur, and values are set to their global default.

Step 13 Determine if you want to enable Dynamic Tx Power Control. The power levels and available channels are defined by the country code setting and are regulated on a country by country basis.

Step 14 The Assignment Mode drop-down list has three dynamic channel modes:

- **Automatic**—The channel assignment is periodically updated for all access points that permit this operation. This is also the default mode.
- **On Demand**—Channel assignments are updated when desired.
- **OFF**—No dynamic channel assignments occur, and values are set to their global default.

Step 15 Select the **Avoid Foreign AP Interference** check box if you want to enable it. Enable this field to have RRM consider interference from foreign Cisco access points (those non-Cisco access points outside RF/mobility domain) when assigning channels. This Radio Resource Management (RRM) field monitors foreign 802.11 interference. Unselect this check box to have RRM ignore this interference.
In certain circumstances with significant interference energy (dB) and load (utilization) from foreign access points, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the foreign access points. This increases capacity and reduces variability for the Cisco WLAN Solution.

**Step 16** Select the **Avoid Cisco AP Load** check box if you want it enabled. Enable this RRM bandwidth-sensing field to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points. Unselect this check box to have RRM ignore this value.

In certain circumstances and with denser deployments, there might not be enough channels to properly create perfect channel reuse. In these circumstances, RRM can assign better reuse patterns to those access points that carry more traffic load.

**Step 17** Select the **Avoid non 802.11 Noise** check box if you want to enable it. Enable this RRM noise-monitoring field to have access points avoid channels that have interference from non-access point sources, such as microwave ovens or Bluetooth devices. Unselect this check box to have RRM ignore this interference.

In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources. This increases capacity and reduces variability for the Cisco WLAN Solution.

**Step 18** The Signal Strength Contribution check box is always enabled (not configurable). RRM constantly monitors the relative location of all access points within the RF/mobility domain to ensure near-optimal channel reuse. The net effect is an increase in Cisco WLAN Solution capacity and a reduction in co-channel and adjacent channel interference.

**Step 19** The client and controller negotiate data rates between them. If the data rate is set to Mandatory, the client must support it to use the network. If a data rate is set as Supported by the controller, any associated client that also supports that same rate might communicate with the access point using that rate. However, it is not required that a client uses all the rates marked supported to associate. For each rate, a drop-down list of Mandatory or Supported is available. Each data rate can also be set to Disabled to match client settings.

**Step 20** From the Channel List drop-down list in the Noise/Interference/Rogue Monitoring Channels section, choose between **all channels**, **country channels**, or **DCA channels** based on the level of monitoring you want. Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation amongst a set of managed devices connected to the controller.

**Step 21** The location measurement interval of the Cisco-compatible Extension can only be changed when measurement mode is enabled to broadcast radio measurement requests. When enabled, this enhances the location accuracy of clients.

**Step 22** Click **Save**.

---

**Configuring Media Parameters Controller Templates (802.11a/n)**

This page enables you to create or modify a template for configuring 802.11a/n voice fields such as call admission control and traffic stream metrics.

To add a new template with 802.11a/n voice fields information (such as Call Admission Control and traffic stream metrics) for a controller, follow these steps:

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **New** beside the template you want to add.
Configuring Controller Templates

**Step 3** Specify an appropriate name for the template.

*Note* Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

**Step 4** On the Voice tab, configure the following fields:

- **Admission Control (ACM)**—Select the check box to enable admission control.
  
  For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, call admission control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keep the maximum allowed number of calls to an acceptable quantity.

- **CAC Method**—If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static.
  
  Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

- **Maximum Bandwidth Allowed**—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled. For controller versions 6.0.188.0 and earlier, the valid range is 40 to 85. For controller versions 6.0.188.1 and later, the valid range is 5 to 85, and the default is 75.

- **Reserved Roaming Bandwidth**—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled. The valid range is 0 to 25, and the default is 6.

- **Expedited Bandwidth**—Select the check box to enable expedited bandwidth as an extension of CAC for emergency calls.
  
  You must have an expedited bandwidth IE that is CCXv5 compliant so that a TSPEC request is given higher priority.

- **SIP CAC**—Select the check box to enable SIP CAC.
  
  SIP CAC should be used only for phones that support status code 17 and do not support TSPEC-based admission control.

- **SIP Codec**—Specify the codec name you want to use on this radio. The available options are **G.711**, **G.729**, and **User Defined**.

- **SIP Call Bandwidth**—Specify the bandwidth in kilobits per second that you want to assign per SIP call on the network. This field can be configured only when the SIP Codec selected is User Defined.

- **SIP Sample Interval**—Specify the sample interval in milliseconds that the codec must operate in.

- **Max Number of Calls per Radio**—Specify the maximum number of calls per Radio.

- **Metric Collection**—Select the check box to enable metric collection.
  
  Traffic stream metrics are a series of statistics about VoIP over your wireless LAN which inform you of the QoS of the wireless LAN. For the access point to collect measurement values, traffic stream metrics must be enabled. When this is enabled, the controller begins collecting statistical data every 90 seconds for the 802.11b/g interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.

**Step 5** On the Video tab, configure the following fields:
• Admission Control (ACM)—Select the check box to enable admission control.

• Maximum Bandwidth—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled. For controller versions 6.0.188.0 and earlier, the valid range is 0 to 100. For controller versions 6.0.188.1 and later, the valid range is 5 to 85.

• Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled. The valid range is 0 to 25.

• Static CAC method—From the SIP Codec drop-down list, choose one of the following options to set the CAC method. The default value is G.711. The options are as follows:
  – Load-Based
  – Static

  **Note** Static CAC method is radio based and load-based CAC method is channel based

• SIP CAC—Select the SIP CAC check box to enable Static CAC support. By default, this check box is disabled.

  **Note** SIP CAC will be supported only if SIP snooping is enabled.

• Unicast Video Redirect—Select the **Unicast Video Redirect** check box to enable all non-media stream packets in video queue are redirected to the best effort queue. If disabled, all packets with video marking are kept in video queue.

• Client Minimum Phy Rate—Specify the physical data rate required for the client to join a media stream from the Client Minimum Phy Rate drop-down list.

• Multicast Direct Enable—Select the **Multicast Direct Enable** check box to set the Media Direct for any WLAN with Media Direct enabled on a WLAN on this radio.

• Maximum Number of Streams per Radio—Specify the maximum number of streams per Radio to be allowed.

• Maximum Number of Streams per Client—Specify the maximum number of streams per Client to be allowed.

• Best Effort QOS Admission—Select the **Best Effort QOS Admission** check box to redirect new client requests to the best effort queue. This happens only if all the video bandwidth has been used.

  **Note** If disabled and maximum video bandwidth has been used, then any new client request is rejected.

**Step 6** On the General tab, specify the following field:

• Maximum Media Bandwidth (0 to 85%)—Specify the percentage of maximum of bandwidth allowed. This option is only available when CAC is enabled.

**Step 7** Click **Save**.

Once saved, the template appears in the Template List page. In the Template List page, you can apply this template to controllers. See the “**Applying Controller Templates**” section on page 11-2 for more information.
Configuring EDCA Parameters Through a Controller Template (802.11a/n)

Enhanced distributed channel access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality of service (QoS) traffic.

To add or configure 802.11a/n EDCA parameters through a controller template, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.

Step 2 Click EDCA Parameters or choose 802.11a/n > EDCA Parameters from the left sidebar menu. The EDCA Parameters template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the EDCP profile and the low latency MAC. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The 802.11a/n EDCA Parameters template page appears.

Step 4 Choose one of the following options from the EDCA Profile drop-down list:
- WMM—Enables the Wi-Fi Multimedia (WMM) default parameters. This is the default value. Choose this option when voice or video services are not deployed on your network.
- Spectralink Voice Priority—Enables Spectralink voice priority parameters. Choose this option if Spectralink phones are deployed on your network to improve the quality of calls.
- Voice Optimized—Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than Spectralink are deployed on your network.
- Voice & Video Optimized—Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.

**Note** Video services must be deployed with admission control (ACM). Video services without ACM are not supported.

**Note** You must shut down radio interface before configuring EDCA Parameters.

Step 5 Select the Low Latency MAC check box to enable this feature.

**Note** Enable low latency MAC only if all clients on the network are WMM compliant.

Configuring a Roaming Parameters Template (802.11a/n)

To add or modify an existing roaming parameter template, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.
**Step 2** Click **Roaming Parameters** or choose **802.11a/n > Roaming Parameters** from the left sidebar menu. The Roaming Parameters template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the minimum RSSI, roaming hysteresis, adaptive scan threshold, and transition time. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n Roaming Parameters template page appears.

**Step 4** Use the Mode drop-down list to choose one of the configurable modes: default values and custom values. When the default values option is chosen, the roaming parameters are unavailable with the default values displayed in the text boxes. When the custom values option is selected, the roaming parameters can be edited in the text boxes. To edit the parameters, continue to Step 5.

**Step 5** In the Minimum RSSI field, enter a value for the minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point. If the average received signal power of the client dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.

Range: -80 to -90 dBm
Default: -85 dBm

**Step 6** In the Roaming Hysteresis field, enter a value to indicate how strong the signal strength of a neighboring access point must be for the client to roam to it. This field is intended to reduce the amount of ping ponging between access points if the client is physically located on or near the border between two access points.

Range: 2 to 4 dB
Default: 2 dB

**Step 7** In the Adaptive Scan Threshold field, enter the RSSI value from the associated access point of the client, below which the client must be able to roam to a neighboring access point within the specified transition time. This field also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold.

Range: -70 to -77 dB
Default: -72 dB

**Step 8** In the Transition Time field, enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the associated access point of the client is below the scan threshold.

The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

Range: 1 to 10 seconds
Default: 5 seconds
Step 9  Click **Save**.

**Configuring an 802.11h Template**

802.11h informs client devices about channel changes and can limit the transmit power of the client device. Create or modify a template for configuration 802.11h parameters (such as power constraint and channel controller announcement) and applying these settings to multiple controllers.

To add or modify an 802.11h template, follow these steps:

**Step 1**  Choose **Configure > Controller Template Launch Pad**.

**Step 2**  Click **802.11h** or choose **802.11a/n > 802.11h** from the left sidebar menu. The 802.11h Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the local power constraint and channel announcement quiet mode. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3**  If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11h template page appears.

**Step 4**  Select the **Power Constraint** check box if you want the access point to stop transmission on the current channel.

**Step 5**  Select the **Channel Announcement** check box to enable channel announcement. Channel announcement is a method in which the access point announces when it is switching to a new channel and the new channel number.

**Step 6**  Click **Save**.

**Configuring a High Throughput Template (802.11a/n)**

To add or modify to an 802.11a/n high throughput template, follow these steps:

**Step 1**  Choose **Configure > Controller Template Launch Pad**.

**Step 2**  Click **High Throughput (802.11n)** or choose **802.11a/n > High Throughput** from the left sidebar menu. The 802.11n Parameters for 2.4 GHz or 802.11n Parameters for 5 GHz Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the 802.11n network status. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.
**Step 3** If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n High Throughput template page appears.

**Step 4** Select the **802.11n Network Status Enabled** check box to enable high throughput.

**Step 5** In the MCS (Data Rate) Settings column, choose which level of data rate you want supported. Modulation coding schemes (MCS) are similar to 802.11a data rate. As a default, 20 MHz and short guarded interval is used.

**Note** When you select the Supported check box, the chosen numbers appear in the Selected MCS Indexes page.

**Step 6** Click **Save**.

---

**Configuring CleanAir Controller Templates (802.11a/n)**

Create or modify a template for configuring CleanAir parameters for the 802.11a/n radio. You can configure the template to enable or disable CleanAir, reporting and alarms for the controllers. You can also configure the type of interfering devices to include for reporting and alarms.

To add a new template with 802.11a/n CleanAir information for a controller, follow these steps:

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** From the left sidebar menu, choose **802.11a/n > CleanAir**. The 802.11a/n CleanAir Controller Templates page displays all currently saved 802.11a/n CleanAir templates. It also displays and the number of controllers and virtual domains to which each template is applied.

**Step 3** From the **Select a command** drop-down list, choose **Add a Template**, and click **Go**. The **New Controller Template** page appears.

**Step 4** Configure the following fields:

- **Template Name**—Enter the template name.
- **CleanAir**—Select the check box to enable CleanAir functionality on the 802.11 b/g/n network, or unselect to prevent the controller from detecting spectrum interference.

**Note** If CleanAir is enabled, the Reporting Configuration and Alarm Configuration group boxes appear.

- **Reporting Configuration**—Use the fields in this group box to configure the interferer devices you want to include for your reports.

  **Report Interferers**—Select the **report interferers** check box to enable CleanAir system to report and detect sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is selected.

  Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect box and any that do not need to be detected appear in the Interferers to Ignore box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources are ignored.
• Alarm Configuration—This group box enables you to configure triggering of air quality alarms.
  – Air Quality Alarm—Select the **Air Quality Alarm** check box to enable the triggering of air quality alarms, or unselect the box to disable this feature.
  – Air Quality Alarm Threshold—If you selected the Air Quality Alarm check box, enter a value between 1 and 100 (inclusive) in the Air Quality Alarm Threshold field to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 1.
  – Interferers For Security Alarm—Select the **Interferers For Security Alarm** check box to trigger interferer alarms when the controller detects specified device types, or unselect it to disable this feature. The default value is unselected.
  – Make sure that any sources of interference that need to trigger interferer alarms appear in the Interferers Selected for Security Alarms box and any that do not need to trigger interferer alarms appear in the Interferers Ignored for Security Alarms box. Use the > and < buttons to move interference sources between these two boxes. By default, all interferer sources for security alarms are ignored.

**Step 5** Click **Save**. Once saved, the template appears in the Template List page. In the Template List page, you can apply this template to controllers. See the “Configuring Controller Templates” section on page 11-4 for more information.

### Configuring 802.11a/n RRM Templates

- Configuring an RRM Threshold Template (802.11a/n), page 11-92
- Configuring an RRM Interval Template (802.11a/n), page 11-93
- Configuring an RRM Dynamic Channel Allocation Template (802.11a/n), page 11-94
- Configuring an RRM Transmit Power Control Template (802.11a/n), page 11-95

#### Configuring an RRM Threshold Template (802.11a/n)

To add or make modifications to an 802.11a/n or 802.11b/g/n RRM threshold template, follow these steps:

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **RRM Thresholds** or choose **802.11a/n > RRM Thresholds**. The 802.11a/n RRM Thresholds Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the interference and noise threshold, maximum clients, and RF utilization. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n RRM Threshold template page appears.

**Step 4** Enter the minimum number of failed clients currently associated with the controller.
Configuring Controller Templates

Step 5 Enter the target range of coverage threshold.

Step 6 Enter the Data RSSI (–60 to –90 dBm). This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) for data required for the client to associate to an access point.

Note You must disable the 802.11a/n network before applying these RRM threshold fields.

Step 7 Enter the Voice RSSI (–60 to –90 dBm). This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) required for voice for the client to associate to an access point.

Step 8 Enter the maximum number of failed clients that are currently associated with the controller.

Step 9 In the RF Utilization text box, enter the percentage of threshold for 802.11a/n.

Step 10 Enter an interference threshold percentage.

Step 11 Enter a noise threshold between -127 and 0 dBm. When the controller is outside of this threshold, it sends an alarm to Prime Infrastructure.

Step 12 Enter the coverage exception level percentage. When the coverage drops by this percentage from the configured coverage for the minimum number of clients, a coverage hole is generated.

Step 13 Click Save.

Configuring an RRM Interval Template (802.11a/n)

To add or make modifications to an 802.11a/n RRM interval template, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.

Step 2 Click RRM Intervals or choose 802.11a/n > RRM Intervals from the left sidebar menu. The 802.11a/n or 802.11b/g/n RRM Threshold Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the neighbor packet frequency, noise measurement interval, and load measurement interval. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The 802.11a/n or 802.11b/g/n RRM Intervals template page appears.

Step 4 In the Neighbor Packet Frequency text box, enter the interval at which you want strength measurements taken for each access point. The default is 300 seconds.

Step 5 Enter the interval at which you want noise and interference measurements taken for each access point. The default is 300 seconds.

Step 6 Enter the interval at which you want load measurements taken for each access point. The default is 300 seconds.

Step 7 At the Coverage Measurement Interval field, enter at which interval you want coverage measurements taken for each access point. The default is 300 seconds.
Configuring an RRM Dynamic Channel Allocation Template (802.11a/n)

The Radio Resource Management (RRM) Dynamic Channel Assignment (DCA) page allows you to choose the DCA channels as well as the channel width for this controller.

RRM DCA supports 802.11n 40-MHz channel width in the 5-GHz band. The higher bandwidth allows radios to achieve higher instantaneous data rates.

Note Choosing a larger bandwidth reduces the non-overlapping channels which could potentially reduce the overall network throughput for certain deployments.

To configure 802.11 a/n RRM DCA template, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.

Step 2 Click DCA or choose 802.11a/n > DCA. The 802.11a/n DCS Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The 802.11a/n TPC template page appears.

Step 4 Configure the following fields:

- Template Name—Enter the template name.
- Assignment Mode—From the Dynamic Assignment drop-down list, choose one of three modes:
  - Automatic—The transmit power is periodically updated for all access points that permit this operation.
  - On Demand—Transmit power is updated when you click Assign Now.
  - Disabled—No dynamic transmit power assignments occur, and values are set to their global default.
- Select the Avoid Foreign AP Interference check box to enable it. Enable this check box to have RRM consider interference from foreign Cisco access points (those non-Cisco access points outside RF/mobility domain) when assigning channels. This foreign 802.11 interference. Unselect this check box to have RRM ignore this interference.

In certain circumstances with significant interference energy (dB) and load (utilization) from foreign access points, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the foreign access points. This increases capacity and reduces variability for the Cisco WLAN Solution.

- Select the Avoid Cisco AP Load check box if you want it enabled. Enable this bandwidth-sensing field to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points. Unselect this check box to have RRM ignore this value.
In certain circumstances and with denser deployments, there might not be enough channels to properly create perfect channel reuse. In these circumstances, RRM can assign better reuse patterns to those access points that carry more traffic load.

- Select the Avoid non 802.11 Noise check box if you want to enable it. Enable this noise-monitoring field to have access points avoid channels that have interference from non-access point sources, such as microwave ovens or Bluetooth devices. Unselect this check box to have RRM ignore this interference.

In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources. This increases capacity and reduces variability for the Cisco WLAN Solution.

- The Signal Strength Contribution check box is always enabled (not configurable). This constantly monitors the relative location of all access points within the RF/mobility domain to ensure near-optimal channel reuse. The net effect is an increase in Cisco WLAN Solution capacity and a reduction in co-channel and adjacent channel interference.

- Enable or disable event-driven Radio Resource Management (RRM) using the following fields. Event Driven RRM is used when a CleanAir-enabled access point detects a significant level of interference.
  - Event Driven RRM—Enable or Disable spectrum event-driven RRM. By default, Event Driven RRM is enabled.
  - Sensitivity Threshold—If Event Driven RRM is enabled, this field displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

**Step 5**  Click **Save**.

---

### Configuring an RRM Transmit Power Control Template (802.11a/n)

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the transmit power of the access points according to how the access points are seen by their third strongest neighbor.

The transmit power control (TPC) algorithm both increases and decreases the power of an access point in response to changes in the RF environment. In most instances, TPC seeks to lower the power of an access point 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 surrounding access points. This feature is different from Coverage Hole Detection. Coverage hole detection is primarily concerned with clients, while TPC is tasked with providing enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

To configure 802.11a/n RRM TPC template, follow these steps:

**Step 1**  Choose **Configure > Controller Template Launch Pad**.

**Step 2**  Click **TPC** or choose **802.11a/n > TPC**. The 802.11a/n TPC Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.
The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n TPC template page appears.

**Step 4** Configure the following fields:

- **Template Name**—Enter the template name in the text box.
- **TPC Version**—Choose TPCv1 or TPCv2.

**Note** The TPCv2 option is applicable only for those controllers running Release 7.2.x or later.

- **Dynamic Assignment**—From the Dynamic Assignment drop-down list, choose one of three modes:
  - **Automatic**—The transmit power is periodically updated for all access points that permit this operation.
  - **On Demand**—Transmit power is updated when you click **Assign Now**.
  - **Disabled**—No dynamic transmit power assignments occur, and values are set to their global default.
- **Maximum Power Assignment**—Indicates the maximum power assigned.
  - **Range**: -10 to 30 dB
  - **Default**: 30 dB
- **Minimum Power Assignment**—Indicates the minimum power assigned.
  - **Range**: -10 to 30 dB
  - **Default**: 30 dB
- **Dynamic Tx Power Control**—Determine if you want to enable Dynamic Tx Power Control.
- **Transmitted Power Threshold**—Enter a transmitted power threshold between -50 and -80.
- **Control Interval**—In seconds (read-only).

**Step 5** Click **Save**.

---

**Configuring Radio Templates (802.11b/g/n)**

- Configuring 802.11b/g/n Parameters Templates, page 11-97
- Configuring Media Parameters Controller Templates (802.11b/g/n), page 11-99
- Configuring EDCA Parameters Controller Templates (802.11b/g/n), page 11-101
- Configuring Roaming Parameters Controller Templates (802.11b/g/n), page 11-102
- Configuring High Throughput (802.11n) Controller Templates (802.11b/g/n), page 11-103
- Configuring CleanAir Controller Templates (802.11 b/g/n), page 11-104
- Configuring 802.11b/g/n RRM Templates, page 11-105
Configuring 802.11b/g/n Parameters Templates

Create or modify a template for configuring 802.11b/g/n parameters (such as power and channel status, data rates, channel list, and CCX location measurement) and/or applying these settings to controller(s).

To add a new template with 802.11b/g/n parameters information for a controller, follow these steps:

**Step 1** Choose Configure > Controller Template Launch Pad.

**Step 2** Click New beside the template you want to add.

**Step 3** Configure the following General parameters:

- **Policy Name**—Security policy in force.
- **802.11b/g Network Status**
- **Beam Forming**—Choose **Enable** or **Disable** from the drop-down list.

**Note** Beam forming refers to a general signal processing technique used to control the directionality of the reception or transmission of a signal.

- **Transmitted Power Threshold**—The valid range is from -50 to -80.
- **Beacon Period**—The rate at which the SSID is broadcast by the access point (the amount of time between beacons). The valid range is from 100 to 600 milliseconds.
- **DTIM Period**—The number of beacon intervals that might elapse between transmission of beacon frames containing a traffic indicator message (TIM) element whose delivery count field is 0. This value is transmitted in the DTIM period field of beacon frames.

When client devices receive a beacon that contains a DTIM, they normally “wake up” to check for pending packets. Longer intervals between DTIMs let clients sleep longer and preserve power. Conversely, shorter DTIM periods reduce the delay in receiving packets but use more battery power because clients wake up more often.

**Note** DTIM period is not applicable in controller Release 5.0.0.0 and later.

- **Fragmentation Threshold**—Determine the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference. The default value is 2346.
- **802.11e Max Bandwidth**—Percentage for 802.11e max bandwidth. The default value is 100.

**Step 4** Configure the following 802.11b/g Power Status parameters:

- **Dynamic Assignment**—From the Dynamic Assignment drop-down list, choose any one of the following dynamic transmit power assignment modes.
  - **Automatic**—The transmit power is periodically updated for all access points that permit this operation.
  - **On Demand**—Transmit power is updated when you click Assign Now.
  - **Disabled**—No dynamic transmit power assignments occur and values are set to their global default. The default is Automatic.
The power levels and available channels are defined by the country code setting and are regulated on a country by country basis.

- **Dynamic Tx Power Control**—Select this check box to enable DTPC support. If this option is enabled, the transmit power level of the radio is advertised in the beacons and the probe responses.

### Step 5

Configure the following 802.11b/g Channel Status parameters:

- **Assignment Mode**—From the Assignment Mode drop-down list, choose any one of the following dynamic channel assignment modes.
  - **Automatic**—The channel assignment is periodically updated for all access points that permit this operation.
  - **On Demand**—Channel assignments are updated when desired.
  - **Disabled**—No dynamic channel assignments occur and values are set to their global default.

  **Note** The default is Automatic.

- **Avoid Foreign AP Interference**—Enable this Radio Resource Management (RRM) foreign 802.11 interference-monitoring parameter to have Radio Resource Management consider interference from foreign (non-Cisco access points outside the RF/mobility domain) access points when assigning channels to Cisco access points.

  Disable this field to have Radio Resource Management ignore this interference.

  **Note** In certain circumstances with significant interference energy (dB) and load (utilization) from Foreign access points, Radio Resource Management might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in Cisco access points close to the Foreign access points to increase capacity and reduce variability for the Cisco WLAN Solution.

- **Avoid Cisco AP Load**—Enable this Radio Resource Management (RRM) bandwidth-sensing parameter to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points.

  Disable this field to have Radio Resource Management ignore this value.

  **Note** In certain circumstances and with denser deployments, there might not be enough channels to properly create perfect channel re-use. In these circumstances, Radio Resource Management can assign better re-use patterns to those APs that carry more traffic load.

- **Avoid non 802.11 Noise**—Enable this Radio Resource Management (RRM) noise-monitoring field to have access points avoid channels that have interference from non-Access Point sources, such as microwave ovens or Bluetooth devices.

  Disable this field to have Radio Resource Management ignore this interference.
Chapter 11      Using Templates

Configuring Controller Templates

Note

In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, Radio Resource Management might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources to increase capacity and reduce variability for the Cisco WLAN Solution.

- Signal Strength Contribution—This check box is always enabled (not configurable). Radio Resource Management (RRM) constantly monitors the relative location of all access points within the RF/mobility domain to ensure near-optimal channel reuse. The net effect is an increase in Cisco WLAN Solution capacity and a reduction in co-channel and adjacent channel interference.

Step 6
Configure the Data Rate parameters.

The data rates set are negotiated between the client and the controller. If the data rate is set to Mandatory, the client must support it to use the network. If a data rate is set as Supported by the controller, any associated client that also supports that same rate might communicate with the access point using that rate. But it is not required that a client be able to use all the rates marked Supported to associate 6, 9, 12, 18, 24, 36, 48, 54 Mbps. For each rate, a drop-down list selection of Mandatory or Supported is available. Each data rate can also be set to Disabled to match Client settings.

Step 7
Configure the Noise/Interference/Rogue Monitoring Channels parameters.

Choose between all channels, country channels, or DCA channels based on the level of monitoring you want. Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation among a set of managed devices connected to the controller.

Step 8
Configure the CCX Location Measurement parameters:

- Mode—Enable or disable the broadcast radio measurement request. When enabled, this enhances the location accuracy of clients.
- Interval—Interval in seconds between requests.

Note
Cisco-compatible Extension location measurement interval can be changed only when measurement mode is enabled.

Step 9
Click Save. Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the “Applying Controller Templates” section on page 11-2 for more information.

Configuring Media Parameters Controller Templates (802.11b/g/n)

Create or modify a template for configuring 802.11b/g/n voice parameters such as Call Admission Control and traffic stream metrics.

To add a new template with 802.11b/g/n voice parameters information (such as Call Admission Control and traffic stream metrics) for a controller, follow these steps:

Step 1
Choose Configure > Controller Template Launch Pad.

Step 2
Click New beside the template you want to add.

Step 3
Specify an appropriate name for the template.
Chapter 11         Using Templates

Configuring Controller Templates

### Note

Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

---

**Step 4** On the Voice tab, configure the following parameters:

- Admission Control (ACM)—Select the check box to enable admission control.
  
  For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, Call Admission Control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keep the maximum allowed number of calls to an acceptable quantity.

- CAC Method—If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static.
  
  Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

- Maximum Bandwidth Allowed—Enter the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled. For controller versions 6.0.188.0 and earlier, the valid range is 40 to 85. For controller versions 6.0.188.1 and later, the valid range is 5 to 85, and the default is 75.

- Reserved Roaming Bandwidth—Enter the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled. The valid range is 0 to 25, and the default is 6.

- Expedited Bandwidth—Select the check box to enable expedited bandwidth as an extension of CAC for emergency calls.
  
  You must have an expedited bandwidth IE that is CCXv5 compliant so that a TSPEC request is given higher priority.

- SIP CAC—Select the check box to enable SIP CAC.
  
  SIP CAC should be used only for phones that support status code 17 and do not support TSPEC-based admission control.

- SIP Codec—Choose the codec name you want to use on this radio from the SIP Codec drop-down list. The available options are G.711, G.729, and User Defined.

- SIP Call Bandwidth—Enter the bandwidth in kilobits per second that you want to assign per SIP call on the network. This field can be configured only when the SIP Codec selected is User Defined.

- SIP Sample Interval—Enter the sample interval in milliseconds that the codec must operate in.

- Max Number of Calls per Radio—Enter the maximum number of calls per radio.

- Metric Collection—Select the check box to enable metric collection.
  
  Traffic stream metrics are a series of statistics about VoIP over your wireless LAN which inform you of the QoS of the wireless LAN. For the access point to collect measurement values, traffic stream metrics must be enabled. When this is enabled, the controller begins collecting statistical data every 90 seconds for the 802.11b/g interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.

---

**Step 5** On the Video tab, configure the following parameters:

- Admission Control (ACM)—Select the check box to enable admission control.
Chapter 11 Using Templates

Configuring Controller Templates

- Maximum Bandwidth—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled. For controller versions 6.0.188.0 and earlier, the valid range is 0 to 100. For controller versions 6.0.188.1 and later, the valid range is 5 to 85.
- Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled. The valid range is 0 to 25, and the default is 0.
- Unicast Video Redirect—Select the Unicast Video Redirect check box to enable all non-media stream packets in video queue are redirected to the best effort queue. If disabled, all packets with video marking are kept in video queue.
- Client Minimum Phy Rate—Choose the physical data rate required for the client to join a media stream from the Client Minimum Phy Rate drop-down list.
- Multicast Direct Enable—Select the Multicast Direct Enable check box to set the Media Direct for any WLAN with Media Direct enabled on a WLAN on this radio.
- Maximum Number of Streams per Radio—Specify the maximum number of streams per Radio to be allowed.
- Maximum Number of Streams per Client—Specify the maximum number of streams per Client to be allowed.
- Best Effort QOS Admission—Select the Best Effort QOS Admission check box to redirect new client requests to the best effort queue. This happens only if all the video bandwidth has been used.

Note

If disabled and maximum video bandwidth has been used, then any new client request is rejected.

Step 6

On the General tab, specify the following field:

- Maximum Media Bandwidth (0 to 85%)—Specify the percentage of maximum of bandwidth allowed. This option is only available when CAC is enabled.

Step 7

Click Save.

Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the “Applying Controller Templates” section on page 11-2 for more information.

Configuring EDCA Parameters Controller Templates (802.11b/g/n)

Create or modify a template for configuring 802.11b/g/n EDCA parameters. EDCA parameters designate pre-configured profiles at the MAC layer for voice and video.

To add a new template with 802.11b/g/n EDCA parameters information for a controller, follow these steps:

Step 1

Choose Configure > Controller Template Launch Pad.

Step 2

Click New beside the template you want to add.

Step 3

Configure the following parameters:

- Template Name
Configuring Controller Templates  

**Note** Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- EDCA Profile—Profiles include Wi-Fi Multimedia (WMM), Spectralink Voice Priority (SVP), Voice Optimized, and Voice & Video Optimized. WMM is the default EDCA profile.

**Note** You must shut down radio interface before configuring EDCA Parameters.

- Streaming MAC—Only enable streaming MAC if all clients on the network are WMM compliant.

**Step 4** Click **Save**. Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the “Applying Controller Templates” section on page 11-2 for more information.

---

**Configuring Roaming Parameters Controller Templates (802.11b/g/n)**

Create or modify a template for configuring roaming parameters for 802.11b/g/n radios.

To add a new template with 802.11b/g/n Roaming parameters information for a controller, follow these steps:

**Step 1** Choose **Configure > Controller Template Launch Pad.**

**Step 2** Click **New** beside the template you want to add.

**Step 3** Configure the following parameters:

- **Template Name**

**Note** Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- **Mode**—Choose **Default Values** or **Custom Values** from the drop-down list.
  - **Default Values**—The roaming parameters are unavailable and the default values are displayed.
  - **Custom Values**—The following roaming parameters can be edited.

- **Minimum RSSI**—Enter a value for the minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point. If the client average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.
  - **Range:** -80 to -90 dBm
  - **Default:** -85 dBm

- **Roaming Hysteresis**—Enter a value to indicate how strong the signal strength of a neighboring access point must be in order for the client to roam to it. This field is intended to reduce the amount of “ping ponging” between access points if the client is physically located on or near the border between two access points.
Configuring Controller Templates

- Range: 2 to 4 dB
- Default: 2 dB

- Adaptive Scan Threshold—Enter the RSSI value, from a client associated access point, below which the client must be able to roam to a neighboring access point within the specified transition time. This field also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold.
  - Range: -70 to -77 dB
  - Default: -72 dB

- Transition Time—Enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client associated access point is below the scan threshold.
  - Range: 1 to 10 seconds
  - Default: 5 seconds

Note
The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

Step 4
Click Save. Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the “Applying Controller Templates” section on page 11-2 for more information.

Configuring High Throughput (80.11n) Controller Templates (802.11b/g/n)

Create or modify a template for configuring high-throughput parameters such as MCS (data rate) settings and indexes and for applying these 802.11n settings to multiple controllers.

To add a new template with High Throughput (802.11n) information for a controller, follow these steps:

Step 1
Choose Configure > Controller Template Launch Pad.

Step 2
Click New beside the template you want to add.

Step 3
Configure the following fields:

- Template Name

Note
Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- 802.11n Network Status—Select the check box to enable high throughput.
- MCS (Data Rate) Settings—Choose which level of data rate you want supported. MCS is modulation coding schemes which are similar to 802.11a data rate.
Configuring Controller Templates

Chapter 11      Using Templates

Configuring CleanAir Controller Templates (802.11 b/g/n)

Create or modify a template for configuring CleanAir parameters for the 802.11 b/g/n radio. You can configure the template to enable or disable CleanAir, reporting and alarms for the controllers. You can also configure the type of interfering devices to include for reporting and alarms.

To add a new template with 802.11b/g/n CleanAir information for a controller, follow these steps:

Step 1  Choose Configure > Controller Template Launch Pad.

Step 2  From the left sidebar menu, choose 802.11b/g/n > CleanAir. The 802.11b/g/n CleanAir Controller Templates page displays all currently saved 802.11b/g/n CleanAir templates. It also displays and the number of controllers and virtual domains to which each template is applied.

Step 3  From the Select a command drop-down list, choose Add a Template, and click Go.

The New Controller Template page appears.

Step 4  Configure the following fields:

- Template Name—Enter the template name in the text box.
- CleanAir—Select the check box to enable CleanAir functionality on the 802.11 b/g/n network, or unselect to prevent the controller from detecting spectrum interference. The default value is selected.
  
  Note  If CleanAir is enabled, the Reporting Configuration and Alarm Configuration group boxes appear.

- Reporting Configuration—Use the parameters in this group box to configure the interferer devices you want to include for your reports.
  
  - Report Interferers—Select the report interferers check box to enable CleanAir system to report and detect sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is selected.
  
  - Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect box and any that do not need to be detected appear in the Interferers to Ignore box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources are ignored.

- Alarm Configuration—This group box enables you to configure triggering of air quality alarms.
- Air Quality Alarm—Select the **Air Quality Alarm** check box to enable the triggering of air quality alarms, or unselect the box to disable this feature.

- Air Quality Alarm Threshold—If you selected the Air Quality Alarm check box, enter a value between 1 and 100 (inclusive) in the Air Quality Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 1.

- Interferers For Security Alarm—Select the **Interferers For Security** Alarm check box to trigger interferer alarms when the controller detects specified device types, or unselect it to disable this feature. The default value is unselected.

- Make sure that any sources of interference that need to trigger interferer alarms appear in the Interferers Selected for Security Alarms box and any that do not need to trigger interferer alarms appear in the Interferers Ignored for Security Alarms box. Use the > and < buttons to move interference sources between these two boxes. By default, all interferer sources for security alarms are ignored.

**Step 5**  
Click **Save**. Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the “Adding Controller Templates” section on page 11-2 for more information.

---

### Configuring 802.11b/g/n RRM Templates

- Configuring RRM Thresholds Controller Templates (802.11b/g/n), page 11-105
- Configuring RRM Intervals Controller Templates (802.11b/g/n), page 11-106
- Configuring an RRM Dynamic Channel Allocation Template (802.11b/g/n), page 11-107
- Configuring an RRM Transmit Power Control Template (802.11b/g/n), page 11-108

#### Configuring RRM Thresholds Controller Templates (802.11b/g/n)

Create or modify a template for setting various RRM thresholds such as load, interference, noise, and coverage.

To add a new template with 802.11b/g/n RRM thresholds information for a controller, follow these steps:

**Step 1**  
Choose **Configure > Controller Template Launch Pad**.

**Step 2**  
Click **New** beside the template you want to add.

**Step 3**  
Add or modify the following template name.

| Note | Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes. |

**Step 4**  
Configure the following Coverage Hole Algorithm parameters:

- Min. Failed Clients (#)—Enter the minimum number of failed clients currently associated with the controller.
- Coverage Level—Enter the target range of coverage threshold (dB).
• Signal Strength—When the Coverage Level field is adjusted, the value of the Signal Strength (dBm) automatically reflects this change. The Signal Strength field provides information regarding what the signal strength is when adjusting the coverage level.

• Data RSSI—Enter the Data RSSI (-60 to -90 dBm). This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) for data required for the client to associate to an access point.

• Voice RSSI—Enter the Voice RSSI (-60 to -90 dBm). This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) required for voice for the client to associate to an access point.

**Step 5** Configure the following Load Thresholds parameters:
- Max. Clients—Enter the maximum number of clients able to be associated with the controller.
- RF Utilization—Enter the percentage of threshold for this radio type.

**Step 6** Configure the following Threshold for Traps parameters:
- Interference Threshold—Enter an interference threshold between 0 and 100 percent.
- Noise Threshold—Enter a noise threshold between -127 and 0 dBm. When outside of this threshold, the controller sends an alarm to Prime Infrastructure.
- Coverage Exception Level—Enter the coverage exception level percentage. When the coverage drops by this percentage from the configured coverage for the minimum number of clients, a coverage hole is generated.

**Step 7** Click **Save**. Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the “Applying Controller Templates” section on page 11-2 for more information.

---

### Configuring RRM Intervals Controller Templates (802.11b/g/n)

Create or modify a template for configuring RRM intervals for 802.11b/g/n radios.

To add a new template with 802.11b/g/n RRM intervals information for a controller, follow these steps:

**Step 1** Choose **Configure > Controller Template Launch Pad**.
**Step 2** Click **New** beside the template you want to add.
**Step 3** Configure the following parameters:
- Template Name

  **Note** Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

  - Neighbor Packet Frequency—Enter at which interval you want strength measurements taken for each access point. The default is 300 seconds.
  - Noise Measurement Interval—Enter at which interval you want noise and interference measurements taken for each access point. The default is 180 seconds.
  - Load Measurement Interval—Enter at which interval you want load measurements taken for each access point. The default is 300 seconds.
Configuring Controller Templates

Channel Scan Duration—Enter at which interval you want coverage measurements taken for each access point. The default is 300 seconds.

Step 4 Click Save. Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the “Applying Controller Templates” section on page 11-2 for more information.

Configuring an RRM Dynamic Channel Allocation Template (802.11b/g/n)

The Radio Resource Management (RRM) Dynamic Channel Assignment (DCA) page allows you to choose the DCA channels as well as the channel width for this controller.

RRM DCA supports 802.11n 40-MHz channel width in the 5-GHz band. The higher bandwidth allows radios to achieve higher instantaneous data rates.

Note Choosing a larger bandwidth reduces the non-overlapping channels, which could potentially reduce the overall network throughput for certain deployments.

To configure 802.11b/g/n RRM DCA template, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.

Step 2 Click DCA or choose 802.11b/g/n > DCA. The 802.11b/g/n DCS Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The 802.11b/g/n TPC template page appears.

Step 4 Configure the following parameters:

- Template Name—Enter the template name.
- Assignment Mode—From the Dynamic Assignment drop-down list, choose one of three modes:
  - Automatic—The transmit power is periodically updated for all access points that permit this operation.
  - On Demand—Transmit power is updated when you click Assign Now.
  - Disabled—No dynamic transmit power assignments occur, and values are set to their global default.
- Select the Avoid Foreign AP Interference check box to enable it. Enable this field to have RRM consider interference from foreign Cisco access points (those non-Cisco access points outside RF/mobility domain) when assigning channels. This foreign 802.11 interference. Unselect this check box to have RRM ignore this interference.
In certain circumstances with significant interference energy (dB) and load (utilization) from foreign access points, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the foreign access points. This increases capacity and reduces variability for the Cisco WLAN Solution.

- Select the **Avoid Cisco AP Load** check box if you want it enabled. Enable this bandwidth-sensing field to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points. Unselect this check box to have RRM ignore this value.

  In certain circumstances and with denser deployments, there might not be enough channels to properly create perfect channel reuse. In these circumstances, RRM can assign better re-use patterns to those access points that carry more traffic load.

- Select the **Avoid non 802.11 Noise** check box if you want to enable it. Enable this noise-monitoring field to have access points avoid channels that have interference from non-access point sources, such as microwave ovens or Bluetooth devices. Unselect this check box to have RRM ignore this interference.

  In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources. This increases capacity and reduces variability for the Cisco WLAN Solution.

- The **Signal Strength Contribution** check box is always enabled (not configurable). constantly monitors the relative location of all access points within the RF/mobility domain to ensure near-optimal channel re-use. The net effect is an increase in Cisco WLAN Solution capacity and a reduction in co-channel and adjacent channel interference.

- Enable or disable event-driven Radio Resource Management (RRM) using the following parameters. Event Driven RRM is used when a CleanAir-enabled access point detects a significant level of interference.

  - **Event Driven RRM**—Enable or Disable spectrum event-driven RRM. By default, Event Driven RRM is enabled.

  - **Sensitivity Threshold**—If Event Driven RRM is enabled, this field displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

**Step 5**  
Click **Save**.

---

**Configuring an RRM Transmit Power Control Template (802.11b/g/n)**

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the transmit power of an access point according to how the access points are seen by their third strongest neighbor.

The transmit power control (TPC) algorithm both increases and decreases the power of an access point in response to changes in the RF environment. In most instances, TPC seeks to lower the power of an access point 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 surrounding access points.
This feature is different from Coverage Hole Detection. Coverage hole detection is primarily concerned with clients, while TPC is tasked with providing enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

To configure 802.11b/g/n RRM TPC template, follow these steps:

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **TPC** or choose **802.11b/g/n > TPC**. The 802.11b/g/n TPC Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11b/g/n TPC template page appears.

**Step 4** Configure the following parameters:

- **Template Name**—Enter the template name in the text box.
- **TPC Version**—Choose TPCv1 or TPCv2 from the drop-down list.

  **Note** The TPCv2 option is applicable only for those controller Release 7.2.x or later.

- **Dynamic Assignment**—From the Dynamic Assignment drop-down list, choose one of three modes:
  - **Automatic**—The transmit power is periodically updated for all access points that permit this operation.
  - **On Demand**—Transmit power is updated when you click **Assign Now**.
  - **Disabled**—No dynamic transmit power assignments occur, and values are set to their global default.

- **Maximum Power Assignment**—Indicates the maximum power assigned.
  - **Range**: -10 to 30 dB
  - **Default**: 30 dB

- **Minimum Power Assignment**—Indicates the minimum power assigned.
  - **Range**: -10 to 30 dB
  - **Default**: 30 dB

- **Dynamic Tx Power Control**—Determine if you want to enable Dynamic Tx Power Control.
- **Transmitted Power Threshold**—Enter a transmitted power threshold between -50 and -80.
- **Control Interval**—In seconds (read-only).

**Step 5** Click **Save**.
Configuring Mesh Templates

Configuring Mesh Setting Templates

You can configure an access point to establish a connection with the controller.

To add or modify a mesh template, follow these steps:

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Mesh Configuration** or choose **Mesh > Mesh Configuration** from the left sidebar menu. The Mesh Configuration Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the rootAP to MeshAP range, the client access on backhaul link, and security mode. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Mesh Configuration template page appears.

**Step 4** The Root AP to Mesh AP Range is 12,000 feet by default. Enter the optimum distance (in feet) that should exist between the root access point and the mesh access point. This global field applies to all access points when they join the controller and all existing access points in the network.

**Step 5** The **Client Access on Backhaul Link** check box is not selected by default. When this option is enabled, mesh access points can associate with 802.11a/n wireless clients over the 802.11a/n backhaul. This client association is in addition to the existing communication on the 802.11a/n backhaul between the root and mesh access points.

**Note** This feature applies only to access points with two radios.

**Step 6** The **Mesh DCA Channels** check box is not selected by default. Select this option to enable backhaul channel deselection on the Controller using the DCA channel list configured in the Controller. Any change to the channels in the Controller DCA list is pushed to the associated access points. This feature applies only to the 1524SB mesh access points. For more information on this feature, see the **Controller Configuration Guide**.

**Step 7** Select the **Background Scanning** check box to enable background scanning or unselect it to disable the feature. The default value is disabled. Background scanning allows Cisco Aironet 1510 Access Points to actively and continuously monitor neighboring channels for more optimal paths and parents. See the “Background Scanning on 1510s in Mesh Networks” section on page 9-54 for further information.

**Step 8** From the Security Mode drop-down list, choose **EAP** (Extensible Authentication Protocol) or **PSK** (Pre-Shared Key).

**Step 9** Click **Save**.
Configuring Management Templates

- Configuring Trap Receiver Templates, page 11-111
- Configuring Trap Control Templates, page 11-111
- Configuring Telnet SSH Templates, page 11-113
- Configuring Legacy Syslog Templates, page 11-114
- Configuring Multiple Syslog Templates, page 11-114
- Configuring Local Management User Templates, page 11-115
- Configuring User Authentication Priority Templates, page 11-116

Configuring Trap Receiver Templates

If you have monitoring devices on your network that receive SNMP traps, you might want to add a trap receiver template.

To add or modify a trap receiver template, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.

Step 2 Click Trap Receivers or choose Management > Trap Receivers from the left sidebar menu.

Step 3 The Management > Trap Receiver page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the IP address and admin status. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 4 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Trap Receivers template page appears.

Note Trap Receiver Template name should not contain space.

Step 5 Enter the IP address of the server in the text box.

Step 6 Select the Admin Status check box to enable the administrator status if you want SNMP traps to be sent to the receiver.

Step 7 Click Save.

Configuring Trap Control Templates

To add or modify a trap control template, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.
Step 2 Click **Trap Control** or choose **Management > Trap Control** from the left sidebar menu. The Management > Trap Control page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the link port up or down and rogue AP. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Trap Control template page appears.

Step 4 Select the appropriate check box to enable any of the following miscellaneous traps:

- **SNMP Authentication**—The SNMPv2 entity has received a protocol message that is not properly authenticated. When a user who is configured in SNMP V3 mode tries to access the controller with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.
- **Link (Port) Up/Down**—Link changes states from up or down.
- **Multiple Users**—Two users log in with the same login ID.
- **Spanning Tree**—Spanning Tree traps. See the STP specification for descriptions of individual parameters.
- **Rogue AP**—Whenever a rogue access point is detected or when a rogue access point was detected earlier and no longer exists, this trap is sent with its MAC address.
- **Controller Config Save**—Notification sent when the configuration is modified.

Step 5 Select the appropriate check box to enable any of the following client-related traps:

- **802.11 Association**—A trap is sent when a client is associated to a WLAN. This trap does not guarantee that the client is authenticated.
- **802.11 Disassociation**—The disassociate notification is sent when the client sends a disassociation frame.
- **802.11 Deauthentication**—The deauthenticate notification is sent when the client sends a deauthentication frame.
- **802.11 Failed Authentication**—The authenticate failure notification is sent when the client sends an authentication frame with a status code other than successful.
- **802.11 Failed Association**—The associate failure notification is sent when the client sends an association frame with a status code other than successful.
- **Excluded**—The associate failure notification is sent when a client is excluded.

Step 6 Select the appropriate check box to enable any of the following access point traps:

- **AP Register**—Notification sent when an access point associates or disassociates with the controller.
- **AP Interface Up/Down**—Notification sent when access point interface (802.11a/n or 802.11b/g/n) status goes up or down.

Step 7 Select the appropriate check box to enable any of the following auto RF profile traps:

- **Load Profile**—Notification sent when Load Profile state changes between PASS and FAIL.
- **Noise Profile**—Notification sent when Noise Profile state changes between PASS and FAIL.
Step 8 Select the appropriate check box to enable any of the following auto RF update traps:

- **Interference Profile**—Notification sent when Interference Profile state changes between PASS and FAIL.
- **Coverage Profile**—Notification sent when Coverage Profile state changes between PASS and FAIL.

Step 9 Select the appropriate check box to enable any of the following AAA traps:

- **User Auth Failure**—This trap is to inform you that a client RADIUS authentication failure has occurred.
- **RADIUS Server No Response**—This trap is to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.

Step 10 Select the appropriate check box to enable the following IP security traps:

- ESP Authentication Failure
- ESP Replay Failure
- Invalid SPI
- IKE Negotiation Failure
- IKE Suite Failure
- Invalid Cookie

Step 11 Select the appropriate check box to enable the following 802.11 security trap:

- WEP Decrypt Error—Notification sent when the controller detects a WEP decrypting error.
- Signature Attack

Step 12 Click **Save**.

## Configuring Telnet SSH Templates

To add or modify a Telnet SSH configuration template, follow these steps:

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Telnet SSH** or choose **Management > Telnet SSH** from the left sidebar menu. The Management > Telnet SSH Configuration page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the session timeout, maximum sessions, and whether Telnet or SSH sessions are allowed. The last column indicates when the template was last saved. The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.
Configuring Controller Templates

Step 3 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Telnet SSH template page appears.

Step 4 Enter the number of minutes a Telnet session is allowed to remain inactive before being logged off. A zero means there is no timeout. The valid range is 0 to 160, and the default is 5.

Step 5 At the Maximum Sessions field, enter the number of simultaneous Telnet sessions allowed. The valid range is 0 to 5, and the default is 5. New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the service port.

Step 6 Use the Allow New Telnet Session drop-down list to determine if you want new Telnet sessions allowed on the DS port. New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the service port. The default is no.

Step 7 Use the Allow New SSH Session drop-down list to determine if you want Secure Shell Telnet sessions allowed. The default is yes.

Step 8 Click Save.

Configuring Legacy Syslog Templates

To add or modify a legacy syslog configuration template, follow these steps:

Note Legacy Syslog applies to controllers Release 5.0.6.0 and earlier.

Step 1 Choose Configure > Controller Template Launch Pad.

Step 2 Click Legacy Syslog or choose Management > Legacy Syslog from the left sidebar menu. The Management > Legacy Syslog page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Legacy Syslog template page appears.

Step 4 Enter a template name. The number of controllers to which this template is applied is displayed.

Step 5 Select the Syslog check box to enable syslog. When you do, a Syslog Host IP Address text box appears.

Step 6 Click Save.

Configuring Multiple Syslog Templates

To add or modify a multiple syslog configuration template, follow these steps:
Chapter 11      Using Templates

Configuring Controller Templates

Note
You can enter up to three syslog server templates.

Step 1
Choose Configure > Controller Template Launch Pad.

Step 2
Click Multiple Syslog or choose Management > Multiple Syslog from the left sidebar menu. The Management > Multiple Syslog page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the syslog server address. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3
If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Multiple Syslog template page appears.

Step 4
Enter a template name and a syslog server IP address in the text boxes.

Step 5
Click Save.

Configuring Local Management User Templates

To add or modify a local management user template, follow these steps:

Step 1
Choose Configure > Controller Template Launch Pad.

Step 2
Click Local Management Users or choose Management > Local Management Users from the left sidebar menu. The Management > Local Management Users Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the username and access level. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3
If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Local Management Users template page appears.

Step 4
Enter a template name

Step 5
Enter a template username.

Step 6
Enter a password for this local management user template.

Step 7
Reenter the password.

Step 8
Use the Access Level drop-down list to choose either Read Only or Read Write.

Step 9
Select the Update Telnet Credentials check box to update the user credentials in Prime Infrastructure for Telnet/SSH access.
Chapter 11  Using Templates

Configuring Controller Templates

Note  If the template is applied successfully and the Update Telnet Credentials option is enabled, the applied management user credentials are used in Prime Infrastructure for Telnet/SSH credentials to that applied controller.

Step 10  Click Save.

Configuring User Authentication Priority Templates

Management user authentication priority templates control the order in which authentication servers are used to authenticate the management users of a controller.

To add a user authentication priority template or make modifications to an existing template, follow these steps:

Step 1  Choose Configure > Controller Template Launch Pad.

Step 2  Click Authentication Priority or choose Management > Authentication Priority from the left sidebar menu. The Management > Local Management Users Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the authentication priority list. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3  If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Local Management Users template page appears.

Step 4  Enter a template name.

Step 5  The local server is tried first. Choose either RADIUS or TACACS+ from the drop-down list to try if local authentication fails.

Step 6  Click Save.

Configuring CLI Templates

Applying a Set of CLI Commands

You can create templates containing a set of CLI commands and apply them to one or more controllers from Prime Infrastructure. These templates are meant for provisioning features in multiple controllers for which there is no SNMP support or custom Prime Infrastructure user interface. The template contents are simply a command array of strings. No support for substitution variables, conditionals, and the like exist.

The CLI sessions to the device are established based on user preferences. The default protocol is SSH.

To add or modify a CLI template, follow these steps:
### Configuring Controller Templates

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose <strong>Configure &gt; Controller Template Launch Pad</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click <strong>CLI &gt; General</strong> or choose <strong>CLI &gt; General</strong> from the left sidebar menu. The CLI &gt; General page appears, and the number of controllers that the template is applied to automatically populates. The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>If you want to add a new template, choose <strong>Add Template</strong> from the Select a command drop-down list, and click <strong>Go</strong>. To modify an existing template, click the template name. The Command-Line Interface General template page appears.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>If you are adding a new template, provide a name that you are giving to this string of commands in the text box. If you are making modifications to an existing template, the Template Name text box cannot be modified.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>In the Commands page, enter the series of CLI commands.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Select the <strong>Refresh Config after Apply</strong> check box to perform a refresh config on the controller after the CLI template is applied successfully.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Click <strong>Save</strong> to save the CLI commands to Prime Infrastructure database without applying to the selected controllers or <strong>Apply to Controllers</strong> to save the commands to Prime Infrastructure database as well as apply to the selected controllers. If you click Apply to Controllers, choose the IP address of the controller to which you want to apply the template.</td>
</tr>
</tbody>
</table>

---

**Note** When the template is applied to the selected controllers, a status screen appears. If an error occurred while you applied the template, an error message is displayed. You can click the icon in the Session Output column to get the entire session output.

**Note** If the Controller Telnet credentials check fails or the Controller CLI template fails with invalid username and password even though the correct username and password are configured on the controller, check whether the controller has exceeded the number of CLI connections it can accept. If the connections have exceeded the maximum limit, then either increase the maximum allowed CLI sessions or terminate any pre-existing CLI sessions on the controller, and then retry the operation.

### Configuring Location Configuration Templates

To add or modify a location setting template, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose <strong>Configure &gt; Controller Template Launch Pad</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click <strong>Location &gt; Location Configuration</strong> or choose <strong>Location &gt; Location Configuration</strong> from the left sidebar menu. The Location &gt; Location Configuration page appears, and the number of controllers that the template is applied to automatically populates.</td>
</tr>
</tbody>
</table>
The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Location Configuration template page appears.

Step 4 Select the **RFID Tag Data Collection** check box to enable tag collection. Before the mobility services engine can collect asset tag data from controllers, you must enable the detection of active RFID tags using the CLI command `config rfid status enable` on the controllers.

Step 5 Select the **Calibrating Client** check box to enable calibration for the client. Controllers send regular S36 or S60 requests (depending on the client capability) by way of the access point to calibrating clients. Packets are transmitted on all channels. All access points irrespective of channel (and without a channel change) gather RSSI data from the client at each location. These additional transmissions and channel changes might degrade contemporaneous voice or video traffic.

**Note** To use all radios (802.11a/b/g/n) available, you must enable multiband in the Advanced page.

Step 6 Select the **Normal Client** check box to have a non-calibrating client. No S36 requests are transmitted to the client.

**Note** S36 and S60 are client drivers compatible with specific Cisco-compatible Extensions. S36 is compatible with CCXv2 or later. S60 is compatible with CCXv4 or later. For details, see the following URL: [http://www.cisco.com/en/US/products/ps9806/products_qanda_item09186a0080af9513.shtml](http://www.cisco.com/en/US/products/ps9806/products_qanda_item09186a0080af9513.shtml)

Step 7 Specify how many seconds should elapse before notification of the found element (tags, clients, and rogue APs/clients).

Step 8 Enter the number of seconds after which RSSI measurements for clients should be discarded.

Step 9 Enter the number of seconds after which RSSI measurements for calibrating clients should be discarded.

Step 10 Enter the number of seconds after which RSSI measurements for tags should be discarded.

Step 11 Enter the number of seconds after which RSSI measurement for rogue access points should be discarded.

Step 12 Click the **Advanced** tab.

Step 13 Enter a value in seconds to set the RFID tag data timeout setting.

Step 14 Select the **Calibrating Client Multiband** check box to send S36 and S60 packets (where applicable) on all channels. Calibrating clients must be enabled in the General group box.

Step 15 Click **Save**.

---

**Configuring IPv6 Templates**

- Configuring Neighbor Binding Timers Templates, page 11-119
- Configuring RA Throttle Policy Templates, page 11-119
Configuring Neighbor Binding Timers Templates

You can create or modify a template for configuring IPv6 Router Neighbor Binding Timers such as Down Lifetime, Reachable Lifetime, State Lifetime, and corresponding intervals.

To configure a Neighbor Binding Timers template, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.
Step 2 Click Neighbor Binding Timers or choose IPv6 > Neighbor Binding Timers from the left sidebar menu. The IPv6 > Neighbor Binding Timers page appears.
Step 3 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The Neighbor Binding Timers template page appears.
Step 4 Enter a template name in the text box.
Step 5 If you want to enable the down lifetime, select the Enable check box. If you have selected this check box, specify the value in the Down Lifetime Interval text box. This indicates the maximum time, in seconds, an entry learned from a down interface is kept in the binding table before the entry is deleted or proof is received that the entry is reachable. The range is 0 to 86,400 seconds, and the default value is 0.
Step 6 If you want to enable the reachable lifetime, select the Enable check box. If you have selected this check box, specify the value in the Reachable Lifetime Interval text box. This indicates the maximum time, in seconds, an entry is considered reachable without getting a proof of reachability (direct reachability through tracking, or indirect reachability through Neighbor Discovery protocol [NDP] inspection). After that, the entry is moved to stale. The range is 0 to 86,400 seconds, and the default value is 0.
Step 7 If you want to enable the stale lifetime, select the Enable check box. If you have selected this check box, specify the value in the Stale Lifetime Interval text box. This indicates the maximum time, in seconds, a stale entry is kept in the binding table before the entry is deleted or proof is received that the entry is reachable. The range is 0 to 86,400 seconds, and the default value is 0.
Step 8 Click Save.

Configuring RA Throttle Policy Templates

The RA Throttle Policy allows you to limit the amount of multicast Router Advertisements (RA) circulating on the wireless network. You can create or modify a template for configuring IPv6 Router Advertisement parameters such as RA Throttle Policy, Throttle Period, and other options.

To configure a RA Throttle Policy template, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.
Step 2 Click RA Throttle Policy or choose IPv6 > RA Throttle Policy from the left sidebar menu. The IPv6 > RA Throttle Policy page appears.
Step 3 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The RA Throttle Policy template page appears.
Configuring Controller Templates

Step 4 Enter a template name in the text box.

Step 5 If you want to enable the down lifetime, select the Enable check box. If you have selected this check box, configure the following parameters:

- Throttle Period—Duration of the throttle period in seconds. The range is 10 to 86,400 seconds.
- Max Through—The number of RA that passes through over a period in seconds.
- Interval Option—Indicates the behavior in case of RA with an interval option.
- Allow At-least—Indicates the minimum number of RA not throttled per router.
- Allow At-most—Indicates the maximum number of RA not throttled per router.

Step 6 Click Save.

Configuring RA Guard Templates

RA Guard is a Unified Wireless solution used to drop RA from wireless clients. It is configured globally, and by default it is enabled. You can create or modify a template for configuring IPv6 Router Advertisement parameters.

To configure an RA Guard template, follow these steps:

Step 1 Choose Configure > Controller Template Launch Pad.

Step 2 Click RA Guard or choose IPv6 > RA Guard from the left sidebar menu. The IPv6 > RA Guard page appears.

Step 3 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The RA Guard template page appears.

Step 4 Enter a template name in the text box.

Step 5 If you want to enable the Router Advertisement Guard, select the Enable check box.

Step 6 Click Save.

Configuring Proxy Mobile IPv6 Templates

Proxy Mobile IPv6 is a network-based mobility management protocol that supports a mobile node by acting as the proxy for the mobile node in any IP mobility-related signaling. The mobility entities in the network track the movements of the mobile node and initiate the mobility signaling and set up the required routing state.

The main functional entities are the Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG). The LMA maintains the reachability state of the mobile node and is the topological anchor point for the IP address of the mobile node. The MAG performs the mobility management on behalf of a mobile node. The MAG resides on the access link where the mobile node is anchored. The controller implements the MAG functionality.

- Configuring PMIP Global Configurations, page 11-121
- Configuring LMA Configurations, page 11-121
Chapter 11  Using Templates

Configuring Controller Templates

Configuring PMIP Global Configurations

Step 1  Choose Configure > Controller Template Launch Pad.

Step 2  Click Global Config or choose PMIP > Global Config from the left sidebar menu.

Step 3  If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name.

Step 4  Enter a template name in the text box.

Step 5  Configure the following fields:

- Domain Name
- Maximum Bindings Allowed—Maximum number of binding updates that the controller can send to the MAG. The valid range is between 0 to 40000.
- Binding Lifetime—Lifetime of the binding entries in the controller. The valid range is between 10 to 65535 seconds. The default value is 65535. The binding lifetime should be a multiple of 4 seconds.
- Binding Refresh Time—Refresh time of the binding entries in the controller. The valid range is between 4 to 65535 seconds. The default value is 300 seconds. The binding refresh time should be a multiple of 4 seconds.
- Binding Initial Retry Timeout—Initial timeout between the proxy binding updates (PBUs) when the controller does not receive the proxy binding acknowledgments (PBAs). The valid range is between 100 to 65535 seconds. The default value is 1000 second.
- Binding Maximum Retry Timeout—Maximum timeout between the proxy binding updates (PBUs) when the controller does not receive the proxy binding acknowledgments (PBAs). The valid range is between 100 to 65535 seconds. The default value is 32000 seconds.
- Replay Protection Timestamp—Maximum amount of time difference between the timestamp in the received proxy binding acknowledgment and the current time of the day. The valid range is between 1 to 255 milliseconds. The default value is 7 milliseconds.
- Minimum BRI Retransmit Timeout—Minimum amount of time that the controller waits before retransmitting the BRI message. The valid range is between 500 to 65535 seconds.
- Maximum BRI Retransmit Timeout—Maximum amount of time that the controller waits before retransmitting the Binding Revocation Indication (BRI) message. The valid range is between 500 to 65535 seconds. The default value is 2000 seconds.

Step 6  Click Save.

Configuring LMA Configurations

Step 1  Choose Configure > Controller Template Launch Pad.

Step 2  Click LMA Config or choose PMIP > LMA Config from the left sidebar menu.

Step 3  If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name.

Step 4  Configure the following fields:

- Configuring PMIP Profile, page 11-122
Configuring Controller Templates

- LMA Name—Name of the LMA connected to the controller.
- LMA IP Address—IP address of the LMA connected to the controller.

**Step 5** Click Save.

### Configuring PMIP Profile

**Step 1** Choose Configure > Controller Template Launch Pad.

**Step 2** Click Profile or choose PMIP > Profile from the left sidebar menu.

**Step 3** If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name.

**Step 4** Enter the profile name.

**Step 5** Click Add and then configure the following fields:
- Network Access Identifier—Name of the Network Access Identifier (NAI) associated with the profile.
- LMA Name—Name of the LMA to which the profile is associated.
- Access Point Node—Name of the access point node connected to the controller.

**Step 6** Click Save.

### Configuring mDNS Templates

Multicast DNS (mDNS) service discovery provides a way to announce and discover services on the local network. mDNS perform DNS queries over IP multicast. mDNS supports zero configuration IP networking.

The following are the guidelines and limitations for mDNS templates:
- You cannot delete a mDNS service when it is mapped to one or more profiles.
- The length of the profile name and the services name can be a maximum of 31 characters.
- The length of the service string can be maximum 255 characters.
- You cannot delete the default profile (default-mdns-profile).
- You cannot delete profiles when they are mapped to interfaces, interface-groups, or WLANs.
- You cannot remove mDNS services from a profile when they are mapped to interface, interface-groups or WLANs. You can add new services.
- Whenever you create and apply any mDNS template, it overwrites existing configuration on controller.
- You cannot enable mDNS snooping for WLAN when FlexConnect local switching is ON.
- You cannot attach mDNS profiles to interfaces when "AP Management” is enabled.

You can create a mDNS template so that the controller can learn about the mDNS services and advertise these services to all clients.

There are two tabs—Services and Profiles.
• Services Tab—This tab enables you to configure the global mDNS parameters and update the Master Services database.

• Profiles Tab—This tab enables you to view the mDNS profiles configured on the controller and create new mDNS profiles. After creating a new profile, you must map the profile to an interface group, an interface, or a WLAN. Clients receive service advertisements only for the services associated with the profile. The controller gives the highest priority to the profiles associated to interface groups, followed by the interface profiles, and then the WLAN profiles. Each client is mapped to a profile based on the order of priority. By default, the controller has an mDNS profile, default-mdns-profile. You cannot delete this default profile.

---

**Step 1** Choose Configure > Controller Template Launch Pad.

**Step 2** Click mDNS or choose mDNS > mDNS from the left sidebar menu.

**Step 3** If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name.

**Step 4** On the Services tab, configure the following parameters:

- Template Name—User-defined name of this template.
- mDNS Global Snooping—Check box that you select to enable snooping of mDNS packets.

**Note** The controller does not support IPv6 mDNS packets even when you enable mDNS snooping.

- Query Interval (10-120)—mDNS query interval, in minutes that you can set. This interval is used by WLC to send periodic mDNS query messages to services which do not send service advertisements automatically after they are started. The range is from 10 to 120 minutes. The default value is 15 minutes.

- Master Services—Click Add Row and then configure the following fields:
  - Master Service Name—Drop-down list from which you can choose the supported services that can be queried. The following services are available:
    - AirTunes
    - AirPrint
    - AppleTV
    - HP Photosmart Printer1
    - HP Photosmart Printer2
    - Apple File Sharing Protocol (AFP)
    - Scanner
    - Printer
    - FTP
    - iTunes Music Sharing
    - iTunes Home Sharing
    - iTunes Wireless Device Syncing
    - Apple Remote Desktop
    - Apple CD/DVD Sharing
    - Time Capsule Backup
Chapter 11      Using Templates

Configuring Controller Templates

To add a new service, enter or choose the service name, enter the service string, and then choose the service status.

- **Service Name**—Name of the mDNS service.
- **Service String**—Unique string associated to an mDNS service. For example, `_airplay._tcp.local.` is the service string associated to AppleTV.
- **Query Status**—Check box that you select to enable an mDNS query for a service.

**Note**

Periodic mDNS query messages will be sent by WLC at configured Query Interval for services only when the query status is enabled; otherwise, service should automatically advertised for other services where the query status is disabled (for example AppleTV).

**Step 5**

On the Profiles tab, configure the following parameters:

- **Profiles**—Click **Add Profile** and then configure the following fields:
  - **Profile Name**—Name of the mDNS profile. You can create a maximum of 16 profiles.
  - **Services**—Select the services (using the check boxes) that you want to map to the mDNS profile.

**Step 6**

Click **Save**.

Configuring AVC Profiles Templates

Application Visibility and Control (AVC) uses the Network Based Application Recognition (NBAR) deep packet inspection technology to classify applications based on the protocol they use. Using AVC, the controller can detect more than 1400 Layer 4 to Layer 7 protocols. AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades.

AVC is supported only on the Cisco 2500 and 5500 Series Controllers, WiSM 2 Controllers, and Cisco Flex 7500 and Cisco 8500 Series Controllers.

**Step 1**

Choose **Configure > Controller Template Launch Pad**.

**Step 2**

Click **AVC Profiles** or choose **Application Visibility And Control > AVC Profiles** from the left sidebar menu.

**Step 3**

If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name.

**Step 4**

Enter a template name in the text box.

**Step 5**

Enter an AVC Profile Name.

**Note**

You can configure only one AVC profile per WLAN and each AVC profile can have up to 32 rules. Each rule states a Mark or Drop action for an application. This allows you to configure up to 32 application actions per WLAN. You can configure up to 16 AVC profiles on a controller and associate an AVC profile with multiple WLANs.
Chapter 11      Using Templates

Configuring Controller Templates

Step 6  Under the AVC Rule List, click Add Row to create AVC rules.

- Application Name—Name of the application.
- Application Group Name—Name of the application group to which the application belongs.
- Action—Drop-down list from which you can choose the following:
  - Drop—Drops the upstream and downstream packets corresponding to the chosen application.
  - Mark—Marks the upstream and downstream packets corresponding to the chosen application with the DSCP value that you specify in the Differentiated Services Code Point (DSCP) drop-down list. The DSCP value helps you provide differentiated services based on the QoS levels.
    The default action is to permit all applications.
- DSCP—Packet header code that is used to define quality of service across the Internet. The DSCP values are mapped to the following QoS levels:
  - Platinum (Voice)—Assures a high QoS for Voice over Wireless.
  - Gold (Video)—Supports the high-quality video applications.
  - Silver (Best Effort)—Supports the normal bandwidth for clients.
  - Bronze (Background)—Provides lowest bandwidth for guest services.
- DSCP Value—You can also choose Custom and specify the DSCP value. The range is from 0 to 63.

Step 7  Click Save.

Configuring NetFlow Templates

NetFlow is a protocol that provides valuable information about network users and applications, peak usage times, and traffic routing. This protocol collects IP traffic information from network devices to monitor traffic. The NetFlow architecture consists of the following components:

- Collector—An entity that collects all the IP traffic information from various network elements.
- Exporter—A network entity that exports the template with the IP traffic information. The controller acts as an exporter.

Configuring NetFlow Monitor Template, page 11-125
Configuring NetFlow Exporter Template, page 11-126

Configuring NetFlow Monitor Template

Step 1  Choose Configure > Controller Template Launch Pad.
Step 2  Click Monitor or choose NetFlow > Monitor from the left sidebar menu.
Step 3  If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name.
Step 4  Enter a template name in the text box.
Step 5  Configure the following parameters:
  - Monitor Name—Name of the NetFlow monitor. The monitor name can be up to 127 case-sensitive alphanumeric characters. You can configure only one monitor in the controller.
Configuring NetFlow Exporter Template

Step 1  Choose Configure > Controller Template Launch Pad.
Step 2  Click Exporters or choose NetFlow > Exporters from the left sidebar menu.
Step 3  If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name.
Step 4  Enter a template name in the text box.
Step 5  Configure the following parameters:
  - Exporter Name—Name of the exporter.
  - Exporter IP —IP address of the exporter.
  - Port Number—The UDP port through which the NetFlow record is exported.
Step 6  Click Save.

Note  You can configure only one NetFlow Exporter per controller.

Configuring AP Configuration Templates

This menu provides access to the access point templates summary details. Use the selector group box to access and configure the respective templates details.
Chapter 11  Using Templates

Configuring AP Configuration Templates

Configuring Lightweight Access Point Templates

- Configuring a New Lightweight Access Point Template, page 11-127
- Editing a Current Lightweight Access Point Template, page 11-134

Configuring a New Lightweight Access Point Template

To configure a new Lightweight Access Point template, follow these steps:

Step 1  Choose Configure > Lightweight AP Configuration Templates.
Step 2  From the Select a command drop-down list, choose Add Template.
Step 3  Click Go.
Step 4  Enter a template name in the text box.
Step 5  Enter a template description in the text box.
Step 6  Click Save as New Template.

The Lightweight AP Template Detail page contains the following tabs:
- AP Parameters Tab, page 11-127
- Mesh Tab, page 11-130
- 802.11a/n/ac Tab, page 11-130
- 802.11a SubBand Tab, page 11-131
- 802.11b/g/n Tab, page 11-131
- CDP Tab, page 11-132
- FlexConnect Tab, page 11-132

AP Parameters Tab

General
- Location—Enter the location in the Location text box.
- Admin Status—Select the Admin and Enabled check box to enable administrative status.

Note  To conserve energy, access points can be turned off at specified times during non-working hours. Select the Enabled check box to allow access points to be turned on or off.
• AP Mode—From the drop-down list, choose one of the following:
  
  - **Local**—Default
  - **Monitor**—Monitor mode only.

  **Note**  Choose **Monitor** to enable this access point template for Cisco Adaptive wIPS. Once Monitor is selected, select the **Enhanced WIPS Engine** check box and the **Enabled** check box.

  - **FlexConnect**—Cisco 1030 remote edge lightweight access point (REAP) used for Cisco 1030 IEEE 802.11a/b/g/n remote edge lightweight access points.
  - **Rogue Detector**—Monitors the rogue access points but does not transmit or contain rogue access points.
  - **Bridge**
  - **Sniffer**—The access point “sniffs” the air on a given channel. It captures and forwards all the packets from the client on that channel to a remote machine that runs AiroPeek (a packet analyzer for IEEE 802.11 wireless LANs). It includes information on timestamp, signal strength, packet size, and so on. If you choose Sniffer as an operation mode, you are required to enter a channel and server IP address on the AP/Radio Templates 802.11b/g/n or 802.11a/n parameters tab.
  - **SE-Connect**—This mode allows a CleanAir-enabled access point to be used extensively for interference detection on all monitored channels. All other functions such as IDS scanning and Wi-Fi are suspended.

• AP Sub Mode—Choose an option from the drop-down list.

  **Note**  Using the AP Sub Mode drop-down list, you can configure the AP Sub Mode for the Cisco unified controllers, but you cannot configure the AP Sub Mode for the Cisco New Generation Wireless Controllers (NGWC) devices. For Cisco NGWC devices, you can use the Enhanced wIPS Engine to change the AP sub-mode.

• Enhanced wIPS Engine—Select the **Enhanced wIPS engine** and the **Enabled** check box to enable.

• AP Height (feet)—Enter the height of the access point (in feet) in the text box.

• Mirror Mode—Select the **Enabled** check box to enable mirror mode.

• Country Code—Choose the appropriate country code from the drop-down list.

• Stats Collection Interval—Enter the stats collection interval in the text box.

• Cisco Discovery Protocol—Select the **Enabled** check box to enable Cisco Discovery Protocol.

• AP Failover Priority—Choose **Low**, **Medium**, **High**, or **Critical** from the drop-down list to indicate the access point failover priority. The default priority is low.

• Pre-Standard 802.3af switches.

• Antenna Band Mode.

• Domain Name—Domain Name can be configured only on APs which have static IP.

• Server IP Address—Domain Name Server IP can be configured only on APs which have static IP.

• Encryption—Select the **Encryption** check box to enable encryption.

• Rogue Detection—Select the check box to enable rogue detection.
- **SSH Access**—Select the **SSH Access** check box to enable SSH access.
- **Telnet Access**—Select the **Telnet Access** check box to enable Telnet access.
- **Link Latency**—You can configure link latency on the controller to measure the link between an access point and the controller.

  **Note** Link latency is supported for use only with FlexConnect access points in connected mode. FlexConnect access points in standalone mode are not supported.

- **TCP Adjust MSS**—Select the **TCP Adjust MSS** check box to enable TCP to adjust MSS.
- **VLAN Tagging**—VLAN Tagging is supported only from controller version 7.3.1.26. If you change the mode or value of VLAN tagging, the access point will be rebooted. VLAN tagging cannot be enabled when the AP is in Bridge mode. Enabling VLAN tagging will ignore the value of Native VLAN ID.
- **AP Group Name**
- **Reboot AP**—Select the check box to enable a reboot of the access point after making any other updates.

**Power Injector Configuration**
- **Power Injector State**—When enabled, this allows you to manipulate power injector settings through Prime Infrastructure without having to go directly to the controllers. If the Enable Power Injector State is selected, power injector options appear.
- **Power Injector Selection**—Choose **installed** or **override** from the drop-down list.
- **Injector Switch MAC Address**—Enter the MAC address of the injector switch.

**Global Username Password Configuration**
- **Override Global Username Password**—Select the check box to enable an override for the global username/password. Enter and confirm the new access point username and password in the appropriate text boxes.

**Supplicant Credentials Configuration**
- **Override Supplicant Credentials**—Select the **Override Supplicant Credentials** check box to prevent this access point from inheriting the authentication username and password from the controller. The default value is unselected. The Override Supplicant Credentials option is supported in controller Release 6.0 and later.
  - In the Username, Password, and Confirm Password text boxes, enter the unique username and password that you want to assign to this access point.

**AP Retransmit Configuration**
- **AP Retransmit Count**—Enter the AP Retransmit Count. The AP Retransmit Count default value is 5 and the range is from 3 to 8.
- **AP Retransmit Interval(secs)**—Enter the AP Retransmit Intervals. The AP Retransmit Interval default value is 3. The range is 2 to 5.

**Controller Configuration**
Select the Controllers Configuration check box to enable the drop-down lists for the primary, secondary, and tertiary controller names.
• Primary, Secondary, and Tertiary Controller Name—The Primary/Secondary/Tertiary Controller names.
• Primary, Secondary, and Tertiary Controller IP—The Primary/Secondary/Tertiary Controller IP is the Management IP of the controller.

Venue Configuration
• Venue Group
• Venue Type
• Secondary Venue Name
• Language

Mesh Tab

Use the Mesh tab to set the following parameters for mesh access points:
• Bridge Group Name—Enter a bridge group name (up to 10 characters) in the text box.

  **Note** Bridge groups are used to logically group the mesh access points to avoid two networks on the same channel from communicating with each other. For mesh access points to communicate, they must have the same bridge group name. For configurations with multiple RAPs, make sure that all RAPs have the same bridge group name to allow failover from one RAP to another.

• Data Rate (Mbps)—Choose the data rate for the backhaul interface from the drop-down list. Data rates available are dictated by the backhaul interface. The default rate is 18 Mbps.

  **Note** This data rate is shared between the mesh access points and is fixed for the whole mesh network. Do not change the data rate for a deployed mesh networking solution.

• Ethernet Bridge—From the Ethernet Bridging drop-down list, enable Ethernet bridging for the mesh access point.
• Role—Choose the role of the mesh access point from the drop-down list (MAP or RAP). The default setting is MAP.

  **Note** An access point in a mesh network functions as either a root access point (RAP) or mesh access point (MAP).

• The Ethernet Interfaces area group box provides information such as interface name, mode, VLAN ID, and Trunk ID. Select the appropriate interface and specify its mode.

802.11a/n/ac Tab

• Select the check boxes of the 802.11a parameters that must be applied:
  – Channel Assignment
  – Channel Width
  – Admin Status
Configuring AP Configuration Templates

802.11a SubBand Tab

In the 802.11a SubBand tab, select the 802.11a Sub Band options (for either 4.9 or 5.8 parameters) that must be applied:

- Admin Status
- Channel Assignment—Select the check box and then choose the appropriate channel from the drop-down list.

*Note*  The channel number is validated against the radio list of supported channels.

- Power Assignment—Select the check box and then choose the appropriate power level from the drop-down list.

*Note*  The power level is validated against the radio list of supported power levels.

- Antenna Type—Select the check box and then choose the antenna type from the drop-down list.
- Antenna Name—Select the Antenna Type check box and then choose the applicable antenna name from the drop-down list.

*Note*  Not all antenna models are supported by radios of different access point types.

802.11b/g/n Tab

Select the check box of the 802.11b/g/n parameters that must be applied:

- Channel Assignment
- Admin Status
- Antenna Mode
- Antenna Diversity
- Antenna Name
- Power Assignment
- Tracking Optimized Monitor Mode
- 11n Antenna Selection
- CleanAir

**CDP Tab**

- In the Cisco Discovery Protocol on Ethernet Interfaces group box, select the check boxes for the slots of Ethernet interfaces for which you want to enable CDP.
- In the Cisco Discovery Protocol on Radio Interfaces group box, select the slots of Radio interfaces for which you want to enable CDP.

**FlexConnect Tab**

- Select the **FlexConnect Configuration** check box to enable FlexConnect configuration (including VLAN support, native VLAN ID, and profile name VLAN mappings).

  **Note** These options are only available for access points in FlexConnect mode.

  - OfficeExtend—The default is Enabled.

  **Note** When you select Enable for the OfficeExtend AP, several configuration changes automatically occur including: encryption and link latency are enabled; rogue detection, SSH access, and Telnet access are disabled.

  **Note** When you enable the OfficeExtend access point, you must configure at least one primary, secondary, and tertiary controller (including name and IP address).

  - Least Latency Controller Join—When enabled, the access point switches from a priority order search (primary, secondary, and then tertiary controller) to a search for the controller with the best latency measurement (least latency). The controller with the least latency provides the best performance.

    **Note** The access point only performs this search once when it initially joins the controller. It does not recalculate the latency measurements of primary, secondary, and tertiary controllers once joined to see if the measurements have changed.

  - VLAN Support
  - Native VLAN ID
Configuring AP Configuration Templates

**Note**
The valid native VLAN ID range is 1—4094. If you are changing the mode to REAP and if the access point is not already in REAP mode, then all other REAP parameters are not applied on the access point.

- Select the **WLAN VLAN Mapping** check box to enable WLAN VLAN mapping (including WLAN profile name and VLAN ID mappings).
- Select the **VLAN ID ACL Mapping** check box to enable VLAN ID ACL Mappings. Enter a VLAN ID and choose the Ingress and Egress ACLs from the drop-down list boxes to map to the VLAN ID specified.
- Select the **Web Auth ACL Mapping** check box to enable Web Auth ACL mapping.
- Select the **Policy ACL Mapping** check box to enable policy ACL mapping.
- Select the **Local Split ACL Mapping** check box to enable Local Split ACL mapping.

**Selecting Access Points for Template Deployment**

- Choose **Configure > Lightweight AP Configuration Templates**.
- Click the applicable template in the Template Name column.
- Select one or more access points by selecting their respective check boxes.

**Note**
You can use the Filter feature to search for specific access points. For details see the Filters section of the Cisco Prime Infrastructure User Guide.

- Click **Deploy** to save and deploy the template to the relevant access points.
- Click **Apply** to save and apply the AP/Radio parameters to the selected access points from the search.

**Note**
You can deploy the template using the AP Selection or Schedule tabs.

**Scheduling Template Deployment**

Allows you to save the current template, apply the current template immediately, or schedule the current template to start the provisioning at the applicable time.

- **Start Time**—Allows you to configure and start the template deployment at a scheduled time.
  - **Now**—Deploys the template right away.
  - **Date**—Enter a date in the text box or use the calendar icon to select a start date.
- **Recurrence**—Select from none, hourly, daily, or weekly to determine how often this scheduling occurs.

**Note**
You can deploy the template using the AP Selection or Schedule tabs.
Viewing the Status of the Template Deployment

Displays all recently applied reports including the apply status and the date and time the apply was initiated. Click the link that is available on the number of access points (next to the Template Deployed to APs field) to view the deployment status information.

- Graph shows the Success or Partial Success status. Click the graph to view status information.
- The Deploy Status section shows the following information:
  - AP Name
  - Status—Indicates success, partial failure, failure, or not initiated. For failed or partially failed provisioning, click Details to view the failure details (including what failed and why it failed).
  - Ethernet MAC—Indicates the Ethernet MAC address for the applicable access point.
  - Controller IP—Indicates the controller IP address for the applicable access point.
  - AP IP
  - Controller Name
  - AP Model
  - Campus
  - Building
  - Floor
  - Outdoor Area
  - FlexConnect Group

Editing a Current Lightweight Access Point Template

To edit a current Lightweight Access Point Template, follow these steps:

Step 1 Choose Configure > Lightweight AP Configuration Templates.

Step 2 Click the applicable template in the Template Name column.

Step 3 Make any necessary changes to the current lightweight access point template or schedule.

Configuring Autonomous Access Point Templates

The Configuring > Autonomous Access Point Templates page allows you to configure CLI templates for autonomous access points.

- Configuring a New Autonomous Access Point Template, page 11-135
- Applying an AP Configuration Template to an Autonomous Access Point, page 11-135
- Editing Current Autonomous AP Migration Templates, page 11-138
Configuring a New Autonomous Access Point Template

To configure a new Autonomous Access Point template, follow these steps:

**Step 1** Choose Configure > Autonomous AP Configuration Templates.
**Step 2** From the Select a command drop-down list, choose Add Template.
**Step 3** Click Go.
**Step 4** Enter a Template Name.
**Step 5** Enter the applicable CLI commands.

<table>
<thead>
<tr>
<th>Note</th>
<th>Do not include any show commands in the CLI commands text box. The show commands are not supported.</th>
</tr>
</thead>
</table>
**Step 6** Click Save.

Applying an AP Configuration Template to an Autonomous Access Point

To apply an AP Configuration template to an autonomous access point, follow these steps:

**Step 1** Choose Configure > Autonomous AP Configuration Templates.
**Step 2** Click the template name link to select a template and apply it to the autonomous access point. The New Autonomous AP Configuration template page appears.
**Step 3** Enter a Template Name.
**Step 4** Enter the applicable CLI commands.
**Step 5** Click Save.
**Step 6** Click Apply to Autonomous Access Points. The Apply to Autonomous Access Points page appears.
**Step 7** Select the desired autonomous access point.
**Step 8** Click OK.

| Note | Select the Ignore errors on Apply template to Controllers check box to ignore errors and apply all commands in the template to the Autonomous AP. If this check box is not selected, any errors encountered while applying a command in the template to a Autonomous AP causes the rest of the commands to be not applied. |

Viewing Template Results

To view the results when you apply an Autonomous AP Configuration template to an access point, follow these steps:

**Step 1** Choose Configure > AP Configuration Templates > Autonomous AP.
### Configuring Switch Location Configuration Templates

You can configure the location template for a switch using the Switch Location Configuration template. To configure a location template for a switch, follow these steps:

**Step 1** Choose **Prime Infrastructure > Configure > Switch Location Configuration Template**. The Switch Location Configuration template page appears.

**Step 2** From the Select a command drop-down list, choose **Add Template**, and click **Go**. The New Template page appears.

**Table 11-4** lists the fields in the New Template page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Template Name</td>
<td>Name of the template.</td>
</tr>
<tr>
<td>Map Location</td>
<td></td>
</tr>
<tr>
<td>Campus</td>
<td>Choose a campus for the map location for a switch/switch port.</td>
</tr>
<tr>
<td>Building</td>
<td>Choose a building for the map location for a switch/switch port.</td>
</tr>
<tr>
<td>Floor</td>
<td>Choose a floor for the map location for a switch/switch port.</td>
</tr>
</tbody>
</table>
Configuring Autonomous AP Migration Templates

This section contains the following topic:

- Migrating an Autonomous Access Point to a Lightweight Access Point, page 11-137
- Viewing the Current Status of Cisco IOS Access Points, page 11-142

Migrating an Autonomous Access Point to a Lightweight Access Point

To make a transition from an Autonomous solution to a Unified architecture, autonomous access points must be converted to lightweight access points. The migration utility is available in the Configure > Autonomous AP Migration Templates page where existing templates are listed.

The Autonomous AP Migration Templates list page displays the following information:

- Name—The template name.
- Description—The description of template.
- AP Count—The number of autonomous access points selected for migration.
- Schedule Run—The time at which the task is scheduled to run.
- Status—Indicates one of the following task statuses:
  - Not initiated—The template is yet to start the migration and starts at the scheduled time.
  - Disabled—The template is disabled and does not run at the scheduled time. This is the default state for a template when it is created without selecting any autonomous access points.
  - Expired—The template did not run at the scheduled time (this might be due to Prime Infrastructure server being down).
  - Enabled—The template is yet to start the migration and starts at the scheduled time.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import</td>
<td>Imports the civic information for the campus, building, and floor selected.</td>
</tr>
</tbody>
</table>

### ELIN and Civic Location

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ELIN</td>
<td>The Emergency Location Identification Number.</td>
</tr>
<tr>
<td>Civic Address tab</td>
<td>The available civic address information for the switch/switch port.</td>
</tr>
<tr>
<td>Advanced tab</td>
<td>Detailed information about the switch/switch port location.</td>
</tr>
<tr>
<td>NMSP</td>
<td>Select or unselect this check box to enable or disable NMSP for the switch.</td>
</tr>
</tbody>
</table>

### Buttons

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves the template.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Discards the template creation.</td>
</tr>
</tbody>
</table>
Chapter 11      Using Templates

Configuring Autonomous AP Migration Templates

- In progress—The template is currently converting the selected autonomous access points to CAPWAP.
- Success—The template has completed the migration of autonomous access point to CAPWAP successfully.
- Failure—The template failed to migrate all the selected autonomous access point to CAPWAP. You can check the detailed status about the failures by using the View Migration Status page.
- Partial Success—The template failed to migrate a subset of the selected autonomous access point to CAPWAP. You can check the detailed status about the failures by using the View Migration Status page.

Note In any of these states, you can edit the template by clicking the Name link.

Note Once an access point is converted to lightweight, the previous status or configuration of the access point is not retained.

From the Select a command drop-down list, the following functions can be performed:

- Add Template—Allows you to provide necessary information for migration.
- Delete Templates—Allows you to delete a current template.
- View Migration Report—Allows you to view information such as AP address, migration status (in progress or fail), timestamp, and a link to detailed logs.
- View Current Status— Allows you to view the progress of the current migration (updated every three seconds).

Note When you migrate an already-managed autonomous access point to lightweight, its location and antenna information is migrated as well. You do not need to reenter the information. Prime Infrastructure automatically removes the autonomous access point after migration.

- View Migration Analysis Summary—Lists the pass or fail status as required for an access point conversion. Only those access points with all criteria as pass are eligible for conversion.

Note The Migration Analysis option does not run during discovery by default. If you prefer to run the migration analysis during discovery, choose Administration > Settings > CLI Session to enable this option.

Note Prime Infrastructure also supports the migration of autonomous access point to CAPWAP access point.

Editing Current Autonomous AP Migration Templates

To edit a current migration template, follow these steps:

**Step 1** Choose Configure > Autonomous AP Migration Templates.

**Step 2** Click the migration template in the Name column.
Step 3

Edit the necessary parameters:

- **General**
  - Name—Indicates the user-defined name of the migration template.
  - Description—Enter a brief description to help you identify the migration template.

- **Upgrade Options**
  - DHCP Support—Click to enable Dynamic Host Configuration Protocol support. This ensures that after the conversion every access point gets an IP from the DHCP server.
  - Retain AP HostName—Click to enable retention of the same hostname for this access point.

  **Note**  
The hostname is retained in the CAPWAP, only when you are migrating the AP to CAPWAP for the first time. It might not be retained if you are upgrading an AP for several times. The CAPWAP access points hostname is set to default if autonomous access points hostname has more than 32 characters.

  **Note**  
  If you upgrade the access points to LWAPP from 12.3(11)JA, 12.3(11)JA1, 12.3(11)JA2, 12.3(11)JA3 autonomous images, the converted access points might not retain their Static IP Address, Netmask, Hostname and Default Gateway.

  - Migrate over WANLink—If you enable this option, the $env_vars$ file stores the remote TFTP server location. This information is copied to the AP. If this option is not selected, then Prime Infrastructure internal TFTP server is used to copy the $env_vars$ file to AP.
  - DNS Address—Enter the DNS address.
  - Domain Name—Enter the domain name.

- **Controller Details**

  **Note**  
  Ensures that the access point authorization information (SSC) can be configured on this controller and the converted access points can join.

  - Controller IP
  - AP Manager IP
  - User Name
  - Password

- **TFTP Details**
  - TFTP Server IP
  - File Path
  - File Name

- **Schedule Details**
  - Apply Template
  - Notification (Optional)
Chapter 11     Using Templates

Step 4  Click Save.

Viewing the Migration Analysis Summary

To view the Migration Analysis Summary, follow these steps:

Note  You can also view the migration analysis summary by choosing Tools > Migration Analysis.

Step 1  Choose Configure > Autonomous AP Migration Templates.

Step 2  Choose View Migration Analysis Summary from the Select a command drop-down list, and click Go. The Migration Analysis Summary page appears.

The autonomous access points are eligible for migration only if all the criteria have a pass status. A red X designates ineligibility, and a green checkmark designates eligibility. These columns represent the following:

- Privilege 15 Criteria—The Telnet credential provided as part of the autonomous access point discovery must be privilege 15.
- Software Version Criteria—Conversion is supported only in Cisco IOS Release 12.3(7)JA excluding 12.3(11)JA, 12.3(11)JA1, 12.3(11)JA2, and 12.3(11)JA3.
- Role Criteria—A wired connection between the access point and controller is required to send the association request; therefore, the following autonomous access point roles are required:
  - root
  - root access point
  - root fallback repeater
  - root fallback shutdown
  - root access point only
- Radio Criteria—in dual-radio access points, the conversion can happen even if only one radio is of the supported type.

Adding/Modifying a Migration Template

If you want to add a migration template, choose Add Template from the Select a command drop-down list in the Configure > Autonomous AP Migration Templates page.

To modify an existing template, click the template name from the summary list.

Enter or modify the following migration parameters:

General

- Name—User-defined name of this migration template.
- Description—Brief description to help you identify the migration template.
Upgrade Options

- DHCP Support—Ensures that after the conversion every access point gets an IP from the DHCP server.
- Retain AP HostName—Allows you to retain the same hostname for this access point.
- Migrate over WANLink—Increases the default timeouts for the CLI commands executed on the access point.
- DNS Address
- Domain Name

Controller Details

Note

Ensure that the access point authorization information (SSC) can be configured on this controller and the converted access points can join.

- Controller IP—Enter the IP address of the WLAN controller you are wanting to add to the newly migrated access point.
- AP Manager IP—Specify the controller the access point should join by entering the access point manager IP address.

Note

For SSC-enabled access points, this IP address must be the same as the controller IP field. For MIC-enabled access points, the IP addresses need not match.

- User Name—Enter a valid username for login of the WLAN controller.
- Password—Enter a valid password for this username used during WLAN controller login.

TFTP Details

Prime Infrastructure provides its own TFTP and FTP server during the installation and setup.

- TFTP Server IP—Enter the IP address of Prime Infrastructure server.
- File Path—Enter the TFTP directory which was defined during Prime Infrastructure setup.
- File Name—Enter the CAPWAP conversion file defined in the TFTP directory during Prime Infrastructure setup (for example, c1240-rcvk9w8-tar.123-11JX1.tar).

Schedule Details

This group box enables you to specify scheduling options for migration templates.

- Apply Template—Choose an option by which you want to apply the template for migration.
  - Now—Choose this option to run the migration task immediately.
  - Schedule for later date/time—If you plan to schedule the migration at a later time, enter the Schedule parameters. Enter a date in the text box, or click the calendar icon to open a calendar from which you can choose a date. Choose the time from the hours and minutes drop-down lists. The report begins running on this data and at this time.
- (Optional) Notification—Enter the e-mail address of recipient to send notifications via e-mail.
Configuring Autonomous AP Migration Templates

Note

To receive e-mail notifications, configure Prime Infrastructure mail server in the Administration > Settings > Mail Server Configuration page.

- Click Save.

Once a template is added in Prime Infrastructure, the following additional buttons appear:

- Select APs—Choosing this option provides a list of autonomous access points in Prime Infrastructure from which to choose the access points for conversion. Only those access points with migration eligibility as pass can be chosen for conversion.
- Select File—To provide CSV information for access points intended for conversion.

Copying a Migration Template

To copy a migration template, follow these steps:

Step 1
Choose Configure > Autonomous AP Migration Templates.

Step 2
Select the check box of the template you want to copy, and then choose Copy Template from the Select a command drop-down list.

Step 3
Click Go.

Step 4
Enter the name for the new template to which you want to copy the current template.

Deleting Migration Templates

To delete migration templates, follow these steps:

Step 1
Choose Configure > Autonomous AP Migration Templates.

Step 2
Select the check box(es) of the template(s) you want to delete, and then choose Delete Templates from the Select a command drop-down list.

Step 3
Click Go.

Step 4
Click OK to confirm the deletion or Cancel to close this page without deleting the template.

Viewing the Current Status of Cisco IOS Access Points

Select View Current Status from the Select a command drop-down list in the Autonomous AP Migration Templates page to view the status of Cisco IOS access point migration.

The following information is displayed:
- IP Address—IP address of the access point.
- Status—Current status of the migration.
- Progress—Summary of the migration progress.
Disabling Access Points that are Ineligible

If an autonomous access point is labelled as ineligible for conversion, you can disable it.
Configuring FlexConnect

This chapter describes FlexConnect and explains how to configure this feature on controllers and access points. It contains the following sections:

- Information About FlexConnect, page 12-1
- Configuring FlexConnect, page 12-4
- FlexConnect Access Point Groups, page 12-9

Information About FlexConnect

*FlexConnect* is a 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 a controller in each office. There is no deployment restriction on the number of FlexConnect access points per location. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller.

FlexConnect is supported only on the 1130AG, 1240AG, 1142 and 1252 access points and on the 2000 and 4400 series controllers, the Catalyst 3750G Integrated Wireless LAN Controller Switch, the Cisco WiSM, the Controller Network Module for Integrated Services Routers, and the controller within the Catalyst 3750G Integrated Wireless LAN Controller Switch. *Figure 12-1* illustrates a typical FlexConnect deployment.
FlexConnect Authentication Process

When a FlexConnect access point boots up, it looks for a controller. If it finds one, it joins the controller, downloads the latest software image from the controller and configuration information, and initializes the radio. It saves the downloaded configuration in non-volatile memory for use in standalone mode.

A FlexConnect access point can learn the controller IP address in one of the following ways:

- If the access point has been assigned an IP address from a DHCP server, it discovers a controller through the regular CAPWAP discovery process [Layer 3 broadcast, over-the-air provisioning (OTAP), DNS, or DHCP option 43.]

  Note
  OTAP does not work on the first boot out of the box.

- If the access point has been assigned a static IP address, it can discover a controller through any of the CAPWAP discovery process methods except DHCP option 43. If the access point cannot discover a controller through Layer 3 broadcast or OTAP, we recommend DNS resolution. With DNS, any access point with a static IP address that knows of a DNS server can find at least one controller.

- If you want the access point to discover a controller from a remote network where CAPWAP discovery mechanisms are not available, you can use priming. This method enables you to specify (through the access point command-line interface) the controller to which the access point is to connect.

When a FlexConnect access point can reach the controller (referred to as connected mode), the controller assists in client authentication. When a FlexConnect access point cannot access the controller, the access point enters standalone mode and authenticates clients by itself.
Note

The LEDs on the access point change as the device enters different FlexConnect modes. See the hardware installation guide for your access point for information on LED patterns.

When a client associates to a FlexConnect access point, the access point sends all authentication messages to the controller and either switches the client data packets locally (locally switched) or sends them to the controller (centrally switched), depending on the WLAN configuration. With respect to client authentication (open, shared, EAP, web authentication, and NAC) and data packets, the WLAN can be in any one of the following states depending on the configuration and state of controller connectivity:

- **central authentication, central switching** — In this state, the controller handles client authentication, and all client data tunnels back to the controller. This state is valid only in connected mode.

- **central authentication, local switching** — In this state, the controller handles client authentication, and the FlexConnect access point switches data packets locally. After the client authenticates successfully, the controller sends a configuration command with a new payload to instruct the FlexConnect access point to start switching data packets locally. This message is sent per client. This state is applicable only in connected mode.

- **local authentication, local switching** — In this state, the FlexConnect access point handles client authentication and switches client data packets locally. This state is valid in standalone mode and connected mode.

Local authentication is useful where you cannot maintain the criteria a remote office setup of minimum bandwidth of 128 kbps with the roundtrip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes. In local switching, the authentication capabilities are present in the access point itself. Thus local authentication reduces the latency requirements of the branch office.

Note

Local authentication can only be enabled on the WLAN of a FlexConnect access point that is in local switching mode.

Local authentication is not supported in the following scenarios:

- Guest Authentication cannot be done on a FlexConnect local authentication enabled WLAN.
- RRM information is not available at the controller for the FlexConnect local authentication enabled WLAN.
- Local radius is not supported.
- Once the client has been authenticated, roaming is only be supported after the WLC and the other FlexConnects in the group are updated with the client information.

- **authentication down, switching down** — In this state, the WLAN disassociates existing clients and stops sending beacon and probe responses. This state is valid only in standalone mode.

- **authentication down, local switching** — In this state, the WLAN rejects any new clients trying to authenticate, but it continues sending beacon and probe responses to keep existing clients alive. This state is valid only in standalone mode.

When a FlexConnect access point enters standalone mode, WLANs that are configured for open, shared, WPA-PSK, or WPA2-PSK authentication enter the “local authentication, local switching” state and continue new client authentications. Other WLANs enter either the “authentication down, switching down” state (if the WLAN was configured to central switching) or the “authentication down, local switching” state (if the WLAN was configured to local-switch).
When a FlexConnect access point enters standalone mode, it disassociates all clients that are on centrally switched WLANs. For 802.1X or web-authentication WLANs, existing clients are not disassociated, but the FlexConnect access point stops sending beacons when the number of associated clients reaches zero (0). It also sends disassociation messages to new clients associating to 802.1X or web-authentication WLANs. Controller-dependent activities such as 802.1X authentication, NAC, and web authentication (guest access) are disabled, and the access point does not send any Intrusion Detection System (IDS) reports to the controller. Furthermore, most Radio Resource Management (RRM) features (such as neighbor discovery; noise, interference, load, and coverage measurements; use of the neighbor list; and rogue containment and detection) are disabled. However, a FlexConnect access point supports dynamic frequency selection in standalone modes.

**Note**
If your controller is configured for Network Access Control (NAC), clients can associate only when the access point is in connected mode. When NAC is enabled, you need to create an unhealthy (or quarantined) VLAN so that the data traffic of any client that is assigned to this VLAN passes through the controller, even if the WLAN is configured for local switching. After a client is assigned to a quarantined VLAN, all of its data packets are centrally switched.

The FlexConnect access point maintains client connectivity even after entering standalone mode. However, once the access point reestablishes a connection with the controller, it disassociates all clients, applies new configuration information from the controller, and reallows client connectivity.

**FlexConnect Guidelines**

Keep the following guidelines in mind when using FlexConnect:

- A FlexConnect access point can be deployed with either a static IP address or a DHCP address. In the case of DHCP, a DHCP server must be available locally and must be able to provide the IP address for the access point at bootup.

- FlexConnect supports a 500-byte maximum transmission unit (MTU) WAN link at minimum.

- Roundtrip latency must not exceed 300 milliseconds (ms) between the access point and the controller, and CAPWAP control packets must be prioritized over all other traffic. In cases where you cannot achieve this, you can configure the access point to perform local authentication. See the “FlexConnect Authentication Process” section on page 12-2 for more information about FlexConnect local authentication and local switching.

- The controller can send multicast packets in the form of unicast or multicast packets to the access point. In FlexConnect mode, the access point receives multicast packets only in unicast form.

- FlexConnect supports CCKM full authentication but not CCKM fast roaming.

- FlexConnect supports a 1-1 network address translation (NAT) configuration. It also supports Port Address Translation (PAT) for all features except true multicast. Multicast is supported across NAT boundaries when configured using the Unicast option.

- VPN, IPsec, L2TP, PPTP, Fortress authentication, and Cranite authentication are supported for locally switched traffic, provided that these security types are accessible locally at the access point.

**Configuring FlexConnect**

To configure FlexConnect, you must follow the instructions in this section in the order provided.

- Configuring the Switch at the Remote Site, page 12-5
Configuring the Switch at the Remote Site

To prepare the switch at the remote site, follow these steps:

**Step 1**
Attach the access point that is enabled for FlexConnect to a trunk or access port on the switch.

**Note** The following sample configuration shows the FlexConnect access point connected to a trunk port on the switch.

**Step 2**
See the sample configuration that follows to configure the switch to support the FlexConnect access point.

In this sample configuration, the FlexConnect access point is connected to trunk interface FastEthernet 1/0/2 with native VLAN 100. The access point needs IP connectivity on the native VLAN. The remote site has local servers/resources on VLAN 101. A DHCP pool is created in the local switch for both VLANs in the switch. The first DHCP pool (NATIVE) is used by the FlexConnect access point, and the second DHCP pool (LOCAL-SWITCH) is used by the clients when they associate to a WLAN that is locally switched. The bolded text in the sample configuration illustrates these settings.

**Note** The addresses in this sample configuration are for illustration purposes only. The addresses that you use must fit into your upstream network.

```plaintext
ip dhcp pool NATIVE
    network 10.10.100.0 255.255.255.0
    default-router 10.10.100.1

ip dhcp pool LOCAL-SWITCH
    network 10.10.101.0 255.255.255.0
    default-router 10.10.101.1

interface FastEthernet1/0/1
    description Uplink port
    no switchport
    ip address 10.10.98.2 255.255.255.0
    spanning-tree portfast

interface FastEthernet1/0/2
    description the Access Point port
    switchport trunk encapsulation dot1q
    switchport trunk native vlan 100
    switchport trunk allowed vlan 100,101
    switchport mode trunk
    spanning-tree portfast

interface Vlan100
    ip address 10.10.100.1 255.255.255.0
    ip helper-address 10.10.100.1

interface Vlan101
```
Configuring the Controller for FlexConnect

This section provides the procedure for configuring the controller for FlexConnect. The controller configuration for FlexConnect consists of creating centrally switched and locally switched VLANs. This procedure uses the following three WLANs as examples.

<table>
<thead>
<tr>
<th>WLAN</th>
<th>Security</th>
<th>Switching</th>
<th>Interface Mapping (VLAN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>employee</td>
<td>WPA1+WPA2</td>
<td>Central</td>
<td>management (centrally switched VLAN)</td>
</tr>
<tr>
<td>employee-local</td>
<td>WPA1+WPA2 (PSK)</td>
<td>Local</td>
<td>101 (local switched VLAN)</td>
</tr>
<tr>
<td>guest-central</td>
<td>Web authentication</td>
<td>Central</td>
<td>management (centrally switched VLAN)</td>
</tr>
</tbody>
</table>

To create a centrally switched WLAN, follow these steps. In our example, this is the first WLAN (employee).

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click the desired controller in the IP Address column.

**Step 3** Choose **WLANs > WLAN Configuration** to access the WLAN Configuration page.

**Step 4** Choose **Add a WLAN** from the Select a command drop-down list, and click **Go**.

**Note** Cisco access points can support up to 16 WLANs per controller. However, some Cisco access points do not support WLANs that have a WLAN ID greater than 8. In such cases, when you attempt to create a WLAN, you get a message that says “Not all types of AP support WLAN ID greater than 8, do you wish to continue?”. Clicking OK creates a WLAN with the next available WLAN ID. However, if you delete a WLAN that has a WLAN ID less than 8, then the WLAN ID of the deleted WLAN is applied to the next created WLAN.

**Step 5** If you want to apply a template to this controller, choose a template name from the drop-down list. The fields populate according to how the template is set. If you want to create a new WLAN template, click the **click here** link to be redirected to the template creation page (see the “Configuring WLAN Templates” section on page 11-18).

**Step 6** Modify the configuration parameters for this WLAN. In our employee WLAN example, you must choose **WPA1+WPA2** from the Layer 2 Security drop-down list.

**Step 7** Be sure to enable this WLAN by selecting the **Status** check box under General Policies.

**Note** If NAC is enabled and you created a quarantined VLAN for use with this, make sure to select it from the Interface drop-down list under General Policies. Also, select the **Allow AAA Override** check box to ensure that the controller validates a quarantine VLAN assignment.
**Step 8** Click **Save** to commit your changes.

**Step 9** Follow these steps to create a locally switched WLAN. In our example, this is the second WLAN (employee-local).

   a. Follow the substeps in **Step** to create a new WLAN. In our example, this WLAN is named “employee-local.”

   b. Click a WLAN ID from the original WLAN page to move to a WLANs edit page. Modify the configuration parameters for this WLAN. In our employee WLAN example, you need to choose **WPA1+WPA2** from the Layer 2 Security drop-down list. Make sure you choose **PSK authentication key management** and enter a preshared key.

   **Note** Make sure you enable this WLAN by selecting the **Admin Status** check box. Also, make sure you enable local switching by selecting the **FlexConnect Local Switching** check box. When you enable local switching, any FlexConnect access point that advertises this WLAN is able to locally switch data packets (instead of tunneling them to the controller).

   **Note** For FlexConnect access points, the interface mapping at the controller for WLANs configured for FlexConnect local switching is inherited at the access point as the default VLAN tagging. This can be easily changed per SSID and per FlexConnect access point. Non-FlexConnect access points tunnel all traffic back to the controller, and VLAN tagging is dictated by each interface mapping of the WLAN.

   c. Click **Save** to commit your changes.

**Step 10** Follow these steps if you also want to create a centrally switched WLAN that is used for guest access. In our example, this is the third WLAN (guest-central). You might want to tunnel guest traffic to the controller so that you can exercise your corporate data policies for unprotected guest traffic from a central site.

   a. Follow the substeps in **Step** to create a new WLAN. In our example, this WLAN is named “guest-central.”

   b. In the WLANs Edit page, modify the configuration parameters for this WLAN. In our employee WLAN example, you must choose **None** from the Layer 2 Security and Layer 3 Security drop-down lists on the Security tab, select the **Web Policy** check box, and make sure **Authentication** is selected.

   **Note** If you are using an external web server, you must configure a preauthentication access control list (ACL) on the WLAN for the server and then choose this ACL as the WLAN preauthentication ACL.

   c. Make sure you enable this by selecting the **Status** check box.

   d. Click **Save** to commit your changes.

   e. If you want to customize the content and appearance of the login page that guest users see the first time they access this, follow the instructions in the “Configuring a Web Authentication Template” section on page 11-61.

   f. To add a local user to this WLAN, choose **Configure > Controller Template Launch Pad**.

   g. Choose **Security > Local Net Users** from the left sidebar menu.
h. When the Local Net Users page appears, choose Add Template from the Select a command drop-down list, and click Go.

i. Unselect the Import from File check box.

j. Enter a username and password for the local user.

k. From the Profile drop-down list, choose the appropriate SSID.

l. Enter a description of the guest user account.

m. Click Save.

Step 11 See the “Configuring an Access Point for FlexConnect” section on page 12-8 to configure two or three access points for FlexConnect.

Configuring an Access Point for FlexConnect

This section provides instructions for configuring an access point for FlexConnect.

To configure an access point for FlexConnect, follow these steps:

Step 1 Make sure that the access point has been physically added to your network.

Step 2 Choose Configure > Access Points.

Step 3 Choose which access point you want to configure for FlexConnect by clicking it in the AP Name list. The Access Point Detail page appears.

The last field listed in the Inventory Information group box indicates whether this access point can be configured for FlexConnect. Only the 1130AG and 1240AG access points support FlexConnect.

Step 4 Verify that the AP Mode field displays FlexConnect. If it does not, continue to Step 5. If FlexConnect is showing as supported, skip to Step 9.

Step 5 Choose Configure > AP Configuration Templates > Lightweight AP or Autonomous AP.

Step 6 Choose which access point you want to configure for FlexConnect by clicking it in the AP Name list. The Lightweight AP Template Detail page appears.

Step 7 Select the FlexConnect Mode supported check box. Enabling this configuration allows you to view all profile mappings.

Note If you are changing the mode to FlexConnect and if the access point is not already in FlexConnect mode, all other FlexConnect parameters are not applied on the access point.

Step 8 Select the VLAN Support check box and enter the number of the native VLAN on the remote network (such as 100) in the Native VLAN ID text box.
By default, a VLAN is not enabled on the FlexConnect access point. When FlexConnect is enabled, the access point inherits the VLAN ID associated to the WLAN. This configuration is saved in the access point and received after the successful join response. By default, the native VLAN is 1. One native VLAN must be configured per FlexConnect access point in a VLAN-enabled domain. Otherwise, the access point cannot send and receive packets to and from the controller. When the client is assigned a VLAN from the RADIUS server, that VLAN is associated to the locally switched WLAN.

**Step 9** Click the Apply/Schedule tab to save your changes.

**Step 10** The Locally Switched VLANS section shows which WLANs are locally switched and provides their VLAN identifier. Click the Edit link to change the number of VLANs from which a client IP address is obtained. You are then redirected to a page where you can save the VLAN identifier changes.

**Step 11** Click Save to save your changes.

**Step 12** Repeat this procedure for any additional access points that need to be configured for FlexConnect at the remote site.

### Connecting Client Devices to the WLANs

Follow the instructions for your client device to create profiles that connect to the WLANs you created in the “Configuring the Controller for FlexConnect” section on page 12-6.

In our example, you create three profiles on the client:

1. To connect to the “employee” WLAN, you create a client profile that uses WPA/WPA2 with PEAP-MSCHAPV2 authentication. When the client becomes authenticated, it gets an IP address from the management VLAN of the controller.

2. To connect to the “employee-local” WLAN, you create a client profile that uses WPA/WPA2 authentication. When the client becomes authenticated, it gets an IP address from VLAN 101 on the local switch.

3. To connect to the “guest-central” WLAN, you create a profile that uses open authentication. When the client becomes authenticated, it gets an IP address from VLAN 101 on the network local to the access point. After the client connects, the local user types any HTTP address in the web browser. You are automatically directed to the controller to complete the web-authentication process. When the web login page appears, enter the username and password.

To see if data traffic of the client is being locally or centrally switched, choose Monitor > Devices > Clients.

### FlexConnect Access Point Groups

FlexConnect enables you 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 a controller in each office. There is no deployment restriction on the number of FlexConnect access points per location, but you can organize and group the access points per floor and limit them per building, because it is likely the branch offices share the same configuration.
By forming access point groups with similar configurations, a procedure such as CCKM fast roaming can be processed more quickly than going through the controller individually. For example, to activate CCKM fast roaming, the FlexConnect access points must know the CCKM cache for all clients that could associate. If you have a controller with 300 access points and 1000 clients that can potentially connect, it is quicker and more practical to process and send the CCKM cache for the FlexConnect group rather than for all 1000 clients. One particular FlexConnect group could focus on a branch office with a small number of access points so that clients in the branch office could only connect to and roam between those few access points. With the established group, features such as CCKM cache and backup RADIUS are configured for the entire FlexConnect group rather than being configured in each access point.

All of the FlexConnect access points in a group share the same WLAN, backup RADIUS server, CCKM, and local authentication configuration information. This feature is helpful if you have multiple FlexConnect access points in a remote office or on the floor of a building and you want to configure them all at once. For example, you can configure a backup RADIUS server for a FlexConnect group rather than having to configure the same server on each access point. Figure 12-2 illustrates a typical FlexConnect group deployment with a backup RADIUS server in the branch office.

Figure 12-2  FlexConnect Group Deployment

- FlexConnect Groups and Backup RADIUS Servers, page 12-10
- FlexConnect Groups and CCKM, page 12-11
- FlexConnect Groups and Local Authentication, page 12-11
- Configuring FlexConnect Groups, page 12-11
- Auditing a FlexConnect Group, page 12-13

**FlexConnect Groups and Backup RADIUS Servers**

You can configure the controller to allow a FlexConnect access point in standalone mode to perform full 802.1x authentication to a backup RADIUS server. You can configure a primary RADIUS server or both a primary and secondary RADIUS server.
FlexConnect Groups and CCKM

FlexConnect groups are required for CCKM fast roaming to work with FlexConnect access points. CCKM fast roaming is achieved by caching a derivative of the master key from a full EAP authentication so that a simple and secure key exchange can occur when a wireless client roams to a different access point. This feature prevents the need to perform a full RADIUS EAP authentication as the client roams from one access point to another. The FlexConnect access points need to obtain the CCKM cache information for all the clients that might associate so they can process it quickly instead of sending it back to the controller. If, for example, you have a controller with 300 access points and 100 clients that might associate, sending the CCKM cache for all 100 clients is not practical. If you create a FlexConnect group comprising a limited number of access points (for example, you create a group for four access points in a remote office), the clients roam only among those four access points, and the CCKM cache is distributed among those four access points only when the clients associate to one of them.

Note: CCKM fast roaming among FlexConnect and non-FlexConnect access points is not supported.

FlexConnect Groups and Local Authentication

You can configure the controller to allow a FlexConnect access point in standalone mode to perform LEAP or EAP-FAST authentication for up to 20 statically configured users. The controller sends the static list of usernames and passwords to each FlexConnect access point when it joins the controller. Each access point in the group authenticates only its own associated clients.

This feature is ideal for customers who are migrating from an autonomous access point network to a lightweight FlexConnect access point network and are not interested in maintaining a large user database nor adding another hardware device to replace the RADIUS server functionality available in the autonomous access point.

Note: This feature can be used in conjunction with the FlexConnect backup RADIUS server feature. If a FlexConnect group is configured with both a backup RADIUS server and local authentication, the FlexConnect access point always attempts to authenticate clients using the primary backup RADIUS server first, followed by the secondary backup RADIUS server (if the primary is not reachable), and finally the FlexConnect access point itself (if the primary and secondary are not reachable).

Configuring FlexConnect Groups

To configure FlexConnect groups, follow these steps. If you want to apply a FlexConnect template to multiple controllers, see the template instructions in the “Configuring FlexConnect AP Groups Templates” section on page 11-40.

Step 1 Choose Configure > Controllers.

Step 2 Choose a specific controller by clicking the desired IP address.

Step 3 From the left sidebar menu choose FlexConnect > FlexConnect AP Groups. The established FlexConnect AP groups appear.
Step 4  The Group Name column shows the group names assigned to the FlexConnect access point groups. If you want to add an additional group, choose **Add FlexConnect AP Group** from the Select a command drop-down list.

or

To make modifications to an existing template, click a template in the Template Name column. The General tab of the FlexConnect AP Groups Template page appears.

*Note*  To delete a group name, click the group name you want to remove and choose **Delete FlexConnect AP Group** from the Select a command drop-down list.

The Template Name field shows the group name assigned to the FlexConnect access point group.

Step 5  Choose the primary RADIUS authentication servers for each group. If a RADIUS authentication server is not present on the controller, Prime Infrastructure-configured RADIUS server does not apply.

*Note*  You must configure the RADIUS server configuration on the controller before you apply FlexConnect RADIUS server configuration from Prime Infrastructure.

Step 6  Choose the secondary RADIUS authentication servers for each group. If a RADIUS authentication server is not present on the controller, Prime Infrastructure-configured RADIUS server does not apply.

Step 7  If you want to add an access point to the group, click the **FlexConnect AP** tab.

Step 8  An access point Ethernet MAC address cannot exist in more than one FlexConnect group on the same controller. If more than one group is applied to the same controller, select the **Ethernet MAC** check box to unselect an access point from one of the groups. You should save this change or apply it to controllers.

Step 9  If you want to enable local authentication for a FlexConnect group, click the **FlexConnect Configuration** tab. The FlexConnect Configuration tab appears.

*Note*  Make sure that the Primary RADIUS Server and Secondary RADIUS Server parameters are set to **None** on the General tab.

Step 10  Select the **FlexConnect Local Authentication** check box to enable local authentication for this FlexConnect group. The default value is unselected.

*Note*  When you attempt to use this feature, a warning message indicates that it is a licensed feature.

Step 11  To allow a FlexConnect access point to authenticate clients using LEAP, select the **LEAP** check box. Otherwise, to allow a FlexConnect access point to authenticate clients using EAP-FAST, select the **EAP-FAST** check box.

Step 12  Perform one of the following, depending on how you want protected access credentials (PACs) to be provisioned:

- To use manual PAC provisioning, enter the key used to encrypt and decrypt PACs in the EAP-FAST Key text box. The key must be 32 hexadecimal characters.
- To allow PACs to be sent automatically to clients that do not have one during PAC provisioning, select the **Auto Key Generation** check box.

Step 13  In the EAP-FAST Authority ID text box, enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.
**Step 14** In the EAP-FAST Authority Info text box, enter the authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.

**Step 15** In the EAP-FAST Pac Timeout text box, specify a PAC timeout value by entering the number of seconds for the PAC to remain viable in the edit box. The valid range is 2 to 4095 seconds.

---

**Note** To verify that an individual access point belongs to a FlexConnect group, click the Users configured in the group link. It advances you to the FlexConnect AP Group page, which shows the names of the groups and the access points that belong in it.

---

### Auditing a FlexConnect Group

If the FlexConnect configuration changes over a period of time either on Prime Infrastructure or the controller, you can audit the configuration. The changes are visible on subsequent screens. You can choose to synchronize the configuration by refreshing Prime Infrastructure or the controller.
Al\textbf{arm and Event Dictionary}

This chapter describes the event and alarm notifications that the wireless LAN controller, access points, and location appliances can receive.

\textbf{What is an Event?}

An \textit{event} is an occurrence or detection of some condition in and around the network. An event is a distinct incident that occurs at a specific point in time. Examples of events include the following:

- Port status change
- Device reset
- Device becomes unreachable by the management station

An event can also be one of the following:

- Possible symptom of a fault that is an error, failure, or exceptional condition in the network. For example, when a device becomes unreachable, an unreachable event is triggered.
- Possible symptom of a fault clearing. For example, when a device state changes from unreachable to reachable, a reachable event is triggered.

One or more events may generate an abnormal state or alarm. The alarm can be cleared, but the event remains. You can view the list of events using the Event Browser.

Choose \texttt{Monitor > Events} to access the Events page.

\textbf{What is an Alarm?}

An \textit{alarm} is a Cisco Prime Infrastructure response to one or more related events. If an event is considered of high enough severity (critical, major, minor, or warning), Prime Infrastructure raises an alarm until the resulting condition no longer occurs.

One or more events can result in a single alarm being raised. An alarm is created in the following sequence:

1. A notification is triggered when a fault occurs in the network.
2. An event is created, based on the notification.
3. An alarm is created after checking if there is no active alarm corresponding to this event.

An alarm is associated with two types of events:
What is an Alarm?

- Active events: Events that have not been cleared. An alarm remains in this state until the fault is resolved in a network.
- Historical events: Events that have been cleared. An event changes its state to an historical event when the fault is resolved in a network.

After an alarm is cleared, it indicates the end of an alarm life cycle. A cleared alarm can be revived if the same fault reoccurs within a preset period of time. The present period is set to 5 minutes in Prime Infrastructure.

Choose Monitor > Alarms to access the Alarms page.

For details about the list of Alarms and Events, see Cisco Prime Infrastructure Alarms and Events.

For more information about the Event creation, Alarms and Events association, and Alarm statuses, see the “Cisco Prime Infrastructure 2.0 User Guide”.

Unsupported Traps

- BROADCAST_STORM_START: broadcastStormStartTrap
- FAN_FAILURE: fanFailureTrap
- BROADCAST_STORM_END: broadcastStormEndTrap
- VLAN_REQUEST_FAILURE: vlanRequestFailureTrap
- VLAN_DELETE_LAST: vlanDeleteLastTrap
- VLAN_DEFAULT_CFG_FAILURE: vlanDefaultCfgFailureTrap
- VLAN_RESTORE_FAILURE_TRAP: vlanRestoreFailureTrap
- IPSEC_ESP_REPLAY_FAILURE: bsnIpsecEspReplayFailureTrap
- IPSEC_ESP_INVALID_SPI: bsnIpsecEspInvalidSpiTrap
- LRAD_UP: bsnAPUp
- LRAD_DOWN: bsnAPDown
- STP_NEWROOT: stpInstanceNewRootTrap
- STP_TOPOLOGY_CHANGE: stpInstanceTopologyChangeTrap
- BSN_DOT11_ESS_CREATED: bsnDot11EssCreated
- BSN_DOT11_ESS_DELETED: bsnDot11EssDeleted
- LRADIF_RTS_THRESHOLD_CHANGED
- LRADIF_ED_THRESHOLD_CHANGED
- LRADIF_FRAGMENTATION_THRESHOLD_CHANGED
- LINK_FAILURE: linkFailureTrap
Reports

The Cisco Prime Infrastructure reporting is necessary to monitor the system and network health as well as troubleshoot problems. A number of reports can be generated to run on an immediate and scheduled basis. Each report type has a number of user-defined criteria to aid in defining of the reports. The reports are formatted as a summary, tabular, or combined (tabular and graphical) layout. Once defined, the reports can be saved for future diagnostic use or scheduled to run and report on a regular basis.

Note
As of Prime Infrastructure 1.x, the size limitations for reports is removed. So, you can view a report of any size with any number of graphs using HTML or saved as CSV/PDF files.

Non Upgradable Reports from the WCS to Prime Infrastructure

The following reports cannot be upgraded to Prime Infrastructure 1.0 and later:

- Adhoc Rogue Count Summary
- Adhoc Rogues
- Client Count
- Client Summary
- Client Throughput
- New Rogue AP Count Summary
- New Rogue APs
- Rogue AP Count Summary
- Rogue APs
- Security Alarm Trending Summary

Note
You cannot upgrade the Guest User Sessions reports to Prime Infrastructure Release 1.1.

For more information about the various types of reports and how they are managed, see the Reports chapter in the Cisco Prime Infrastructure 2.0 User Guide.
Performing Administrative Tasks

The Administration enables you to schedule tasks, administer accounts, and configure local and external authentication and authorization. Also, set logging options, configure mail servers, and data management related to configuring the data retain periods. Information is available about the types of Cisco Prime Infrastructure licenses and how to install a license.

For information about the Prime Infrastructure administrative tasks, see *Cisco Prime Infrastructure 2.2 Administrator Guide*. 
Prime Infrastructure Services

This chapter describes the role of the Cisco mobility services engine (MSE), within the overall Cisco Unified Wireless Network (CUWN).

- Mobility Services, page 16-1
- Mobile Concierge Service, page 16-94
- Identity Services, page 16-102

Mobility Services

This section briefly describes the Location service, wIPS, Mobile Concierge service, and CMX Analytics service, CMX Connect & Engage service that Cisco Prime Infrastructure supports and provides the mobility procedures that are common across all services.

Location Service

Also known as Context Aware Service (CAS). This is the core service of the Mobility Services Engine (MSE) that turns on Wi-Fi client tracking and location API functionality. Allows MSE to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as presence, location, telemetry data, and historical information.

Note

You must purchase licenses from Cisco to retrieve contextual information on tags and clients from access points. Licenses for tags and clients are offered independently. See the Cisco 3355 Mobility Services Engine Release Note at the following URL for details on tag and client licenses:


wIPS

Provides wireless-specific network threat detection and mitigation against malicious attacks, security vulnerabilities, and sources of performance disruption within the CUWN infrastructure. wIPS visualizes, analyzes, and identifies wireless threats, and centrally manages mitigation and resolution of security and performance issues using Cisco monitor mode and Enhanced Local Mode (ELM) Access Points. Proactive threat prevention is also supported to create a hardened wireless network core that is impenetrable by most wireless attacks.
Mobile Concierge Service

Mobile Concierge enables the Cisco Mobility Services Advertisement Protocol (MSAP). This protocol enables direct communication between the MSE and mobile devices, allowing content to be pushed directly to the mobile device pre-association. This functionality is dependent on the mobile device supporting 802.11u and MSAP.

CMX Analytics Service

- The CMX Analytics service analyzes wireless device location information in a particular network. The CMX Analytics service uses the data provided by the Cisco Mobility Services Engine (MSE) to calculate the location of Wi-Fi devices in the Wireless Local Area Network (WLAN). In addition, the FastLocate feature sends information about the RSSI strength of data packets to the Cisco WLC that can be used for location calculations.
- When a wireless device is enabled in a network, it transmits probe request packets to identify the wireless network in its neighborhood. Even after connecting to the access point in the WLAN, the client devices continue to transmit probe request packets to identify other access points for better quality of service. The access points gather these requests and the associated RSSI from the various wireless devices and forwards them to the Wireless LAN Controller (WLC). The controller then forwards this information to the MSE.
- The basic data that is collected from various APs, when analyzed, produces information and knowledge about the movement and behavior patterns of people who are using Wi-Fi devices in the building. For example, the building can be an airport, shopping mall, city center, and so on. The CMX Analytics service helps the airport authorities or the building owners to understand the movement of passengers or customer within their building. This helps them improve the signage, make changes to the under utilized areas, and so on.

CMX Connect and Engage Service

Formerly known as Browser Engage Service. The CMX Connect and Engage service provides Connect, a guest Wi-Fi onboarding solution, as well as zone and message configuration for the CMX Software Development Kit (SDK).

Cisco Context-Aware Mobility Solution

The foundation of the CAM solution is the controller-based architecture of the CUWN. The CUWN contains the following primary components:
- Cisco Prime Infrastructure, page 3
- WLAN Controllers, page 3
- Access Points, page 3
- Cisco Mobility Services Engines, page 4
Cisco Prime Infrastructure

With the Prime Infrastructure, network administrators have a single solution for RF prediction, policy provisioning, network optimization, troubleshooting, user tracking, security monitoring, and wired and wireless LAN systems management. Robust graphical interfaces make wired and wireless LAN deployment and operations simple and cost-effective. Detailed trending and analysis reports make the Prime Infrastructure vital to ongoing network operations.

WLAN Controllers

The WLAN controllers are highly scalable and flexible platforms that enable system wide services for mission-critical wireless in medium to large-sized enterprises and campus environments. Designed for 802.11n performance and maximum scalability, the WLAN controllers offer enhanced uptime with the ability to simultaneously manage from 5000 access points to 250 access points; superior performance for reliable streaming video and toll quality voice; and improved fault recovery for a consistent mobility experience in the most demanding environments.

The Prime Infrastructure supports the Cisco wireless controllers that help reduce the overall operational expense of Cisco Unified Networks by simplifying network deployment, operations, and management. The following WLAN controllers are supported in the Prime Infrastructure:

- Cisco 2700 Series Location Appliance
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 2500 Series Wireless Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless Controllers
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless Services Module 2 (WiSM2) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless Controller on SRE for ISR G2 Routers
- Cisco Flex 7500 Series Wireless Controllers
- Cisco WLAN Controller Network Modules for Cisco Integrated Services Routers

Access Points

The following access points are supported:

- Cisco Aironet 801, 802, 1000, 1040, 1100, 1130, 1140, 1200, 1230, 1240, 1250, 1260, 1310, 1500, 1524, 1552, 1600i, 1600e, 2600i, 2600e, 3500i, 3500e, 3500p, 3600i, and 3600e Series Lightweight Access Points.
- Cisco Aironet 1040, 1100, 1130, 1141, 1142, 1200, 1240, 1250, and 1260.
- Cisco 600 Series OfficeExtend Access Points.
Cisco Mobility Services Engines

There are two models of the mobility services engine:

- Cisco 3355 Mobility Services Engine
- Cisco Virtual Appliance

Accessing Services

You can access the MSE installation guides as follows:

MSE 3355 Installation guide:

Licensing Information for MSE

The Cisco Mobility Services Engine (MSE) provides a wide variety of location-based services. To enable these services, the following are required:

- Cisco MSE hardware or software appliance
  - Physical Appliance—An activation license is not required.
  - Virtual Appliance—Virtual Appliance instance requires a MSE Virtual Appliance Activation license (L-MSE-7.0-K9). It is not sufficient to simply have a service/feature license on an MSE Virtual Appliance.
- Licenses
- Support

There are three types of MSE licenses available:

<table>
<thead>
<tr>
<th>Table 1</th>
<th>MSE License Types</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MSE Service License</strong></td>
<td><strong>Provides</strong></td>
</tr>
<tr>
<td>Base Location License</td>
<td>Provides advanced spectrum capability with the ability to detect, track, and trace rogue devices, Cisco CleanAir® interferers, Wi-Fi clients, and RFID tags. The Base Location license also enables customers and partners to use standard MSE APIs.</td>
</tr>
</tbody>
</table>
Client and wIPS licenses are installed from the Prime Infrastructure UI (Administration > License Center). See, Chapter 2: “Adding and Deleting Mobility Services Engines and Licenses” in the Cisco Connected Mobile Experiences Configuration Guide, Release 8.0, Cisco Wireless Intrusion Prevention System, Release 8.0, and Cisco Location Analytics Configuration Guide, Release 8.0 respectively.

For complete details on ordering and downloading licenses, see the Cisco Mobility Services Engine Licensing and Ordering Guide at the following URL:

### Viewing Current Mobility Services

To see a list of current Mobility Services, choose Services > Mobility Services Engines.

The Mobility Services Engines page provides the following information and features for each device:

---

**Table 1**  MSE License Types (continued)

<table>
<thead>
<tr>
<th>MSE Service License</th>
<th>Provides</th>
</tr>
</thead>
</table>
| CMX License         | Provides the above Base Location license capabilities and the CMX features:  
  |  - CMX Analytics, a user-friendly location analytics platform to view and analyze how, where, and when visitors move through a venue.  
  |  - CMX Connect and Engage for a customizable and location-aware captive portal to on-board guest users to Wi-Fi including:  
  |  - CMX for Facebook Wi-Fi, helping guests connect to Wi-Fi and use the Internet. Enterprises or merchants gain social demographic data via Facebook Insights.  
  |  - CMX SDK for enabling organizations to integrate Wi-Fi-based indoor navigation with push notification and auto-launch capabilities into mobile applications. |
| wIPS License        | Provides complete wireless threat detection and mitigation in the wireless network infrastructure  
  |  - Rogue Detection, Classification, and Mitigation  
  |  - Over-the-Air Attack Detection  
  |  - Security Vulnerability Monitoring  
  |  - Performance Monitoring, and Auto-Optimization  
  |  - Management, Monitoring, and Reporting |
|                     | Requires a separate MSE running the wIPS service. |
|                     | There are 3 deployment options:  
  |  - Enhanced Local mode: Number of wIPS licenses required equals the number of access points in local mode (data serving) deployed in the network.  
  |  - Monitor mode: Number of wIPS licenses required equals the number of access points configured in the full-time monitor mode.  
  |  - Wireless Security Module (WSM)/Monitor module: Number of wIPS licenses required equals the number of wireless security and spectrum intelligence modules deployed in the network. |
• Device Name—User-assigned name for the mobility services engine. Click the device name to see and manage mobility services engine details. See the “Managing System Properties for a Mobility Services Engine” section on page 16-20 for more information.

• Device Type—Indicates the type of mobility services engine. Indicates whether the device is a virtual appliance or not.

• IP Address—Indicates the IP address for the mobility services engine.

• Version—Indicates the version number of the mobility services engine.

• Reachability Status—Indicates whether or not the mobility services engine is reachable.

• Secondary Server—Indicates whether or not the secondary server is installed.

• Mobility Service:
  - Name—Indicates the name of the mobility service.
  - Admin Status—Indicates whether the mobility service is enabled or disabled.
  - Service Status—Indicates whether the mobility service is currently up or down.

• Select a command drop-down list:
  - Add Location Server
  - Add Mobility Services Engine—Contains Context-Aware Service, Cisco Adaptive Wireless IPS (wIPS) service, Mobile Concierge Service, and Location Analytics Service.
  - Delete Service(s)
  - Synchronize Services
  - Synchronization History
  - Edit Configuration
  - Add NG MSE
  - Edit NG MSE

Note
Location and mobility services engine features of the Prime Infrastructure do not support partitioning.

Adding a Mobility Services Engine

You can add an MSE using the Add Mobility Services Engine dialog box in the Mobility Service page. In this dialog box, you can add licensing files, tracking parameters, and assign maps to the MSE. If you launch the wizard with an existing MSE for configuration, then the Add MSE option appears as Edit MSE Details.

Tip
To learn more about Cisco Adaptive wIPS features and functionality, go to Cisco.com to watch a multimedia presentation. Here you can find the learning modules for a variety of Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

Note
The Prime Infrastructure Release 1.0 recognizes and supports the MSE 3355 appropriately.
The Services > Mobility Services Engine page is available only in root virtual domain.

To add a mobility services engine to the Prime Infrastructure, log into the Prime Infrastructure and follow these steps:

**Step 1** Verify that you can ping the mobility service engine that you want to add from the Prime Infrastructure.

**Step 2** Choose Services > Mobility Services Engines to display the Mobility Services page.

**Step 3** From the Select a command drop-down list, choose Add Mobility Services Engine, and click Go. The Add Mobility Services Engine page appears.

**Step 4** Enter the following information:
- **Device Name**—User-assigned name for the mobility services engine.
- **IP Address**—The IP address of the mobility service engine.
- **Contact Name (optional)**—The mobility service engine administrator.
- **Username**—The default username is admin. This is the Prime Infrastructure communication username configured for MSE.
- **Password**—The default password is admin. This is the Prime Infrastructure communication password configured for MSE.

**Note** A mobility services engine is added only if a valid IP address is entered. The Device Name helps you distinguish between devices if you have multiple Prime Infrastructures with multiple mobility services engines, but it is not considered when validating a mobility services engine.

- **Select the Delete synchronized service assignments check box if you want to permanently remove all service assignments from the mobility services engine.** This option is applicable for network designs, wired switches, controllers, and event definitions. The existing location history data is retained, however you must use manual service assignments to perform any future location calculations.

**Step 5** Click Next. The Prime Infrastructure automatically synchronizes the selected elements with the MSE. After the synchronization, the MSE License Summary page appears. You can use the MSE License Summary page to install a license, add a license, remove a license, install an activation license, and install service license.

**Configuring Services for MSE**

**Step 6** To enable a service on the mobility services engine, select the check box next to the service. The different type of services are:
- **Context Aware Service**—If you select the Context Aware Service check box, then you must select a location engine to perform location calculation. You can choose CAS to track clients, rogues, interferers, and tags. You can choose Cisco Context-Aware Engine for Clients and Tag to track tags.
- WIPS—The Wireless Intrusion Prevention System check box, it detects wireless and performance threats.
- Mobile Concierge Service—The Mobile Concierge Service check box, it provides service advertisements that describe the available services for the mobile devices.
- CMX Analytics Service—The CMX Analytics Service check box, it provides a set of data analytic tools packaged for analyzing Wi-Fi device location data that comes from the MSE.
- CMX Connect & Engage—The CMX Connect and Engage service provides a guest Wi-Fi onboarding solution, as well as zone and message configuration for the CMX Software Development Kit (SDK).
- HTTP Proxy Service—The HTTP Proxy service on the MSE terminates all HTTP traffic intercepted using Policy Based Routing (PBR) and acts as a forward proxy by pulling contents on behalf of wireless clients.

**Note** From release 7.5 onward, wIPS service requires a dedicated MSE because it does not support CAS and wIPS on the same MSE.

**Configuring MSE Tracking and History Parameters**

**Step 7** After you enable services on the mobility services engine, the Select Tracking & History Parameters page appears.

**Note** If you skip configuring the tracking parameters, the default values are selected.

**Step 8** You can select the clients that you want to keep track of by selecting the corresponding Tracking check box(es). The various tracking parameters are as follows:
- Wired Clients
- Wireless Clients
- Rogue Access Points
  - Exclude Adhoc Rogue APs
- Rogue Clients
- Interferers
- Active RFID Tags

**Step 9** You can enable the history tracking of devices by selecting the corresponding devices check box(es). The different history parameters are as follows:
- Wired Stations
- Client Stations
- Rogue Access Points
- Rogue Clients
- Interferers
- Asset Tags

**Step 10** Click **Next** to Assign Maps to the MSE.
Assigning Maps to the MSE

**Note** The Assigning Maps page is available only if you select CAS as one of the services to be enabled on the MSE.

**Step 11** Once you configure MSE tracking and history parameters, the Assigning Maps page appears. The Assign Maps page shows the following information:
- Name
- Type (building, floor, campus)
- Status

**Step 12** You can see the required map type by selecting either All, Campus, Building, Floor Area, or Outdoor Area from the Filter option available on the page.

**Step 13** To synchronize a map, select the **Name** check box, and click **Synchronize**.

Upon synchronization of the network designs, the appropriate controllers that have APs assigned on a particular network design are synchronized with the MSE automatically.

**Step 14** Click **Next** to configure mobile app enablement.

### Mobile App Enablement

Enabling this integration will allow the MSE to send floor maps and wireless client position notification to Meridian. Meridian used this information to provide location-based services to your users without requiring them to connect to your network and access the MSE directly. After enabling Meridian, you will receive an e-mail with instructions on how to activate your account and share access with others in your organization. You can utilize Meridians platform to provide location services to your visitors either through the Meridian mobile app or your own apps using their mobile SDKs for Android and iOS. The data bandwidth for each wireless client position or zone notification from MSE to Meridian can be maximum of 1 MB/second. For more information, please visit [http://www.meridianapps.com/mse](http://www.meridianapps.com/mse)

**Step 15** Once you assign maps to the MSE, the Mobile App Enablement page appears.

**Step 16** Select the **Enable Mobile App Integration** check box to enable the mobile application integration. You can click an icon to open the Mobile App Enablement Help page.

**Step 17** Enter the name for the location on the **Location Name** text box. The name you enter here will appear in the Meridian app so that you can try out the location services on your own device.

**Step 18** Enter the email address in the **E-mail Address** text box to access the Meridian online editor and SDK. Meridian will email these addresses with instructions on how to access your account and share it with others in your organization.

**Step 19** Enter the server where the MSE can register its UDI and send the maps that are synchronized to the MSE in the **Registration Endpoint** text box.

**Step 20** Enter the server detail where the MSE can send location update notifications in the data format specified in the **Notifications Endpoint** text box.

**Step 21** Select the **Notifications Data Format** radio button. This is the data format of the notifications sent from the MSE. The different data formats are: Legacy SOAP/XML, XML, JSON, and Protocol Buffers.

**Step 22** Enter the street address of your location in the **Street Address** text box.

**Step 23** Enter the phone number where Meridian can reach you for additional information in the **Phone Number** text box.

**Step 24** Click **Advanced** to open the Advanced pane.
Step 25 If you want MSE to send real-time notifications to Meridian when ever the wireless clients enter the selected zones, then select the Enable Zone Notifications for zones check box and choose floors and zones from the drop-down list.

The Enable zone notifications for zones drop-down list shows all the floors and zones that are added to the Prime Infrastructure and synced to the MSE.

Step 26 Click OK after selecting zones and floors.

Step 27 Click Save.

Step 28 Click Done to save the MSE settings.

Deleting an MSE License File

To delete an MSE license file, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Service Engine.

The Mobility Services page appears.

Step 2 Click Device Name to delete a license file for a particular service.

Step 3 From the Select a command drop-down list, choose Edit Configuration.

The Edit Mobility Services Engine dialog box appears.

Step 4 Click Next in the Edit Mobility Services Engine dialog box.

The MSE License Summary page appears.

Step 5 Choose the MSE license file that you want to delete in the MSE License Summary page.

Step 6 Click Remove License.

Step 7 Click OK to confirm the deletion or Cancel to close this page without deleting the license.

Step 8 Click Next to enable services on the mobility services engine.

Deleting MSEs from Prime Infrastructure

To delete a mobility services engine from the Prime Infrastructure database, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engine.

The Mobility Services page appears.

Step 2 Select the mobility services engine(s) to be deleted by selecting the corresponding Device Name check box(es).

Step 3 From the Select a command drop-down list, choose Delete Service(s).

Step 4 Click Go.

Step 5 Click OK to confirm that you want to delete the selected mobility services engine from the Prime Infrastructure database.

Step 6 Click Cancel to stop the deletion.
Installing Device and wIPS License Files

You can install device and wIPS licenses from the Prime Infrastructure.

- **Step 1**: Choose **Administration > Licenses**.
- **Step 2**: Choose **Files > MSE Files**.
- **Step 3**: Click **Add**. The Add a License File dialog appears.
- **Step 4**: Choose the appropriate MSE name from the MSE Name drop-down list.

**Note**: Verify that the UDI of the selected mobility services engine matches the one you entered when registering the PAK.

- **Step 5**: Click **Choose File** to browse and to select the license file.
- **Step 6**: Click **Upload**. The newly added license appears in the MSE license file list.

Adding a Location Server

To add a location server, follow these steps:

- **Step 1**: Choose **Services > Mobility Services**.
- **Step 2**: From the Select a command drop-down list, choose **Add Location Server**.
- **Step 3**: Click **Go**.
- **Step 4**: Enter the following information:
  - Device Name
  - IP Address
  - Contact Name
  - User Name
  - Password
  - 1Port
  - HTTPS—When enabled, HTTPS is used for communication between the Prime Infrastructure and location server.

- **Step 5**: Select the **Delete synchronized service assignments** check box if you want to permanently remove all service assignments from the mobility services engine.

  This option is applicable for network designs, wired switches, controllers, and event definitions. The existing location history data is retained, however, you must use manual service assignments to perform any future location calculations.

- **Step 6**: Click **Save**.

**Note**: After adding a location server, it must be synchronized with the Prime Infrastructure. See the “Synchronizing Services” section on page 16-12 for more information.
Synchronizing Services

This section describes how to synchronize Cisco wireless LAN controllers and the Prime Infrastructure with mobility services engines.

Note

The Synchronize Services page on the Services tab is available only in the root virtual domain in Release 7.3.

Keeping Mobility Services Engines Synchronized

This section describes how to synchronize the Prime Infrastructure and mobility services engines manually and automatically.

After adding a mobility service engine to the Prime Infrastructure, you can synchronize network designs (campus, building, floor, and outdoor maps), event groups, controller information (name and IP address), or wired switches to the mobility services engine.

Note

Be sure to verify software compatibility between the controller, the Prime Infrastructure, and the mobility services engine before performing synchronization. See the latest mobility services engine release notes at the following URL: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html.

Note

Communication between the mobility services engine, the Prime Infrastructure, and the controller is in Coordinated Universal Time (UTC). Configuring NTP on each system provides devices with the UTC time. The mobility services engine and its associated controllers must be mapped to the same NTP server and the same Prime Infrastructure server. An NTP server is required to automatically synchronize time between the controller, the Prime Infrastructure, and the mobility services engine.

Synchronizing the Prime Infrastructure and a Mobility Services Engine

This section describes how to synchronize the Prime Infrastructure and mobility services engines manually and smartly.

After adding a mobility services engine to the Prime Infrastructure, you can synchronize network designs (campus, building, floor, and outdoor maps), controllers (name and IP address), specific Catalyst 3000 Series and 4000 switches, and event groups with the mobility services engine.

- Network Designs—A logical mapping of the physical placement of access points throughout facilities. A hierarchy of a single campus, the buildings that comprise that campus and the floors of each building constitute a single network design.
- Controllers—A selected controller that is associated and regularly exchanges location information with a mobility services engine. Regular synchronization ensures location accuracy.
- Event Groups—a group of predefined events that define triggers that generate an event. Regular synchronization ensures that the latest defined events are tracked.

- Wired Switches—Wired Catalyst switches that provide an interface to wired clients on the network. Regular synchronization ensures that location tracking of wired clients in the network is accurate.
  - The mobility services engine can be synchronized with Catalyst stackable switches (3750, 3750-E, 3560, 2960, IE-3000 switches), switch blades (3110, 3120, 3130, 3040, 3030, 3020), and switch ports.
  - The mobility services engine can also be synchronized with the following Catalyst series switches 4000: WS-C4948, WS-C4948-10GE, ME-4924-10GE, WS-4928-10GE, WS-C4900M, WS-X4515, WS-X4516, WS-X4013+, WS-X4013+TS, WS-X4516-10GE, WS-X4013+10GE, WS-X45-SUP6-E, and WS-X45-SUP6-LE

- Third Party Elements—When you synchronize elements with MSE, there might be event groups on the MSE that have been created by third-party applications. You can either delete the unused elements or mark them as third-party elements.

- Service Advertisements—Mobile Concierge Service provides service advertisements on the mobile devices. This shows the service advertisement that has synchronized with the MSE.

**Note**
Be sure to verify software compatibility between the controller, the Prime Infrastructure, and the mobility services engine before synchronizing. See the latest mobility services engine release notes at the following URL:

**Note**
Communication between the mobility services engine, the Prime Infrastructure, and the controller is in Coordinated Universal Time (UTC). Configuring NTP on each system provides devices with the UTC time. The mobility services engine and its associated controllers must be mapped to the same NTP server and the same Prime Infrastructure server. An NTP server is required to automatically synchronize time between the controller, the Prime Infrastructure, and the mobility services engine.

**Synchronizing Prime Infrastructure Network Designs, Controllers, Wired Switches, or Event Groups**

To synchronize the Prime Infrastructure network designs, controllers, wired switches, or event groups with the mobility services engine, follow these steps:

**Step 1** Choose Services > Synchronize Services.

**Step 2** Choose the appropriate menu option (Network Designs, Controllers, Event Groups, Wired Switches, Third Party Elements, or Service Advertisements) from the left sidebar menu.

**Step 3** To assign a network design to a mobility services engine, from the left sidebar menu, choose Network Designs.

**Step 4** Select all the maps to be synchronized with the mobility services engine by selecting the corresponding Name check box.

**Note**
Through 6.0, you can assign only up to a campus level to a mobility services engine. Beginning with 7.0 this option is granular to a floor level. For example, you can choose to assign floor1 to MSE 1, floor2 to MSE 2, and floor3 to MSE 3.
Step 5  Click Change MSE Assignment.

Step 6  Select the mobility services engine to which the maps are to be synchronized.

**Note**  A network design might include a floor in a campus or a large campus with several buildings, each monitored by a different mobility services engine. Because of this, you might need to assign a single network design to multiple mobility services engines.

Step 7  Click either of the following in the MSE Assignment dialog box:

- **Save**—Saves the mobility services engine assignment. The following message appears in the Messages column of the Network Designs page with a yellow arrow icon:
  
  “To be assigned - Please synchronize”.

- **Cancel**—Discards the changes to the mobility services engine assignment and return to the Network Designs page.

You can also click **Reset** to undo the mobility services engine assignments.

**Note**  A network design may include a floor in a campus or a large campus with several buildings, each monitored by a different mobility services engine. Because of this, you may need to assign a single network design to multiple mobility services engines.

**Note**  Network design assignments also automatically picks up the corresponding controller for synchronization.

Step 8  Click **Synchronize** to update the mobility services engine(s) database(s).

When items are synchronized, a green two-arrow icon appears in the Sync.

You can use the same procedure to assign wired switches or event groups to a mobility services engine. To assign a controller to a mobility services engine, see “Synchronizing Controllers with Mobility Services Engines” section on page 16-14 for more information.

---

**Synchronizing Controllers with Mobility Services Engines**

You can assign an MSE to any wireless controller on a per-service (CAS or wIPS) basis.

To assign an MSE service to wireless controllers, follow these steps:

**Step 1**  In the synchronization page, choose **Controllers**.

**Step 2**  Choose the controllers to be assigned to the mobility services engine.

**Step 3**  Click **Change MSE Assignment**.

**Step 4**  Choose the mobility services engine to which the controllers must be synchronized.

**Step 5**  Click either of the following in the dialog box:

- **Save**—Saves the mobility services engine assignment. The following message appears in the Messages column of the Controllers page:
  
  To be assigned - Please synchronize.
• **Cancel**—Discards the changes to the mobility services engine assignment and returns to the Controllers page.

  You can also click **Reset** to undo the yellow button assignments.

**Step 6**
Click **Synchronize** to complete the synchronization process.

**Step 7**
Verify that the mobility services engine is communicating with each of the controllers for only the chosen service. This can be done by clicking the **NMSP status** link in the status page.

---

**Note**
After Synchronizing a controller, verify that the timezone is set on the associated controller. See the “Setting and Verifying the Timezone on a Controller” section on page 16-16 for more information.

---

**Note**
Controller names must be unique for synchronizing with a mobility services engine. If you have two controllers with the same name, only one is synchronized.

---

To unassign a network design, controller, wired switch, or event group from a mobility services engine, follow these steps:

**Step 1**
On the respective tabs, click one or more elements, and click **Change MSE Assignment**. The Choose Mobility Services Engine dialog box appears.

**Step 2**
Unselect the **Mobility Services Engine** check box if you do not want the elements to be associated with that mobility services engine.

**Step 3**
Click **Save** to save the changes to the assignments.

**Step 4**
Click **Synchronize**. A two-arrow icon appears in the Sync Status column.

---

**Working with Third-Party Elements**

When you synchronize elements with MSE, there might be event groups on the MSE that have been created by third-party applications. You can either delete the unused elements or mark them as third-party elements.

To delete the elements or mark them as third-party elements, follow these steps:

**Step 1**
Choose **Services > Synchronize Services**.

The Network Design page appears.

In the Network Design page, choose **Third Party Elements** from the left sidebar menu.

The Third Party Elements page appears.

**Step 2**
Select one or more elements.

**Step 3**
Click one of the following buttons:

- **Delete Event Groups**—Deletes the selected event groups.
- **Mark as 3rd Party Event Group(s)**—Marks the selected event groups as third-party event groups.
Chapter 16  Prime Infrastructure Services

Mobility Services

Setting and Verifying the Timezone on a Controller

For controller Releases 4.2 and later, if a mobility services engine (Release 5.1 or greater) is installed in your network, it is mandatory that the time zone be set on the controller to ensure proper synchronization between the two systems.

Greenwich Mean Time (GMT) is used as the standard for setting the time zone system time of the controller.

You can automatically set the time zone during initial system setup of the controller or manually set it on a controller already installed in your network.

To manually set the time and time zone on an existing controller in your network using the CLI, follow these steps:

Step 1  Configure the current local time in GMT on the controller by entering the following commands:

(Cisco Controller) >config time manual 09/07/07 16:00:00
(Cisco Controller) >config end

Note  When setting the time, the current local time is entered in terms of GMT and as a value between 00:00 and 24:00. For example, if it is 8 AM Pacific Standard Time (PST) in the US, you enter 16:00 (4 PM PST) as the PST time zone is 8 hours behind GMT.

Step 2  Verify that the current local time is set in terms of GMT by entering the following command:

(Cisco Controller) >show time
Time............................................. Fri Sep 7 16:00:02 2007
Timezone delta................................... 0:0

Step 3  Set the local time zone for the system by entering the following commands:

Note  When setting the time zone, you enter the time difference of the local current time zone with respect to GMT (+/-). For example, Pacific Standard Time (PST) in the United States (US) is 8 hours behind GMT (UTC) time. Therefore, it is entered as -8.

(Cisco Controller) >config time timezone -8
(Cisco Controller) >config end

Step 4  Verify that the controller shows the current local time with respect to the local time zone rather than in GMT by entering the following command:

(Cisco Controller) >show time
Time............................................. Fri Sep 7 08:00:26 2007
Timezone delta................................... -8:0

Note  The time zone delta parameter in the show time command shows the difference in time between the local time zone and GMT (8 hours). Before configuration, the parameter setting is 0.0.
Configuring Smart Mobility Services Engine Database Synchronization

Manual synchronization of the Prime Infrastructure and mobility services engine databases provides immediate synchronization. However, future deployment changes (such as making changes to maps and access point positions), can yield incorrect location calculations and asset tracking until resynchronization reoccurs.

To prevent out-of-sync conditions, use the Prime Infrastructure to carry out synchronization. This policy ensures that synchronization between the Prime Infrastructure and mobility services engine databases is triggered periodically and any related alarms are cleared.

Any change to one or more of any synchronized components is automatically synchronized with the mobility services engine. For example, if a floor with access points is synchronized with a particular mobility services engine and then one access point is moved to a new location on the same floor or another floor which is also synchronized with the mobility services engine, then the changed location of the access point is automatically communicated.

To further ensure that the Prime Infrastructure and MSE are in sync, smart synchronization happens in the background.

To configure smart synchronization, follow these steps:

Step 1 Choose Administration > Background Tasks.

The Background Tasks summary page appears.

Step 2 Select the Mobility Service Synchronization check box.

Step 3 The Mobility Services Synchronization page appears.

Step 4 To set the mobility services engine to send out-of-sync alerts, select the Enabled check box in the Out of Sync Alerts group box.

Step 5 To enable smart synchronization, select the Smart Synchronization Enabled check box.

Note Smart synchronization does not apply to elements (network designs, controllers, or event groups) that have not yet been assigned to a mobility services engine. However, out-of-sync alarms are still generated for these unassigned elements. For smart synchronization to apply to these elements, you need to manually assign them to a mobility services engine.

Note When a mobility services engine is added to the Prime Infrastructure, the data in the Prime Infrastructure is always treated as the primary copy that is synchronized with the mobility services engine. All synchronized network designs, controllers, event groups and wired switches that are present in the mobility services engine and not in the Prime Infrastructure are removed automatically from mobility services engine.

Step 6 Enter the time interval, in minutes, that the smart synchronization is to be performed.

By default, smart-sync is disabled.

Step 7 Click Submit.

See the “Smart Controller Assignment and Selection Scenarios” section on page 16-18 for more information on smart controller assignment and selection scenarios.
Smart Controller Assignment and Selection Scenarios

Scenario 1
If a floor having at least one access point from a controller is chosen to be synchronized with the mobility services engine from the Network Designs section of the Synchronization page, then the controller to which that access point is connected is automatically selected to be assigned to the mobility services engine for CAS service.

Scenario 2
When at least one access point from a controller is placed on a floor that is synchronized with mobility services engine, the controller to which the access point is connected is automatically assigned to the same mobility services engine for CAS service.

Scenario 3
An access point is added to a floor and is assigned to an mobility services engine. If that access point is moved from controller A to controller B, then controller B is automatically synchronized to the mobility services engine.

Scenario 4
If all access points placed on a floor which is synchronized to the mobility services engine are deleted then that controller is automatically removed from mobility services engine assignment or unsynchronized.

Out-of-Sync Alarms

Out-of-sync alarms are of Minor severity (yellow) and are raised in response to the following conditions:

- Elements have been modified in the Prime Infrastructure (the auto-sync policy pushes these elements).
- Elements have been modified in the mobility services engine.
- Elements except controllers exist in the mobility services engine database but not in the Prime Infrastructure.
- Elements have not been assigned to any mobility services engine (the auto-sync policy does not apply).

Out-of-sync alarms are cleared when the following occurs:

- The mobility services engine is deleted

Note: When you delete a mobility services engine, the out-of-sync alarms for that system is also deleted. In addition, if you delete the last available mobility services engine, the alarms for “elements not assigned to any server” are also deleted.

- Elements are synchronized manually or automatically
- User manually clears the alarms (although the alarms might reappear the future when the scheduled task is next executed)
By default, out-of-sync alarms are enabled. You can disable them in the Prime Infrastructure by choosing Administration > Scheduled Tasks, clicking Mobility Service Synchronization, unselecting the Auto Synchronization check box, and clicking Submit.

Viewing Mobility Services Engine Synchronization Status

You can use the Synchronize Servers command in the Prime Infrastructure to view the status of network design, controller, and event group synchronization with a mobility services engine.

To view synchronization status, follow these steps:

Step 1  Choose Services > Synchronize Services.
Step 2  From the left sidebar menu, choose Network Designs, Controllers, Event Groups, Wired Switches Third Party Elements, or Service Advertisements.

For each of the elements, the Sync. Status column shows the synchronization status. A green two-arrow icon indicates that its corresponding element is synchronized with the specified server such as a mobility services engine. A gray two-arrow icon with a red circle indicates that its corresponding item is not synchronized with a provided server.

A green two-arrow icon does not indicate the NMSP connection status for a controller.

You can also view the synchronization status at Monitor > Maps > System Campus > Building > Floor where Building is the building within the campus and Floor is a specific floor in that campus building. The MSE Assignment option on the left sidebar menu shows which mobility services engine the floor is currently assigned to. You can also change mobility services engine assignment from this page.

Viewing Synchronization History

You can view the synchronization history for the last 30 days for a mobility services engine. This is especially useful when automatic synchronization is enabled as alarms are automatically cleared. Synchronization History provides a summary of those cleared alarms.

The Synchronization History page on the Services tab is available only in the root virtual domain in Release 7.3.

To view synchronization history, choose Services > Synchronization History and click the column headers to sort the entries.
Viewing Notification Statistics

You can view the notification statistics for a specific mobility services engine. To view the Notification Statistics for a specific mobility services engine:

Choose Services > Mobility Services Engines > MSE-name > Context Aware Service > Notification Statistics.

where MSE-name is the name of a mobility services engine.

Table 16-2 describes the fields in the Notification statistics page.

Table 16-2 Notification Statistics fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td></td>
</tr>
<tr>
<td>Destinations</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>Total destination count.</td>
</tr>
<tr>
<td>Unreachable</td>
<td>Unreachable destination count.</td>
</tr>
<tr>
<td><strong>Notification Statistics Summary</strong></td>
<td></td>
</tr>
<tr>
<td>Destination Address</td>
<td>The destination address to which the notifications are sent.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>The destination port to which the notifications are sent.</td>
</tr>
<tr>
<td>Destination Type</td>
<td>The type of the destination. Example: SOAP_XML</td>
</tr>
<tr>
<td>Destination Status</td>
<td>Status of the track definition. Track notification status can be either Enabled or Disabled.</td>
</tr>
<tr>
<td>Last Sent</td>
<td>The date and time at which the last notification was sent to the destination device.</td>
</tr>
<tr>
<td>Last Failed</td>
<td>The date and time at which the notification failed.</td>
</tr>
<tr>
<td>Track Definition (Status)</td>
<td></td>
</tr>
<tr>
<td>Total Count</td>
<td>The total count of notifications sent to the destination. Click the count link to view the notification statistics details of the destination device.</td>
</tr>
</tbody>
</table>

Configuring High Availability

For more information on configuring high availability, see the following URL:
http://www.cisco.com/c/en/us/t d/docs/wireless/mse/8-0/MSE_CMX/8_0_MSE_CAS/7_4_MSE_CAS_chapter_0100.html#ID5

Managing System Properties for a Mobility Services Engine

You can manage the system properties of a mobility services engine using the Prime Infrastructure. This section describes the various system properties of a mobility services engine.
Editing General Properties for a Mobility Services Engine

You can use the Prime Infrastructure to edit the general properties of a mobility services engine registered in the Prime Infrastructure database. General properties include contact name, username, password, and HTTP.

To edit the general properties of a mobility services engine, follow these steps:

**Step 1** Choose Services > Mobility Services Engine to display the Mobility Services page.

**Step 2** Click the name of the mobility services engine that you want to edit. The General Properties page (with a General tab and Performance tab) appears.

On the General tab, the following read-only server details appear:

- Device Name
- Device Type
- Device UDI

**Note** For licensing, the Device UID is the string between double quote characters (including spaces in the end, if any). Exclude the double quote characters using copy-paste.

- Version
- Start Time
- IP Address

**Step 3** In the General Properties page, modify the following Server Details as necessary:

- **Contact Name**—Enter a contact name for the mobility service.
- **Username**—Enter the login username for the Prime Infrastructure server that manages the mobility service.
- **Password**—Enter the login password for the Prime Infrastructure server that manages the mobility service.
- **HTTP**—Select the **HTTP enable** check box to enable HTTP.

**Note** When you have a non-default port or HTTPS turned on, you must pass the correct information along with the command. For example, `getserverinfo` must include `-port <<port>> -protocol <<HTTP/HTTPS>>`. Similarly, for stopping the server, `stoplocserver -port <<port>> -protocol <HTTP/HTTPS>`.

- **Legacy Port**—8001
- **Legacy HTTPS**—Select the check box to enable the legacy HTTPS.
- **Delete synchronized service assignments and enable synchronization**—Select the **Delete synchronized service assignments** check box if you want to permanently remove all service assignments from the mobility services engine. This option shows up only if the delete synchronized service assignments check box was unselected while adding a mobility services engine.

**Note** The Prime Infrastructure always uses HTTPS to communicate with a mobility services engine.
Note The following tcp ports are in use on the MSE in Release 6.0: tcp 22: MSE SSH port, tcp 80: MSE HTTP port, tcp 443: MSE HTTPS port, tcp 1411: AeroScout, tcp 1999: AeroScout internal port, tcp 4096: AeroScout notifications port, tcp 5900X: AeroScout (X can vary from 1 to 10), and tcp 8001: Legacy port. Used for location APIs.

Note The following udp ports are in use on the MSE in Release 6.0: udp 123: NTPD port (open after NTP configuration), udp 162: AeroScout SNMP, udp/tcp 4000X: AeroScout proxy (X can vary from 1 to 5), udp 12091: AeroScout devices (TDOA Wi-Fi Receivers, chokepoints), udp 12092: AeroScout devices (TDOA Wi-Fi Receivers, chokepoints), udp 32768: Location internal port, udp 32769: AeroScout internal port, and udp 37008: AeroScout internal port.

Step 4 In the Mobility Services dialog box, select the Admin Status check box to enable the applicable (Context Aware Service, WIPS, Mobile Concierge Service, Location Analytics Service, Billboard service) service.

If you select Context Aware Service, then you must select a location engine to perform location calculation.

Choose either of the following:

- **Cisco Tag Engine**
  
or

- **Partner Tag Engine**

Note With MSE 6.0, you can enable multiple services (CAS and wIPS) simultaneously. Before Version 6.0, mobility services engines can only support one active service at a time.

The Mobility Services dialog box also shows the following:

- Service Name
- Service Version
- Service Status
- License Type

Note Use the Click here link to view mobility services engine licensing details.

Step 5 Click Save to update the Prime Infrastructure and mobility service databases.

Note Use the Click here link to view mobility services engine licensing details.

Step 6 Click the Performance tab to view a graph of CPU and memory utilization percentages.
Editing NMSP Parameters for a Mobility Services Engine

Network Mobility Services Protocol (NMSP) manages communication between the mobility service and the controller. Transport of telemetry, emergency, and RSSI values between the mobility service and the controller is managed by this protocol.

**Note**
- The NMSP parameter is supported in mobility services installed with Release 3.0 through 7.0.105.0. It is not supported on releases later than 7.0.105.0.
- NMSP replaces the LOCP term introduced in Release 3.0.
- Telemetry and emergency information is only seen on controllers and the Prime Infrastructure installed with Release 4.1 software or greater and on mobility service engine running release 3.0 or later software.
- The TCP port (16113) that the controller and mobility service communicate over must be open (not blocked) on any firewall that exists between the controller and mobility service for NMSP to function.

The NMSP Parameters dialog box in the Prime Infrastructure enables you to modify NMSP parameters such as echo and neighbor dead intervals as well as response and retransmit periods.

To configure NMSP parameters, follow these steps:

**Step 1** Choose Services > Mobility Services Engine.
**Step 2** Click the name of the mobility services engine whose properties you want to edit.
**Step 3** From the left sidebar menu, choose Status > NMSP Parameters.
**Step 4** Modify the NMSP parameters as appropriate.

**Note** No change in the default parameter values is recommended unless the network is experiencing slow response or excessive latency.

NMSP parameters include the following:
- **Echo Interval**—Defines how frequently an echo request is sent from a mobility service to a controller. The default value is 15 seconds. Allowed values range from 1 to 120 seconds.
  
  **Note** If a network is experiencing slow response, you can increase the values of the echo interval, neighbor dead interval and the response timeout values to limit the number of failed echo acknowledgements.

- **Neighbor Dead Interval**—The number of seconds that the mobility service waits for a successful echo response from the controller before declaring the neighbor dead. This timer begins when the echo request is sent.
  The default values is 30 seconds. Allowed values range from 1 to 240 seconds.

  **Note** This value must be at least two times the echo interval value.


- Response Timeout—Indicates how long the mobility service waits before considering the pending request as timed out. The default value is one second. Minimum value is one (1). There is no maximum value.

- Retransmit Interval—Interval of time that the mobility service waits between notification of a response time out and initiation of a request retransmission. The default setting is 3 seconds. Allowed values range from 1 to 120 seconds.

- Maximum Retransmits—Defines the maximum number of retransmits that are done in the absence of a response to any request. The default setting is 5. Allowed minimum value is zero (0). There is no maximum value.

Step 5 Click Save to update the Prime Infrastructure and mobility service databases.

**Viewing Active Session Details for a Mobility Services Engine**

The Active Sessions dialog box in the Prime Infrastructure enables you to view active user sessions on the mobility services engine.

To view active user sessions, follow these steps:

Step 1 Choose Services > Mobility Services Engines.

Step 2 Click the name of the mobility service.

Step 3 From the left sidebar menu, choose System > Active Sessions.

The Prime Infrastructure shows a list of active mobility service sessions. For every session, the Prime Infrastructure shows the following information:

- Session identifier
- IP address from which the mobility service is accessed
- Username of the connected user
- Date and time when the session started
- Date and time when the mobility service was last accessed
- How long the session was idle since the last access

**Viewing and Adding Trap Destinations for a Mobility Services Engine**

The Trap Destinations dialog box of the Prime Infrastructure enables you to specify which Prime Infrastructure or Cisco Security Monitoring, Analysis, and Response System (CS-MARS) network management platform is the recipient of SNMP traps generated by the mobility services engine.

To view or manage trap destination for a mobility services engine, follow these steps:

Step 1 Choose Services > Mobility Services Engines.

Step 2 Click the name of the mobility service.

Step 3 From the left sidebar menu, choose System > Trap Destinations.

The Prime Infrastructure shows a list of current trap destinations including the following information:
To add a trap destination, follow these steps:

**Step 1** Choose **Services > Mobility Services**.

**Step 2** Click the name of the mobility service.

**Step 3** From the left sidebar menu, choose **System > Trap Destinations**.

**Step 4** Choose **Add Trap Destination** from the command drop-down list and click **Go**.

The New Trap Destination page appears.

**Step 5** Enter the following details (see **Table 16-3**).

---

**Table 16-3  Add Trap Destination Page**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address for the trap destination</td>
</tr>
<tr>
<td>Port No.</td>
<td>Port number for the trap destination. The default port number is 162.</td>
</tr>
<tr>
<td>Destination Type</td>
<td>This field is not editable and has a value of <strong>Other</strong>.</td>
</tr>
<tr>
<td>Snmp Version</td>
<td>Select either v2c or v3.</td>
</tr>
<tr>
<td>The following set of fields appear only if you select v3 as the SNMP version.</td>
<td></td>
</tr>
<tr>
<td>User Name</td>
<td>Username for the SNMP Version 3.</td>
</tr>
<tr>
<td>Security Name</td>
<td>Security name for the SNMP Version 3.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>HMAC-MD5</td>
</tr>
<tr>
<td></td>
<td>HMAC-SHA</td>
</tr>
<tr>
<td>Authentication Password</td>
<td>Authentication password for the SNMP Version 3.</td>
</tr>
<tr>
<td>Privacy Type</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>CBC-DES</td>
</tr>
<tr>
<td></td>
<td>CFB-AES-128</td>
</tr>
<tr>
<td></td>
<td>CFB-AES-192</td>
</tr>
<tr>
<td></td>
<td>CFB-AES-256</td>
</tr>
<tr>
<td>Privacy Password</td>
<td>Privacy password for the SNMP Version 3.</td>
</tr>
</tbody>
</table>
Step 6  Click **Save** to save the changes or **Cancel** to discard the changes.

---

**Editing Advanced Parameters for a Mobility Services Engine**

The Advanced Parameters dialog box in the Prime Infrastructure enables you to set the number of days events are kept, set session time out values, set an absent data interval cleanup interval, and enable or disable Advanced Debug.

---

**Note**

You can use the Prime Infrastructure to modify troubleshooting parameters for a mobility services engine.

To edit advanced parameters for a mobility services engine, follow these steps:

---

**Step 1**  Choose **Services > Mobility Services Engines**.

**Step 2**  Click the name of the mobility service whose properties you want to edit.

**Step 3**  From the left sidebar menu, choose **System > Advanced Parameters**.

**Step 4**  View or modify the advanced parameters as necessary.

- **General Information**
- **Advanced Parameters**

---

**Caution**

Because advanced debugging slows the mobility service down, enable advanced debugging only under the guidance of Cisco TAC personnel.

---

- **Number of Days to keep Events**—Enter the number of days to keep logs. Change this value as required for monitoring and troubleshooting.

- **Session Timeout**—Enter the number of minutes before a session times out. Change this value as required for monitoring and troubleshooting. Currently this option appears dimmed.

- **Cisco UDI**
  - **Product Identifier (PID)**—The Product ID of the mobility services engine.
  - **Version Identifier (VID)**—The version number of the mobility services engine.
  - **Serial Number (SN)**—Serial number of the mobility services engine.

- **Advanced Commands**
  - **Reboot Hardware**—Click to reboot the mobility service hardware. See the “Rebooting the Mobility Services Engine Hardware” section on page 16-27 for more information.
  - **Shutdown Hardware**—Click to turn off the mobility service hardware. See the “Shutting Down the Mobility Services Engine Hardware” section on page 16-27 for more information.
  - **Clear Database**—Click to clear the mobility services database. See the “Clearing the Mobility Services Engine Database” section on page 16-27 for more information. Unselect the **Retain current service assignments in the Prime Infrastructure** check box to remove all existing service assignments from the Prime Infrastructure and MSE. The resources have to be reassigned from **Services > Synchronize Services** page. This option is selected by default.
Step 5  Click **Save** to update the Prime Infrastructure and mobility service databases.

**Rebooting the Mobility Services Engine Hardware**

If you need to restart a mobility services engine, follow these steps:

- **Step 1** Choose **Services > Mobility Services Engines**.
- **Step 2** Click the name of the mobility services engine that you want to reboot.
- **Step 3** Click **System**.
- **Step 4** Click **Advanced Parameters**.
- **Step 5** In the Advanced Commands dialog box, click **Reboot Hardware**.
- **Step 6** Click **OK** to confirm that you want to reboot the mobility services engine hardware.

The rebooting process takes a few minutes to complete.

**Shutting Down the Mobility Services Engine Hardware**

If you need to shut down a mobility services engine, follow these steps:

- **Step 1** Choose **Services > Mobility Services Engines**.
- **Step 2** Click the name of the mobility services engine that you want to shut down.
- **Step 3** Click **System**.
- **Step 4** Click **Advanced Parameters**.
- **Step 5** In the Advanced Commands dialog box, click **Shutdown Hardware**.
- **Step 6** Click **OK** to confirm that you want to shut down the mobility services engine.

**Clearing the Mobility Services Engine Database**

To clear a mobility services engine configuration and restore its factory defaults, follow these steps:

- **Step 1** Choose **Services > Mobility Services Engines**.
- **Step 2** Click the name of the mobility services engine you want to configure.
- **Step 3** Click **System**.
- **Step 4** Click **Advanced Parameters**.
- **Step 5** In the Advanced Commands dialog box, unselect the **Retain current service assignments** in the **Prime Infrastructure** check box to remove all existing service assignments from the Prime Infrastructure and MSE.

The resources have to be reassigned in the Services > Synchronize Services page. By default, this option is selected.
Step 6 In the Advanced Commands dialog box, click Clear Database.
Step 7 Click OK to clear the mobility services engine database.

Working with Logs

This section describes how to configure logging options and how to download log files.

Configuring Logging Options

You can use the Prime Infrastructure to specify the logging level and types of messages to log.

To configure logging options, follow these steps:

Step 1 Choose Services > Mobility Services Engines.
Step 2 Click the name of the mobility services engine that you want to configure.
Step 3 Choose System > Logs. The advanced parameters for the selected mobility services engine appear.
Step 4 Choose the appropriate options from the Logging Level drop-down list.

There are four logging options: Off, Error, Information, and Trace.

All log records with a log level of Error or preceding are logged to a new error log file locserver-error-%u-%g.log. This is an additional log file maintained along with the location server locserver-%u-%g.log log file. The error log file consists of logs of Error level along with their context information. The contextual information consists of 25 log records prior to the error. You can maintain up to 10 error log files. The maximum size allowed for each log file is 10 MB.

Caution Use Error and Trace only when directed to do so by Cisco TAC personnel.

Step 5 Select the Enabled check box next to each element listed in that section to begin logging its events.
Step 6 Select the Enable check box in the Advanced Parameters dialog box to enable advanced debugging. By default, this option is disabled.
Step 7 To download log files from the server, click Download Logs. See the “Downloading Mobility Services Engine Log Files” section on page 16-29 for more information.
Step 8 In the Log File group box, enter the following:
   - The number of log files to be maintained in the mobility services engine. You can maintain a minimum of 5 log files and a maximum of 20 log files in the mobility services engine.
   - The maximum log file size in MB. The minimum log file size is 10 MB and the maximum is 50 MB.
Step 9 In the MAC Address Based Logging group box, do the following:
   - Select the Enable check box to enable MAC address logging. By default, this option is disabled.
   - Add one or more MAC addresses for which you want to enable logging. You can also remove MAC addresses that you have already added by selecting the MAC address from the list and clicking Remove.

See the “MAC Address-based Logging” section on page 16-29 for more information on MAC Address-based logging.
Step 10 Click Save to apply your changes.

**MAC Address-based Logging**

This feature allows you to create log files that are specific to an entity whose MAC address is specified. The log files are created in the locserver directory under the following path:

```
/opt/mse/logs/locserver
```

A maximum of 5 MAC addresses can be logged at a time. The Log file format for MAC address aa:bb:cc:dd:ee:ff is macaddress-debug-aa-bb-cc-dd-ee-ff.log

You can create a maximum of two log files for a MAC Address. The two log files might consist of one main and one backup or rollover log file.

The minimum size of a MAC log file is 10 MB. The maximum size allowed is 20 MB per MAC Address. The MAC log files that are not updated for more than 24 hours are pruned.

**Downloading Mobility Services Engine Log Files**

If you need to analyze mobility services engine log files, you can use the Prime Infrastructure to download them to your system. The Prime Infrastructure downloads a zip file containing the log files.

To download a .zip file containing the log files, follow these steps:

**Step 1** Choose Services > Mobility Services Engines.
**Step 2** Click the name of the mobility services engine to view its status.
**Step 3** From the left sidebar menu, choose Logs.
**Step 4** Click Download Logs.
**Step 5** Follow the instructions in the File Download dialog box to open the file or save the zip file to your system.

**Managing User and Group Accounts for a Mobility Services Engine**

This section describes how to configure and manage users and groups on the mobility services engine.

This section describes how to add, delete, and edit users for a mobility services engine.

- **Note** See the “Viewing Active Session Details for a Mobility Services Engine” section on page 16-24 for information on viewing active sessions for each user.

- Managing Group Accounts—This section describes how to add, delete, and edit user groups for a mobility services engine and contains the following topics:
  - Adding User Groups, page 16-31
  - Deleting User Groups, page 16-31
  - Editing Group User Permissions, page 16-32
Adding Users for a Mobility Services Engine

To add a user to a mobility services engine, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Services &gt; Mobility Services Engines.</td>
</tr>
<tr>
<td>2</td>
<td>Click the device name of the mobility services engine that you want to edit.</td>
</tr>
<tr>
<td>3</td>
<td>From the left sidebar menu, choose Systems &gt; Accounts &gt; Users.</td>
</tr>
<tr>
<td>4</td>
<td>From the Select a command drop-down list, choose Add User.</td>
</tr>
<tr>
<td>5</td>
<td>Click Go.</td>
</tr>
<tr>
<td>6</td>
<td>Enter the username in the Username text box.</td>
</tr>
<tr>
<td>7</td>
<td>Enter a password in the Password text box.</td>
</tr>
<tr>
<td>8</td>
<td>Enter the name of the group to which the user belongs in the Group Name text box.</td>
</tr>
<tr>
<td>9</td>
<td>Choose a permission level from the Permission drop-down list.</td>
</tr>
</tbody>
</table>

There are three permission levels to choose from: Read Access, Write Access, and Full Access (required for Prime Infrastructure to access a mobility services engine).

Caution

Group permissions override individual user permissions. For example, if you give a user full access and add that user to a group with read access, that user is unable to configure mobility services engine settings.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Click Save to add the new user to the mobility services engine.</td>
</tr>
</tbody>
</table>

Deleting Users

To delete a user from a mobility services engine, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Services &gt; Mobility Services.</td>
</tr>
<tr>
<td>2</td>
<td>Click the device name of the mobility services engine that you want to edit.</td>
</tr>
<tr>
<td>3</td>
<td>From the left sidebar menu, choose Systems &gt; Accounts &gt; Users.</td>
</tr>
<tr>
<td>4</td>
<td>Select the check box(es) of the user(s) that you want to delete.</td>
</tr>
<tr>
<td>5</td>
<td>From the Select a command drop-down list, choose Delete User.</td>
</tr>
<tr>
<td>6</td>
<td>Click Go.</td>
</tr>
<tr>
<td>7</td>
<td>Click OK to confirm that you want to delete the selected users.</td>
</tr>
</tbody>
</table>

Editing User Properties

To change user properties, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Services &gt; Mobility Services.</td>
</tr>
<tr>
<td>2</td>
<td>Click the device name of the mobility services engine that you want to edit.</td>
</tr>
</tbody>
</table>
Step 3  From the left sidebar menu, choose Systems > Accounts > Users.
Step 4  Click the username of the user that you want to edit.
Step 5  Make the required changes to the Password, Group Name, and Permission text boxes.
Step 6  Click Save to apply your change.

Adding User Groups

To add a user group to a mobility services engine, follow these steps:

Step 1  Choose Services > Mobility Services.
Step 2  Click the device name of the mobility services engine that you want to edit.
Step 3  From the left sidebar menu, choose Systems > Accounts > Groups.
Step 4  From the Select a command drop-down list, choose Add Group.
Step 5  Click Go.
Step 6  Enter the name of the group in the Group Name text box.
Step 7  Choose a permission level from the Permission drop-down list.
       There are three permissions levels to choose from:
       • Read Access
       • Write Access
       • Full Access (required for Prime Infrastructure to access mobility services engines)
Step 8  Click Save to add the new group to the mobility services engine.

Caution Group permissions override individual user permissions. For example, if you give a user full access and add that user to a group with read access permission, that user cannot configure mobility services engine settings.

Deleting User Groups

To delete user groups from a mobility services engine, follow these steps:

Step 1  Choose Services > Mobility Services.
Step 2  Click the device name of the mobility services engine that you want to edit.
Step 3  From the left sidebar menu, choose Systems > Accounts > Groups.
Step 4  Select the check box(es) of the group(s) that you want to delete.
Step 5  From the Select a command drop-down list, choose Delete Group.
Step 6  Click Go.
Step 7  Click OK to confirm that you want to delete the selected users.
Editing Group User Permissions

To change user group permissions, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Services &gt; Mobility Services</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the device name of the mobility services engine that you want to edit.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the left sidebar menu, choose <strong>Systems &gt; Accounts &gt; Groups</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click the group name of the group that you want to edit.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Choose a permission level from the Permission drop-down list.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>Save</strong> to apply your change.</td>
</tr>
</tbody>
</table>

⚠️ **Caution**

Group permissions override individual user permissions. For example, if you give a user permission for full access and add that user to a group with read access, that user is unable to configure mobility services engine settings.

Monitoring Status Information for a Mobility Services Engine

The **System > Status** page enables you to monitor server events, Prime Infrastructure alarms and events, and NMSP connection status for the mobility services engine.

Viewing Server Events for a Mobility Services Engine

To view a list of server events, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Services &gt; Mobility Services</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the name of the applicable mobility services engine.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the left sidebar menu, choose <strong>System &gt; Status &gt; Server Events</strong>.</td>
</tr>
</tbody>
</table>

The **Status > Server Events** page provides the following information:

- **Timestamp**—Time of the server event.
- **Severity**—Severity of the server event.
- **Event**—Detailed description of the event.
- **Facility**—The facility in which the event took place.

Viewing Audit Logs from a Mobility Services Engine

You can view the audit logs for User-triggered operations using the **Audit Logs** option available in a Mobility Services Engine. To view the audit logs, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Services &gt; Mobility Services</strong>.</td>
</tr>
</tbody>
</table>
Step 2  Click the name of the applicable mobility services engine.

Step 3  From the left sidebar menu, choose System > Status > Audit Logs.

The Status > Audit Logs page provides the following information:
- Username—The Username which has triggered the audit log.
- Operation—The operation that has been performed by the User.
- Operation Status—The status of the operation and it can be SUCCESSFUL or FAILED.
- Invocation Time—The date and time at which the audit log was recorded for the specified operation.

Viewing Prime Infrastructure Alarms for a Mobility Services Engine

To view a list of Prime Infrastructure alarms, follow these steps:

Step 1  Choose Services > Mobility Services.

Step 2  Click the name of the applicable mobility service.

Step 3  From the left sidebar menu, choose System > Status > Prime Infrastructure Alarms. See the “Monitoring Alarms” section on page 5-126 for more information.

Viewing Prime Infrastructure Events for a Mobility Services Engine

To view a list of Prime Infrastructure events, follow these steps:

Step 1  Choose Services > Mobility Services.

Step 2  Click the name of the applicable mobility service.

Step 3  From the left sidebar menu, choose System > Status > Prime Infrastructure Events. See the “Monitoring Events” section on page 5-141 for more information.

Viewing NMSP Connection Status for a Mobility Services Engine

The NMSP Connection Status page allows you to verify the NMSP connection between the mobility services engine and the Cisco controller to which the mobility services engine is assigned.

Note  Network Mobility Services Protocol (NMSP) is the protocol that manages communication between the mobility service and the controller.

To verify the NMSP connection between the controller and the mobility services engine, follow these steps:

Step 1  Choose Services > Mobility Services.
Step 2  Click the name of the applicable mobility service.

Step 3  From the left sidebar menu, choose **System > Status > NMSP Connection Status**.

The NMSP Connection Status page shows the following information:

- **Summary**—The Summary section shows each device type, the total number of connections, and the number of inactive connections.

- **NMSP Connection Status**—This group box shows the following:
  - **IP address**—Click the device IP address to view NMSP connection status details for this device. See the “Viewing NMSP Connection Status Details” section on page 16-34 for additional information.
  - **Target Type**—Indicates the device to which the NMSP connection is intended.
  - **Version**—Indicates the current software version for the device.
  - **NMSP Status**—Indicates whether the connection is active or inactive.
  - **Echo Request Count**—Indicates the number of echo requests that were sent.
  - **Echo Response Count**—Indicates the number of echo responses that were received.
  - **Last Message Received**—Indicates the date and time of the most recent message received.

Step 4  Verify that the NMSP Status is ACTIVE.

- If active, you can view details on wired switches, controllers, and wired clients.
- If not active, resynchronize Prime Infrastructure device and the mobility services engine.

**Note**

You can launch an NMSP troubleshooting tool for an inactive connection.

---

**Viewing NMSP Connection Status Details**

To view NMSP Connection Status details, follow these steps:

**Step 1** Choose **Services > Mobility Services**.

**Step 2**  Click the name of the applicable mobility service.

**Step 3**  From the left sidebar menu, choose **System > Status > NMSP Connection Status**.

**Step 4**  Click the device IP address to open the NMSP Connection Status Details page. The Details page shows the following information:

- **Summary**
  - **IP Address**
  - **Version**—The current software version for the device.
  - **Target Type**—The device to which the NMSP connection is intended.
  - **NMSP Status**—Indicates whether the connection is active or inactive.
  - **Echo Request Count**—The number of echo requests that were sent.
  - **Echo Response Count**—The number of echo responses that were received.
  - **Last Activity Time**—The date and time of the most recent message activity between the device and the mobility services engine.
– Last Echo Request Message Received At—The date and time the last echo request was received.
– Last Echo Response Message Received At—The date and time the last echo response was received.
– Model—The device model.
– MAC Address—The MAC address of the device, if applicable.
– Capable NMSP Services—Indicates the NMSP-capable services for this device such as ATTACHMENT or LOCATION.

• Subscribed Services—Indicates subservices for each subscribed NMSP service. For example, MOBILE_STATION_ATTACHMENT is a subservice of ATTACHMENT.

• Messages
  – Message Type—Message types might include: ATTACHMENT_NOTIFICATION, ATTACHMENT_REQUEST, ATTACHMENT_RESPONSE, CAPABILITY_NOTIFICATION, ECHO_REQUEST, ECHO_RESPONSE, LOCATION_NOTIFICATION, LOCATION_REQUEST, SERVICE_SUBSCRIBE_REQUEST, SERVICE_SUBSCRIBE_RESPONSE.
  – In/Out—Indicates whether the message was an incoming or outgoing message.
  – Count—Indicates the number of incoming or outgoing messages.
  – Last Activity Time—The date and time of the most recent activity or message.
  – Bytes—Size of the message in Bytes.

Managing Maintenance for Mobility Services

Viewing or Editing Mobility Services Backup Parameters

To view or edit mobility service backup parameters, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Services &gt; Mobility Services.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the name of the mobility service whose properties you want to edit.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the left sidebar menu, choose Maintenance &gt; Backup.</td>
</tr>
</tbody>
</table>
  • Backups located at—Indicates the location of the backup file.
  • Enter a name for the Backup—Enter or edit the name of the backup file.
  • Timeout (in secs)—Indicates the length of time (in seconds) before attempts to back up files times out.

Backing Up Mobility Services Engine Historical Data

The Prime Infrastructure contains functionality for backing up mobility services engine data. To back up mobility services engine data, follow these steps:
Step 1  In the Prime Infrastructure UI, choose Services > Mobility Services.

Step 2  Click the name of the mobility services engine that you want to back up.

Step 3  From the left sidebar menu, choose Maintenance > Backup.

Step 4  Enter the name of the backup.

Step 5  Enter the time in seconds after which the backup times out.

Step 6  Click Submit to back up the historical data to the hard drive of the server running Prime Infrastructure. Status of the backup can be seen on the page while the backup is in process. Three items are displayed on the page during the backup process: (1) Last Status field provides messages noting the status of the backup; (2) Progress field shows what percentage of the backup is complete; and (3) Started at field shows when the backup began noting date and time.

**Note**  
You can run the backup process in the background while working on other mobility services engine operations in another Prime Infrastructure page.

**Note**  
Backups are stored in the FTP directory that you specify during the Prime Infrastructure installation. However, in the Prime Infrastructure installation, the FTP directory is not specified. It might be necessary to provide the full path of the FTP root.

---

**Restoring Mobility Services Engine Historical Data**

To restore a file back into the mobility service, follow these steps:

**Step 1**  Choose Services > Mobility Services.

**Step 2**  Click the name of the mobility service whose properties you want to edit.

**Step 3**  From the left sidebar menu, choose Maintenance > Restore.

**Step 4**  Choose the file to restore from the drop-down list.

**Step 5**  Select the Delete synchronized service assignments check box if you want to permanently remove all service assignments from the mobility services engine. This option is applicable for network designs, wired switches, controllers and event definitions. The existing location history data is retained, however you must use manual service assignments to perform any future location calculations.

**Step 6**  Click Submit to start the restoration process.

**Step 7**  Click OK to confirm that you want to restore the data from the Prime Infrastructure server hard drive. When the restoration is complete, the Prime Infrastructure shows a message to that effect.

**Note**  
You can run the restore process in the background while working on other mobility services engine operations in another Prime Infrastructure page.
Downloading Software to a Mobility Services Engine Using the Prime Infrastructure

To download software to a mobility services engine using the Prime Infrastructure, follow these steps:

**Step 1** Verify that you can ping the location appliance from the Prime Infrastructure or an external FTP server, whichever you are going to use for the application code download.

**Step 2** Choose **Services > Mobility Services**.

**Step 3** Click the name of the mobility services engine to which you want to download software.

**Step 4** On the left sidebar menu, choose **Maintenance**.

**Step 5** Click **Download Software**.

To download software, do one of the following:

- To download software listed in the Prime Infrastructure directory, select the **Select from uploaded images to transfer into the Server** check box. Then, choose a binary image from the drop-down list.
  
  The Prime Infrastructure downloads the binary images listed in the drop-down list into the FTP server directory you specified during the Prime Infrastructure installation.

  In the Prime Infrastructure installation, FTP directory is not specified. It might be necessary to give the full path of the FTP root.

- To use downloaded software available locally or over the network, select the **Browse a new software image to transfer into the Server** check box and click **Browse**. Locate the file and click **Open**.

**Step 6** Enter the time, in seconds (between 1 and 1800), after which the software download times out.

**Step 7** Click **Download** to send the software to the /opt/installers directory on the mobility services engine.

Configuring Partner System for a Mobility Services Engine

The System > Partner Systems page enables you to do MSE-Qualcomm PDS configuration. This configuration is aimed at providing better navigation capability for the mobile devices. The Partner Discovery Server (PDS) generates encrypted assistance data using the floor plan and AP data which is provided by the MSE. The PDS converts this information into an optimized format that will be used by Qualcomm smart phones.

Qualcomm PDS Configuration

To configure Qualcomm PDS for MSE, follow these steps:

**Step 1** Choose Services > Mobility Services.

**Step 2** Click the name of the mobility services.

**Step 3** From the left sidebar menu, choose System > Partner Systems.

The Qualcomm PDS Configuration for MSE page appears.

**Step 4** If you want to enable MSE-qualcomm communication, then select the **Enable Qualcomm** check box.
Step 5 In the Qualcomm PDS Endpoint text box, enter the Qualcomm PDS server URL. This is the URL of the PDS from where you can fetch data assistance. The default URL is http://207.114.133.174:8000/AssistanceDataMgr/AssistanceDataMgrSOAP?wsdl.

Step 6 In the MSE URL to request assistance data text box, enter the MSE URL. This is the URL at which the MSE is accessible by the devices at the venue.

Step 7 In the Cisco Mobile Concierge SSID text box, enter the Mobile Concierge SSID information of the venue to which mobile clients should connect. The Qualcomm smart phones will associate this SSID and communicate with MSE.

Step 8 Enter the venue description in the Venue Description text box.

Step 9 Enter refresh time period for assistance data for MSE in the Refresh time period for assistance data on MSE text box.

Step 10 Enter refresh time period for assistance data for mobile clients in the Refresh time period for assistance data on mobile clients text box.

Step 11 Select the Include Copyright Information check box if the messages/assistance data sent to Qualcomm PDS server and mobile clients should be copyrighted.

Step 12 In the Copyright Owner text box, enter the copyright owner information that has to be included.

Step 13 Enter the copyright year to be included in the Copyright Year text box.

Step 14 Click Save to save the configuration and Cancel to go back.

MSE-Qualcomm Configuration

The MSE-Qualcomm configuration involves the following steps:

- Generate Map Extraction Tool (MET) output from CAD file.
- Input MET Output into Prime Infrastructure
- Addition of GPS Markers
- Synchronize the Floor to MSE
- Provide Qualcomm QUIPS/PDS and Copyright Information
- On MSE, perform F2 Interface request to Qualcomm PDS server

Generating Map Extraction Tool (MET) Output from CAD File

Qualcomm’s MET is an application that allows you to customize and select various layers from a map file (DXF file) and generates a zip file containing:

- Image file (.PNG format) to be used as floor map on the Prime Infrastructure.
- Span.xml file that contains the dimensions of the floor (horizontal and vertical) in meters.
- Qualcomm specific map XML file containing geometric feature information related to walls, doors, points of interest, and so on.

Note MET application is independent of Prime Infrastructure and MSE and can reside on any host machine. Only the output of MET is used as MAP related input information on the Prime Infrastructure.

Step 1 Start Qualcomm MET tool by following the steps in ReadMe.txt within the MET Tool folder.
Step 2  Input the DXF File in the Map Extraction Tool.
Step 3  Select necessary layers from the left sidebar menu.
Step 4  Save the output of Map Extraction Tool to desired location on the Map Extraction Tool user interface.

Managing Cisco Adaptive wIPS Service Parameters

The wIPS Service page allows you to view or manage wIPS service administrative settings.

Note  Cisco Adaptive wIPS functionality is not supported for non-root partition users.

Managing wIPS Service Administration Settings

To view or manage wIPS service administration settings, follow these steps:

Step 1  Choose Services > Mobility Services Engines.
Step 2  Choose the device name of the applicable mobility services engine.
Step 3  From the left sidebar menu, choose wIPS Service.
Step 4  View or edit the following parameters:
  - Log level—Choose the applicable log level from the drop-down list. Log levels include Debug, Error, Important Event, Major Debug, None, and Warning.
  - Forensic size limit (GB)—Enter the maximum allowable size of forensic files.
  - Alarm ageout (hours)—Enter the age limit, in hours, for each alarm.
  - Device ageout (days)—Enter the age limit, in days, for the device to send alarms.
Step 5  Click Save to confirm the changes or Cancel to close the page with no changes applied.

Managing Context-Aware Service Software Parameters

Context-Aware Service (CAS) software allows a mobility services engine to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as location, temperature and asset availability about a client or tag (Cisco CX version or later) from Cisco access points.

CAS relies on two engines for processing the contextual information it receives. The Context-Aware Engine for Clients processes data received from Wi-Fi clients and the Context-Aware Engine for Tags processes data received from Wi-Fi tags; these engines can be deployed together or separately depending on the business need.

Note  Mobility services engines do not track or map non-Cisco CX tags.

Note  CAS was previously referred to as Cisco location-based services.
You can modify Context-Aware Service Software properties as to the type and number of clients or tags that are tracked and whether or not locations are calculated for those clients or tags.

You can also modify parameters that affect the location calculation of clients and tags such as Received Signal Strength Indicator (RSSI) measurements.

Viewing Contextual Information

Before you can use the Prime Infrastructure to view contextual information, initial configuration for the mobility services engine is required using a command-line interface (CLI) console session. See the Cisco 3355 Mobility Services Engine Getting Started Guide and the Cisco 3100 Mobility Services Engine Getting Started Guide at the following URL: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html.

After its installation and initial configuration are complete, the mobility services engine can communicate with multiple Cisco wireless LAN controllers to collect operator-defined contextual information. You can then use the associated Prime Infrastructure to communicate with each mobility services engine to transfer and display selected data.

You can configure the mobility services engine to collect data for clients, rogue access points, rogue clients, mobile stations, interferers, and active RFID asset tags.

Licensing for Clients and Tags

You must purchase licenses from Cisco to retrieve contextual information on tags and clients from access points.

- Licenses for tags and clients are offered separately.
- The clients license also contains tracking of rogue clients and rogue access points, and interferers (if enabled).
- Licenses for tags and clients are offered in a variety of quantities, ranging from 1,000 to 12,000 units.

The AeroScout Context-Aware Engine for Tags supports 100 permanent tag licenses; Context-Aware Services consists of permanent tag licenses.

Note


For additional information on Context-Aware parameters, see the following topics:

- Context-Aware Service General Parameters, page 16-40
- Context-Aware Service Administration Parameters, page 16-41
- Context-Aware Service Advanced Parameters, page 16-59

Context-Aware Service General Parameters

To access the Context Aware Service > General page, choose Services > Mobility Services Engines > General from the left sidebar menu. This page provides the following information:

- Version
Operational Status
Number of Tracked Wireless Clients
Number of Traced Tags
Number of Tracked Rogue APs
Number of Tracked Rogue Clients
Number of Tracked Interferers
Number of Tracked Wired Clients
Total Elements Tracked
Tracked Elements (Wireless Clients, Rogue APs, Rogue Clients, Interferers, and Wired Clients) Limit
Tracked Tags Limit

Context-Aware Service Administration Parameters

Modifying Tracking Parameters for Mobility Services

The mobility services engine can track up to 25,000 clients or up to 25,000 tags (with the proper license purchase). Updates on the locations of elements being tracked are provided to the mobility services engine from the Cisco wireless LAN controller.

Only those elements designated for tracking by the controller are viewable in the Prime Infrastructure maps, queries, and reports. No events and alarms are collected for non-tracked elements and none are used in calculating the 25,000 element limit for clients or tags.

You can modify the following tracking parameters using the Prime Infrastructure:

- Enable and disable element locations (client stations, active asset tags, interferers, wired clients, rogue clients, and rogue access points) you actively track.
  - Wired client location tracking enables servers in a data center to more easily find wired clients in the network. Servers are associated with wired switch ports in the network.

- Set limits on how many of specific elements you want to track.
  For example, given a client license of 12,000 trackable units, you can set a limit to track only 8,000 client stations (leaving 4,000 units available to track rogue clients and rogue access points). Once the tracking limit is met for a given element, the number of elements not being tracked is summarized in the Tracking Parameters page.

- Disable tracking and reporting of ad hoc rogue clients and access points.

To configure tracking parameters for a mobility services engine, follow these steps:

**Step 1** Choose Services > Mobility Services Engines to open the Mobility Services page.

**Step 2** Click the name of the mobility services engine whose properties you want to edit. The General Properties page appears.

**Step 3** Choose Context-Aware Software > Tracking Parameters from the Administration subheading to display the configuration options.

**Step 4** Modify the following tracking parameters as appropriate (see Table 16-4).
Table 16-4  Tracking Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking Parameters</td>
<td></td>
</tr>
<tr>
<td>Wired Clients</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of client stations by the mobility services engine.</td>
</tr>
<tr>
<td></td>
<td>In 7.0, the client license encompasses all network location service elements and is shared among wireless clients, wired clients, rogue clients, access points, and interferers.</td>
</tr>
<tr>
<td></td>
<td>The wired client limiting is supported from mobility services engine 7.0 and Prime Infrastructure 1.0. In other words, you can limit wired clients to a fixed number, say 500. This limit is set to ensure that the licenses are not taken up completely by wired clients and some licenses are available for other devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution</strong> When upgrading the mobility services engine from 6.0 to 7.0, if any limits have been set on wireless clients or rogues, they reset because of the wired client limit change in 7.0.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Active Value (Display only): Indicates the number of wired client stations currently being tracked.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not Tracked (Display only): Indicates the number of wired client stations beyond the limit.</td>
</tr>
<tr>
<td>Wireless Clients</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of client stations by the mobility services engine.</td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>Enable Limiting</strong> check box to set a limit on the number of client stations to track.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 25,000 which is the maximum number of clients that can be tracked by a mobility services engine.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The actual number of tracked clients is determined by the license purchased.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Active Value (Display only): Indicates the number of client stations currently being tracked.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not Tracked (Display only): Indicates the number of client stations beyond the limit.</td>
</tr>
</tbody>
</table>
### Chapter 16 Prime Infrastructure Services

#### Mobility Services

**16-43**

**Table 16-4 Tracking Parameters (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rogue Access Points</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of rogue clients and asset points by the mobility services engine.</td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>Enable Limiting</strong> check box to set a limit on the number of rogue clients and asset tags stations to track.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 25,000 which is the maximum number of rogue clients and access points that can be tracked by a mobility services engine.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The actual number of tracked rogues (clients and access points) is driven by the client license purchased. The user must consider the number of clients that are being tracked in determining the available quantity to allocate to track rogue clients and access points because clients and rogue clients and access points are addressed by the same license.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Active Value (Display only): Indicates the number of rogue clients and access points currently being tracked.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not Tracked (Display only): Indicates the number of rogue clients and access points beyond the limit.</td>
</tr>
<tr>
<td>Exclude Ad-Hoc Rogues</td>
<td>Select the check box to turn off the tracking and reporting of ad hoc rogues in the network. As a result, ad hoc rogues are not displayed on the Prime Infrastructure maps or its events and alarms reported.</td>
</tr>
<tr>
<td>Rogue Clients</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of rogue clients by the mobility services engine.</td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>Enable Limiting</strong> check box to set a limit on the number of rogue clients to track.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 25,000 which is the maximum number of rogue clients that can be tracked by a mobility services engine.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The actual number of tracked rogues (clients and access points) is driven by the client license purchased. The user must consider the number of clients that are being tracked in determining the available quantity to allocate to track rogue clients and access points because clients and rogue clients and access points are addressed by the same license.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Active Value (Display only): Indicates the number of rogue clients being tracked.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not Tracked (Display only): Indicates the number of rogue clients beyond the limit.</td>
</tr>
</tbody>
</table>
Table 16-4  Tracking Parameters (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interferers</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of the interferers by the mobility services engine. In 7.0, the client license encompasses all network location service elements and is shared among wireless clients, wired clients, rogue clients, access points, and interferers.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Active Value (Display only): Indicates the number of interferers currently being tracked.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not Tracked (Display only): Indicates the number of interferers beyond the limit.</td>
</tr>
<tr>
<td>Asset Tracking Elements</td>
<td></td>
</tr>
<tr>
<td>Active RFID Tags</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of active RFID tags by the mobility services engine.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The actual number of tracked active RFID tags is determined by the license purchased.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Active Value (Display only): Indicates the number of active RFID tags currently being tracked. It also depends on the tag engine chosen.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not Tracked (Display only): Indicates the number of active RFID tags beyond the limit.</td>
</tr>
<tr>
<td>SNMP Parameters</td>
<td>Not applicable to mobility services 7.0.105.0 and later.</td>
</tr>
<tr>
<td>SNMP Retry Count</td>
<td>Enter the number of times to retry a polling cycle the default value is 3. Allowed values are from 1 to 99999. (Configurable in controller Release 4.1 and earlier only.)</td>
</tr>
<tr>
<td>SNMP Timeout</td>
<td>Enter the number of seconds before a polling cycle times out, the default value is 5. Allowed values are from 1 to 99999. (Configurable in controller Release 4.1 and earlier only.)</td>
</tr>
<tr>
<td>SNMP Polling Interval</td>
<td>Select the <strong>Enable</strong> check box to enable client station polling and enter the polling interval in seconds. Default value is 300. Allowed values are from 1 to 99999. (Configurable in controller Release 4.1 and earlier only.)</td>
</tr>
<tr>
<td>Active RFID Tags</td>
<td>Select the <strong>Enable</strong> check box to enable active RFID tag polling and enter the polling interval in seconds. Allowed values are from 1 to 99999.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Before the mobility service can collect asset tag data from controllers, you must enable the detection of active RFID tags using the <code>config rfid status enable</code> CLI command on the controllers.</td>
</tr>
<tr>
<td>Rogue Clients and Access Points</td>
<td>Select the <strong>Enable</strong> check box to enable rogue access point polling and enter the polling interval in seconds. Default value is 600. Allowed values are from 1 to 99999. (Configurable in controller Release 4.1 and earlier only.)</td>
</tr>
<tr>
<td>Statistics</td>
<td>Select the <strong>Enable</strong> check box to enable statistics polling for the mobility service, and enter the polling interval in seconds. Default value is 900. Allowed values are from 1 to 99999. (Configurable in controller Release 4.1 and earlier only.)</td>
</tr>
</tbody>
</table>
Step 5 Click **Save** to store the new settings in the mobility services engine database.

**Filtering Parameters for Mobility Services**

In the Prime Infrastructure, you can limit the number of asset tags, wired clients, rogue clients, interferers and access points whose location is tracked by filtering on the following:

- **MAC addresses**

  Specific MAC addresses can be entered and labeled as allowed or disallowed from location tracking. You can import a file with the MAC addresses that are to be allowed or disallowed, or you can enter them individually in the Prime Infrastructure GUI page.

  The format for entering MAC addresses is `xx:xx:xx:xx:xx:xx`. If a file of MAC addresses is imported, the file must follow a specific format as follows:

  - Each MAC address should be listed on a single line.
  - Allowed MAC addresses must be listed first and preceded by an “[Allowed]” line item. Disallowed MAC addresses must be preceded by “[Disallowed].”
  - Wildcard listings can be used to represent a range of MAC addresses. For example, the first entry “00:11:22:33:*” in the Allowed listing that follows is a wildcard.

  **Note**

  Allowed MAC address formats are viewable in the Filtering Parameters configuration page. See **Table 16-5** for details.

  **EXAMPLE file listing:**

  ```
  [Allowed]
  00:11:22:33:*
  22:cd:34:ae:56:45
  02:23:23:34:*
  [Disallowed]
  00:10:*
  ae:bc:de:ea:45:23
  ```

- **Probing clients**

  Probing clients are clients that are associated to another controller but whose probing activity causes them to be seen by another controller and be counted as an element by the “probed” controller as well as its primary controller.

**Modifying Filtering Parameters**

To configure filtering parameters for a mobility services engine, follow these steps:

- **Step 1** Choose **Services > Mobility Services Engines**. The Mobility Services page appears.
- **Step 2** Click the name of the mobility services engine whose properties you want to edit. The General Properties page appears.
- **Step 3** From the Context-Aware Software menu, choose **Filtering Parameters** from the Administration subheading to display the configuration options.
- **Step 4** Modify the following filtering parameters as appropriate (see **Table 16-5**).
### Table 16-5 Filtering Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Filtering Params</td>
<td>Enter the duty cycle cutoff value for interferers so that only those interferers whose duty cycle meets the specified limits are tracked and counted against the Base location license. The default value for the Duty Cycle Cutoff Interferers is 0% and the configurable range is from 0% to 100%. To better utilize the location license, you can choose to specify a filter for interferers based on the duty cycle of the interferer.</td>
</tr>
<tr>
<td>Duty Cycle Cutoff Interferers</td>
<td></td>
</tr>
<tr>
<td>MAC Filtering Params</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 16  Prime Infrastructure Services

Step 5  Click Save to store the new settings in the mobility services engine database.

| Table 16-5  Filtering Parameters (continued) |
|------------|--------------------------------------------------|
| **Field**  | **Configuration Options**                        |
| Exclude Probing Clients | Select the check box to prevent location calculation of probing clients. |
| Enable Location MAC Filtering | **1.** Select the check box to enable MAC filtering of specific elements by their MAC address.  
 **2.** To import a file of MAC addresses (Upload a file for Location MAC Filtering field), browse for the filename and click Save to load the file. The imported list of MAC addresses auto-populates the Allowed List and Disallowed List based on their designation in the file.  
**Note** To view allowed MAC address formats, click the red question mark next to the Upload a file for Location MAC Filtering field.  
**3.** To add an individual MAC address, enter the MAC addresses (format is xx:xx:xx:xx:xx:xx) and click either Allow or Disallow. The address appears in the appropriate column.  
**Note** To move an address between the Allow and Disallow columns, highlight the MAC address entry and click the button under the appropriate column.  
**Note** To move multiple addresses, click the first MAC address and press Ctrl to highlight additional MAC addresses. Click Allow or Disallow based on its desired destination.  
**Note** If a MAC address is not listed in the Allow or Disallow column, by default, it appears in the Blocked MACs column. If you click the Unblock button, the MAC address automatically moves to the Allow column. You can move it to the Disallow column by selecting the Disallow button under the Allow column. |

*OL-32295-01*  16-47  
Cisco Prime Infrastructure Classic View Configuration Guide for Wireless Devices
Modifying History Parameters for Mobility Services

You can use the Prime Infrastructure to specify how long to store (archive) histories on client stations, rogue clients, and asset tags. These histories are received from those controllers that are associated with the mobility service.

You can also program the mobility service to periodically remove (prune) duplicate data from its historical files to reduce the amount of data stored on its hard drive.

To configure mobility service history settings, follow these steps:

---

**Step 1** Choose Services > Mobility Services.

**Step 2** Click the name of the mobility service whose properties you want to edit.

**Step 3** From the left sidebar menu, choose Context Aware Service > History Parameters.

**Step 4** Modify the following history parameters as appropriate (see Table 16-6).

---

**Table 16-6 History Parameters**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive for</td>
<td>Enter the number of days for the location appliance to retain a history of each enabled category. The default value is 30. Allowed values are from 1 to 99999.</td>
</tr>
<tr>
<td>Prune data starting at</td>
<td>Enter the number of hours and minutes at which the location appliance starts data pruning (between 0 and 23 hours, and between 1 and 59 minutes). Enter the interval, in minutes, after which data pruning starts again (between 0, which means never, and 99900000). The default start time is 23 hours and 50 minutes, and the default interval is 1440 minutes.</td>
</tr>
</tbody>
</table>
| Enable History Logging of Location Transitions for | To enable history logging of Location transitions, choose one or more of the following:  
  - Client Stations  
  - Wired Stations  
  - Asset Tags  
  - Rogue Clients  
  - Rogue Access Points  
  - Interferers |

---

**Note** Before the mobility service can collect asset tag data from controllers, you must enable the detection of RFID tags using the `config rfid status enable` CLI command.

---

**Step 5** Click Save to store your selections in the location appliance database.
Enabling Location Presence for Mobility Services

You can enable location presence on the mobility services engine to provide expanded Civic (city, state, postal code, country) and GEO (longitude, latitude) location information beyond the Cisco default setting (campus, building, floor, and X, Y coordinates). This information can then be requested by wireless and wired clients on a demand basis for use by location-based services and applications.

You can also import advanced location information such as the MAC address of a wired client and the wired switch slot and port to which the wired client is attached.

Location Presence can be configured when a new Campus, Building, Floor or Outdoor Area is being added or configured at a later date.

Once enabled, the mobility services engine is capable of providing any requesting Cisco CX v5 client its location.

---

**Note**

Before enabling this feature, synchronize the mobility services engine.

To enable and configure location presence on a mobility services engine, follow these steps:

**Step 1** Choose Services > Mobility Services > Device Name. Select the mobility services engine to which the campus or building or floor is assigned.

**Step 2** From the left sidebar menu, choose Context Aware Services > Administration > Presence Parameters.

**Step 3** Select the Service Type On Demand check box to enable location presence for Cisco CX clients v5.

**Step 4** Select one of the following Location Resolution options:

a. When Building is selected, the mobility services engine can provide any requesting client, its location by building.
   - For example, if a client requests its location and the client is located in Building A, the mobility services engine returns the client address as Building A.

b. When AP is selected, the mobility services engine can provide any requesting client, its location by its associated access point. The MAC address of the access point appears.
   - For example, if a client requests its location and the client is associated with an access point with a MAC address of 3034:00hh:0adg, the mobility services engine returns the client address of 3034:00hh:0adg.

c. When X,Y is selected, the mobility services engine can provide any requesting client, its location by its X and Y coordinates.
   - For example, if a client requests its location and the client is located at (50, 200) the mobility services engine returns the client address of 50, 200.

**Step 5** Select any or all of the location formats:

a. Select the Cisco check box to provide location by campus, building and floor and X and Y coordinates. Default setting.

b. Select the Civic check box to provide the name and address (street, city, state, postal code, country) of a campus, building, floor, or outdoor area.

---

**Note**

See the “Importing Civic Information for Mobility Services” section on page 16-51 for more information on importing a file with multiple Civic listings.
Step 6  By default, the Location Response Encoding check box is selected. It indicates the format of the information when received by the client. There is no need to change this setting.

Step 7  Select the Retransmission Rule check box to allow the receiving client to retransmit the received information to another party.

Step 8  Enter a Retention Expiration value in minutes. This determines how long the received information is stored by the client before it is overwritten. The default value is 24 hours (1440 minutes).

Step 9  Click Save.

### Importing Asset Information for Mobility Services

To import asset, chokepoint, and TDOA receiver information for the mobility services engine using the Prime Infrastructure, follow these steps:

**Step 1** Choose Services > Mobility Services.

**Step 2** Click the name of the mobility services engine for which you want to import information.

**Step 3** Choose Context Aware Service > Administration > Import Asset Information.

**Step 4** Enter the name of the text file or browse for the filename.

Specify information in the imported file in the following formats:

- tag format: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname
- station format: #station, 00:00:00:00:00:00, categoryname, groupname, assetname

**Step 5** When the import filename is located in the Browse text box, click Import.

### Exporting Asset Information for Mobility Services

To export asset, chokepoint, and TDOA receiver information from the mobility services engine to a file using the Prime Infrastructure, follow these steps:

**Step 1** Choose Services > Mobility Services.

**Step 2** Click the name of the mobility services engine from which you want the export information.

**Step 3** Choose Context Aware Service > Administration > Export Asset Information.

Information in the exported file is in the following formats:

- tag format: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname
- station format: #station, 00:00:00:00:00:00, categoryname, groupname, assetname

**Step 4** Click Export.

Click Open (display to screen), Save (to external PC or server), or Cancel (to cancel the request).
Importing Civic Information for Mobility Services

To import civic information for the mobility services engine using the Prime Infrastructure, follow these steps:

**Step 1** Choose **Services > Mobility Services**.

**Step 2** Click the name of the mobility services engine for which you want to import asset information.

**Step 3** From the left sidebar menu, choose **Context Aware Software**.

**Step 4** From the Administration left sidebar menu, choose **Import Civic Information**.

**Step 5** Enter the name of the text file or browse for the filename.

Information in the imported file should be one of the following formats:

Switch IP Address, Slot Number, Port Number, Extended Parent Civic Address, X, Y, Floor ID, Building ID, Network Design ID, ELIN:"ELIN", PIDF-Lo-Tag:"Civic Address Element Value"

**Note** Each entry must appear on a separate line.

**Step 6** Click **Import**.

Context-Aware Service Wired Parameters

This section describes the Context Aware Service > Wired drop-down list parameters.

Monitoring Wired Switches

You can review details on the wired switch (IP address, MAC address, serial number, software version, and ELIN), its port, its wired clients (count and status), and its civic information.

Wired switch data is downloaded to the mobility services engine through the Prime Infrastructure when the Ethernet switch and the mobility services engine are synchronized (Services > Synchronize Services > Switches). Communication between a location-capable switch and the mobility services engine is over NMSP. The Prime Infrastructure and the mobility services engine communicate over XML.

To view details on wired switches, follow these steps:

**Step 1** Choose **Services > Mobility Services**.

**Step 2** In the Mobility Services page, click the device name link of the appropriate wired location switch.

**Step 3** Choose **Context Aware Service > Wired > Wired Switches**. A summary of wired switches that are synchronized with the mobility services engine appears.
Step 4  See the “Wired Switch Details” section on page 16-52 for more information on the switch, its port, its wired clients (count and status), and its civic information click the IP address link.

Wired Switch Details

To view wired switch details, follow these steps:

Step 1  Choose Services > Mobility Services.

Step 2  In the Mobility Services page, click the device name link of the appropriate mobility services engine.

Step 3  Choose Context Aware Service > Wired > Wired Switches. A summary of wired switches that are synchronized with the mobility services engine appears.

Step 4  Click the IP address link for the applicable wired switch. The Wired Switch Details page appears.

The Wired Switch Details page has four tabs: Switch Information, Switch Ports, Civic, and Advanced.

Note  You can export civic information from the switch by choosing that option from the Select a command drop-down list. This option is available in all four dashlets of the Wired Switches page.

The Wired Switch Details tabs shows the following information:

- Switch Information—Displays a total count summary of wired clients connected to the switch along with the state of the client (connected, disconnected, and unknown).
  - Connected clients—Clients that are connected to the wired switch.
  - Disconnected clients—Clients that are disconnected from the wired switch.
  - Unknown clients—Clients are marked as unknown when the NMSP connection to the wired switch is lost.

Note  You can view detailed wired client information by clicking in one of the client count links (total clients, connected, disconnected, and unknown). See the “Monitoring Wired Clients” section on page 16-52 section for more information.

- Switch Ports—Displays a detailed list of the ports on the switch.

Note  You can change the listing order (ascending, descending) of port IP addresses, slot numbers, module number, port type, and port number by clicking in the respective column heading.

- Civic—Displays a detailed list of the civic information for the wired switch.
- Advanced—Displays a detailed list of the additional civic information for the wired switch.

Monitoring Wired Clients

You can view details on a wired client (MAC address, IP address, username, serial number, UDI, model no., software version, VLAN ID, and VLAN ID), port association, and its civic information.
Wired client data is downloaded to the mobility services engine through the Prime Infrastructure when the switch and the mobility services engine are synchronized (Services > Synchronize Services > Switches).

The Prime Infrastructure and the mobility services engine communicate over XML.

You can view the details of the wired client on either the wired switches page (Context Aware Service > Wired > Wired Switches) or wired clients page (Context Aware Service > Wired > Wired Clients).

- If you know the IP address, MAC address, VLAN ID, serial number, or username, you can use the search field on the wired clients page.
- If you want to examine wired clients as they relates to a specific switch, you can view that information on the wired switches page. See the “Monitoring Wired Switches” section on page 16-51 section for more information.

To view details on a wired client, follow these steps:

---

**Step 1** Choose **Services > Mobility Services.** The Mobility Services page appears.

**Step 2** Click the device name link of the appropriate wired location switch.

**Step 3** Choose **Context Aware Service > Wired > Wired Clients.**

In the Wired Clients summary page, clients are grouped by their switch.

A client status is noted as connected, disconnected, or unknown:

- Connected clients—Clients that are active and connected to a wired switch.
- Disconnected clients—Clients that are disconnected from the wired switch.
- Unknown clients—Clients that are marked as unknown when the NMSP connection to the wired switch is lost. See the “Viewing NMSP Connection Status for a Mobility Services Engine” section on page 16-33 for more information about NMSP connections.

If you know the MAC address of the wired client, you can click that link to reach the detail page of the client or use the search field. See the “Wired Client Details” section on page 16-53 for more information on wired client details.

- You can also search for a wired client by its IP address, username, or VLAN ID.

If you click the IP address of the switch, you are forwarded to the detail page of the switch. See the “Monitoring Wired Switches” section on page 16-51 for more information.

**Step 4** Click the MAC Address for the applicable client to view wired client details. See the “Wired Client Details” section on page 16-53 for more information on wired client details.

---

### Wired Client Details

To view wired client details, follow these steps:

---

**Step 1** Choose **Services > Mobility Services.**

**Step 2** In the Mobility Services page, click the device name link of the appropriate mobility services engine.

**Step 3** Choose **Context Aware Service > Wired > Wired Clients.** A summary of wired clients that are synchronized with the mobility services engine appears.

**Step 4** Click the MAC address link for the applicable wired client. The Wired Client Details page appears.
The Wired Client Details page has four tabs: Device Information, Port Association, Civic Address, and Advanced.

The Wired Switch Details tabs show the following information:

- **Device Information**—Display MAC and IP address, username, serial and model number, UDI, software version, VLAN ID, and VLAN name.
- **Port Association**—Displays the physical location of the switch port/slot/module on which the wired client terminates, the client status (connected, disconnected, unknown), and the switch IP address.
- **Civic Address**—Displays any civic address information.
- **Advanced**—Displays extended physical address details for the wired clients, if applicable.

Note: A client takes on the civic address and advanced location information that is configured for the port on which the client terminates. If no civic and advanced information is defined for the its port (port/slot/module) then no location data is displayed.

### Monitoring Interferers

The Monitor > Interferers page allows you to monitor interference devices detected by the CleanAir-enabled access points.

This section provides information on the interferers detected by the CleanAir-enabled access points. By default, the **Monitor > Interferers > AP Detected Interferers, page 16-54** page is displayed.

**Monitor > Interferers > AP Detected Interferers**

Choose **Monitor > Interferers** to view all the interfering devices detected by the CleanAir-enabled access points on your wireless network. This page enables you to view a summary of the interfering devices including the following default information:

- **Interferer ID**—A unique identifier for the interferer. Click this link to know more about the interferer.
- **Type**—Indicates the category of the interferer. Click to read more about the type of device. The dialog box appears displaying more details. The categories include the following:
  - **Bluetooth link**—A Bluetooth link (802.11b/g/n only)
  - **Microwave Oven**—A microwave oven (802.11b/g/n only)
  - **802.11 FH**—An 802.11 frequency-hopping device (802.11b/g/n only)
  - **Bluetooth Discovery**—A Bluetooth discovery (802.11b/g/n only)
  - **TDD Transmitter**—A time division duplex (TDD) transmitter
  - **Jammer**—A jamming device
  - **Continuous Transmitter**—A continuous transmitter
  - **DECT-like Phone**—A digital enhanced cordless communication (DECT)-compatible phone
  - **Video**—A video camera
  - **802.15.4**—An 802.15.4 device (802.11b/g/n only)
  - **WiFi Inverted**—A device using spectrally inverted Wi-Fi signals
- WiFi Invalid—A device using non-standard Wi-Fi channels
- SuperAG—An 802.11 SuperAG device
- Canopy—A Motorola Canopy device
- Radar—A radar device (802.11a/n only)
- XBox—A Microsoft Xbox (802.11b/g/n only)
- WiMAX Mobile—A WiMAX mobile device (802.11a/n only)
- WiMAX Fixed—A WiMAX fixed device (802.11a/n only)
- TDD Exalt
- Motorola Canopy

• Status—Indicates the status of the interfering device.
  - Active—Indicates that the interferer is currently being detected by the CleanAir-enabled access point.
  - Inactive—Indicates that the interferer is no longer being detected by the CleanAir-enabled access point or the CleanAir-enabled access point determined that the interferer is no longer reachable by the Prime Infrastructure.

• Severity—Displays the severity ranking of the interfering device.
• Affected Band—Displays the band in which this device is interfering.
• Affected Channels—Displays the affected channels.
• Duty Cycle (%)—The duty cycle of interfering device in percentage.
• Discovered—Displays the time at which it was discovered.
• Last Updated—The last time the interference was detected.
• Floor—The location where the interfering device is present.

---

**Note**

These devices appear only if the option to track Interferers is enabled in the Tracking Parameters page. This option is disabled by default. See the “Modifying Tracking Parameters for Mobility Services” section on page 16-41 for more information on tracking parameters.

---

**Monitor > Interferers > AP Detected Interferers > Interferer Details**

Choose Monitor > Interferers > Interferer ID to view this page. This page enables you to view the details of the interfering devices detected by the access points. This page provides the following details about the interfering device.

• Interferer Properties
  - Type—Displays the type of the interfering device detected by the AP.
  - Status—The status of the interfering device. Indicates the status of the interfering device.
    - Active—Indicates that the interferer is currently being detected by the CleanAir-enabled access point.
    - Inactive—Indicates that the interferer is no longer being detected by the CleanAir-enabled access point or the CleanAir-enabled access point saw the interferer no longer reachable by the Prime Infrastructure.
    - Severity—Displays the severity ranking of the interfering device.
- Duty Cycle (%)—The duty cycle of interfering device in percentage.
- Affected Band—Displays the band in which this device is interfering.
- Affected Channels—Displays the affected channels.
- Discovered—Displays the time at which it was discovered.
- Last Updated—The last time the interference was detected.

• Location
  - Floor—The location where this interfering device was detected.
  - Last Located At—The last time where the interfering device was located.
  - On MSE—The Mobility Server Engine on which this interference device was located.

• Clustering Information
  - Clustered By—Displays the following:
    - IP address of the controller if clustered by a controller.
    - IP address of the mobility services engine if clustered by a mobility services engine.
  - Detecting APs—Displays the details of the access point that has detected the interfering device. The details include: Access Point Name (Mac), Severity, and Duty Cycle(%).

Note
The detecting access point information is available only for active devices. And even for some active devices, this information might not be available. This is because these interferers are in the process of being marked inactive and in the next refresh of Monitor > Interferers page, these appear as inactive.

• Details—Displays a short description about the interfering type.

Select a command
The Select a command drop-down list provides access to the location history of the interfering device detected by the access point. See the “Monitor > Interferers > AP Detected Interferer Details > Interference Device ID > Location History” section on page 16-56 for more information.

Monitor > Interferers > AP Detected Interferer Details > Interference Device ID > Location History
Choose Monitor > Interferers > Interference Device ID, choose Location History from the Select a command drop-down list, and click Go to view this page.

• Interferer Information—Displays the basic information about the interfering device.
  - Data Collected At—The time stamp at which the data was collected.
  - Type—The type of the interfering device.
  - Severity—The severity index of the interfering device.
  - Duty Cycle—The duty cycle (in percentage) of the interfering device.
  - Affected Channels—A comma separated list of the channels affected.

• Interferer Location History—Displays the location history of the interfering devices.
  - Time Stamp
  - Floor

• Clustering Information
Clustered By

**Detecting APs**
- AP Name—The access point that detected the interfering device.
- Severity—The severity index of the interfering device.
- Duty Cycle(%)—The duty cycle (in percentage) of the interfering device.

**Location**
- Location Calculated At—Displays the time stamp at which this information was generated.
- Floor—Displays location information of the interfering device.

A graphical view of the location of the interfering device is displayed in a map. Click the **Enlarge** link to view an enlarged image.

### Monitor > Interferers > Edit View

The Edit View page allows you to add, remove, or reorder columns in the AP Detected Interferers Summary page. It also allows you to search for Interferers. By default, only those interferers that are in Active state and with a severity greater than or equal to 5 are displayed in the AP Detected Interferers page. See the “Monitor > Interferers > Edit View > Edit Search” section on page 16-57 for more information on editing search criteria.

To edit the columns in the AP Detected Interferers page, follow these steps:

**Step 1** Choose **Monitor > Interferers**. The AP Detected Interferers page appears showing details of the interferers detected by the CleanAir-enabled access points.

**Step 2** Click the **Edit View** link in the AP Detected Interferers page.

**Step 3** To add an additional column to the access points table, click to highlight the column heading in the left column. Click **Show** to move the heading to the right column. All items in the right column are displayed in the table.

**Step 4** To remove a column from the access points table, click to highlight the column heading in the right column. Click **Hide** to move the heading to the left column. All items in the left column are not displayed in the table.

**Step 5** Use the **Up/Down** buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click **Up** or **Down** to move it higher or lower in the current list.

**Step 6** Click **Reset** to restore the default view.

**Step 7** Click **Submit** to confirm the changes.

### Monitor > Interferers > Edit View > Edit Search

You can search for interferers based on certain criteria. By default only those interferers that are in Active state and with severity greater than or equal to 5 are displayed in the AP Detected Interferers page. Use the Edit Search option to customize the interferer search.

To edit the search criteria, follow these steps:

**Step 1** Choose **Monitor > Interferers**. The AP Detected Interferers page appears.
Step 2  Click **Edit Search** and select the appropriate criteria. This option allows you to specify the following search criteria:

- **Search Category**—For interferer search, the search category is Interferers.
- **Detected By**—From the drop-down list, choose **Access Points** or **Spectrum Experts**.
- **Search By**—From the drop-down list, choose any one of the following options:
  - All Interferers
  - Interferer ID
  - Interferer Type
  - Severity
  - Duty Cycle
  - Location
- **Severity greater than**—Enter the severity level in the text box.
- **Detected within the last**—From the drop-down list, choose any one of the following options:
  - 5 Minutes
  - 15 Minutes
  - 30 Minutes
  - 1 Hour
  - 3 Hours
  - 6 Hours
  - 12 Hours
  - 24 Hours
  - All History
- **Interferer status**—From the list, choose any of the following options:
  - Active
  - Inactive
  - All
- **Restrict By Radio Band/Channels**—Select this check box if you want to restrict certain radio frequencies or channels from the search. By default, this check box is unselected. On selection of this check box, a list appears with 2.4-GHz, 5-GHz and Individual Channel options. If you select Individual Channel, an Affected Channels text box appears. Specify the channel and select either the **Match All** or **Match Any** radio button.

Step 3  Select the number of items per page that you want to view in the search results.

Step 4  Select the **Save Search** check box if you want to save the search.

Step 5  After specifying the search criteria. Click **Go** to view the search results.
Context-Aware Service Advanced Parameters

Modifying Northbound Notifications

Northbound notifications define which tag notifications the mobility services engine sends to third-party applications.

To configure northbound parameters, follow these steps:

**Step 1** Choose Services > Mobility Services Engines.

**Step 2** Click the name of the mobility services engine you want to configure.

**Step 3** Choose Context Aware Service > Advanced > Notification Parameters to display the configuration options.

**Step 4** Select the Enable Northbound Notifications check box to enable the function.

**Step 5** Select the Notification Contents check box to send notifications to third-party applications (northbound).

**Step 6** Select one or more of the following Notification Contents check boxes:
- Chokepoints
- Telemetry
- Emergency
- Battery Level
- Vendor Data
- Location

**Step 7** Select the Notification Triggers check box.

**Step 8** Select one or more of the following Notification Triggers check boxes:
- Chokepoints
- Telemetry
- Emergency
- Battery Level
- Vendor Data
- Location Recalculation

**Step 9** Enter the IP address or hostname and port for the system that is to receive the northbound notifications.

**Step 10** Choose the transport type from the drop-down list.

**Step 11** Select the HTTPS check box if you want to use HTTPS protocol for secure access to the destination system.

**Step 12** To modify the notification parameter settings, enter the new value in the appropriate text box in the Advanced tab of this page. See Table 16-9.
Table 16-7  User-Configurable Conditional and Northbound Notifications Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Limit</td>
<td>Enter the rate, in milliseconds, at which the mobility services engine generates notifications. A value of 0 (default) means that the mobility services engine generates notifications as fast as possible (Northbound notifications only).</td>
</tr>
<tr>
<td>Queue Limit</td>
<td>Enter the event queue limit for sending notifications. The mobility services engine drops any event above this limit.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Enter the number of times to generate an event notification before the refresh time expires. This parameter can be used for asynchronous transport types which do not acknowledge the receipt of the notification and there is a possibility that the notification may be lost in transit. Default value is 1. <strong>Note</strong> The mobility services engine does not store events in its database.</td>
</tr>
<tr>
<td>Refresh Time</td>
<td>Enter the wait time in minutes that must pass before a notification is resent. For example, if a device is configured for In Coverage Area notification and it is constantly being detected within the Coverage Area. The notification is sent once every refresh time. Default value is 0 minutes.</td>
</tr>
<tr>
<td>Drop Oldest Entry on Queue Overflow</td>
<td>(Read-only). The number of event notifications dropped from the queue since startup.</td>
</tr>
<tr>
<td>Serialize Events per Mac address per Destination</td>
<td>Select this option if you want the successive events for the same MAC address to be sent to a single destination in a serial manner.</td>
</tr>
</tbody>
</table>

Step 13  Click Save.

Modifying Location Parameters for Mobility Services

You can use the Prime Infrastructure to specify whether the mobility service retains its calculation times and how soon the mobility service deletes its collected Received Signal Strength Indicator (RSSI) measurement times. You can also apply varying smoothing rates to manage location movement of an element.

To configure location parameters, follow these steps:

Step 1  Choose Services > Mobility Services.
Step 2  Click the name of the mobility service whose properties you want to edit.
Step 3  From the left sidebar menu, choose Context Aware Service > Location Parameters.
Step 4  Modify the location parameters as appropriate (see Table 16-8).
Table 16-8  Location Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
</tr>
<tr>
<td>Enable Calculation Time</td>
<td>Select the check box to enable the calculation of the time required to compute location.</td>
</tr>
<tr>
<td><strong>Caution</strong></td>
<td>Enable only under Cisco TAC personnel guidance because enabling this field slows down overall location calculations.</td>
</tr>
<tr>
<td>Enable OW Location</td>
<td>Select the check box to enable Outer Wall (OW) calculation as part of location calculation.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The OW Location parameter is ignored by the location server.</td>
</tr>
<tr>
<td>Relative discard RSSI time</td>
<td>Enter the number of minutes since the most recent RSSI sample after which RSSI measurement should be considered stale and discarded. Default value is 3. Allowed values range from 0 to 99999. A value of less than 3 is not recommended.</td>
</tr>
<tr>
<td>Absolute discard RSSI time</td>
<td>Enter the number of minutes after which RSSI measurement should be considered stale and discarded, regardless of the most recent sample. Default value is 60. Allowed values range from 0 to 99999. A value of less than 60 is not recommended.</td>
</tr>
<tr>
<td>RSSI Cutoff</td>
<td>Enter the RSSI cutoff value, in decibels (dBs) with respect to one (1) mW (dBm), preceding which the mobility service always use the access point measurement. Default value is -75.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When 3 or more measurements are available preceding the RSSI cutoff value, the mobility service discards any weaker values and use the 3 (or more) strongest measurements for calculation; however, when only weak measurements following the RSSI cutoff value are available, those values are used for calculation.</td>
</tr>
<tr>
<td><strong>Caution</strong></td>
<td>Modify only under Cisco TAC personnel guidance. Modifying this value can reduce the accuracy of location calculation.</td>
</tr>
</tbody>
</table>
Table 16-8 Location Parameters (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Location Filtering</td>
<td>If enabled, the location filter is applied only for client location calculation. Enabling location filter allows previous location estimates to be used in estimating current location. This reduces location jitter for stationary clients and improve tracking for mobile clients.</td>
</tr>
<tr>
<td>Chokepoint Usage</td>
<td>Select the check box to enable the usage of chokepoint proximity to determine location. Applies to Cisco-compatible Tags capable of reporting chokepoint proximity.</td>
</tr>
<tr>
<td>Use Chokepoints for Interfloor conflicts</td>
<td>Allows the use of chokepoints to determine the correct floor during Interfloor conflicts. Choose <strong>Never</strong>, <strong>Always</strong>, or <strong>Floor Ambiguity</strong>.</td>
</tr>
<tr>
<td>Chokepoint Out of Range Timeout</td>
<td>After a Cisco-compatible Tag leaves a chokepoint proximity range, this is the timeout (in seconds) after which RSSI information is used again to determine location.</td>
</tr>
<tr>
<td>Absent Data Cleanup Interval</td>
<td>Enter the interval period (in minutes) for removing inactive elements from the database.</td>
</tr>
<tr>
<td>Use Default Heatmaps for Non Cisco Antennas</td>
<td>Select this check box to enable the usage of default heatmaps for non-Cisco antennas during the Location Calculation. This option is disabled by default.</td>
</tr>
</tbody>
</table>

**Movement Detection**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual RSSI change threshold</td>
<td>This field specifies the Individual RSSI movement recalculation trigger threshold. Enter a threshold value between 0-127 dBm. Do not modify without Cisco TAC guidance.</td>
</tr>
<tr>
<td>Aggregated RSSI change threshold</td>
<td>This field specifies the Aggregated RSSI movement recalculation trigger threshold. Enter a threshold value between 0-127 dBm. It should not be modified without Cisco TAC guidance.</td>
</tr>
<tr>
<td>Many new RSSI change percentage threshold</td>
<td>This field specifies Many new RSSI movement recalculation trigger threshold in percentage. It should not be modified without Cisco TAC guidance.</td>
</tr>
<tr>
<td>Many missing RSSI percentage threshold</td>
<td>This field specifies Many missing RSSI movement recalculation trigger threshold in percentage. It should not be modified without Cisco TAC guidance.</td>
</tr>
</tbody>
</table>
Step 5  Click **Save** to store your selections in the Prime Infrastructure and mobility service databases.

---

**Modifying Notification Parameters for Mobility Services**

You can use the Prime Infrastructure to configure mobility services engine event notification parameters that define such items as how often the notifications are generated or resent by the mobility services engine.

*Note*

Modify notification parameters only if you expect the mobility services engine to send a large number of notifications or if notifications are not being received.

You can also enable forwarding of northbound notifications for tags to be sent to third-party applications. The format of northbound notifications sent by the mobility services engine is available on the Cisco developers support portal at the following URL:


To configure notification parameters, follow these steps:

**Step 1**  Choose **Services > Mobility Services**.

**Step 2**  Click the name of the mobility services engine you want to configure.

**Step 3**  From the Context Aware Software left sidebar menu, choose **Notification Parameters** from the Advanced sub-heading to display the configuration options.

**Step 4**  Select the **Enable Northbound Notifications** check box to enable the function.

**Step 5**  Select the **Notification Contents** check box to send notifications to third-party applications (northbound).

**Step 6**  Select one or more of the following Notification content options:

- Chokepoints
- Telemetry
- Emergency
- Battery Level
- Vendor Data
- Location

**Step 7**  Select the **Notification Triggers** check box.

**Step 8**  Select one or more of the following Notification trigger options:

- Chokepoints
- Telemetry
- Emergency
- Battery Level
- Vendor Data
- Location Recalculation

**Step 9**  Enter the IP address and port for the system that is to receive the northbound notifications.
Step 10  Choose the transport type from the drop-down list.

Step 11  Select HTTPS if you want to use HTTPS protocol for secure access to the destination system.

Step 12  To modify the notification parameter settings, enter the new value in the appropriate text box in the Advanced tab of the page. Table 16-9 describes each parameter.

### Table 16-9  User-Configured Conditional and Northbound Notifications Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Limit</td>
<td>Enter the rate in milliseconds at which the mobility services engine generates notifications. A value of 0 (default) means that the mobility services engine generates notifications as fast as possible (Northbound notifications only).</td>
</tr>
<tr>
<td>Queue Limit</td>
<td>Enter the event queue limit for sending notifications. The mobility services engine drops any event preceding this limit.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Enter the number of times to generate an event notification before the refresh time expires. This field can be used for asynchronous transport types which do not acknowledge the receipt of the notification and there is a possibility that the notification might be lost in transit. Default value is 1.</td>
</tr>
<tr>
<td>Note</td>
<td>The mobility services engine does not store events in its database.</td>
</tr>
<tr>
<td>Refresh Time</td>
<td>Enter the wait time, in minutes, that must pass before a notification is resent. For example if a device is configured for In Coverage Area notification and it is constantly being detected within the Coverage Area. The notification is sent once every refresh time.</td>
</tr>
<tr>
<td>Drop Oldest Entry on Queue Overflow</td>
<td>(Read-only). The number of event notifications dropped from the queue since startup.</td>
</tr>
<tr>
<td>Serialize Events per Mac address per Destination</td>
<td>Select this option if you want the successive events for the same MAC address to be sent to a single destination in a serial manner.</td>
</tr>
</tbody>
</table>

Step 13  Click Save.

### Viewing Partner Engine Status

To access the Partner Engine Status page, choose Services > Mobility Services > MSE Name > Context Aware Service > Partner Engine > Status.

If tag licenses are available, then Aeroscout Tag Engine is enabled. Otherwise, Cisco Partner Engine is enabled by default.

If only the evaluation license is available, then the Cisco Partner Engine is enabled by default. The Partner Engine status page shows status based on whether it is a Aeroscout Tag Engine or Cisco Tag Engine.

**Note** The Aeroscout engine fails to start on MSE if the Prime Infrastructure map names have special characters such as ‘&’.

Table 16-10 describes the fields in the Tag Engine Status page for the Aeroscout Tag Engine.
If you selected Cisco Tag Engine for Context Aware Service, the Tag Engine Status page displays the following information. Table 16-11 describes the fields in the Tag Engine Status page for the Cisco Tag Engine.

### Table 16-10  Partner Engine Status Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner Location Engine Name</td>
<td>The Partner engine name, which is <strong>aeroscout</strong>.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the Aeroscout Tag Engine.</td>
</tr>
<tr>
<td>Description</td>
<td>Description for the Tag Engine.</td>
</tr>
<tr>
<td>Registered</td>
<td>Appears as True when the Aeroscout Tag Engine has established communication with the mobility services engine.</td>
</tr>
<tr>
<td>Active</td>
<td>Appears as True when the Aeroscout Tag Engine is up and running.</td>
</tr>
<tr>
<td>License Information</td>
<td>The maximum tags that are available with the Aeroscout Tag Engine.</td>
</tr>
</tbody>
</table>

If you selected Cisco Tag Engine for Context Aware Service, the Tag Engine Status page displays the following information. Table 16-11 describes the fields in the Tag Engine Status page for the Cisco Tag Engine.

### Table 16-11  Tag Engine Status Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag Location Engine Name</td>
<td>The Tag location engine name, which is <strong>Cisco</strong>.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the Cisco Tag Engine.</td>
</tr>
<tr>
<td>Description</td>
<td>Description for the Cisco Tag Engine.</td>
</tr>
<tr>
<td>Active</td>
<td>Displays as True when the Cisco Tag Engine is up and running.</td>
</tr>
<tr>
<td>License Information</td>
<td>The maximum tags that are available with the Cisco Tag Engine.</td>
</tr>
</tbody>
</table>

### Viewing Notification Information for Mobility Services

The Services > Context Aware Notifications page provides the ability to define events.

### Viewing the Notifications Summary for Mobility Services

To view the Notification Summary, choose Services > Context Aware Notifications > Notification Summary.

The mobility service sends event notifications and does not store them (fire and forget). However, if the Prime Infrastructure is a destination of notification events, it stores the notifications it receives and groups them into the following seven categories:

- Absence (Missing)—Generated when the mobility service cannot see the asset in the WLAN for the specified time.
Mobility Services

• Location Change Events—Generated when client stations, asset tags, rogue clients, and rogue access points move from their previous location.

• Chokepoint Notifications—Generated when a tag is seen (stimulated) by a chokepoint. This information is only reported and displayed for CCX v.1-compliant tags.

• Battery Level—Generated when a tracked asset tag hits the designated battery level.

• In/Out Area—Generated when an asset is moved inside or outside a designated area.

**Note** You define a containment area (campus, building, or floor) in the Maps section of the Prime Infrastructure (Monitor > Maps). You can define a coverage area using the Map Editor.

• Movement from Marker—Generated when an asset is moved beyond a specified distance from a designated marker you define on a map.

• Emergency—Generated for a CCX v.1 compliant asset tag when the panic button of the tag is triggered or the tag becomes detached, tampered with, goes inactive or reports an unknown state. This information is only reported and displayed for CCX v.1 compliant tags.

The summary details include the following:

• All Notifications

• Client Stations

• Asset Tags

• Rogue Clients

• Rogue Access Points

**Note** To view details for each of the notifications, click the number under the Last Hour, Last 24 Hours, or Total Active column to open the details page for the applicable notification.

**Notifications Cleared**

A mobility service sends event notifications when it clears an event condition in one of the following scenarios:

• Missing (Absence)—Elements reappear.

• In/Out Area (Containment)—Elements move back in or out of the containment area.

• Distance—Elements move back within the specified distance from a marker.

• Location Changes—Clear state is not applicable to this condition.

• Battery Level—Tags are detected again operating with Normal battery level.

• Emergency

• Chokepoint

**Note** In the Prime Infrastructure, the Notifications Summary page reflects whether notifications for cleared event conditions have been received.
Viewing and Managing Notifications for Mobility Services

To view the Notification Definitions, choose Services > Context Aware Notifications > Notification Definition. You can add event groups and event definitions to a group in this page. Every groups help you organize your event notifications. An event definition must belong to a particular group.

For more information on adding event groups and event definitions, see “Adding Event Groups” section on page 16-69 and “Adding Event Definitions” section on page 16-72.

The Notification Definition page displays the following parameters only after adding event groups and event definitions:

Table 16-13 lists and describes the fields in the Notification Definition page.

<table>
<thead>
<tr>
<th><strong>Table 16-12</strong></th>
<th><strong>Notification Definition Page</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Group Name</td>
<td>Name of the group to which the event definition is added.</td>
</tr>
<tr>
<td>Event Definitions</td>
<td>Existing event definitions for the event group.</td>
</tr>
<tr>
<td>Created On</td>
<td>Date on which the event groups are created.</td>
</tr>
</tbody>
</table>

Viewing Notification Statistics

You can view the notification statistics for a specific mobility services engine. To view the Notification Statistics for a specific mobility services engine, choose Services > Mobility Services > MSE-name > Context Aware Service > Notification Statistics.

where MSE-name is the name of a mobility services engine.

Table 16-13 lists and describes the fields in the Notification statistics page.

<table>
<thead>
<tr>
<th><strong>Table 16-13</strong></th>
<th><strong>Notification Statistics Fields</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Summary</td>
<td></td>
</tr>
<tr>
<td>Destinations</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>Total count of the destinations.</td>
</tr>
<tr>
<td>Unreachable</td>
<td>Count of unreachable destinations.</td>
</tr>
<tr>
<td>Notification Statistics Summary</td>
<td>Status of the track definition. Track notification status can be either Enabled or Disabled.</td>
</tr>
<tr>
<td>Track Definition Status</td>
<td>Track definition can be either Northbound or CAS event notification.</td>
</tr>
<tr>
<td>Track Definition</td>
<td></td>
</tr>
<tr>
<td>Destination IP Address</td>
<td>The destination IP address to which the notifications are sent.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>The destination port to which the notifications are sent.</td>
</tr>
<tr>
<td>Destination Type</td>
<td>The type of the destination. For example, SOAP_XML.</td>
</tr>
</tbody>
</table>
Mobile Concierge Service Parameters

Viewing the Configured Service Advertisements

To view the configured service advertisements, follow these steps:

Step 1  Choose Services > Mobility Services Engine.

Step 2  Click Device Name to view its properties.
        The General Properties page appears.

Step 3  Choose Mobile Concierge Service > Advertisements from the left sidebar menu.
        The following information appears in the Mobile Concierge Service page:
        •  Icon—Displays an icon associated with the service provider.
        •  Provide Name—Displays the service providers name.
        •  Venue Name—Displays the venue name.
        •  Advertisements
          –  Friendly Name—Friendly name that is displayed in the handset.
          –  Advertisement Type—Type of advertisement that is displayed in the handset.

Viewing Mobile Concierge Service Statistics

To view Mobile Concierge service statistics, follow these steps:

Step 1  Choose Services > Mobility Services Engine.

Step 2  Click Device Name to view its properties.
        The General Properties page appears.

Step 3  Choose Mobile Concierge service > Statistics from the left sidebar menu.
The following information appears in the Mobile Concierge Service page:

- Top 5 Active Mobile MAC addresses—Displays information of the most active mobiles in a given venue.
- Top 5 Service URIs—Displays information of the usage of the services across a given venue or provider.

### About Event Groups

To manage events more efficiently, you can use the Prime Infrastructure to create event groups. Event groups help you organize your event definitions.

**Note**

For more information about synchronizing the Cisco wireless LAN controllers and the Prime Infrastructure with mobility services engines see the “Synchronizing Services” section on page 16-12.

### Adding Event Groups

To add an event group, follow these steps:

**Step 1** Choose Services > Context Aware Notifications.

**Step 2** Choose Notification Definitions from the left sidebar menu.

**Step 3** From the Select a command drop-down list, choose Add Event Group.

**Step 4** Click Go.

**Step 5** Enter the name of the group in the Group Name text box.

**Step 6** Click Save.

The new event group appears in the Event Settings page.

### Deleting Event Groups

To delete an event group, follow these steps:

**Step 1** Choose Services > Context Aware Notifications.

**Step 2** Choose Notification Definitions from the left sidebar menu.

**Step 3** Select the check box of the event group you want to delete.

**Step 4** From the Select a command drop-down list, choose Delete Event Group(s).

**Step 5** Click Go.

**Step 6** Click OK to confirm the deletion.

**Step 7** Click Save.
Working with Event Definitions

An event definition contains information about the condition that caused the event, the assets to which the event applies, and the event notification destinations. This section describes how to add, delete, and test event definitions.

Note
The Prime Infrastructure enables you to add definitions on a per-group basis. Any new event definition must belong to a particular group.

To add an event definition, follow these steps:

Step 1 Choose Services > Context Aware Notifications.
Step 2 From the left sidebar menu, choose Notification Definitions.
Step 3 Click the name of the group to which you want to add the event. An event definition summary page appears for the selected event group.
Step 4 From the Select a command drop-down list, choose Add Event Definition.
Step 5 Click Go.
Step 6 Enter the name of the event definition in the Event Definition Name text box.

Note The event definition name must be unique within the event group.

Step 7 Click Save.
Step 8 On the General tab, manage the following parameters:
- Admin Status—Enable event generation by selecting the Enabled check box (disabled by default).
- Priority—Set the event priority by choosing a number from the drop-down list. Zero is highest.

Note An event definition with higher priority is serviced before event definitions with lower priority.

- Activate—To continuously report events, choose the All the Time check box. To indicate specific days and times for activation, unselect the All the Time check box and choose the applicable days and From/Until times. Click Save.

Step 9 On the Conditions tab, add one or more conditions. For each condition, specify the rules for triggering event notification. To add a condition, follow these steps:

a. Click Add to open the Add/Edit Condition page.

b. Choose a condition type from the Condition Type drop-down list and configure its associated Trigger If parameters see (Table 16-14).
Table 16-14  Condition Type/Trigger If Parameters

<table>
<thead>
<tr>
<th>Condition Type</th>
<th>Trigger If</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing</td>
<td>Missing for Time (mins)—Enter the number of minutes after which a missing asset event is generated. For example, if you enter 10 in this text box, the mobility services engine generates a missing asset event if the mobility services engine has not located the asset for more than 10 minutes.</td>
</tr>
<tr>
<td>In/Out</td>
<td>Inside of or Outside of—Click Select Area and choose the area parameters from the Select page. Click Select. The area to monitor can be an entire campus, building within a campus, a floor in a building, or a coverage area (you can define a coverage area using the map editor).</td>
</tr>
<tr>
<td>Distance</td>
<td>In the distance of $x$ (feet) from Marker text box—Enter the distance in feet that triggers an event notification if the monitored asset moves beyond the specified distance from a designated marker. Click Select Marker and choose the marker parameters in the Select page. Click Select.</td>
</tr>
<tr>
<td>Battery Level</td>
<td>Battery Level Is—Low, Medium, Normal. Select the appropriate battery level that triggers an event.</td>
</tr>
<tr>
<td>Location Change</td>
<td>An event is triggered if the location of the asset changes.</td>
</tr>
<tr>
<td>Emergency</td>
<td>Select Any, Panic Button, Tampered, or Detached check box.</td>
</tr>
<tr>
<td>Chokepoint</td>
<td>In the range of Chokepoints—Click Select Chokepoint check box and choose the chokepoint parameters in the Select page. Click Select.</td>
</tr>
</tbody>
</table>

c. In the Apply To drop-down list, choose the type of asset (Any, Clients, Tags, Rogue APs, Rogue Clients or Interferers) for which an event is generated if the trigger condition is met.

Note  Emergency and chokepoint events are only applicable to tags (CCXv.1 compliant).

d. From the Match By drop-down list, choose the matching criteria (MAC Address, Asset Name, Asset Group, or Asset Category), the operator (Equals or Like), and enter the relevant text for the selected Match By element.

e. Click Add.

Step 10  On the Destination and Transport tab, follow these steps to add one or more destinations to receive event notifications and configure the transport settings:

a. Click Add to open the Add/Edit Destination and Transport page.

b. To add one or more new destinations, click Add New, enter the applicable IP address, and click OK.
Note

The recipient system must have an event listener running to process notifications. By default, when you create an event definition, the Prime Infrastructure adds its IP address as the destination.

c. To select a destination to receive notifications, click to highlight one or more IP addresses in the box on the right and click Select to add the IP address(es) to the box on the left.

d. From the Message Format field drop-down list, select XML or Plain Text.

Note

If you select Prime Infrastructure as the destination, you must select XML format.

e. Choose one of the following transport types from the Transport Type drop-down list:

- SOAP—Simple Object Access Protocol. Use SOAP to send notifications over HTTP/HTTPS and to be processed by web services on the destination.
  Specify whether to send notifications over HTTPS by selecting its corresponding check box. Enter the destination port number in the Port Number text box.

- Mail—Use this option to send notifications through e-mail.
  Choose the protocol for sending the e-mail from the Mail Type drop-down list. Enter the following: username and password (if Authentication is enabled), name of the sender, prefix to add to the subject line, e-mail address of recipient, and a port number if necessary.

- SNMP—Simple Network Management Protocol. Use this option to send notifications to SNMP-capable devices.
  If you have selected SNMP version v2c then you are prompted to enter the SNMP community string in the SNMP Community text box and the applicable port number in the Port Number text box.
  If you have selected SNMP version v3 then you are prompted to enter the username, security name, choose the authentication type from the drop-down list, enter the authentication password, choose the privacy type from the drop-down list and enter the privacy password.

- SysLog—Specifies the system log on the destination system as the recipient of event notifications.
  Enter the notification priority in the Priority text box, the name of the facility, and the port number on the destination system.

f. Click Add.

Step 11

Verify that the new event definition is listed for the event group (Context Aware Service > Notifications > Event > Settings > Event Group Name).

Adding Event Definitions

An event definition contains information about the condition that caused the event, the assets to which the event applies, and the event notification destination.

The Prime Infrastructure enables you to add definitions for each group. An event definition must belong to a group. See the Cisco Content-Aware Software Configuration Guide for more information on deleting or testing event definitions.
To add an event definition, follow these steps:

**Step 1** Choose Services > Context Aware Notifications.

**Step 2** Choose Notification Definitions from the left sidebar menu.

**Step 3** Click the name of the group to which you want to add to the event. An event definition summary page appears for the selected event group.

**Step 4** From the Select a command drop-down list, choose Add Event Definition, and click Go.

**Step 5** On the Conditions tab, add one or more conditions. For each condition you add, specify the rules for triggering event notifications.

---

**Tip**

For example, to keep track of heart monitors in a hospital, you can add rules to generate event notifications when a heart monitor is missing for one hour, a heart monitor moves off its assigned floor, or a heart monitor enters a specific coverage area within a floor.

---

To add a condition, follow these steps:

a. Click Add to add a condition that triggers this event.

b. In the Add/Edit Condition dialog box, follow these steps:

1. Choose a condition type from the Condition Type drop-down list.

   If you chose Missing from the Condition Type drop-down list, enter the number of minutes after which a missing asset event is generated. For example, if you enter 10 in this text box, the mobility service engine generates a missing asset event if the mobility service engine has not found the asset for more than 10 minutes. Proceed to Step c.

   If you chose In/Out from the Condition Type drop-down list, choose Inside of or Outside of, then select Select Area to select the area to monitor for assets going into it or out of it. In the Select dialog box, choose the area to monitor, then click Select. The area to monitor can be an entire campus, building within a campus, a floor in a building, or a coverage area (you can define a coverage area using the map editor). For example, to monitor part of a floor in a building, choose a campus from the Campus drop-down list, choose a building from the Building drop-down list, and choose the floor to monitor from the Floor Area drop-down list. Then click Select. Proceed to Step c.

   If you chose Distance from the Condition Type drop-down list, enter the distance in feet that triggers an event notification if the monitored asset moves beyond the specified distance from a designated marker, then click Select Marker. In the Select dialog box, choose the campus, building, floor, and marker from the corresponding drop-down list, and click Select. For example, if you add a marker to a floor plan and set the distance in the Trigger. If the text box is set to 60 feet, an event notification is generated if the monitored asset moves more than 60 feet away from the marker. Proceed to Step c.

   If you chose Battery Level from the Condition Type drop-down list, select the check box next to the battery level (low, medium, normal) that triggers an event. Proceed to Step c.

   If you chose Location Change from the Condition Type drop-down list, proceed to Step c.

---

**Note**

You can create markers and coverage areas using the Map Editor. When you create marker names, make sure they are unique across the entire system.

If you chose Battery Level from the Condition Type drop-down list, select the check box next to the battery level (low, medium, normal) that triggers an event. Proceed to Step c.

If you chose Location Change from the Condition Type drop-down list, proceed to Step c.
If you chose Emergency from the Condition Type drop-down list, click the button next to the emergency (any, panic button, tampered, detached) that triggers an event. Proceed to Step c.

If you chose Chokepoint from the Condition Type drop-down list, proceed to Step c. There is only one trigger condition, and it is displayed by default. No configuration is required.

c. From the Apply To drop-down list, choose the type of asset (Any, Clients, Tags, Rogue APs, Rogue Clients, or Interferers) for which an event is generated if the trigger condition is met.

<table>
<thead>
<tr>
<th>Note</th>
<th>If you choose the any option from the Apply to drop-down list, the battery condition is applied to all tags, clients, and rogue access points and rogue clients.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Note</th>
<th>Emergency and chokepoint events apply only to Cisco-compatible extension tags Version 1 (or later).</th>
</tr>
</thead>
</table>

d. From the Match By drop-down list, choose the matching criteria (MAC Address, Asset Name, Asset Group, or Asset Category), the operator (Equals or Like) from the drop-down list, and enter the relevant text for the selected Match By element.

Some examples of asset matching criteria that you can specify:

- If you choose MAC Address from the Match By drop-down list, choose Equals from the Operator drop-down list, and enter a MAC address (for example, 12:12:12:12:12:12), the event condition applies to the element whose MAC address is 12:12:12:12:12:12 (exact match).

- If you choose MAC Address from the Match By drop-down list, choose Like from the Operator drop-down list, and enter 12:12, the event condition applies to elements whose MAC address starts with 12:12.

e. Click Add to add the condition you have just defined.

<table>
<thead>
<tr>
<th>Note</th>
<th>If you are defining a chokepoint, you must select the chokepoint after you add the condition.</th>
</tr>
</thead>
</table>

To select a chokepoint, do the following:

1. Click Select Chokepoint. An entry page appears.

2. Choose Campus, Building, and Floor from the appropriate drop-down lists.

3. Choose a Chokepoint from the menu that appears.

You are returned to the Add/Edit Condition page, and the location path (Campus > Building > Floor) for the chokepoint auto-populates the text area next to the Select Checkpoint button.

**Step 6**

On the Destination and Transport tab, follow these steps to add one or more destinations to receive event notifications and to configure the transport settings:

a. To add a new destination, click Add. The Add/Edit Destination configuration page appears.

b. Click Add New.

c. Enter the IP address of the system that receives event notifications, and click OK.

The recipient system must have an event listener running to process notifications. By default, when you create an event definition, the Prime Infrastructure adds its IP address as the destination.

d. To select a destination to send event notifications to, highlight one or more IP addresses in the box on the right, and click Select to add the IP addresses to the box on the left.
e. Choose XML or Plain Text to specify the message format.

f. Choose one of the following transport types from the Transport Type drop-down list:
   - SOAP—Specifies Simple Object Access Protocol, a simple XML protocol, as the transport type for sending event notifications. Use SOAP to send notifications over HTTP/HTTPS that are processed by web services on the destination.
     If you choose SOAP, specify whether to send notifications over HTTPS by selecting its corresponding check box. If you do not, HTTP is used. Also, enter the destination port number in the Port Number text box.
   - Mail—Use this option to send notifications through e-mail.
     If you choose Mail, you need to choose the protocol for sending the e-mail from the Mail Type drop-down list. You also need to enter the following information: username and password (if Authentication is enabled), name of the sender, prefix to add to the subject line, e-mail address of recipient, and a port number if necessary.
   - SNMP—Use Simple Network Management Protocol, a very common technology for network monitoring used to send notifications to SNMP-capable devices.
     If you choose SNMP, enter the SNMP community string in the SNMP Community text box and the port number to send notifications to in the Port Number text box.
   - SysLog—Specifies the system log on the destination system as the recipient of event notifications.
     If you choose SysLog, enter the notification priority in the Priority text box, the name of the facility in the Facility text box, and the port number of the destination system in the Port Number text box.


g. To enable HTTPS, select the Enable check box next to it.

h. Click Save.

Step 7

On the General tab, follow these steps:

a. Select the Enabled check box for Admin Status to enable event generation (disabled by default).

b. Set the event priority by choosing a number from the Priority drop-down list. Zero is the highest priority.

Note

An event notification with high priority is serviced before event definitions with lower priority.

c. To select how often the event notifications are sent:
   1. Select the All the Time check box to continuously report events. Proceed to Step g.
   2. Unselect the All the Time check box to select the day and time of the week that you want event notifications sent. Days of the week and time fields appear for the selection. Proceed to Step d.

d. Select the check box next to each day you want the event notifications sent.

e. Select the time for starting the event notification by selecting the appropriate hour, minute, and AM/PM options from the Apply From heading.

f. Select the time for ending the event notification by selecting the appropriate hour, minute, and AM/PM options from the Apply Until heading.

g. Click Save.
Step 8 Verify that the new event notification is listed for the event group (Mobility > Notifications > Settings > Event Group Name).

Deleting an Event Definition

To delete one or more event definitions from the Prime Infrastructure, follow these steps:

- **Step 1** Choose Services > Context Aware Notifications.
- **Step 2** From the left sidebar menu, choose Settings.
- **Step 3** Click the name of the group from which you want to delete the event definitions.
- **Step 4** Select the event definition that you want to delete by selecting its corresponding check box.
- **Step 5** From the Select a command drop-down list, choose Delete Event Definition(s).
- **Step 6** Click Go.
- **Step 7** Click OK to confirm that you want to delete the selected event definitions.

Client Support on MSE

You can use the Prime Infrastructure advanced search feature to narrow the client list based on specific categories and filters. You can also filter the current list using the Show drop-down list.

- **Searching a Wireless Client from the Prime Infrastructure on the MSE by IPv6 Address**, page 16-76
- **Viewing the Clients Detected by the MSE**, page 16-78

Searching a Wireless Client from the Prime Infrastructure on the MSE by IPv6 Address

- **Note** Only wireless clients have IPv6 addresses in this release.

To search for a MSE located clients using the Prime Infrastructure Advanced search feature, follow these steps:

- **Step 1** Click Advanced Search.
- **Step 2** In the New Search dialog, choose Clients as the search category from the Search Category drop-down list.
- **Step 3** From the Media Type drop-down list, choose Wireless Clients.
- **Note** The Wireless Type drop-down list appears only when you choose Wireless Clients as the media type.
- **Step 4** From the Wireless Type drop-down list, choose any of the following types: All, Lightweight or Autonomous Clients.
Step 5 From the Search By drop-down list, choose **IP Address**.

>Note Searching a client by IP address can contain either full or partial IP address. Each client can have up to 16 IPv6 addresses and 4 IPv4 addresses.

Step 6 From the Clients Detected By drop-down list, choose clients detected by as MSE.

This displays clients located by Context-Aware Service in the MSE by directly communicating with the controllers.

Step 7 From the Last detected within drop-down list, choose the time within which the client was detected.

Step 8 Enter the client IP address in the Client IP Address text box. You can enter wither a partial or full IPv6 address.

>Note If you are searching for the client from the Prime Infrastructure on the MSE by IPv4 address, enter the IPv4 address in the Client IP address text box.

Step 9 From the Client States drop-down list, choose the client states. The possible values for wireless clients are **All States, Idle, Authenticated, Associated, Probing**, or **Excused**. The possible values for wired clients are **All States, Authenticated**, and **Associated**.

Step 10 From the Posture Status drop-down list, choose the posture status to know if the devices are clean or not. The possible values are **All, unknown, Passed, and Failed**.

Step 11 Select the **CCX Compatible** check box to search for clients that are compatible with Cisco Client Extensions. The possible values are **All Versions, V1, V2, V3, V4, V5, and V6**.

Step 12 Select the **E2E Compatible** check box to search for clients that are end-to-end compatible. The possible values are **All Versions, V1, and V2**.

Step 13 Select the **NAC State** check box to search for clients identified by a certain Network Admission Control (NAC) state. The possible values are **Quarantine, Access, Invalid**, and **Not Applicable**.

Step 14 Select the **Include Disassociated** check box to include clients that are no longer on the network but for which the Prime Infrastructure has historical records.

Step 15 From the Items per page drop-down list, choose the number of records to be displayed in the search results page.

Step 16 Select the **Save Search** check box to save the selected search option.

Step 17 Click **Go**.

The Clients and Users page appears with all the clients detected by the MSE.
Viewing the Clients Detected by the MSE

Note You can see the clients in probing state on 2.4 GHz on Cisco WLC but in probing state only on "a" radio (in the Monitor > Clients and Users > Client detected by MSE page). None of the clients shows up in probing state on "b/g" radio. This is because when clients are in the probing state, Prime Infrastructure does not get details on the protocol and by default these are shown to be on 5 GHz channel. Once they are associated, the INFO messages are received from the controller which contain details on the protocol and the channel. But when they are probing with Measurement messages, Prime Infrastructure does not have this information and defaults it to 5 GHz.

To view all the clients detected by the MSE, follow these steps:

Step 1 Choose Monitor > Clients and Users to view both wired and wireless clients information.

The Client and Users page appears.

The Clients and Users table displays a few column by default. If you want to display the additional columns that are available, click Columns, and then click Columns. The available columns appear. Select the columns that you want to show in the Clients and Users table. When you click anywhere in a row, the row is selected and the client details are shown.

Step 2 Filter the current list to choose all the clients that are detected by the MSE by choosing Clients detected by MSE from the Show drop-down list.

All the clients detected by MSE including wired and wireless appear.

The following different parameters are available in the Clients Detected by MSE table:

- MAC Address—Client MAC address.
- IP Address—Client IP address.

The IP Address that appears in the IP Address column is determined by a predefined priority order. The first IP address available in the following order appears in the IP address text box:

- IPv4 address

Note Only wireless clients have IPv6 addresses in this release. Each client can have up to 16 IPv6 addresses and 4 IPv4 addresses.

- IPv6 global unique address. If there are multiple addresses of this type, most recent IPv6 address that the client received is shown, because a user could have two Global IPv6 addresses but one might have been from an older Router Advertisement that is being aged out.
- IPv6 local unique address. If there are multiple IPv6 local unique addresses, then the most recent address appears.
- IPv6 link local address. For an IPv6 client it always have at least a link local address.

The following are the different IPv6 address types:

- Link-local Unicast—The link-local addresses are designed to be used for addressing on a single link for purposes such as auto-address configuration, neighbor discovery, or when no routers are present.
- Site-local Unicast—The site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix.
– Aggregatable Global Unicast—The aggregatable global unicast address uniquely identifies the client in global network and equivalent to public IPv4 address. A client can have multiple aggregatable global unicast addresses.

– IP Type—The IP address type can be IPv4 and IPv6.
  – Global Unique
  – Unique Local
  – Link Local

– User Name—Username based on 802.1x authentication. Unknown is displayed for client connected without a username.

– Type—Indicates the client type.
  – ✅ indicates a lightweight client
  – ✅ indicates a wired client
  – ✅ indicates an autonomous client

– Vendor—Device vendor derived from OUI.

– Device Name—Network authentication device name. For example, WLC and switch.

– Location—Map location of the connected device.

– VLAN—Indicates the access VLAN ID for this client.

– Status—Current client status.
  – Idle—Normal operation; no rejection of client association requests.
  – Auth Pending—Completing a AAA transaction.
  – Authenticated—802.11 authenticated complete.
  – Associated—802.11 association complete. This is also used by wired clients to represent that a client is currently connected to the network.
  – Disassociated—802.11 disassociation complete. This is also used by wired clients to represent that a client is currently not on the network.
  – To Be Deleted—The client is deleted after disassociation.
  – Excluded—Automatically disabled by the system due to perceived security threat.

– Interface—Controller interface (wireless) or switch interface (wired) that the client is connected to.

– Protocol
  – 802.11—wireless
  – 802.3—wired

– Association Time—Last association start time (for wireless client). For a wired client, this is the time when a client is connected to a switch port. This is blank for a client which is associated but has problems being on the network.

– CCX—Lightweight wireless only.

**Step 3** Select the radio button next to MAC Address in the Client and User page to view the associated client information. The following different client parameters appear.

– Client Attributes
– Client IPv6 Addresses
– Client Statistics
Client Statistics shows the statistics information after the client details are shown.

- Client Association History
- Client Event Information
- Client Location Information
- Wired Location History
- Client CCX Information

Client Attributes

When you select a client from the Clients and Users list, the following client details are displayed. Clients are identified using the MAC address.

These following details are displayed:
- General—Lists the following information:
  - User Name
  - IP Address
  - MAC address
  - Vendor
  - Endpoint Type
  - Client Type
  - Media Type
  - Mobility Role
  - Hostname
  - E2E
  - Power Save
  - CCX
  - Foundation Service
  - Management Service
  - Voice Service
  - Location Service

Note

Click the icon next to the username to access the correlated users of a user.

- Session—Lists the following client session information:
  - Controller Name
  - AP Name
  - AP IP Address
  - AP Type
  - AP Base Radio MAC
- Anchor Address
- 802.11 State
- Association ID
- Port
- Interface
- SSID
- Profile Name
- Protocol
- VLAN ID
- AP Mode

- Security (wireless and Identity wired clients only)—Lists the following security information:
  - Security Policy Type
  - EAP Type
  - On Network
  - 802.11 Authentication
  - Encryption Cipher
  - SNMP NAC State
  - RADIUS NAC State
  - AAA Override ACL Name
  - AAA Override ACL Applied Status
  - Redirect URL
  - ACL Name
  - ACL Applied Status
  - FlexConnect Local Authentication
  - Policy Manager State
  - Authentication ISE
  - Authorization Profile Name
  - Posture Status
  - TrustSec Security Group
  - Windows AD Domain

**Note**  The identity clients are the clients whose authentication type is 802.1x, MAC Auth Bypass or Web Auth. For non-identity clients, the authentication type is N/A.

**Note**  The data that appears under the client attributes differs based on identity and non-identity clients. For identity clients, you can see the security information such as Authentication status, Audit Session ID, and so on.
• Statistics (wireless only)
• Traffic—Shows the client traffic information.
• For wireless clients, client traffic information comes from controller. For wired clients, the client traffic information comes from ISE, and you must enable accounting information and other necessary functions on switches.

Statistics
The Statistics group box contains the following information for the selected client:
• Client AP Association History
• Client RSSI History (dBm)—History of RSSI (Received Signal Strength Indicator) as detected by the access point with which the client is associated.
• Client SNR History—History of SNR (signal-to-noise Ratio of the client RF session) as detected by the access point with which the client is associated.
• Bytes Sent and Received (Kbps)—Bytes sent and received with the associated access point.
• Packets Sent and Received (per sec)—Packets sent and received with the associated access point.
• Client Data rate

Note Hover your mouse cursor over points on the graph for additional statistical information.

Client IPv6 Addresses
The IPv6 address group box contains the following information for the selected client:
• IP Address—Shows the clients IPv6 address.
• Scope—Contains 3 types scope. They are Global Unique, Local Unique, and Link Local.
• Address Type—Shows the address type.
• Discovery Time—Time when the IP was discovered.

Association History
The association history dashlet shows information regarding the last ten association times for the selected client. This information helps in troubleshooting the client.

The Association History dashlet contains the following information:
• Association Time
• Duration
• User Name
• IP Address
• IP Address Type
• AP Name
• Controller Name
• SSID

Events
The Event group box of the Client Details page display all events for this client including the event type as well as the date and time of the event:
- Event Type
- Event Time
- Description

**Map**
Click **View Location History** to view location history details of wired and wireless clients. You can view the location details for wired and wireless clients.
The following location history information is displayed for a wired or wireless client:
- Timestamp
- State
- Port Type
- Slot
- Module
- Port
- User Name
- IP Address
- Switch IP
- Server Name
- Map Location Civic Location

**Upgrading from 5.0 to 6.0 or 7.0**

**Caution**
The number of supported clients, tags, and access points (wIPS) is reset to 100 clients, 100 tags, and 20 access points when you upgrade to Release 6.0 or later. All tracking beyond these limits is lost. These limits correspond to the 120-day evaluation licenses that are standard.

**Caution**
When upgrading the mobility services engine from 6.0 to 7.0, if any limits have been set on wireless clients or rogues, they are reset because of the wired client limit change in 7.0.

**Caution**
You must back up the mobility services engine database before upgrading from Release 5.1 or 6.0 to 7.0 to preserve client, tag, and access point configurations. You can restore the database after the software upgrade.

**Note**
Release 5.1 did not support licenses. You must order, register, and install licenses to track client and tag locations (CA) or access points (wIPS) beyond the limits of the 120-day evaluation licenses.

To upgrade to Release 7.0, follow these steps:
Step 1
Register the Product Authorization Key (PAK).

Note: You receive a PAK when you order a license. If you have lost your PAK, you can use your sales order or the UDI number of the mobility services engine to register.

- Client and wIPS licenses are registered at: www.cisco.com/go/license
- Tag licenses are registered at aeroscout website.

Step 2
Back up the mobility services engine database:

a. Choose Services > Mobility Services.
b. Click the name of the mobility services engine on which you want to back up.
c. Choose System > Maintenance.
d. Click Backup.
e. Enter the name of the backup file.
f. Click Submit to backup the historical data to the hard drive of the server running the Prime Infrastructure.

Step 3
Download Release 7.0:

a. Choose Services > Mobility Services.
b. Click the name of the mobility services engine to which you want to download the software.
c. Choose System > Maintenance > Download Software from the left sidebar menu.
d. To download software, do one of the following:
   - To download software listed in the Prime Infrastructure directory, select the Select from uploaded images to transfer into the Server radio button. Choose a binary image from the drop-down list. The Prime Infrastructure downloads the binary image to the FTP server directory you specified during the Prime Infrastructure installation.
   - To use downloaded software available locally or over the network, select the Browse a new software image to transfer into the Server radio button and click Choose File. Locate the file and click Open.
e. Click Download to send the software to the /opt/installers directory on the mobility services engine.

Step 4
Install Release 7.0 using the MSE CLI:

a. To overwrite existing software, enter:

```
/etc/init.d/msed stop
cd /opt/installers
./mse software file name
```
b. To perform a fresh install, enter:

```
/etc/init.d/msed stop
cd /opt/mes/uninstall
./uninstall (enter this once in directory)
```
(Enter no when prompted to keep old database)
cd /opt/installers
./<mse software file name>

Step 5  Restore the mobility services engine database (For Step 4 b.):
   a. Choose Services > Mobility Services.
   b. Click the name of the mobility services engine on which you upgraded the software.
   c. Choose Maintenance > Restore from left sidebar menu.
   d. Choose the filename to restore from the drop-down list. Click Submit.

Step 6  Install the licenses.
See the Chapter 2 of the Context-Aware Services Configuration Guide Release 7.0 at
ml for more information.

Viewing the MSE Alarm Details

In the Monitor > Alarms page, click an MSE item under Failure Source column to access the alarms
details for a particular MSE.

Alternatively, you can choose Services > Mobility Services Engines> MSE Name > System > Status >
Prime Infrastructure Alarms page and click a particular MSE item under Failure Source column to
access the alarms details for a particular MSE.

Table 16-15 describes the various fields in the Alarm Detail page for an MSE.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure Source</td>
<td>The MSE that generated the alarm.</td>
</tr>
<tr>
<td>Owner</td>
<td>Name of person to which this alarm is assigned, or blank.</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>Displays whether or not the alarm is acknowledged by the user.</td>
</tr>
<tr>
<td>Category</td>
<td>The category of the alarm. The Alarm category is Mobility Services for MSEs.</td>
</tr>
<tr>
<td>Created</td>
<td>Month, day, year, hour, minute, second, AM or PM alarm created.</td>
</tr>
<tr>
<td>Modified</td>
<td>Month, day, year, hour, minute, second, AM or PM alarm last modified.</td>
</tr>
<tr>
<td>Generated By</td>
<td>This field displays MSE.</td>
</tr>
<tr>
<td>Severity</td>
<td>Level of security: Critical, Major, Minor, Warning, Clear, Info, Color coded.</td>
</tr>
</tbody>
</table>
The General information might vary depending on the type of alarm. For example, some alarm details might include location and switch port tracing information.

- Related Alarm List—Displays all the alarms related to a particular attack.
- Rogue Client Details—Displays information about the rogue clients.
- Annotations—Enter any new notes in this text box and click **Add** to update the alarm. Notes appear in the “Annotations” display page.
- Messages—Displays information about the alarm.
- Device Details—
- Switch Port Tracing
- Location Notification
- Map Location
- Device Events
- Related History
- Audit Report—Click to view config audit alarm details. This report is only available for Config Audit alarms.
  
  Configuration audit alarms are generated when audit discrepancies are enforced on config groups.

  **Note**

  If enforcement fails, a critical alarm is generated on the config group. If enforcement succeeds, a minor alarm is generated on the config group.

  The alarms have links to the audit report where you can view a list of discrepancies for each controller.

- Event History—Opens the MSE Alarm Events page to view events for this alarm. When there are multiple alarm pages, the page numbers appear at the top of the page with a scroll arrow on each side. Use these scroll arrows to view additional alarms.

### Select a command

The Select a command drop-down list provides access to the following functions:

- Assign to me—Assign the selected alarm(s) to the current user.
- Unassign—Unassign the selected alarm(s).
- Delete—Delete the selected alarm(s).
- Clear—Clear the selected alarm(s). Indicates that the alarm is no longer detected by any access point.

  **Note**

  Once the severity is Clear, the alarm is deleted from the Prime Infrastructure after 30 days.

- Acknowledge—You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality.
- Unacknowledge—You can choose to unacknowledge an already acknowledged alarm.
- Email Notification—Takes you to the All Alarms > Email Notification page to view and configure e-mail notifications.
- Event History—Takes you to the Monitor > Events page to view events for this alarm.

**MSE License Overview**

The MSE packages together multiple product features related to network topology, design such as NMSP, Network Repository along with related Service Engines, and application processes, such as the following:

- Context-Aware Service
- Wireless Intrusion Prevention System (wIPS)
- Location Analytics Service
- Mobile Concierge Service
- Mobile Billboard service

To enable smooth management of MSE and its services, various licenses are offered.

**Note** You must have a Cisco Prime Infrastructure license to use MSE and its associated services.

**MSE License Structure Matrix**

Table 16-16 lists the breakdown of the licenses between the High-end, Low-end and Evaluation licenses for MSE, Location services, SCM, wIPS and MIR.

**Table 16-16 MSE License Structure Matrix**

<table>
<thead>
<tr>
<th></th>
<th>High End</th>
<th>Low End</th>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MSE Platform</strong></td>
<td>High-end appliance and infrastructure platform such as the Cisco 3350 and 3355 mobility services engines.</td>
<td>Low-end appliance and infrastructure platform such as Cisco 3310 mobility services engine.</td>
<td>—</td>
</tr>
<tr>
<td><strong>Context Aware Service</strong></td>
<td>25,000 Tags 2000 Tags 25,000 Elements</td>
<td>2000 Tags 2000 Elements</td>
<td>Validity 120 days, 100 Tags and 100 Elements.</td>
</tr>
<tr>
<td><strong>wIPS</strong></td>
<td>3000 access points</td>
<td>2000 access points</td>
<td>Validity 120 days, 20 access points.</td>
</tr>
</tbody>
</table>

**Sample an MSE License File**

The following is a sample MSE license file:

```
FEATURE MSE cisco 1.0 permanent uncounted \ 
   VENDOR_STRING=UDI=udi,COUNT=1 \ 
   HOST ID=ANY \ 
   NOTICE="<LicFileID>MSELicense</LicFileID><LicLineID>0</LicLineID> \
```
This sample file has 5 license entries. The first word of the first line of any license entry tells you what type of license it is. It can either be a Feature or Increment license. A feature license is a static lone item to license. There can be multiple services engines running in MSE. An Increment license is an additive license. In the MSE, the individual service engines are treated as increment licenses.

The second word of the first line defines the specific component to be licensed. For example, MSE, LOCATION_TAG. The third word depicts the vendor of the license, for example Cisco. The fourth word denotes the version of the license, example 1.0. The fifth word denotes the expiration date, this can be permanent for licenses that never expire or a date in the format dd-mm-yyyy. The last word defines whether this license is counted.

Revoking and Reusing an MSE License

You can revoke an MSE appliance license from one system and reuse it on another system. When you revoke a license, the license file is deleted from the system. If you want to reuse the license on another system, then the license needs to be rehosted.

If you want to reuse a license with an upgrade SKU on another system, then you must have the corresponding base license SKU installed in the system to which you want to reuse the upgrade SKU. You cannot reuse the upgrade license SKU in a system if the corresponding base license SKU is deleted from it.

When you revoke a license, MSE restarts the individual service engines to reflect the changes to the licenses. Then the service engines receives the updated capacity from MSE during startup.

Deploying the MSE Virtual Appliance

MSE is also offered as a virtual appliance. The MSE virtual appliance software is distributed as an Open Virtualization Archive (OVA) file.

Note See the VMware cSphere 4.0 documentation for more information about setting up your VMware environment.

Note See the Cisco Prime Infrastructure Getting Started Guide, Release 1.0 for more information on the physical appliance.

When the MSE is located on the physical appliance, the license installation process is based on Cisco UDI (Unique Device Identifier). Choose Administration > License Center on the Prime Infrastructure UI to add the license. When the MSE is located on the virtual appliance, the license installation is done using a VUDI (Virtual Unique Device Identifier) instead of UDI.

Note MSE is available as a virtual appliance for this release and later. Virtual appliance must be activated first before installing any other service licenses.
For a virtual appliance, you must have an activation license. Without an activation license, if the MSE starts in evaluation mode even if the licenses are present on the host, it rejects the permanent license if the activation license is not installed. If the virtual appliance is added to the Prime Infrastructure, the Prime Infrastructure, Prime Infrastructure does not allow the MSE to be synchronized unless the activation license is added to the MSE.

Note

Virtual licenses are not allowed on physical appliances.

You can add and delete a virtual appliance license either using the Services > Mobility Services Engine > Add Mobility Services Engine page when you are installing the MSE for the first time or you can use Administration > License Center page to add or delete a license.

See the “Adding a License File to the MSE Using the License Center” section on page 16-89 and the “Deleting an MSE License File” section on page 16-10 for more information on adding a license and deleting a license using the Mobility Services Engine wizard.

Adding a License File to the MSE Using the License Center

To add a license, follow these steps:

1. Install the MSE virtual appliance.
2. Add the MSE to the Prime Infrastructure using the “Adding a Mobility Services Engine” section on page 16-6.
3. Choose Administration > License Center on the Prime Infrastructure UI to access the License Center page.
4. Choose Files > MSE Files from the left sidebar menu.
5. Click Add to add a license.
   The Add A License File menu appears.
6. Select the MSE and browse to the activation license file.
7. Click Submit.
   Once you submit, the license is activated and license information appears in the License Center page.

Viewing the MSE License Information using License Center

The license center allows you to manage the Prime Infrastructure, Wireless LAN Controllers, and MSE licenses. To view the license information, follow these steps:

1. Choose Administration > License Center to access the License Center page.
2. Choose Summary > MSE from the left sidebar menu, to view the summary page.
   The MSE Summary page displays the following information. See Table 16-17.
Chapter 16  Prime Infrastructure Services

Removing a License File Using the License Center

To remove a license, follow these steps:

Step 1  Install the MSE virtual appliance.
Step 2  Add MSE to Prime Infrastructure using the wizard.
Step 3  Choose Administration > License Center on the Prime Infrastructure UI to access the License Center page.
Step 4  Choose Files > MSE Files from the left sidebar menu.
Step 5  Choose an MSE license file that you want to remove by selecting the radio button, and click Remove.
Step 6  Click OK to confirm the deletion.

Table 16-17  General Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSE Name</td>
<td>Provides a link to the MSE license file list page.</td>
</tr>
<tr>
<td>Service</td>
<td>Type of service using: CAS or wIPS.</td>
</tr>
<tr>
<td>Platform Limit by AP</td>
<td>Platform limit.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the type of MSE.</td>
</tr>
<tr>
<td>Installed Limit by AP</td>
<td>Displays the total number of client elements licensed across MSEs.</td>
</tr>
<tr>
<td>License Type</td>
<td>The three different types of licenses. They are permanent, evaluation, and extension.</td>
</tr>
<tr>
<td>Count by elements</td>
<td>The number of CAS or wIPS elements currently licensed across MSEs.</td>
</tr>
<tr>
<td>Unlicensed Count</td>
<td>Displays the number of client elements that are not licensed.</td>
</tr>
<tr>
<td>%Used</td>
<td>The percentage of CAS or wIPS elements licensed across MSEs.</td>
</tr>
</tbody>
</table>

Auto Switch Port Tracing and Auto Containment of Rogue APs

Currently, the Prime Infrastructure provides rogue access point detection by retrieving information from the controller. The rogue access point table is populated with any detected BSSID addresses from any frames that are not present in the neighbor list. At the end of a specified interval, the contents of the rogue table are sent to the controller in a CAPWAP Rogue AP Report message. With this method, the Prime Infrastructure simply gathers the information received from controllers; but from the software Release 5.1, you can incorporate switch port tracing of wired rogue access point switch ports.
The auto SPT and containment is introduced in Release 7.3. The auto SPT is more preferable for a large wireless network. The auto SPT starts automatically when a rogue AP is reported to the Prime Infrastructure. The auto SPT complements to manual SPT feature by providing a quicker scan based on the wired location association of the rogue AP. The Prime Infrastructure UI allows you to configure the criteria for auto SPT and auto containment so that you can run a trace and contain the detected rogue access points on the wire.

**Note**

Switches are not required to be managed in Prime Infrastructure for manual SPT whereas, for auto SPT to work switches should be managed.

When the multiple controllers report that a rogue AP should be auto contained, the Prime Infrastructure finds the controller that reports the strongest RSSI sends the containment request to the controller.

**Configuring Auto Switch Port Tracing Criteria on the Prime Infrastructure**

To configure auto switch port tracing settings on the Prime Infrastructure, follow these steps:

**Step 1** Choose *Administration > System Settings*.

**Step 2** From the left sidebar menu, choose *Rogue AP Settings*. The Rogue AP Settings page appears.

**Step 3** Select the *Enable Auto Switch Port Tracing* check box to allow the Prime Infrastructure to automatically trace the switch port to which the rogue access point is connected. You can configure the following parameters:

- **Repeat Search After**—Enter the number of minutes after which you want the Prime Infrastructure to automatically repeat the search for Rogue APs. By default, the Prime Infrastructure repeats the search for Rogue APs every 120 minutes.
- **Allow Trace For Found On Wire Rogue AP**—Select the check box to enable auto SPT to trace wired rogue APs.
- **Critical**—Select the check box to set the alarm severity to critical.
- **Major**—Select the check box to set the alarm severity to major.
- **Minor**—Select the check box to set the alarm severity to minor.

**Note**

The maximum hop count value configured in *Administration > System Settings > Switch Port Trace* is not applicable for Auto SPT.

**Step 4** Click *Ok*.

**Configuring Auto Containing Settings on the Prime Infrastructure**

To configure auto containment settings on the Prime Infrastructure, follow these steps:

**Step 1** Choose *Administration > Settings*.

**Step 2** From the left sidebar menu, choose *Rogue AP Settings*. The Rogue AP Settings page appears.
Step 3  Select the **Enable Auto Containment** check box to allow the Prime Infrastructure to trigger auto containment when a rogue AP is received by the Prime Infrastructure. You can configure the following parameters:

- Exclude Rogue APs Found On Wire By Switch Port Tracing—Select the check box to automatically exclude those APs that are detected on the wired network through auto SPT.
- Critical—Select the check box to set the alarm severity to critical.
- Major—Select the check box to set the alarm severity to major.
- Containment Level—Select the check box enable the auto containment level. This indicates the containment level of the rogue APs.
  - 1 AP Containment—Target the rogue access point for containment by one access point. (Lowest containment level). When you select this, one access point in the vicinity of the rogue unit sends deauthenticate and disassociate messages to the client devices that are associated to the rogue unit.
  - 2 AP Containment—Target the rogue access point for containment by two Cisco lightweight access points. Two access points in the vicinity of the rogue unit send deauthenticate and disassociate messages to the rogues clients.
  - 3AP Containment—Target the rogue access point for containment by three Cisco lightweight access points.
  - 4AP Containment—Target the rogue access point for containment by four Cisco lightweight access points. (Highest containment level).

**Note**  The higher the threat of the rogue access point, the higher the containment required.

**Caution**  Attempting to contain a rogue access point might lead to legal consequences. When you select any of the AP Containment commands and click **Go**, a message “Containing a Rogue AP may have legal consequences. Do you want to continue?” appears. Click **OK** if you are sure or click **Cancel** if you do not wish to contain any access points.

Step 4  Click OK.

**Location Assisted Client Troubleshooting from the Context Aware Dashboard**

You can use the Context Aware dashboard on the Prime Infrastructure home page to troubleshoot a client. You can specify a MAC address or Username or IP address as the search criteria, and click **Troubleshoot**.

**Note**  Username, IP address, and partial MAC address-based troubleshooting is supported only on MSEs Version 7.0.200.0 and later.
The Troubleshoot Client page appears.
You can view the Context Aware History report on the Context Aware History tab.
You can filter this report based on MSE Name. You can further filter the report based on Timezone, State or All. The states can be either associated or dissociated.
If you select timezone, then you can choose any of the following:
- Date and Time
Or
- Any one of these values from the drop-down list:
  - Last 1 Hour
  - Last 6 Hours
  - Last 1 Day
  - Last 2 Days
  - Last 3 Days
  - Last 4 Days
  - Last 5 Days
  - Last 6 Days
  - Last 7 Days
  - Last 2 Weeks
  - Last 4 Weeks

Alternately, you can use the Generate Report link to generate a Client Location History report. You can also opt to export to CSV or PDF format or e-mail the report using the icons available in the report page.

### MSE Analytics Reports

You can generate many MSE Analytics reports using the Report Launch Pad.

### Monitoring Maps

Maps provide a summary view of all your managed system on campuses, buildings, outdoor areas, and floors. See the “About Maps” section on page 6-1 for more information on maps.

### Disabling Mobility Services Engine Admin View

Prime Infrastructure enables its own Mobility Services (MSE) Administrator view by default. Users who need to use the legacy MSE admin view instead can do so using the User Preferences page.

**Step 1** Choose Administration > User Preferences.
You can also access the User Preferences page by clicking the arrow next to your login name in the Global Toolbar at the top right.

**Step 2** To disable the Prime Infrastructure MSE Admin view, unselect the Use MSE Admin View check box.
Mobile Concierge Service

The Mobile Concierge service allows the venue owners and service providers to monitor their WLAN. The Mobile Concierge solution delivers a unique in-store experience to customers who are using smartphones.

Mobile Concierge service uses wireless smart phones that have been configured with a set of policies for establishing network connectivity. Mobile Concierge service facilitates smartphones to discover network-based services available. Once you are connected to the stores Wi-Fi network, you can join the stores wireless guest network and can access variety of different services including electronic coupons, promotional offers, customer loyalty data, main product suggestions, allow you to organize shopping lists, receive unique digital signature based on shopping preferences.

Licensing for Mobile Concierge

The Mobile Concierge service can be enabled only if you have a valid advanced location license (Base location license, Mobile Concierge, and Analytics license). The evaluation license is valid for 120 days and the permanent license is based on the MSE platform and the number of service advertisements supported.

Defining a Venue

To define a venue, follow these steps:

**Step 1** Choose Services > Application Visibility & Control > Mobile Concierge.

**Step 2** Choose Mobile Concierge Services > Venues from the left sidebar menu.

The Venues page appears.

**Step 3** From the Select a command drop-down list, choose Define New Venue and click Go.

The Venue Wizard page appears.

**Step 4** Enter the venue name in the Venue Name text box and click Next.

**Step 5** In the Floor/Outdoor Association group box, you can configure the following:

- From the Area Type drop-down list, choose the area type where you want to display the service advertisement. The possible values are Floor Area and Outdoor Area.

**Note** The Building, Floor Area, and Coverage Area drop-down lists are displayed only if you select Floor Area as the area type.

- From the Campus drop-down list, choose the campus name where you want to display the service advertisements.
- From the Building drop-down list, choose the building name where you want the advertisements to appear.
From the Floor drop-down list, choose the floor type.
From the Coverage Area drop-down list, choose the coverage area within the floor.
From the Outdoor Area drop-down list, choose the outdoor area where you want to display the service advertisements. This field is displayed only if you select Outdoor Area as the Area Type.

Step 6 Click Next. The Audio group box appears.
Step 7 From the Audio group box, click Choose File to browse and select the audio file to play the audio notification.
Step 8 Click Next. The Icons group box appears.
Step 9 From the Icons group box, click Choose File to browse and select the icon that you want to display on the clients handset.
Step 10 Click Next. The Venue Apps group box appears.
Step 11 From the Venue Apps group box, choose the venue app on which you want to display the service advertisement from the Web App drop-down list.
Step 12 Click Next. The Additional Venue Information group box appears.
Step 13 From the Additional Information group box, you can provide any additional information that the venue would like to provide to the mobile application. You can configure the following:
  • Enter the location detail in the Location Detail text box. This provides details such as store address, zip code, or street address of the venue.
  • Enter the GPS latitude and longitude of the venue in the Latitude and Longitude text box. This helps the applications to identify the venue accurately.
  • Enter any other additional information that the venue would like to provide to the mobile application in the Additional Information text box.
Step 14 Click Save. This information is applied to the MSE and the synchronization happens automatically.

Deleting the Venue

To delete a venue, follow these steps:

Step 1 Choose Services > Mobile Concierge.
The Venues page appears.
Step 2 Select the check box of the venue that you want to delete.
Step 3 From the Select a command drop-down list, choose Delete Venue, and click Go.
Step 4 Click OK to confirm the deletion.

Defining a Provider with Policies

Step 1 Choose Service > Mobile Concierge.
Step 2 Choose Mobile Concierge Services > Providers from the left sidebar menu.
Step 3  From the Select a command drop-down list, choose Define New Provider and click Go. The Provider Wizard page appears.

Step 4  Enter the providers venue name in the Provider Name text box.

Step 5  Click Next. The Icons group box appears.

Step 6  From the Icons group box, click Choose File to browse and select the icon that you want to display on the clients handset.

Step 7  Click Next. The Local Services group box appears.

Step 8  From the Local Services group box, do the following:
- Click the blue inverted triangle icon location at the left side of the Local Service # name to expand the Local Service and configure the following:
  - Choose the service type from the Service Type drop-down list. The possible options are: Directory Info, Sign Up, Discount Coupon, Network Help, and Other.
  - Enter the display name in the Display Name text box.
  - Enter the description in the Description text box.
  - Choose the service URIs from the drop-down list.
  - Recommended Apps - recommended application for the venue.

Step 9  Click Save.

Deleting the Provider

To delete a venue, follow these steps:

Step 1  Choose Services > Mobile Concierge. The Venues page appears.

Step 2  Choose Mobile Concierge Services > Providers from the left sidebar menu. The Providers page appears.

Step 3  Select the check box of the provider that you want to delete.

Step 4  From the Select a command drop-down list, choose Delete Provider, and click Go. Click OK to confirm the deletion.

Defining New Policies

To define policies, follow these steps:

Step 1  Choose Services > Mobile Concierge.

Step 2  Choose Mobile Concierge Services > Policies from the left sidebar menu.
The Policies page appears.

Step 3 From the Select a command drop-down list, choose Define New Policy and click Go.

The Policy Wizard page appears.

Step 4 Choose the venue on which you want the policy to be applied from the Venue drop-down list.

Step 5 Click Next. The Provider group box appears.

Step 6 Choose the provider from the Provider drop-down list.

Step 7 Click Next. The SSID group box appears.

Step 8 From the SSID drop-down list, choose the SSIDs on which you want to broadcast the service advertisements and click OK. You can choose multiple SSIDs.

Step 9 Click Next. The Display Rule group box appears.

Step 10 From the Display Rule group box, you can do the following:

- Select the Display Rule radio button. You can select either Everywhere or Near selected APs radio button. By default, Display everywhere is selected.

If you select Display everywhere, then it searches for all the Mobile Concierge-supported controllers that provide these SSIDs and assigns these controllers to the MSE.

If you select Display near selected APs, then you can configure the following parameters:

- AP—Select those APs on which you want the advertisements to broadcast.
- Radio—Select the radio frequency on which you want the advertisements to be broadcasted. The service advertisement is displayed when the mobile device is near the radio band that you have selected. The possible values are 2.4 GHz or 5 GHz.
- min RSSI—Enter a value for RSSI at which you want the service advertisements to be displayed on the user interface.

Step 11 Click Finish.

---

Deleting New Policies

To delete a venue, follow these steps:

Step 1 Choose Services > Mobile Concierge.

The Venues page appears.

Step 2 Choose Mobile Concierge Services > Policies from the left sidebar menu.

The Policies page appears.

Step 3 Select the check box of the policy that you want to delete.

Step 4 From the Select a command drop-down list, choose Delete Policy, and click Go.

Click OK to confirm the deletion.
Adding Service Advertisements to the Floor Map

To add service advertisements to a coverage area within the floor map, follow these steps:

**Step 1** Choose Monitor > Site Maps.
The Site Maps page appears.

**Step 2** Choose the appropriate floor location link from the list.
A map appears showing the placement of all installed access points, client, and tags and their relative signal strength.

**Step 3** Click the Services icon on the floor map page.
The Venue dialog box to associate service advertisement to that particular venue appears.

**Step 4** Click the Show/Associate Services link to open the Add/Edit Mobile Concierge Service Services page.
The list of all the available service advertisements are displayed and you can associate service advertisements by selecting them.

**Step 5** To associate a service advertisement, you can do the following:
- Choose an advertisement by filtering based on either the provider name or friendly name by choosing them from the Filter By drop-down list.
  or
- Select the Associate check box to associate that particular service advertisement.

**Step 6** Click OK.

Creating Service Advertisements from the Floor Map

To create service advertisements from the floor map, follow these steps:

**Step 1** Choose Monitor > Site Maps.
The Site Maps page appears.

**Step 2** Choose the appropriate floor location link from the list.
A map appears showing the placement of all installed access points, client and tags, and their relative signal strength.

**Step 3** Click the Services icon on the floor map page.
The Venue dialog box to associate service advertisement to that particular venue appears.

**Step 4** Click the Show/Associate Services link to open the Add/Edit Mobile Concierge Services.
The list of all the available service advertisements is displayed and you can associate service advertisements by choosing them.

**Step 5** Click Create Mobile Concierge Service to create service advertisements.
You are redirected to the Service > Mobile Concierge > Add Service Advertisements page.
Step 6  Follow the steps in the “Adding Service Advertisements to the Floor Map” section on page 16-98 to create the service advertisements provided.

Related Topics

- Adding Service Advertisements to the Floor Map
- Viewing the Configured Service Advertisements
- Viewing Mobile Concierge Service Statistics
- Viewing the MSE Summary Page for Mobile Concierge License Information
- Viewing Service Advertisements Synchronization Status
- Adding a Mobile Concierge Service License Using the License Center
- Mobile Concierge Reports

Viewing the Configured Service Advertisements

To view the configured service advertisements, follow these steps:

Step 1  Choose Services > Mobility Services Engine.
Step 2  Click Device Name to view its properties.

The General Properties page appears.

Step 3  Choose Mobile Concierge Service > Advertisements from the left sidebar menu.

The following information appears in the Mobile Concierge Service page:

- Icon—Displays an icon associated with the service provider.
- Provide Name—Displays the service providers name.
- Venue Name—Displays the venue name.
- Advertisements
  - Friendly Name—Friendly name that is displayed in the handset.
  - Advertisement Type—Type of advertisement that is displayed in the handset.

Related Topics

- Adding Service Advertisements to the Floor Map
- Viewing Mobile Concierge Service Statistics
- Viewing the MSE Summary Page for Mobile Concierge License Information
- Viewing Service Advertisements Synchronization Status
- Adding a Mobile Concierge Service License Using the License Center
- Mobile Concierge Reports
Viewing Mobile Concierge Service Statistics

To view Mobile Concierge Service statistics, follow these steps:

**Step 1** Choose Services > Mobility Services Engine.

**Step 2** Click Device Name to view its properties.

The General Properties page appears.

**Step 3** Choose Mobile Concierge Service > Statistics from the left sidebar menu.

The following information appears in the Mobile Concierge Service page:

- Top 5 Active Mobile MAC addresses—Displays information of the most active mobiles in a given venue.
- Top 5 Service URIs—Displays information of the usage of the services across a given venue or provider.

Related Topics

- Adding Service Advertisements to the Floor Map
- Viewing the Configured Service Advertisements
- Viewing the MSE Summary Page for Mobile Concierge License Information
- Viewing Service Advertisements Synchronization Status
- Adding a Mobile Concierge Service License Using the License Center
- Mobile Concierge Reports

Viewing the MSE Summary Page for Mobile Concierge License Information

See the “Performing Administrative Tasks” section on page 15-1 for more information on MSE licensing.

Viewing Service Advertisements Synchronization Status

To view service advertisements synchronization status, follow these steps:

**Step 1** Choose Services > Synchronize Services.

**Step 2** Choose Service Advertisements from the left side menu bar.

The following information appears in the Service Advertisements page:

- Provider Name—Shows the name of the service provider.
- Service—Shows the type of service that a particular advertisement is using.
- MSE—Shows whether the service advertisement is synchronized with the MSE or not.
- Sync Status—Shows the synchronization status. A green two-arrow icon indicates that its corresponding element is synchronized with the given server such as MSE. A gray two-arrow icon with a red circle indicates that its corresponding item is not synchronized with a given server.
• Message—Shows any message related to the advertisement synchronization failure.

Related Topics

• Adding Service Advertisements to the Floor Map
• Viewing Mobile Concierge Service Statistics
• Viewing the MSE Summary Page for Mobile Concierge License Information
• Adding a Mobile Concierge Service License Using the License Center
• Mobile Concierge Reports

Adding a Mobile Concierge Service License Using the License Center

To add a Mobile Concierge service license using the license center, follow these steps:

Step 1  Choose Administration > Licenses.
Step 2  Choose Files > MSE Files from the left sidebar menu.
        The License Center page appears.
Step 3  Click the Add to select the license file.
Step 4  Click OK to add the license.
        The Mobile Concierge Service license is added.

Related Topics

• Adding Service Advertisements to the Floor Map
• Viewing Mobile Concierge Service Statistics
• Viewing the MSE Summary Page for Mobile Concierge License Information
• Viewing Service Advertisements Synchronization Status
• Mobile Concierge Reports

Mobile Concierge Reports

You can generate 2 types of Mobile Concierge reports:

• Service URI Statistics—In this report, you can retrieve information about the top services that you have used based on the filters like venue, provider, mobile mac. With this report, you can get the additional information about the usage of the services across a given venue.
• Mobile MAC Statistics—In this report, you can retrieve information about the most active clients based on the filters like venue. With this report, you can get additional information about the most active mobiles in a given venue.
Identity Services

Cisco Identity Services Engine (ISE) is a next-generation identity and policy-based network access platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations.

The Prime Infrastructure manages the wired and the wireless clients in the network. When Cisco ISE is used as a RADIUS server to authenticate clients, the Prime Infrastructure collects additional information about these clients from the ISE and provides all relevant client information to the Prime Infrastructure to be visible in a single console.

**Note** The Prime Infrastructure communicates with the ISE using REST API. See [http://www.cisco.com/en/US/docs/security/ise/1.0/api_ref_guide/ise10_api_ref_guide_ch1.html](http://www.cisco.com/en/US/docs/security/ise/1.0/api_ref_guide/ise10_api_ref_guide_ch1.html) for more information on Cisco ISE APIs.

**Note** Accounting data for wired clients are collected from ISE every 15 minutes. There is a background ISE Status task that polls all ISEs added to the Prime Infrastructure for every 15 minutes for the status of ISEs and updates the status.

The ISE integration in the Prime Infrastructure provides the following features:

- Periodic polling to the ISE for collecting client statistics and other attributes requires for client list, dashboard charts, and reports.
- On demand query to the ISE for getting additional client details such as Authorization Profile, Posture, Endpoint Type (profiler), and so on.
- Cross launch the ISE user interface with automatic single sign on.


- **Viewing Identify Services**, page 16-102
- **Adding an Identity Services Engine**, page 16-103
- **Removing an Identity Services Engine**, page 16-103

**Viewing Identify Services**

To see the Identity Services Engines that are added in the Prime Infrastructure, choose **Services > Identity Services**. The following parameters appear:

- Server Address—IP address of ISE.
- Port—HTTPS port number for the server.
- Retries—Indicates the number of retry attempts.
- Version—Indicates the version of the ISE.
- Status—Indicates the reachability status, that is, Reachable or Unreachable.
- Role—Indicates if a node is a primary, standalone or, standby node.
Adding an Identity Services Engine

**Note** A maximum of two ISEs can be added in the Prime Infrastructure. If you add two ISEs, one should be primary and the other should be standby. When you are adding a standalone node, you can add only one standalone node and cannot add second node.

To add an Identity Services Engine, follow these steps:

**Step 1** Choose Services > Identity Services.

**Step 2** From the Select a command drop-down list, choose Add Identity Services Engine.

**Step 3** In the Server Address text box, type the IP address of the server.

**Step 4** In the Port text box, enter the port number of the server. The default is 443.

**Step 5** In the Username text box, enter the username.

**Step 6** In the Password text box, enter the password.

**Step 7** Reenter the password in the Confirm Password text box.

**Note** The credentials should be superuser credentials. Otherwise, ISE integration does not work.

**Step 8** In the HTTP Connection Timeout text box, enter the amount of time (in seconds) allowed before the process time outs. The default is 30 seconds.

**Step 9** Click Save.

Removing an Identity Services Engine

To remove an Identity Services Engine, follow these steps:

**Step 1** Choose Services > Identity Services.

**Step 2** Select the check box(es) of the identity services engines that you want to delete.

**Step 3** From the Select a command drop-down list, choose Delete Identity Services Engine(s).

**Step 4** Click OK to confirm the deletion.

Mobility Services Engine Admin User Interface

For more information on Mobility Services Engine Admin User Interface see the following URL:

Launching the MSE Admin User Interface

To launch the MSE admin user interface, follow these steps:

**Step 1**
To launch the MSE admin user interface (UI), type https://mseip/mseui/ in the Web Browser or you can launch it from the Cisco Prime Infrastructure (PI) by clicking the MSE name link from Services > Mobility Services Engines page.

**Note**
The MSE admin UI is displayed only if you have selected the MSE Admin View check box in the Administration > User Preference Page from the Prime Infrastructure user interface.

**Step 2**
Enter the username and password.

**Step 3**
Click **Sign In**.
Tools

The Tools menu provides access to the Voice Audit, Location Accuracy Tool, Configuration Audit Summary, and Migration Analysis features of Cisco Prime Infrastructure.

- Running Voice Audits, page 17-1
- Running Voice Diagnostic, page 17-1
- Configuring the Location Accuracy Tools, page 17-1
- Configuring Audit Summary, page 17-2
- Configuring Migration Analysis, page 17-2
- Configuring TAC Case Attachments, page 17-2

Running Voice Audits

Prime Infrastructure provides voice auditing mechanism to check the controller configuration and to ensure that any deviations from the deployment guidelines are highlighted as an Audit Violation.

To access the Voice Audit feature, choose Tools > Voice Audit. For more information about how to run voice audits, see the Working with Wireless Operational Tools chapter in the Cisco Prime Infrastructure 2.0 User Guide.

Running Voice Diagnostic

The Voice diagnostic tool is an interactive tool to diagnose the voice calls in real time. This tool reports call control related errors, roaming history of the clients and the total active calls accepted and rejected by an associated AP. This tool enables you to start or stop the voice diagnostic.

To access the Voice Diagnostic feature, choose Tools > Voice Diagnostic. For more information about how to start voice diagnostic test, see the Working with Wireless Operational Tools chapter in the Cisco Prime Infrastructure 2.0 User Guide.

Configuring the Location Accuracy Tools

You can analyze the location accuracy of non-rogue and rogue clients, interferers, and asset tags by using the Location Accuracy Tools.
By verifying for location accuracy, you are ensuring that the existing access point deployment can estimate the true location of an element within 10 meters at least 90% of the time.

To access the Location Accuracy Tool feature, choose Tools > Location Accuracy Tool. For more information about the Location Accuracy Tool, see the Working with Wireless Operational Tools chapter in the Cisco Prime Infrastructure 2.0 User Guide.

Configuring Audit Summary

Choose Tools > Config Audit to launch the Config Audit Summary page. For information about the audit summary displayed in this page, see the Working with Wireless Operational Tools chapter in the Cisco Prime Infrastructure 2.0 User Guide.

Configuring Migration Analysis

Choose Tools > Migration Analysis to launch the Migration Analysis Summary page. For information about the migration analysis summary displayed in this page, see the Working with Wireless Operational Tools chapter in the Cisco Prime Infrastructure 2.0 User Guide.

Configuring TAC Case Attachments

Note: You must configure a valid mail server before configuring TAC case attachments.

The TAC Case Attachment tool helps you easily attach all the relevant controller TAC case information in one step. This tool provides two options:

- Send—Sends an e-mail to attach@cisco.com.
- Download—Downloads the information to a local computer. You must manually e-mail the data to attach@cisco.com. This option is handy if there is no e-mail connectivity between Prime Infrastructure server and Cisco or if the information is too large to be attached through e-mail.

This tool sends the following information:

- Network Information—Sends device inventory details and the client types.
- Controller Information—Sends running configuration details, tech-support, message logs, trap logs, and the controller crash files.
- Access Point Information—Sends crash files and radio core dumps.

Before you send the information of TAC case, you should provide attach@cisco.com email address in the To text box of Mail Server Configuration page (Administration > Settings > Mail Server Configuration).

To Send or Download information, you must enter the following details:

- Enter a valid TAC Case Number.
- Select a controller if you want to send the controller or AP information.
Note: You can also send additional information using the additional comments text box. After sending the information, you can verify whether the data has reached Cisco by looking at the attachment section in the Case tool.

Note: This tool requires read-write access on the controller to collect and upload controller or access point information.
Security IDS/IPS Overview

The addition of WLANs in the corporate environment introduces a new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue access points installed by employees for their personal use usually do not adhere to the corporate security policy. A rogue access point can put the entire corporate network at risk for outside penetration and attack. Not to underestimate the threat of the rogue access point, there are many other wireless security risks and intrusions such as mis-configured and unconfigured access points and DoS (denial of service) attacks.

The Cisco Adaptive Wireless IPS is designed to help manage against security threats by validating proper security configurations and detecting possible intrusions. With the comprehensive suite of security monitoring technologies, the Cisco Adaptive Wireless IPS alerts the user on more than 100 different threat conditions in the following categories:

- User authentication and traffic encryption
- Rogue and ad-hoc mode devices
- Configuration vulnerabilities
- Intrusion detection on security penetration
- Intrusion detection on DoS attacks

To maximize the power of the Cisco Adaptive Wireless IPS, security alarms can be customized to best match your security deployment policy. For example, if your WLAN deployment includes access points made by a specific vendor, the product can be customized to generate the rogue access point alarm when an access point made by another vendor is detected by the access point or sensor.

Pre-configured Profiles for Various WLAN Environments

During installation, the user can select an appropriate profile based on the WLAN network implemented. The Cisco Adaptive Wireless IPS provides separate profiles for the following:

- Enterprise best practice
- Enterprise rogue detection only
Intrusion Detection—Denial of Service Attack

Wireless DoS (denial of service) attacks aim to disrupt wireless services by taking advantage of various vulnerabilities of WLANs at layer one and two. DoS attacks may target the physical RF environment, access points, client stations, or the back-end authentication RADIUS servers. For example, RF jamming attacks with a high-power directional antenna from a distance can be carried out from the outside of your office building. Attack tools used by intruders leverage hacking techniques such as spoofed 802.11 management frames, spoofed 802.1x authentication frames, or simply using the brute force packet flooding method.

The nature and protocol standards for wireless are subject to some of these attacks. Cisco has developed Management Frame Protection, the basis of 802.11i, to proactively prevent many of these attacks. (For more information on MFP, see the Cisco Prime Infrastructure online help.) The Cisco Adaptive Wireless IPS contributes to this solution by an early detection system where the attack signatures are matched. The Cisco Adaptive Wireless IPS DoS detection focuses on WLAN layer one (physical layer) and two (data link layer, 802.11, 802.1x). When strong WLAN authentication and encryption mechanisms are used, higher layer (IP layer and above) DoS attacks are difficult to execute. The wIPS server tightens your WLAN defense by validating strong authentication and encryption policies. In addition, the Cisco Adaptive Wireless IPS Intrusion Detection on denial of service attacks and security penetration provides 24 X 7 air tight monitoring on potential wireless attacks.
This section describes the denial of service attack subcategories and contains the following topics:

- Denial of Service Attack Against Access Points, page 18-3
- Denial of Service Attack Against Infrastructure, page 18-9
- Denial of Service Attack Against Station, page 18-15

### Denial of Service Attack Against Access Points

DoS attacks against access points are typically carried out on the basis of the following assumptions:

- Access points have limited resources. For example, the per-client association state table.
- WLAN management frames and authentication protocols 802.11 and 802.1x have no encryption mechanisms.

Wireless intruders can exhaust access point resources, most importantly the client association table, by emulating large number of wireless clients with spoofed MAC addresses. Each one of these emulated clients attempts association and authentication with the target access point but leaves the protocol transaction mid-way. When the access point resources and the client association table is filled up with these emulated clients and their incomplete authentication states, legitimate clients can no longer be serviced by the attacked access point. This creates a denial of service attack.

The Cisco Adaptive Wireless IPS tracks the client authentication process and identifies DoS attack signatures against the access point. Incomplete authentication and association transactions trigger the attack detection and statistical signature matching process. Detected DoS attacks result in setting off wIPS alarms which include the usual alarm detail description and target device information.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing.

This section describes the DoS attacks against access points and contains the following topics:

- Denial of Service Attack: Association Flood, page 18-3
- Denial of Service Attack: Association Table Overflow, page 18-4
- Denial of Service Attack: Authentication Flood, page 18-5
- Denial of Service Attack: EAPOL-Start Attack, page 18-6
- Denial of Service Attack: PS Poll Flood, page 18-6
- Denial of Service Attack: Probe Request Flood, page 18-7
- Denial of Service Attack: Unauthenticated Association, page 18-8

### Denial of Service Attack: Association Flood

**Alarm Description and Possible Causes**

This DoS attack exhausts the access point resources, particularly the client association table, by flooding the access point with a large number of spoofed client associations. At the 802.11 layer, shared-key authentication is flawed and rarely used. The other alternative is open authentication (null authentication) that relies on higher level authentication such as 802.1x or VPN. Open authentication allows any client to authenticate and then associate. An attacker using such a vulnerability can emulate a large number of clients to flood a target access point client association table by creating many clients reaching State 3. When the client association table overflows, legitimate clients cannot get associated; therefore, a DoS attack is committed. (see Figure 18-1)
Intrusion Detection—Denial of Service Attack

Figure 18-1  DoS Attack: Association Flood

wIPS Solution

The Cisco Adaptive Wireless IPS detects spoofed MAC addresses and tracks the 802.1x actions and data communication after a successful client association to detect this form of DoS attack. After this attack is reported by the Cisco Adaptive Wireless IPS, you may log onto this access point to inspect its association table for the number of client associations.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing.

Denial of Service Attack: Association Table Overflow

Alarm Description and Possible Causes

Wireless intruders can exhaust access point resources, most importantly the client association table, by imitating a large number of wireless clients with spoofed MAC addresses. Each one of these imitated clients attempts association and authentication with the target access point. The 802.11 authentication typically completes because most deployments use 802.11 open system authentication, which is a null authentication process. Association with these imitated clients follows the authentication process. These imitated clients do not, however, follow up with higher level authentication such as 802.1x or VPN, which leaves the protocol transaction half-finished. At this point, the attacked access point maintains a state in the client association table for each imitated client. When the access point resources and client association table is filled with these imitated clients and their state information, legitimate clients can no longer be serviced by the attacked access point. This creates a DoS attack.
wIPS Solution

The Cisco Adaptive Wireless IPS tracks the client authentication process and identifies a DoS attack signature against an access point. Incomplete authentication and association transactions trigger the Cisco Adaptive Wireless IPS attack detection and statistical signature matching process.

Denial of Service Attack: Authentication Flood

Attack tool: Void11

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement such a state machine according to the IEEE standard (see Figure 18-2). On the access point, each client has a state recorded in the access point client table (association table). This recorded state has a size limit that can either be a hard-coded number or a number based on the physical memory constraint.

![Figure 18-2 Client State Machine](image)

A form of DoS attack floods the access point client state table (association table) by imitating many client stations (MAC address spoofing) sending authentication requests to the access point. Upon receipt of each individual authentication request, the target access point creates a client entry in State 1 of the association table. If open system authentication is used for the access point, the access point returns an authentication success frame and moves the client to State 2. If shared-key authentication is used for the access point, the access point sends an authentication challenge to the attacker imitated client, which does not respond. In this case, the access point keeps the client in State 1. In either case, the access point contains multiple clients hanging in either State 1 or State 2 which fills up the access point association table. When the table reaches its limit, legitimate clients cannot authenticate and associate with this access point. This results in a DoS attack.
wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security analyst can log onto the access point to check the current association table status.

Denial of Service Attack: EAPOL-Start Attack

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using EAP over LANs (EAPOL). The 802.1x protocol starts with an EAPOL-Start frame sent by the client station to begin the authentication transaction. The access point responds to an EAPOL-start frame with a EAP-identity-request and some internal resource allocation. (see Figure 18-3)

An attacker attempts to disrupt an access point by flooding it with EAPOL-start frames to exhaust the access point internal resources.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking the 802.1x authentication state transition and particular attack signature.

Denial of Service Attack: PS Poll Flood

Alarm Description and Possible Causes

Power management is probably one of the most critical features of wireless LAN devices. Power management helps to conserve power by enabling stations to remain in power saving state mode for longer periods of time and to receive data from the access point only at specified intervals.
The wireless client device must inform the access point of the length of time that it is in the sleep mode (power save mode). At the end of the time period, the client wakes up and checks for waiting data frames. After it completes a handshake with the access point, it receives the data frames. The beacons from the access point also include the Delivery Traffic Indication Map (DTIM) to inform the client when it needs to wake up to accept multicast traffic.

The access point continues to buffer data frames for the sleeping wireless clients. Using the Traffic Indication Map (TIM), the access point notifies the wireless client that it has buffered data buffered. Multicast frames are sent after the beacon that announces the DTIM.

The client requests the delivery of the buffered frames using PS-Poll frames to the access point. For every PS-Poll frame, the access point responds with a data frame. If there are more frames buffered for the wireless client, the access point sets the data bit in the frame response. The client then sends another PS-Poll frame to get the next data frame. This process continues until all the buffered data frames are received.

A potential hacker could spoof the MAC address of the wireless client and send out a flood of PS-Poll frames. The access point then sends out the buffered data frames to the wireless client. In reality, the client could be in the power save mode and would miss the data frames.

**wlPS Solution**

The Cisco Adaptive Wireless IPS can detect this DoS attack that can cause the wireless client to lose legitimate data. Locate and remove the device from the wireless environment.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing.

**Denial of Service Attack: Probe Request Flood**

**Alarm Description and Possible Causes**

A form of Denial of Service attack allows the attacker to force the target AP into a constant stream of wireless packets intended to serve nonexistent clients. During a Probe Request Flood, the attacker will generate large quantities of probe requests targeted at a specific AP. Typical wireless design specifies that an AP will respond to a probe request by sending a probe response, which contains information about the corporate network. Due to the volume of probe requests transmitted during a flood attack, the AP will be stuck continuously responding, thus resulting in a denial of service for all clients depending on that AP.

**wlPS Solution**

The wIPS server monitors the levels of probe request frames detected and will trigger a Probe Request Flood alarm when the threshold is exceeded. Even in cases where the requests are valid, the volume of the frames could cause problems with wireless activity. Consequently, the source(s) of the offending frames should be located and removed from the enterprise environment.

**Denial of Service Attack: Re-association Request Flood**

**Alarm Description and Possible Causes**

A form of Denial-of-service attack is to exhaust the AP’s resources, particularly the client association table, by flooding the AP with a large number of emulated and spoofed client re-associations. At the 802.11 layer, Shared-key authentication is flawed and rarely used any more. The only other alternative
is Open authentication (null authentication) that relies on higher level authentication such as 802.1x or VPN. Open authentication allows any client to authenticate and then associate. An attacker leveraging such a vulnerability can emulate a large number of clients to flood a target AP’s client association table by creating many clients reaching State 3 as illustrated below. Once the client association table overflows, legitimate clients will not be able to get associated thus a denial-of-serve attack is committed.

**wIPS Solution**

The wIPS server monitors the levels of re-association requests on the network and triggers this alarm if the threshold is exceeded.

**Denial of Service Attack: Unauthenticated Association**

**Alarm Description and Possible Causes**

A form of DoS attack is to exhaust the access point resources, particularly the client association table, by flooding the access point with a large number of spoofed client associations. At the 802.11 layer, shared-key authentication is flawed and rarely used. The other alternative is open authentication (null authentication) which relies on higher level authentication such as 802.1x or VPN. Open authentication allows any client to authenticate and then associate. An attacker using such a vulnerability can imitate a large number of clients to flood a target access point client association table by creating many clients reaching State 3. When the client association table overflows, legitimate clients cannot get associated causing a DoS attack. (see Figure 18-4)
wIPS Solution

The Cisco Adaptive Wireless IPS detects spoofed MAC addresses and tracks 802.1x actions and data communication after a successful client association to detect this form of DoS attack. After this attack is reported by the Cisco Adaptive Wireless IPS, you may log onto this access point to inspect its association table for the number of client associations.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing.

Denial of Service Attack Against Infrastructure

In addition to attacking access points or client stations, the wireless intruder may target the RF spectrum or the back-end authentication RADIUS server for DoS attacks. The RF spectrum can be easily disrupted by injecting RF noise generated by a high power antenna from a distance. Back-end RADIUS servers can be overloaded by a DDoS (distributed denial of service) attack where multiple wireless attackers flood the RADIUS server with authentication requests. This attack does not require a successful authentication to perform the attack.

This section describes the DoS attacks against infrastructure and contains the following topics:

- Denial of Service Attack: Beacon Flood, page 18-10
- Denial of Service Attack: CTS Flood, page 18-11
- Denial of Service Attack: MDK3-Destruction Attack, page 18-10
- Denial of Service Attack: Queensland University of Technology Exploit, page 18-11
- Denial of Service attack: RF Jamming, page 18-12
- Denial of Service: RTS Flood, page 18-13
Denial of Service Attack: Beacon Flood

Attack tool: CTS Jack

Alarm Description and Possible Causes

A form of Denial of Service attack allows an attacker to inhibit wireless activity for the entire enterprise infrastructure by preventing new associations between valid APs and stations. Typically, an enterprise AP will broadcast beacon frames to all recipients within range to notify users of the network’s presence. Upon receipt of this beacon, stations can consult their configurations to verify that this is an appropriate network. During a beacon flood attack, stations that are actively seeking a network are bombarded with beacons from networks generated using different MAC addresses and SSIDs. This flood can prevent the valid client from detecting the beacons sent by the corporate APs, and thus a denial of service attack is initiated.

wIPS Solution

The wIPS server monitors the levels of beacon frames detected and will trigger a Beacon Flood alarm when the threshold is exceeded. Even in cases where the beacons are valid, the volume of the frames could cause problems with wireless activity. Consequently, the sources of the offending frames should be located and removed from the enterprise environment.

Denial of Service Attack: MDK3-Destruction Attack

Attack tool: CTS Jack

Alarm Description and Possible Causes

MDK3 is a suite of hacking tools that allows users to utilize a number of different security penetration methods against corporate infrastructures. MDK3-Destruction mode is a specific implementation of the suit that uses an array of the tools to effectively completely shut down a wireless deployment. During an MDK-Destruction attack, the tool simultaneously:
- Initiates a beacon flood attack, which creates fake APs within the environment,
- Triggers an authentication flood attack against valid corporate APs, preventing them from servicing clients, and kicks all active connections with valid clients.

Additional enhancements allow for the tool to be used to connect the valid clients to the fake APs generated with the beacon flood, causing further confusion in the environment.

wIPS Solution

The wIPS server monitors for the combination of symptoms of an MDK3-Destruction attack and triggers an alarm when they are detected. Due to the dramatic impact that this attack can have on a wireless deployment, it is strongly recommended that the source of the attack be identified and removed immediately in order to resume normal network operations.
Denial of Service Attack: CTS Flood

Attack tool: CTS Jack

Alarm Description and Possible Causes

As an optional feature, the IEEE 802.11 standard includes the RTS/CTS (request-to-send/clear-to-send) functionality to control the station access to the RF medium. The wireless device ready for transmission sends a RTS frame to acquire the right to the RF medium for a specified time duration. The receiver grants the right to the RF medium to the transmitter by sending a CTS frame of the same time duration. All wireless devices observing the CTS frame should yield the media to the transmitter for transmission without contention. (see Figure 18-5)

Figure 18-5 Standard RTS/CTS Functionality Compared to the CTS DoS Attack

A wireless DoS attacker may take advantage of the privilege granted to the CTS frame to reserve the RF medium for transmission. By transmitting back-to-back CTS frames, an attacker can force other wireless devices sharing the RF medium to hold back their transmission until the attacker stops transmitting the CTS frames.

wIPS Solution

The Cisco Adaptive Wireless IPS detects the abuse of CTS frames for a DoS attack.

Denial of Service Attack: Queensland University of Technology Exploit

Alarms Description and Possible Causes

802.11 WLAN devices use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as the basic access mechanism in which the WLAN device listens to the medium before starting any transmission and backs-off when it detects any existing transmission taking place. Collision avoidance combines the physical sensing mechanism and the virtual sense mechanism that includes the Network Allocation Vector (NAV), the time before which the medium is available for transmission. Clear Channel Assessment (CCA) in the DSSS protocol determines whether a WLAN channel is clear so an 802.11b device can transmit on it.

Mark Looi, Christian Wullems, Kevin Tham and Jason Smith from the Information Security Research Centre, Queensland University of Technology, Brisbane, Australia, have recently discovered a flaw in the 802.11b protocol standard that could potentially make it vulnerable to DoS radio frequency jamming attacks.

This attack specifically attacks the CCA functionality. According to the AusCERT bulletin, "an attack against this vulnerability exploits the CCA function at the physical layer and causes all WLAN nodes within range, both clients and access points, to defer transmission of data for the duration of the attack. When under attack, the device behaves as if the channel is always busy, preventing the transmission of any data over the wireless network."

This DoS attack affects DSSS WLAN devices including IEEE 802.11, 802.11b, and low-speed (below 20 Mbps) 802.11g wireless devices. IEEE 802.11a (using OFDM), high-speed (above 20 Mbps using OFDM) 802.11g wireless devices are not affected by this attack. Devices that use FHSS are also not affected.

Any attacker using a PDA or a laptop equipped with a WLAN card can launch this attack on SOHO and enterprise WLANs. Switching to the 802.11a protocol is the only solution or known protection against this DoS attack.

For more information on this DoS attack, refer to:
- www.isrc.qut.edu.au
- www.isrc.qut.edu.au/wireless
- http://www.kb.cert.org/vuls/id/106678

wIPS Solution

The Cisco Adaptive Wireless IPS detects this DoS attack and sets off the alarm. Locate and remove the responsible device from the wireless environment.

Denial of Service attack: RF Jamming

Alarm Description and Possible Causes

WLAN reliability and efficiency depend on the quality of the radio frequency (RF) media. Each RF is susceptible to RF noise impact. An attacker using this WLAN vulnerability can perform two types of DoS attacks:

- Disrupt WLAN service—At the 2.4 GHz unlicensed spectrum, the attack may be unintentional. A cordless phone, Bluetooth devices, microwave, wireless surveillance video camera, or baby monitor can all emit RF energy to disrupt WLAN service. Malicious attacks can manipulate the RF power at 2.4 GHz or 5 GHz spectrum with a high-gain directional antenna to amplify the attack impact from a distance. With free-space and indoor attenuation, a 1-kW jammer 300 feet away from a building...
can jam 50 to 100 feet into the office area. The same 1-kW jammer located inside a building can jam 180 feet into the office area. During the attack, WLAN devices in the target area are out of wireless service.

- Physically damage AP hardware—An attacker using a high-output transmitter with directional high gain antenna 30 yards away from an access point can pulse enough RF power to damage electronics in the access point putting it being permanently out of service. Such High Energy RF (HERF) guns are effective and are inexpensive to build.

**wIPS Solution**

The Cisco Adaptive Wireless IPS detects continuous RF noise over a certain threshold for a potential RF jamming attack.

Cisco Spectrum Intelligence also provides specific detection of non-802.11 jamming devices. For more information on Cisco Spectrum Intelligence, refer to the *Cisco Wireless Control System Configuration Guide*.

**Denial of Service: RTS Flood**

**Alarm Description and Possible Causes**

As an optional feature, the IEEE 802.11 standard includes the RTS/CTS (Request-To-Send/Clear-To-Send) functionality to control access to the RF medium by stations. The wireless device ready for transmission sends an RTS frame to acquire the right to the RF medium for a specified duration. The receiver grants the right to the RF medium to the transmitter by sending a CTS frame of the same duration. All wireless devices observing the CTS frame should yield the RF medium to the transmitter for transmission without contention. See Figure 18-6.
A wireless denial of service attacker may take advantage of the privilege granted to the CTS frame to reserve the RF medium for transmission. By transmitting back-to-back RTS frames with a large transmission duration field, an attacker reserves the wireless medium and force other wireless devices sharing the RF medium to hold back their transmissions.

**wIPS Solution**

The Cisco Adaptive Wireless IPS detects the abuse of RTS frames for denial of service attacks.

**Denial of Service Attack: Virtual Carrier Attack**

**Alarm Description and Possible Causes**

The virtual carrier-sense attack is implemented by modifying the 802.11 MAC layer implementation to allow random duration values to be sent periodically. This attack can be carried out on the ACK, data, RTS, and CTS frame types by using large duration values. By doing this the attacker can prevent channel access to legitimate users.

Under normal circumstances, the only time a ACK frame carries a large duration value is when the ACK is part of a fragmented packet sequence. A data frame legitimately carries a large duration value only when it is a subframe in a fragmented packet exchange.

One approach to deal with this attack is to place a limit on the duration values accepted by nodes. Any packet containing a larger duration value is truncated to the maximum allowed value. Low cap and high cap values can be used. The low cap has a value equal to the amount of time required to send an ACK frame, plus media access backoffs for that frame. The low cap is used when the only packet that can follow the observed packet is an ACK or CTS. This includes RTS and all management (association, and so on) frames. The high cap is used when it is valid for a data packet to follow the observed frame. The
The high cap must be used in two places: when observing an ACK (because the ACK may be part of a MAC level fragmented packet) and when observing a CTS.

A station that receives an RTS frame also receives the data frame. The IEEE 802.11 standard specifies the exact times for the subsequent CTS and data frames. The duration value of RTS is respected until the following data frame is received or not received. Either the observed CTS is unsolicited or the observing node is a hidden terminal. If this CTS is addressed to a valid in-range station, the valid station can nullify this by sending a zero duration null function frame. If this CTS is addressed to an out-of-range station, one method of defense is to introduce authenticated CTS frames containing cryptographically signed copies of the preceding RTS. With this method, there is a possibility of overhead and feasibility issues.

**wIPS Solution**

The Cisco Adaptive Wireless IPS detects this DoS attack. Locate the device and take appropriate steps to remove it from the wireless environment.

**Denial of Service Attack Against Station**

DoS (denial of service) attacks against wireless client station are typically carried out based on the fact that 802.11 management frames and 802.1x authentication protocols have no encryption mechanism and thus can be spoofed. For example, wireless intruders can disrupt the service to a client station by continuously spoofing a 802.11 dis-association or deauthentication frame from the access point to the client station. The 802.11 association state machine as specified by the IEEE standard is illustrated in Figure 18-7 to show how an associated station can be tricked out of the authenticated and associated state by various types of spoofed frames.

**Figure 18-7  802.11 Association and Authentication State Machine**

Besides the 802.11 authentication and association state attack, there are similar attack scenarios for 802.1x authentication. For example, 802.1x EAP-Failure or EAP-logoff messages are not encrypted and can be spoofed to disrupt the 802.1x authenticated state to disrupt wireless service. See Figure 18-8 for 802.1x authentication and key exchange state change.
Chapter 18  wIPS Policy Alarm Encyclopedia

**Figure 18-8  802.1x User Authentication Process**

The Cisco Adaptive Wireless IPS tracks the client authentication process and identifies DoS attack signatures. Incomplete authentication and association transactions trigger the attack detection and statistical signature matching process. Detected DoS attack results in setting off wIPS alarms that include the usual alarm detail description and target device information.

This section describes the DoS attacks against client station and contains the following topics:

- Denial of Service Attack: Authentication-Failure Attack, page 18-16
- Denial of Service Attack: Block ACK Flood, page 18-17
- Denial of Service Attack: De-Auth Broadcast Flood, page 18-18
- Denial of Service Attack: De-Auth Flood, page 18-19
- Denial of Service Attack: Dis-Assoc Broadcast Flood, page 18-20
- Denial of Service Attack: Dis-Assoc Flood, page 18-22
- Denial of Service Attack: EAPOL-Logoff Attack, page 18-23
- Denial of Service Attack: FATA-Jack Tool, page 18-23
- Denial of Service Attack: Premature EAP-Failure, page 18-25
- Denial of Service Attack: Premature EAP-Success, page 18-25
- Denial of Service Attack: Probe Response Flood, page 18-26

**Denial of Service Attack: Authentication-Failure Attack**

**Alarm Description and Possible Causes**

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this client state machine based on the IEEE standard (see Figure 18-9). A successfully associated client remains in State 3 to continue wireless communication. A client in State 1 and in State 2 cannot participate in the WLAN data communication process until it is authenticated and associated to State 3. IEEE 802.11 defines two authentication services: open system authentication and shared key authentication. Wireless clients go through one of these authentication processes to associate with an access point.
A denial of service (DoS) attack spoofs invalid authentication request frames (with bad authentication service and status codes) being sent from an associated client in State 3 to an access point. Upon receipt of the invalid authentication requests, the access point updates the client to State 1, which disconnects client wireless service.

**wIPS Solution**

The Cisco Adaptive Wireless IPS detects this form of a DoS attack by monitoring for spoofed MAC addresses and authentication failures. This alarm may also indicate an intrusion attempt. When a wireless client fails too many times in authenticating with an access point, the server raises this alarm to indicate a potential intruder attempt to breach security.

**Note**

This alarm focuses on IEEE 802.11 authentication methods, such as open system and shared key. EAP and 802.1x based authentications are monitored by other alarms.

### Denial of Service Attack: Block ACK Flood

**Alarm Description & Possible Causes**

A form of denial of service attack allows an attacker to prevent an 802.11n AP from receiving frames from a specific valid corporate client. With the introduction of the 802.11n standard, a transaction mechanism was introduced which allows a client to transmit a large block of frames at once, rather than dividing them up into segments. To initiate this exchange, the client sends an Add Block Acknowledgement (ADDBA) to the AP, which contains sequence numbers to inform the AP of the size of the block being transmitted. The AP then accepts all frames that fall within the specified sequence (consequently dropping any frames that fall outside of the range) and transmits a BlockACK message back to the client when the transaction has been completed.
To exploit this process, an attacker can transmit an invalid ADDBA frame while spoofing the valid client MAC address. This process causes the AP to ignore any valid traffic transmitted from the client until the invalid frame range has been reached.

**wIPS Solution**

The wIPS server monitors ADDBA transactions for signs of spoofed client information. When an attacker is detected attempting to initiate a Block ACK attack, an alarm is triggered. We recommend that users locate the offending device and eliminate it from the wireless environment as soon as possible.

**Denial of Service Attack: De-Auth Broadcast Flood**

Attack tool: WLAN Jack, Void11, Hunter Killer

**Alarm Description and Possible Causes**

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client remains in State 3 to continue wireless communication. A client in State 1 and State 2 cannot participate in WLAN data communication until it is authenticated and associated to State 3. (see Figure 18-10)
A form of DoS attack sends all clients of an access point to the unassociated or unauthenticated State 1 by spoofing deauthentication frames from the access point to the broadcast address. With current client adapter implementation, this form of attack is very effective and immediate in disrupting wireless services against multiple clients. Typically, client stations reassociate and reauthenticate to regain service until the attacker sends another deauthentication frame.

**wIPS Solution**

The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed deauthentication frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security analyst can log onto the access point to verify the current association table status.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MAC spoofing. For more information on MFP, refer to the *Cisco Wireless Control System Configuration Guide*.

**Denial of Service Attack: De-Auth Flood**

Attack tool: WLAN Jack, Void11

**Alarm Description and Possible Causes**

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client stays in State 3 to continue wireless communication. A client in State 1 and State 2 cannot participate in WLAN data communication until it is authenticated and associated to...
State 3. (see Figure 18-11)

**Figure 18-11  Client State Machine and Deauthentication Flood Attack**

A form of DoS attack aims to send an access point client to the unassociated or unauthenticated State 1 by spoofing deauthentication frames from the access point to the client unicast address. With current client adapter implementations, this form of attack is very effective and immediate for disrupting wireless services against the client. Typically, client stations reassociate and reauthenticate to regain service until the attacker sends another deauthentication frame. An attacker repeatedly spoofs the deauthentication frames to keep all clients out of service.

**wIPS Solution**

The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed deauthentication frames and tracking client authentication and association states. When the alarm is triggered, the access point and client under attack are identified. The WLAN security officer can log onto the access point to check the current association table status.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MAC spoofing. For more information on MFP, refer to the *Cisco Wireless Control System Configuration Guide*.

**Denial of Service Attack: Dis-Assoc Broadcast Flood**

Attack tool: ESSID Jack
Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client station stays in State 3 to continue wireless communication. A client station in State 1 and State 2 can not participate in WLAN data communication until it is authenticated and associated to State 3. (see Figure 18-12)

Figure 18-12  Client State Machine and Disassociation Broadcast Attack

A form of DoS attack aims to send an access point client to the unassociated or unauthenticated State 2 by spoofing disassociation frames from the access point to the broadcast address (all clients). With current client adapter implementations, this form of attack is effective and immediate for disrupting wireless services against multiple clients. Typically, client stations reassociate to regain service until the attacker sends another disassociation frame. An attacker repeatedly spoofs the disassociation frames to keep all clients out of service.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed disassociation frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security officer can log onto the access point to check the current association table status.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MAC spoofing. For more information on MFP, refer to the Cisco Wireless Control System Configuration Guide.
Denial of Service Attack: Dis-Assoc Flood

Attack tool: ESSID Jack

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client stays in State 3 to continue wireless communication. A client in State 1 and State 2 cannot participate in WLAN data communication until it is authenticated and associated to State 3. (see Figure 18-13)

![Figure 18-13 Client State Machine and Disassociation Flood Attack]

A form of DoS attack aims to send an access point to the unassociated or unauthenticated State 2 by spoofing disassociation frames from the access point to a client. With client adapter implementations, this form of attack is effective and immediate for disrupting wireless services against this client. Typically, client stations reassociate to regain service until the attacker sends another disassociation frame. An attacker repeatedly spoofs the disassociation frames to keep the client out of service.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed disassociation frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security officer can log onto the access point to check the current association table status.
Denial of Service Attack: EAPOL-Logoff Attack

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using Extensible Authentication Protocol (EAP) over LANs or EAPOL. The 802.1x protocol starts with an EAPOL-start frame to begin the authentication transaction. At the end of an authenticated session when a client station logs off, the client station sends an 802.1x EAPOL-logoff frame to terminate the session with the access point. (see Figure 18-14)

Figure 18-14   EAPOL-Logoff Protocol and EAPOL-Logoff Attack

Because the EAPOL-logoff frame is not authenticated, an attacker can potentially spoof this frame and log the user off the access point, thus committing a DoS attack. The fact that the client is logged off from the access point is not obvious until it attempts communication through the WLAN. Typically, the disruption is discovered and the client re-associates and authenticates automatically to regain the wireless connection. The attacker can continuously transmit the spoofed EAPOL-logoff frames to be effective on this attack.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking 802.1x authentication states. When the alarm is triggered, the client and access point under attack are identified. The WLAN security officer logs onto the access point to check the current association table status.

Denial of Service Attack: FATA-Jack Tool

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this state machine based on the IEEE standard. A successfully associated client station stays in State 3 to continue wireless communication. A client station in State 1 and in State 2 cannot participate in the WLAN data communication process until it is
Intrusion Detection—Denial of Service Attack

authenticated and associated to State 3. IEEE 802.11 defines two authentication services: open system and shared key. Wireless clients go through one of these authentication processes to associate with an access point. (see Figure 18-15)

Figure 18-15  Client State Machine and DoS Attack

A form of DoS attack spoofs invalid authentication request frames (with bad authentication service and status codes) from an associated client in State 3 to an access point. Upon reception of the invalid authentication requests, the access point updates the client to State 1, which disconnects its wireless service.

FATA-jack is one of the commonly used tools to run a similar attack. It is a modified version of WLAN-jack and it sends authentication-failed packets along with the reason code of the previous authentication failure to the wireless station. This occurs after it spoofs the MAC address of the access point. FATA-jack closes most active connections and at times forces the user to reboot the station to continue normal activities.

wIPS Solution

The Cisco Adaptive Wireless IPS detects the use of FATA-jack by monitoring on spoofed MAC addresses and authentication failures. This alarm may also indicate an intrusion attempt. When a wireless client fails too many times in authenticating with an access point, the Cisco Adaptive Wireless IPS raises this alarm to indicate a potential intruder’s attempt to breach security.

Note

This alarm focuses on 802.11 authentication methods (open system, shared key, and so on). EAP and 802.1x based authentications are monitored by other alarms.

Cisco Management Frame Protection also provides complete proactive protection against frame and device spoofing.
Denial of Service Attack: Premature EAP-Failure

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using Extensible Authentication Protocol over LANs or EAPOL. The 802.1x protocol starts with an EAPOL-Start frame to begin the authentication transaction. When the 802.1x authentication packet exchange is complete with the back-end RADIUS server, the access point sends an EAP-success or EAP-failure frame to the client to indicate authentication success or failure. (see Figure 18-16)

![Figure 18-16 EAP-Failure Protocol and Premature EAP-Failure Attack](image)

The IEEE 802.1X specification prohibits a client from displaying its interface when the required mutual authentication is not complete. This enables a well-implemented 802.1x client station to avoid being fooled by a fake access point sending premature EAP-success packets.

An attacker keeps the client interface from appearing by continuously spoofing pre-mature EAP-failure frames from the access point to the client to disrupt the authentication state on the client.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking the spoofed premature EAP-failure frames and the 802.1x authentication states for each client station and access point. Find the device and remove it from the wireless environment.

Denial of Service Attack: Premature EAP-Success

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using Extensible Authentication Protocol over LANs or EAPOL. The 802.1x protocol starts with an EAPOL-start frame to begin the authentication transaction. When the 802.1x authentication packet exchange is completed with the back-end RADIUS server, the access point sends an EAP-success frame to the client to indicate a successful authentication. (see Figure 18-17)
Intrusion Detection—Denial of Service Attack

Figure 18-17  EAP-Success Protocol and EAP-Success Attack

The IEEE 802.1X specification prohibits a client from displaying its interface when the required mutual authentication has not been completed. This enables a well-implemented 802.1x client station to avoid being fooled by a fake access point sending premature EAP-success packets to bypass the mutual authentication process.

An attacker keeps the client interface from appearing by continuously spoofing premature EAP-success frames from the access point to the client to disrupt the authentication state.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking spoofed premature EAP-success frames and the 802.1x authentication states for each client station and access point. Find the device and remove it from the wireless environment.

Denial of Service Attack: Probe Response Flood

Alarm Description and Possible Causes

A form of Denial of Service attack allows the attacker to prevent a station from associating to a valid corporate AP. In a typical wireless transaction, when a station wishes to associate to an AP, it transmits a probe request from to obtain information about the AP's network. The station will then wait for the resulting probe response frame from the AP. An attacker can take advantage of this process by flooding the environment with invalid probe responses, thus preventing the station from receiving the response from the valid AP. As a result, the station is rendered unable to connect to the wireless network, and a denial of service attack is initiated.

wIPS Solution

The wIPS server monitors the levels of probe response frames detected and will trigger a Probe Request Flood alarm when the threshold is exceeded. Even in cases where the responses are valid, the volume of the frames could cause problems with wireless activity. Consequently, the source(s) of the offending frames should be located and removed from the enterprise environment.

*
Intrusion Detection—Security Penetration

A form of wireless intrusion is to breach the WLAN authentication mechanism to gain access to the wired network or the wireless devices. Dictionary attacks on the authentication method is a common attack against an access point. The intruder can also attack the wireless client station during its association process with an access point. For example, a faked access point attack on an unsuspicious wireless client may fool the client into associating with faked access point. This attack allows the intruder to gain network access to the wireless station and potentially hack into its file system. The intruder can then use the station to access the wired enterprise network.

These security threats can be prevented if mutual authentication and strong encryption techniques are used. The Cisco Adaptive Wireless IPS looks for weak security deployment practices as well as any penetration attack attempts. The Cisco Adaptive Wireless IPS ensures a strong wireless security umbrella by validating the best security policy implementation as well as detecting intrusion attempts. If such vulnerabilities or attack attempts are detected, the Cisco Adaptive Wireless IPS generates alarms to bring these intrusion attempts to the administrator notice.

This section describes the security penetration attacks and contains the following topics:

- ASLEAP Tool Detected, page 18-28
- AirDrop Session Detected, page 18-29
- AirPwn, page 18-30
- Airsnarf Attack, page 18-30
- Bad EAP-TLS Frames, page 18-32
- Beacon Fuzzed Frame Detected, page 18-32
- Brute Force Hidden SSID, page 18-32
- Chopchop Attack, page 18-33
- DHCP Starvation Attack Detected, page 18-33
- Day-0 Attack by WLAN Performance Anomaly, page 18-35
- Day-0 Attack by WLAN Security Anomaly, page 18-36
- Day-0 Attack by Device Performance Anomaly, page 18-37
- Day-0 Attack by Device Security Anomaly, page 18-39
- Device Broadcasting XSS SSID, page 18-40
- Device Probing for APs, page 18-40
- Dictionary Attack on EAP Methods, page 18-42
- EAP Attack Against 802.1x Authentication, page 18-43
- Fake Access Points Detected, page 18-43
- Fake DHCP Server Detected, page 18-44
- Fast WEP Crack Tool Detected, page 18-44
- Fragmentation Attack, page 18-45
- HT_Intolerant Degradation of Service, page 18-47
- Honey Pot AP Detected, page 18-56
- Hot-Spotter Tool Detected, page 18-48
- Identical Send and Receive Address, page 18-47
ASLEAP Tool Detected

Alarm Description and Possible Causes

WLAN devices using static WEP key for encryption are vulnerable to the WEP key cracking attack (See Weaknesses in the Key Scheduling Algorithm of RC4-I by Scott Fluhrer, Itsik Mantin, and Adi Shamir for more information).

Cisco Systems introduced LEAP (Lightweight Extensible Authentication Protocol) to leverage the existing 802.1x framework to avoid such WEP key attacks. The Cisco LEAP solution provides mutual authentication, dynamic per session and per user keys, and configurable WEP session key time out. The LEAP solution was considered a stable security solution and is easy to configure.

There are hacking tools that compromise wireless LAN networks running LEAP by using off-line dictionary attacks to break LEAP passwords. After detecting WLAN networks that use LEAP, this tool de-authenticates users which forces them to reconnect and provide their username and password credentials. The hacker captures packets of legitimate users trying to re-access the network. The attacker can then analyze the traffic off-line and guess the password by testing values from a dictionary.

The main features of the ASLEAP tool include:

- Reading live from any wireless interface in RFMON mode with libpcap.
- Monitoring a single channel or performing channel hopping to look for target networks running LEAP.
- Actively de authenticating users on LEAP networks, forcing them to reauthenticate. This allows quick LEAP password captures.
• Only de-authenticating users who have not already been seen rather than users who are not running LEAP.
• Reading from stored libpcap files.
• Using a dynamic database table and index to allow quick lookups on large files. This reduces the worst-case search time to .0015% as opposed to lookups in a flat file.
• Writing only the LEAP exchange information to a libpcap file.

This could be used to capture LEAP credentials with a device short on disk space (like an iPaq); the LEAP credentials are then stored in the libpcap file on a system with more storage resources to mount the dictionary attack.

The source and Win32 binary distribution for the tool are available at http://asleap.sourceforge.net.

Cisco Systems has developed the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) protocol which stops these dictionary attacks. EAP-FAST helps prevent man-in-the-middle attacks, dictionary attacks, and packet and authentication forgery attacks. In EAP-FAST, a tunnel is created between the client and the server using a PAC (Protected Access Credential) to authenticate each other. After the tunnel establishment process, the client is then authenticated using the user-name and password credentials.

Some advantages of EAP-FAST include:
• It is not proprietary.
• It is compliant with the IEEE 802.11i standard.
• It supports TKIP and WPA.
• It does not use certificates and avoids complex PKI infrastructures.
• It supports multiple Operating Systems on PCs and Pocket PCs.

**wIPS Solution**

The Cisco Adaptive Wireless IPS detects the deauthentication signature of the ASLEAP tool. When detected, the server alerts the wireless administrator. The user of the attacked station should reset the password. The best solution to counter the ASLEAP tool is to replace LEAP with EAP-FAST in the corporate WLAN environment.

Prime Infrastructure also provides automated security vulnerability scanning that proactively reports any access points configured to utilize weak encryption or authentication. For more information on automated security vulnerability scanning, see the Cisco Prime Infrastructure online help.

**AirDrop Session Detected**

**Alarm Description and Possible Causes**

Starting with Apple OSX Lion, Apple has a new feature called AirDrop. This new feature is supported on "newer" MacBook, MacBook Pro and iMac. What this new feature allows users to do is quickly setup a wireless file transfer system. To achieve this, both of the users that want to share files need to open their finder and click on the AirDrop link. Once both of the systems are in range of each other and the link is setup, the users will see the other user's login icon in the AirDrop window. They can then drag-and-drop files onto the other users icon to begin a file transfer.

This could potentially create a security risk due to unauthorized Peer-to-Peer networks being dynamically created in your WLAN environment. File sharing is also a concern here.
**AirPwn**

**Alarm Description and Possible Causes**

AirPwn is a framework for 802.11 packet injection. Airpwn listens to incoming wireless packets, and if the data matches a pattern specified in the config files, custom content is injected (spoofed) from the wireless access point. Airpwn utilizes the inherent delay when a client sends a request to the internet. Since the Airpwn attacker is closer, it will be able to quickly respond. As an example, the hacker might replace all images on a website that the visitor is trying to view, showing only what the hacker wants the visitor to see.

Airpwn only works on open wireless networks and WEP encrypted networks when the attacker knows the WEP key.

**wIPS Solution**

Cisco Enterprise monitors the wireless network for potential traffic that is consistent with an Airpwn attack against Open or WEP decrypted Access Points and notifies the WLAN administrator. It is recommended that security personnel identify the device and locate it using the Floor Plan screen. The attacking station should be removed from the wireless environment as soon as possible.

**Airsnarf Attack**

**Alarm Description and Possible Causes**

A hotspot is any location where Wi-Fi network access is made available for the general public. Hotspots are found in airports, hotels, coffee shops, and other places where business people tend to congregate. They are important network access services for business travelers.

Customers are able to connect to the legitimate access point and receive service using a wireless-enabled laptop or handheld. Most hotspots do not require the user to have any advanced authentication mechanism to connect to the access point other than popping up a web page for the user to log in. The criterion for entry is dependent only on whether or not the subscriber has paid the subscription fees. In a wireless hotspot environment, no one should be trusted. Due to current security concerns, some WLAN hotspot vendors are using 802.1x or higher authentication mechanisms to validate the identity of the user. (see Figure 18-18)
The 4 components of a basic hotspot network include:

- **Hotspot Subscribers**—Valid users with a wireless-enabled laptop or handheld and valid login for accessing the hotspot network.

- **WLAN Access Points**—Can be SOHO gateways or enterprise level access points depending upon the hotspot implementation.

- **Hotspot Controllers**—Deals with user authentication, gathering billing information, tracking usage time, filtering functions, and so on. This can be an independent machine or incorporated in the access point itself.

- **Authentication Server**—Contains the login credentials for the subscribers. Most hotspot controllers verify subscribers credentials with the authentication server.

Airsnarf is a wireless access point setup utility that shows how a hacker can steal username and password credentials from public wireless hotspots.

Airsnarf, a shell script-based tool, creates a hotspot complete with a captive portal where the users enter their login information. Important values such as local network information, gateway IP address, and SSID can be configured within the airsnarf configuration file. This tool initially broadcasts a very strong signal that disassociates the hotspot wireless clients from the authorized access point connected to the Internet. The wireless clients assume that they are temporarily disconnected from the Internet due to some unknown issue and they try to log in again. Wireless clients that associate to the Airsnarf access point receive the IP address, DNS address, and gateway IP address from the rogue Airsnarf access point instead of the legitimate access point installed by the hotspot operator. A web page requests a username and password and the DNS queries are resolved by the rogue Airsnarf access point. The username and password entered are collected by the hacker.

The username and password can be used in any other hotspot location of the same provider anywhere in the nation without the user realizing the misuse. The only case where it could have lesser impact is if the hotspot user is connected using a pay-per-minute usage scheme.

The Airsnarf tool can also penetrate the laptop clients that are unknowingly connected to the Airsnarf access point. The AirSnarf tool can be downloaded by hackers from:

http://airsnarf.shmoo.com/
**Intrusion Detection—Security Penetration**

**Chapter 18      wIPS Policy Alarm Encyclopedia**

**Bad EAP-TLS Frames**

**Alarm Description and Possible Causes**

Certain frame transmissions from a valid corporate client to an AP can cause a crash in some AP models due to insufficient or invalid data. A wireless attacker can take advantage of this vulnerability by transmitting the defective frames in order to bring down a corporate AP. By sending EAP-TLS packets with flags set to 'c0' and no TLS message length or data, APs from some vendors can be rendered inoperable until they are rebooted. During this reboot process, attackers may have a brief opportunity to gain access to the corporate network, resulting in a potential security leak.

**wIPS Solution**

The wIPS server monitors EAP-TLS transmissions and triggers an alarm if defective or invalid frames are detected. Although this issue may not always represent a wireless attack, it is an issue that should be remedied in order to maintain the health of the overall wireless deployment.

**Beacon Fuzzed Frame Detected**

**Alarm Description and Possible Causes**

802.11 Fuzzing is the process of introducing invalid, unexpected or random data into the 802.11 frames and then replaying those modified frames into the air. This can cause unexpected behavior to the destination device including driver crashes, operating system crashes and stack based overflows which would allow execution of arbitrary code on the affected system. The CVE website (http://cve.mitre.org/index.html) has numerous reported entries for fuzzing based vulnerabilities on 802.11 frames.

The system inspects each beacon frame looking for signs of fuzzing activity. Most common forms of beacon fuzzing involve expanding the SSID field beyond the limit of 32 bytes and changing the supported data rates to invalid rates. The system looks for these anomalies and will generate the Beacon Fuzzing alarm when the field values are beyond the 802.11 specification.

**wIPS Solution**

The system monitors the wireless network for traffic consistent with Beacon Fuzzing. It is recommended to locate the device and take it offline.

**Brute Force Hidden SSID**

**Alarm Description and Possible Causes**

A common practice amongst WLAN Administrators is to disable broadcasting of the SSID for an Access Point. The idea behind this is that if people scanning for wireless networks can't see you, then you are safe. Basically you would need to know the SSID in order to connect to that wireless network. This protects your wireless network from casual drive by users who don't have the tools to extract the SSID from hidden networks. But hackers are a different story. They have the tools, the time and energy to
extract the SSID from hidden networks. There are many tools to perform this type of snooping. If a hidden SSID is not found through normal methods, hackers can use a brute force method using the tool mdk3. With the tool mdk3, they can perform a Dictionary attack or a word list attack on the hidden network to extract the SSID.

**wIPS Solution**

Cisco Enterprise monitors the wireless network for potential traffic that is consistent with a brute force attack against a hidden SSID and notifies the WLAN administrator. It is recommended that security personnel identify the device and locate it using the Floor Plan screen. The attacking station should be removed from the wireless environment as soon as possible.

**DHCP Starvation Attack Detected**

**Alarm Description and Possible Causes**

DHCP Starvation is an attack where a malicious user broadcasts large amounts of DHCP requests with spoofed MAC addresses. If enough DHCP request frames flood the network, the attacker could use up all of the remaining DHCP IP addresses that are available for valid users. This would create a DoS condition on the network. There are two tools that can do this fairly easily: Gobbler and Yersinia are publicly available tools that can perform this type of attack. This type of attack is especially harmful on guest networks or hotspot networks where the user is allowed to get an IP address before the authentication happens.

Mitigation options for this type of attack can be handled at the switch level. For Cisco IOS switches, enable DHCP Snooping. For Cisco CatOS, enable port security.

**wIPS Solution**

The system monitors the wireless network for traffic consistent with a DHCP Starvation attack. Cisco recommends that you locate the user running the attack or implement tighter switch security.

**Chopchop Attack**

**Alarm Description and Possible Causes**

It is well publicized that a WLAN device using a static WEP key for encryption is vulnerable to various WEP cracking attacks. Refer to *Weaknesses in the Key Scheduling Algorithm of RC4 - I* by Scott Fluhrer, Itsik Mantin, and Adi Shamir for more information. See Figure 18-19 for the WEP Encipher Process Block.
A cracked WEP secret key offers no encryption protection for data to be transmitted, leading to compromised data privacy. The WEP key, which is in most cases 64-bit or 128-bit (some vendors also offer 152-bit encryption), is a secret key specified by the user, linked with the 24-bit IV (Initialization Vector). The chopchop tool was written for the Linux operating system by Korek to exploit a weakness in WEP and decrypt the WEP data packet. However, the chopchop tool only reveals the plaintext. The attacker uses the packet capture file of a previously injected packet during the initial phase and decrypts the packet by retransmitting modified packets to the attacked network. When the attack is completed, the chopchop tool produces an unencrypted packet capture file and another file with PRGA (Pseudo Random Generation Algorithm) information determined during the decryption process. The PGRA is then XORed with the cyphertext to obtain the plaintext. See Figure 18-20 for commands used to initiate a Chopchop attack.

Access points that drop data packets shorter than 60 bytes may not be vulnerable to this kind of attack. If an access point drops packets shorter than 42 bytes, aireplay tries to guess the rest of the missing data, as far as the headers are predictable. If an IP packet is captured, it additionally checks if the checksum of the header is correct after guessing the missing parts of it. This attack requires at least one WEP data packet. A chopchop attack also works against dynamic WEP configurations. The Cisco Adaptive Wireless IPS is able to detect potential attacks using the chopchop tool.

**wIPS Solution**

The Cisco Adaptive Wireless IPS activates an alert when a potential chopchop attack is in progress. WEP should not be used in the corporate environment and appropriate measures should be taken to avoid any security holes in the network and upgrade the wireless network infrastructure and devices to use the more secure IEEE 802.11i standard.
Day-0 Attack by WLAN Performance Anomaly

Alarm Description and Possible Causes

WLAN performance efficiency is constantly challenged by the dynamics of the RF environment and the mobility of client devices. A closely monitored and well-tuned WLAN system can achieve a higher throughput than a poorly managed one. Radio Resource Management (RRM) built into the Cisco Unified Wireless Network monitors and dynamically corrects performance issues found in the RF environment. Further performance anomaly monitoring may be done via the Wireless IPS system. For more information on RRM, see the Cisco Prime Infrastructure online help.

The Cisco Adaptive Wireless IPS ensures WLAN performance and efficiency by monitoring the WLAN on a continued basis and alerting the wireless administrator on early warning signs for trouble. Performance alarms are generated and classified in the following categories in the event of any performance degradation:

- **RF Management**—The Cisco Adaptive Wireless IPS monitors the physical RF environment that is dynamic and very often the source of WLAN performance problems. While monitoring on the RF environment, the server characterizes the following WLAN fundamentals and reports problems accordingly:
  - Channel interference and channel allocation problems
  - Channel noise and non-802.11 signals
  - WLAN RF service under-coverage area
  - Classic RF hidden-node syndrome

- **Problematic traffic pattern**—Many WLAN performance problems including the RF multipath problem manifest themselves in the MAC layer protocol transactions and statistics. By tracking and analyzing the wireless traffic, the Cisco Adaptive Wireless IPS is able to spot performance inefficiencies and degradations early on. In many cases, the Cisco Adaptive Wireless IPS can determine the cause of the detected performance problem and suggest counter measures. The Cisco Adaptive Wireless IPS tracks MAC layer protocol characteristics including the following:
  - Frame CRC error
  - Frame re-transmission
  - Frame speed (1, 2, 5.5, 11, ... Mbps) usage and distribution
  - Layer 2 frame fragmentation
  - Access point and station association/re-association/dis-association relationship
  - Roaming hand-off

- **Channel or device overloaded**—The Cisco Adaptive Wireless IPS monitors and tracks the load to ensure smooth operation with both channel bandwidth limitation or the WLAN device resource capacity. In the event of unsatisfactory performance by the WLAN due to under-provisioning or over-growth, the Cisco Adaptive Wireless IPS raises alarms and offers specific details. RF has no boundaries that could lead to your WLAN channel utilization to increase significantly even when your neighbor installs new WLAN devices in an adjoining channel. The Cisco Adaptive Wireless IPS monitors your WLAN to ensure proper bandwidth and resource provisioning.

- **Deployment and operation error**—The Cisco Adaptive Wireless IPS scans the airwaves for configuration and operation errors. The following specific areas are continuously monitored:
  - Inconsistent configuration among access points servicing the same SSID
  - Configuration against the principles of best practice
Intrusion Detection—Security Penetration

- Connection problems caused by client/access point mismatch configuration
- WLAN infrastructure device down or reset
- Flaws in WLAN device implementation

- IEEE 802.11e and VoWLAN issues—The IEEE 802.11e standard adds QoS (quality of service) features and multimedia support to the existing 802.11 a/b/g wireless standard. This is done while maintaining full backward compatibility with these standards. The QoS feature is critical to voice and video applications. Wireless LAN has limited bandwidth and high overheads as compared to the traditional wired Ethernet. The throughput is reduced for a variety of reasons including the RTS/CTS mechanism, packet fragmentation, packet retransmission, acknowledgements, and collisions.

wIPS Solution

The Cisco Adaptive Wireless IPS has detected a single Performance Intrusion policy violation on a large number of devices in the wireless network. Either the number of devices violating the specific policy in the time period specified are observed or there is a sudden percentage increase in the number of devices as specified in the threshold settings for the alarm. Depending on the Performance Intrusion violation, it is suggested that the devices be monitored and located to carry out further analysis.

For example:

- If the AP overloaded by stations alarm is generated by a large number of devices, it may indicate that a hacker has generated thousands of stations and forcing them to associate to the corporate access point. If this occurs, legitimate corporate clients cannot connect to the access point.
- Excessive frame retries on the wireless devices may indicate such things as noise, interference, packet collisions, multipath, and hidden node syndrome.

Day-0 Attack by WLAN Security Anomaly

Alarm Description and Possible Causes

The addition of WLANs in the corporate environment introduces a whole new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue access points installed by employees for their personal use usually do not adhere to the corporate security policy. A rogue access point can put the entire corporate network at risk of outside penetration and attack. Besides rogue access points, there are many other wireless security vulnerabilities which compromise the wireless network such as misconfigured and unconfigured access points. There can also be DoS (denial of service) attacks from various sources against the corporate network.

Prime Infrastructure provides automated security vulnerability assessment within the wireless infrastructure that proactively reports any security vulnerabilities or mis-configurations. Further assessment may be done over-the-air via the Wireless IPS system. With the comprehensive suite of security monitoring technologies, the Cisco Adaptive Wireless IPS alerts the user on more than 100 different threat conditions in the following categories:

- User authentication and traffic encryption (Static WEP encryption, VPN, Fortress, Cranite, 802.11i and 802.1x)—Common security violations in this category (authentication and encryption) include mis-configurations, out-of-date software or firmware, and suboptimal choice of corporate security policy.
- Rogue, monitored, and ad-hoc mode devices—Rogue devices must be detected and removed immediately to protect the integrity of the wireless and wired enterprise network.
Chapter 18      wIPS Policy Alarm Encyclopedia

Intrusion Detection—Security Penetration

- Configuration vulnerabilities—Implementing a strong deployment policy is fundamental to a secure WLAN. However, enforcing the policy requires constant monitoring to catch violations caused by mis-configuration or equipment vendor implementation errors. With the increased trend on laptops with built-in Wi-Fi capabilities, the complexity of WLAN configuration extends beyond access points to the user laptops. WLAN device configuration management products can make the configuration process easier, but the need for validation persists especially in laptops with built-in but unused and unconfigured Wi-Fi.

- Intrusion detection on security penetration—A form of wireless intrusion includes breaching the WLAN authentication mechanism to gain access to the wired network or the wireless devices. A Dictionary attack on the authentication method is a very common attack against an access point. The intruder can also attack the wireless client station during its association process with an access point. For example, a faked AP attack on an unsuspicious wireless client may fool the client into associating with a fake access point. This attack allows the intruder to gain network access to the wireless station and potentially hack into its file system. The intruder can then use the station to access the wired enterprise network.

- Intrusion detection on denial of service attacks—Wireless DoS (denial of service) attacks aim to disrupt wireless services by taking advantage of various vulnerabilities of WLAN at layer one and two. DoS attacks may target the physical RF environment, access points, client stations, or the back-end authentication RADIUS servers. For example, RF jamming attack with high power directional antenna from a distance can be carried out from the outside of your office building. Attack tools used by intruders leverage hacking techniques such as spoofed 802.11 management frames, spoofed 802.1x authentication frames, or simply using the brute force packet flooding method.

**wIPS Solution**

The Cisco Adaptive Wireless IPS has detected a single Security IDS/IPS policy violation on a large number of devices in the wireless network. Either the number of devices violating the specific policy in the time period specified are observed or there is a sudden percentage increase in the number of devices as specified in the threshold settings for the alarm. Depending on the Security IDS/IPS violation, it is suggested that the devices are monitored and located to carry out further analysis to check if they are compromising the Enterprise wireless network in any way (attack or vulnerability). If this is an increase in the number of rogue devices, it may indicate an attack against the network. The WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find it.

If there is a sudden increase in the number of client devices with encryption disabled, it may be necessary to revisit the Corporate Security Policy and enforce users to use the highest level of encryption and authentication according to the policy rules.

**Day-0 Attack by Device Performance Anomaly**

**Alarm Description and Possible Causes**

WLAN performance efficiency is constantly challenged by the dynamics of the RF environment and the mobility of client devices. A closely monitored and well-tuned WLAN system can achieve a higher throughput than a poorly managed one. Radio Resource Management built into the Cisco Unified Wireless Network monitors and dynamically corrects performance issues found in the RF environment. Further performance anomaly monitoring may be done via the Wireless IPS system. For more information on RRM, see the Cisco Prime Infrastructure online help.
Chapter 18      wIPS Policy Alarm Encyclopedia

Intrusion Detection—Security Penetration

The Cisco Adaptive Wireless IPS ensures WLAN performance and efficiency by monitoring the WLAN on a continued basis and alerting the wireless administrator on early warning signs for trouble. Performance alarms are generated and classified in the following categories in the event of any performance degradation:

- **RF Management**—The Cisco Adaptive Wireless IPS monitors the physical RF environment that is dynamic and very often the source of WLAN performance problems. While monitoring on the RF environment, the server characterizes the following WLAN fundamentals and reports problems accordingly:
  - Channel interference and channel allocation problems
  - Channel noise and non-802.11 signals
  - WLAN RF service under-coverage area
  - Classic RF hidden-node syndrome

- **Problematic traffic pattern**—Many WLAN performance problems including the RF multipath problem manifest themselves in the MAC layer protocol transactions and statistics. By tracking and analyzing the wireless traffic, the Cisco Adaptive Wireless IPS is able to spot performance inefficiencies and degradations early on. In many cases, the Cisco Adaptive Wireless IPS can determine the cause of the detected performance problem and suggest counter measures. The Cisco Adaptive Wireless IPS tracks MAC layer protocol characteristics including the following:
  - Frame CRC error
  - Frame re-transmission
  - Frame speed (1, 2, 5.5, 11, ... Mbps) usage and distribution
  - Layer 2 frame fragmentation
  - Access point and station association/re-association/dis-association relationship
  - Roaming hand-off

- **Channel or device overloaded**—The Cisco Adaptive Wireless IPS monitors and tracks the load to ensure smooth operation with both channel bandwidth limitation or the WLAN device resource capacity. In the event of unsatisfactory performance by the WLAN due to under-provisioning or over-growth, the Cisco Adaptive Wireless IPS raises alarms and offers specific details. RF has no boundaries that could lead to your WLAN channel utilization to increase significantly even when your neighbor installs new WLAN devices in an adjoining channel. The Cisco Adaptive Wireless IPS monitors your WLAN to ensure proper bandwidth and resource provisioning.

- **Deployment and operation error**—The Cisco Adaptive Wireless IPS scans the airwaves for configuration and operation errors. The following specific areas are continuously monitored:
  - Inconsistent configuration among access points servicing the same SSID
  - Configuration against the principles of best practice
  - Connection problems caused by client/access point mismatch configuration
  - WLAN infrastructure device down or reset
  - Flaws in WLAN device implementation

- **IEEE 802.11e and VoWLAN issues**—The IEEE 802.11e standard adds QoS (quality of service) features and multimedia support to the existing 802.11 a/b/g wireless standard. This is done while maintaining full backward compatibility with these standards. The QoS feature is critical to voice and video applications. Wireless LAN has limited bandwidth and high overheads as compared to the traditional wired Ethernet. The throughput is reduced for a variety of reasons including the RTS/CTS mechanism, packet fragmentation, packet retransmission, acknowledgements, and collisions.
To maximize the power of the Cisco Adaptive Wireless IPS, performance alarms can be customized to best match your WLAN deployment specification. For example, if your WLAN is designed for all users to use 5.5 and 11 Mbps speed only, customize the threshold for performance alarm 'Low speed tx rate exceeded' to reflect such an expectation.

**wIPS Solution**

The Cisco Adaptive Wireless IPS detects a device violating a large number of performance intrusion policies. This device has either generated a large number of performance intrusion violations in the time period specified or there is a sudden percentage increase as specified in the threshold settings for the various alarms. It is suggested that the device is monitored and located to carry out further analysis to check if this device is causing any issues in the overall performance of the network.

For example, if there is a device which has caused an increase in the number of "access points overloaded by stations" and "access points overloaded by utilization" alarms, this could indicate that the access point cannot handle the stations. The administrator may need to reconsider re-deployment of the access points.

**Day-0 Attack by Device Security Anomaly**

**Alarm Description and Possible Causes**

The addition of WLANs in the corporate environment introduces a new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue access points installed by employees for their personal use usually do not adhere to the corporate security policy. Rogue access points can put the entire corporate network at risk for outside penetration and attack. Besides rogue access points, there are many other wireless security vulnerabilities which compromise the wireless network such as misconfigured and unconfigured access points. There can also be DoS attacks from various sources against the corporate network.

Prime Infrastructure provides automated security vulnerability assessment within the wireless infrastructure that proactively reports any security vulnerabilities or mis-configurations. Further assessment may be done over-the-air via the Wireless IPS system. With the comprehensive suite of security monitoring technologies, the Cisco Adaptive Wireless IPS alerts the user on more than 100 different threat conditions in the following categories:

- **User authentication and traffic encryption (Static WEP encryption, VPN, Fortress, Cranite, 802.11i and 802.1x)**—Common security violations in this category (authentication and encryption) include mis-configurations, out-of-date software or firmware, and suboptimal choice of corporate security policy.
- **Rogue, monitored, and ad-hoc mode devices**—Rogue devices must be detected and removed immediately to protect the integrity of the wireless and wired enterprise network.
- **Configuration vulnerabilities**—Implementing a strong deployment policy is fundamental to a secure WLAN. However, enforcing the policy requires constant monitoring to catch violations caused by mis-configuration or equipment vendor implementation errors. With the increased trend on laptops with built-in Wi-Fi capabilities, the complexity of WLAN configuration extends beyond access points to the user laptops. WLAN device configuration management products can make the configuration process easier, but the need for validation persists especially in laptops with built-in but unused and unconfigured Wi-Fi.
- **Intrusion detection on security penetration**—A form of wireless intrusion includes breaching the WLAN authentication mechanism to gain access to the wired network or the wireless devices. A Dictionary attack on the authentication method is a very common attack against an access point. The intruder can also attack the wireless client station during its association process with an access point. For example, a faked AP attack on an unsuspicous wireless client may fool the client into associating
Intrusion detection with a fake access point. This attack allows the intruder to gain network access to the wireless station and potentially hack into its file system. The intruder can then use the station to access the wired enterprise network.

- Intrusion detection on DoS attacks—Wireless DoS (denial of service) attacks aim to disrupt wireless services by taking advantage of various vulnerabilities of WLAN at layer one and two. DoS attacks may target the physical RF environment, access points, client stations, or the back-end authentication RADIUS servers. For example, RF jamming attack with high power directional antenna from a distance can be carried out from the outside of your office building. Attack tools used by intruders leverage hacking techniques such as spoofed 802.11 management frames, spoofed 802.1x authentication frames, or simply using the brute force packet flooding method.

**wIPS Solution**

The Cisco Adaptive Wireless IPS detects a device violating a large number of Security IDS/IPS policies. This device has either generated a number of Security IDS/IPS violations in the time period specified or there is a sudden percentage increase as specified in the threshold settings for the various alarms. The device should be monitored and located to carry out further analysis to check if this device is compromising the Enterprise Wireless Network in any way (attack or vulnerability). If this is a rogue device, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find it.

### Device Broadcasting XSS SSID

**Alarm Description and Possible Causes**

Cross-Site scripting vulnerabilities are well known and consist of publicized attacks that target web applications to gain access to the underlying server or the web application itself. It does this by injecting a client-side script into web pages viewed by the user.

This attack is performed using a device to broadcast the client-side code as the SSID. Once a WLAN monitoring system picks up the malicious SSID and records it, if the system is web based and there are Cross-Site Scripting vulnerabilities, then that system will be exploited once the device with the malicious SSID is clicked.

**wIPS Solution**

Cisco Enterprise monitors the wireless network for Access Points and Ad-hoc devices broadcasting malicious Cross-site scripting (XSS) traffic. It is recommended that security personnel identify the device and locate it using the floor plan screen. The device should then be removed from the wireless environment as soon as possible.

### Device Probing for APs

Some commonly used scan tools include: NetStumbler (newer versions), MiniStumbler (newer versions), MACStumbler, WaveStumbler, PrismStumbler, dStumbler, iStumbler, Aerosol, Boingo Scans, WiNc, AP Hopper, NetChaser, Microsoft Windows XP scans.

**Alarm Description and Possible Causes**

The Cisco Adaptive Wireless IPS detects wireless devices probing the WLAN and attempting association (such as association request for an access point with any SSID).
Such devices could pose potential security threats in one of the following ways:

- War-driving, WiLDing (Wireless LAN Discovery), war-chalking, war-walking, war cycling, war-lightailing, war-busing, and war-flying.
- Legitimate wireless client attempting risky promiscuous association.

War-driving, war-chalking, war-walking, and war-flying activities include:

- War-driving—A wireless hacker uses war-driving tools to discover access points and publishes information such as MAC address, SSID, and security implemented on the Internet with the access points geographical location information.
- War-chalking—War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols (see Figure 18-21).

- War-walking—War-walking is similar to war-driving, but the hacker is on foot instead of a car.
- War-flying—War-flying refers to sniffing for wireless networks from the air. The same equipment is used from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet relay chat sessions from an altitude of 1,500 feet on a war-flying trip.

**Legitimate Wireless Client Attempting Risky Association**

The second potential security threat for this alarm may be more damaging. Some of these alarms could be from legitimate and authorized wireless clients on your WLAN who are attempting to associate with any available access point including your neighbor access point or the more damage-causing rogue access point. This potential security threat can be from a Microsoft Windows XP laptop with a built-in Wi-Fi card or laptops using wireless connectivity tools such as the Boingo client utility and the WiNc client utility. When associated, this client station can be accessed by an intruder leading to a major security breach. Even worse, the client station may bridge the unintended access point with your company wired LAN. Typically, laptops are equipped with built-in Wi-Fi cards and, at the same, are physically attached to your company WLAN for network connectivity. Your wired network is exposed if the Windows bridging service is enabled on that Windows laptop. To be secure, configure all client stations with specific SSIDs to avoid associating with an unintended access point. Also, consider mutual authentication such as 802.1x and various EAP methods.
Intrusion Detection—Security Penetration

Chapter 18  wIPS Policy Alarm Encyclopedia

The Cisco Adaptive Wireless IPS also detects a wireless client station probing the WLAN for an anonymous association such as an association request for an access point with any SSID) using the NetStumbler tool. The device probing for access point alarm is generated when hackers use the latest versions of the NetStumbler tool. For older versions, the NetStumbler detected alarm is triggered.

NetStumbler is the most widely used tool for war-driving and war-chalking. The NetStumbler website (http://www.netstumbler.com/) offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It can run on a machine running Windows 2000, Windows XP, or more recent operating systems. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers like to use MiniStumbler and similar products to search shopping malls and retail stores.

wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure the access points to not broadcast SSIDs. Use the Cisco Adaptive Wireless IPS to determine which access points are broadcasting (announcing) their SSID in the beacons.

Dictionary Attack on EAP Methods

Alarm Description and Possible Causes

EEE 802.1x provides an EAP framework for wired or wireless LAN authentication. An EAP framework allows flexible authentication protocol implementation. Some implementations of 802.1x or WPA use authentication protocols such as LEAP, MD5, OTP (one-time-password), TLS, and TTLS. Some of these authentication protocols are based on the username and password mechanism in which the username is transmitted without encryption and the password is used to answer authentication challenges.

Most password-based authentication algorithms are susceptible to dictionary attacks. During a dictionary attack, an attacker gains the username from the unencrypted 802.1x identifier protocol exchange. The attacker then tries to guess a user password to gain network access by using every word in a dictionary of common passwords or possible combinations of passwords. A dictionary attack relies on a password being a common word, name, or combination of both with a minor modification such as a trailing digit or two.

A dictionary attack can take place actively online, where an attacker repeatedly tries all the possible password combinations. Online dictionary attacks can be prevented using lock-out mechanisms available on the authentication server (RADIUS servers) to lock out the user after a certain number of invalid login attempts. A dictionary attack can also take place offline, where an attacker captures a successful authentication challenge protocol exchange and then tries to match the challenge response with all possible password combinations. Unlike online attacks, offline attacks are not easily detected. Using a strong password policy and periodically expiring user passwords significantly reduces an offline attack tool's success.

wIPS Solution

The Cisco Adaptive Wireless IPS detects online dictionary attacks by tracking 802.1x authentication protocol exchange and the user identifier usages. When a dictionary attack is detected, the alarm message identifies the username and attacking station MAC address.

The Cisco Adaptive Wireless IPS advises switching username and password based authentication methods to encrypted tunnel based authentication methods such as PEAP and EAP-FAST, which are supported by many vendors including Cisco.
**EAP Attack Against 802.1x Authentication**

**Alarm Description and Possible Causes**

IEEE 802.1x provides an Extensible Authentication Protocol (EAP) framework for wired or wireless LAN authentication. An EAP framework allows flexible authentication protocol implementation. Some implementations of 802.1x or WPA use authentication protocols such as LEAP, MD5, OTP (one-time-password), TLS, TTLS, and EAP-FAST. Some of these authentication protocols are based on the username and password mechanism, where the username is transmitted clear without encryption and the password is used to answer authentication challenges.

Most password-based authentication algorithms are susceptible to dictionary attacks. During a dictionary attack, an attacker gains the username from the unencrypted 802.1x identifier protocol exchange. The attacker attempts to guess a user password and gain network access by using every “word” in a dictionary of common passwords or possible combinations of passwords. A dictionary attack relies on the fact that a password is often a common word, name, or combination of words or names with a minor modification such as a trailing digit or two.

Intruders with the legitimate 802.1x user identity and password combination (or valid certificate) can penetrate the 802.1x authentication process without the proper knowledge of the exact EAP-type. The intruder tries different EAP-types such as TLS, TTLS, LEAP, EAP-FAST, or PEAP to successfully log onto the network. This is a trial and error effort because there are only a handful of EAP-types for the intruder to try and manage to get authenticated to the network.

**wIPS Solution**

The Cisco Adaptive Wireless IPS detects an attempt by an intruder to gain access to the network using different 802.1x authentication types. Take appropriate steps to locate the device and remove it from the wireless environment.

**Fake Access Points Detected**

**Alarm Description and Possible Causes**

The Fake AP tool is meant to protect your WLAN acting as a decoy to confuse war-drivers using NetStumbler, Wellenreiter, MiniStumbler, Kismet, and so on. The tool generates beacon frames imitating thousands of counterfeit 802.11b access points. War-drivers encountering a large number of access points cannot identify the real access points deployed by the user. This tool, although very effective in fending off war-drivers, poses other disadvantages such as bandwidth consumption, misleading legitimate client stations, and interference with the WLAN management tools. Running the Fake AP tool in your WLAN is not recommended.

**wIPS Solution**

The administrator should locate the device running the Fake AP tool and remove it from the wireless environment.
Fake DHCP Server Detected

Alarm Description and Possible Causes

Dynamic Host Configuration Protocol (DHCP) is used for assigning dynamic IP addresses to devices on a network.

DHCP address assignment takes place as follows:

Step 1  The client NIC sends out a DHCP discover packet, indicating that it requires a IP address from a DHCP server.

Step 2  The server sends a DHCP offer packet with the IP address.

Step 3  The client NIC sends a DHCP request, informing the DHCP server that it wants to be assigned the IP address sent by the servers offer.

Step 4  The server returns a DHCP ACK, acknowledging that the NIC has sent a request for a specific IP address.

Step 5  The client interface assigns or binds the initially offered IP address from the DHCP server.

The DHCP server should be a dedicated machine and part of the enterprise wired network or it could be a wireless/wired gateway. Other wireless devices can have the DHCP service running innocently or maliciously so as to disrupt the WLAN IP service. Wireless clients that are requesting an IP address from the DHCP server may then connect to these fake DHCP servers to get their IP address because the clients do not have any means to authenticate the server. These fake DHCP servers may give the clients non-functional network configurations or divert all the client's traffic through them. The hackers can then eavesdrop on every packet sent by the client. With the aid of rogue DNS servers, the hacker could also send the users to fake web page logins to get username and password credentials. It could also give out non-functional and non-routable IP addresses to achieve a DoS attack. This sort of attack is generally against a WLAN without encryption such as hotspots or trade show networks.

wIPS Solution

The Cisco Adaptive Wireless IPS detects such wireless STAs running the DHCP service and providing IP addresses to unaware users.

When the client is identified and reported, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the device.

Fast WEP Crack Tool Detected

Alarm Description and Possible Causes

It is well publicized that WLAN devices using static WEP key for encryption are vulnerable to WEP key cracking attack (Refer to Weaknesses in the Key Scheduling Algorithm of RC4 - 1 by Scott Fluhrer, Itsik Mantin, and Adi Shamir). See Figure 18-22 for WEP Enciphement block.
The WEP secret key that has been cracked by any intruder results in no encryption protection, thus leading to compromised data privacy. The WEP key that is in most cases 64-bit or 128-bit (few vendors also offer 152-bit encryption) consists of the secret key specified by the user linked with the 24-bit IV (Initialization Vector). The IV that is determined by the transmitting station can be reused frequently or in consecutive frames, thus increasing the possibility of the secret key to be recovered by wireless intruders.

The most important factor in any attack against the WEP key is the key size. For 64-bit WEP keys, around 150 K unique IVs and for 128-bit WEP keys around 500 k to a million unique IVs should be enough. With insufficient traffic, hackers have created a unique way of generating sufficient traffic to perform such an attack. This is called the replay attack based on arp-request packets. Such packets have a fixed length and can be spotted easily. By capturing one legitimate arp-request packet and resending them repeatedly, the other host responds with encrypted replies, providing new and possibly weak IVs.

**wIPS Solution**

The Cisco Adaptive Wireless IPS alerts on weak WEP implementations and recommends a device firmware upgrade if available from the device vendor to correct the IV usage problem. Ideally, enterprise WLAN networks can protect against WEP vulnerability by using the TKIP (Temporal Key Integrity Protocol) encryption mechanism, which is now supported by most enterprise level wireless equipment. TKIP enabled devices are not subject to any such WEP key attacks.

Prime Infrastructure also provides automated security vulnerability scanning that proactively reports any access points configured to utilize weak encryption or authentication. For more information on automated security vulnerability scanning, see the Cisco Prime Infrastructure online help.

**Fragmentation Attack**

**Alarm Description and Possible Causes**

It is well publicized that a WLAN device using a static WEP key for encryption is vulnerable to various WEP cracking attacks. Refer to *Weaknesses in the Key Scheduling Algorithm of RC4 - I* by Scott Fluhrer, Itsik Mantin, and Adi Shamir for more information. (See Figure 18-23)
A cracked WEP secret key offers no encryption protection for data to be transmitted which leads to compromised data privacy. The WEP key, which is in most cases 64-bit or 128-bit (few vendors also offer 152-bit encryption), is the secret key specified by the user and linked with the 24-bit IV (Initialization Vector).

According to http://www.aircrack-ng.org/doku.php?id=fragmentation&s=fragmentation, the aircrack program obtains a small amount of keying material from the packet and then attempts to send ARP and/or LLC packets with known information to an access point. If the packet gets successfully echoed back by the access point, then a larger amount of keying information can be obtained from the returned packet. This cycle is repeated several times until 1500 bytes (less in some cases) of PRGA are obtained. This attack does not recover the WEP key itself, but merely obtains the PRGA. The PRGA can then be used to generate packets with “packetforge-ng” which can be used for various injection attacks.

The Cisco Adaptive Wireless IPS detects potential fragmentation attacks in progress against the Wi-Fi network.

**wIPS Solution**

The Cisco Adaptive Wireless IPS alerts on detecting a potential fragmentation attack in progress, and recommends that WEP not be used in the corporate environment and that appropriate measures be taken to avoid any security holes in the network and upgrade the wireless network infrastructure and devices to use the more secure IEEE 802.11i standard.
**HT_Intolerant Degradation of Service**

**Alarm Description and Possible Causes**

While 802.11n deployments provide the potential for dramatically increased wireless range and speed over legacy implementations, these benefits can be easily lost or offset if a single legacy device is introduced to the network. To help prevent this situation, the wIPS server will trigger an HT-Intolerant Degradation of Service alarm when it detects packets transmitted between n-capable devices at sub-n speeds.

**wIPS Solution**

Although this degradation of service doesn't necessarily indicate a wireless attack, the reduction in transmit speed can have a negative affect on network performance. As such, users should identify and eliminate the legacy device in order to maintain an optimal 802.11n deployment.

**Identical Send and Receive Address**

**Alarm Description and Possible Causes**

In order to inhibit wireless activity in a corporate network, attackers will often modify wireless packets to emulate various different characteristics, including changes to the packets' Source and Destination MAC information. In cases where these fields are identical, the Identical Send and Receive Address alarm will be triggered in order to alert IT personnel of a potential attack.

**wIPS Solution**

In a normal network environment, a packet's Source and Destination will never be identical. As such, the enterprise administrators should take immediate steps to locate the root cause of the modified packets.

**Improper Broadcast Frames**

**Alarm Description and Possible Causes**

Standard 802.11 deployments allow for certain frames to be transmitted to individual destinations (also known as unicast frames, such as an ACK) and other frames to be 'broadcast' to all recipients in the wireless deployment. In general, these two categories should not overlap, e.g., an Association Request frame should not be sent out as a broadcast to all listening devices. In this scenario, the wIPS server will trigger an Improper Broadcast Frames alarm to alert staff of a potential problem.

**wIPS Solution**

An Improper Broadcast Frames alarm is indicative of a potential attack which, if left unchecked, could impede network performance. Steps should be taken to locate the source of the invalid frames and eliminate it from the wireless environment as soon as possible.
Karma Tool Detected

Alarm Description and Possible Causes

The Karma tool allows a wireless attacker to configure a client as a soft AP that will respond to any probe request detected. This implementation is designed to respond to queries from stations configured to connect to multiple different networks, e.g., SSID "Corporate" for work and SSID "Home" for home use. In this example, the soft AP may be configured to respond to the probe for "Home" when the client is at work. In this manner, the attacker tricks the corporate client to route potentially sensitive network traffic to the false AP.

wIPS Solution

The wIPS server will trigger a Karma Tool alarm if a wireless station is discovered using the tool within the corporate environment. Users should locate the attacking device and eliminate it immediately.

Hot-Spotter Tool Detected

Alarm Description and Possible Causes

A hotspot is any location where Wi-Fi network access available for the general public. Hotspots are often found in airports, hotels, coffee shops, and other places where business people tend to congregate. It is currently one of the most important network access service for business travelers. The customer requires a wireless-enabled laptop or handheld to connect to the legitimate access point and to receive service. Most hotspots do not require the user to have an advanced authentication mechanism to connect to the access point, other than using a web page to log in. The criterion for entry is only dependent on whether or not the subscriber has paid subscription fees. In a wireless hotspot environment, no one should trust anyone else. Due to current security concerns, some WLAN hotspot vendors are using 802.1x or higher authentication mechanisms to validate the identity of the user. (see Figure 18-25)
Figure 18-25  Basic Components of a WLAN Hotspot Network

The four components of a basic hotspot network are:

- **Hotspot Subscribers**—Valid users with a wireless enabled laptop or handheld and valid login for accessing the hotspot network.

- **WLAN Access Points**—SOHO gateways or enterprise level access points depending upon the hotspot implementation.

- **Hotspot Controllers**—Deals with user authentication, gathering billing information, tracking usage time, filtering functions, and so on. This can be an independent machine or can be incorporated in the access point itself.

- **Authentication Server**—Contains the login credentials for the subscribers. In most cases, hotspot controllers verify subscriber credentials with the authentication server.

"Hotspotter" automates a method of penetration against wireless clients, independent of the encryption mechanism used. Using the Hotspotter tool, the intruder can passively monitor the wireless network for probe request frames to identify the SSIDs of the networks of the Windows XP clients.

After it acquires the preferred network information, the intruder compares the network name (SSID) to a supplied list of commonly used hotspot network names. When a match is found, the Hotspotter client acts as an access point. The clients then authenticate and associate unknowingly to this fake access point.

When the client gets associated, the Hotspotter tool can be configured to run a command such as a script to kick off a DHCP daemon and other scanning against the new victim.

Clients are also susceptible to this kind of attack when they are operating in different environments (home and office) while they are still configured to include the hotspot SSID in the Windows XP wireless connection settings. The clients send out probe requests using that SSID and make themselves vulnerable to the tool.
When the rogue access point is identified and reported by the Cisco Adaptive Wireless IPS, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the rogue device.

**Malformed 802.11 Packets Detected**

**Alarm Description and Possible Causes**

Hackers using illegal packets (malformed non-standard 802.11 frames) can force wireless devices to behave in an unusual manner. Illegal packets can cause the firmware of a few vendor wireless NICs to crash.

Examples of such vulnerability includes NULL probe response frame (null SSID in the probe response frame) and oversized information elements in the management frames. These ill-formed frames can be broadcasted to cause multiple wireless clients to crash.

**wIPS Solution**

The Cisco Adaptive Wireless IPS can detect these illegal packets that may cause some NICs to lock up and crash. Also, wireless clients experiencing blue screen or lock-up problem during the attack period should consider upgrading the WLAN NIC driver or the firmware.

When the client is identified and reported by the Cisco Adaptive Wireless IPS, the WLAN administrator may use the device locator to locate it.

**Man-in-the-Middle Attack**

**Alarm Description and Possible Causes**

A Man-in-the-middle (MITM) attack is one of the most common 802.11 attacks that can lead to confidential corporate and private information being leaked to hackers. In a MITM attack, the hacker can use a 802.11 wireless analyzer and monitor 802.11 frames sent over the WLAN. By capturing the wireless frames during the association phase, the hacker gets IP and MAC address information about the wireless client card and access point, association ID for the client, and the SSID of the wireless network. (see Figure 18-26)
A common MITM attack involves the hacker sending spoofed disassociation or deauthentication frames. The hacker station then spoofs the MAC address of the client to continue an association with the access point. At the same time, the hacker sets up a spoofed access point in another channel to keep the client associated. All traffic between the valid client and access point then passes through the hacker station.

One of the most commonly used MITM attack tools is Monkey-Jack.

**wIPS Solution**

The Cisco Adaptive Wireless IPS recommends the use of strong encryption and authentication mechanisms to thwart any MITM attacks by hackers. One way to avoid such an attack is to prevent MAC address spoofing by using MAC address exclusion lists and monitoring the RF channel environment.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MITM attacks.

**Monitored Device Detected**

**Alarm Description and Possible Causes**

There are some cases in which the access points and STAs activity must be continuously monitored:

- Malicious intruders attempting to hack into the enterprise wired network must be monitored. It is important to keep track of these access points and STAs to help avoid repeated rogue-related and intrusion attempt problems.
Intrusion Detection—Security Penetration

- Lost enterprise wireless equipment must be located.
- Vulnerable devices with previous security violations must be monitored.
- Devices used by ex-employees who may have not returned all their wireless equipment must be monitored.

These nodes may be added to the monitor list to alert the wireless administrator the next time the access point or STA shows up in the RF environment.

wIPS Solution

The wireless administrator can add the access point or STA to the monitor list by identifying it as a monitored device on the Cisco Adaptive Wireless IPS.

NetStumbler Detected

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS detects a wireless client station probing the WLAN for an anonymous association (such as an association request for an access point with any SSID) using the NetStumbler tool. The Device probing for Access Point alarm is generated when hackers use recent versions of the NetStumbler tool. For older versions, the Cisco Adaptive Wireless IPS generates the NetStumbler detected alarm. (see Figure 18-27)

Figure 18-27 War-Chalker Universal Symbols

NetStumbler is the most widely used tool for war-driving and war-chalking. A wireless hacker uses war-driving tools to discover access points and to publish their information (MAC address, SSID, security implemented, and so on.) on the Internet with the access points' geographical location information. War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols as illustrated above. War-walking is similar to war-driving, but the hacker is on foot instead of a car. The NetStumbler website (http://www.netstumbler.com/) offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It can run on a machine running Windows 2000, Windows XP, or later versions. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers like to use MiniStumbler and similar products to sniff shopping malls and big-box retail stores. War-flying is sniffing for wireless networks from the air. The same equipment is used from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up email and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip. (see Figure 18-28)
To prevent your access points from being discovered by these hacking tools, configure your access points to not broadcast its SSID. You can use the Cisco Adaptive Wireless IPS to see which of your access points is broadcasting an SSID in the beacons.

Prime Infrastructure also provides automated security vulnerability scanning that reports any access points configured to broadcast their SSIDs. For more information on automated security vulnerability scanning, see the Cisco Prime Infrastructure online help.

**NetStumbler Victim Detected**

**Alarm Description and Possible Causes**

The Cisco Adaptive Wireless IPS detects a wireless client station probing the WLAN for an anonymous association (such as association request for an access point with any SSID) using the NetStumbler tool. The Device probing for access point alarm is generated when hackers more recent versions of the NetStumbler tool. For older versions, the Cisco Adaptive Wireless IPS generates the NetStumbler detected alarm.

NetStumbler is the most widely used tool for war-driving, war-walking, and war-chalking. A wireless hacker uses war-driving tools to discover access points and publish their information (MAC address, SSID, security implemented, and so on.) on the Internet with the access point geographical location information. War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols as illustrated above. War-walking is similar to war-driving, but the hacker conducts the illegal operation on foot instead of by car. The NetStumbler website (http://www.netstumbler.com/) offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It can run on a machine running Windows 2000, Windows XP, or later. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers typically use MiniStumbler and similar products to sniff shopping malls and big-box retail stores. War-flying is sniffing for wireless networks from the air. The same equipment is used, but from a low-flying private plane with high-power antennas. It has been reported that a Perth, Australia-based war-flyer picked up e-mail and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip. (see Figure 18-29)
Intrusion Detection—Security Penetration

Chapter 18  wIPS Policy Alarm Encyclopedia

Figure 18-29  Posted 802.11 Access Point Locations

The Cisco Adaptive Wireless IPS alerts the user when it observes that a station running Netstumbler is associated to a corporate access point.

wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure your access points to not broadcast its SSID. You can use the Cisco Adaptive Wireless IPS to see which access point is broadcasting its SSID in the beacons.

Publicly Secure Packet Forwarding (PSPF) Violation Detected

Alarm Description and Possible Causes

PSPF is a feature implemented on WLAN access points to block wireless clients from communicating with other wireless clients. With PSPF enabled, client devices cannot communicate with other client devices on the wireless network. (see Figure 18-30)
For most WLAN environments, wireless clients communicate only with devices such as web servers on the wired network. By enabling PSPF it protects wireless clients from being hacked by a wireless intruder. PSPF is effective in protecting wireless clients especially at wireless public networks (hotspots) such as airports, hotels, coffee shops, and college campuses where authentication is null and anyone can associate with the access points. The PSPF feature prevents client devices from inadvertently sharing files with other client devices on the wireless network.

**wIPS Solution**

The Cisco Adaptive Wireless IPS detects PSPF violations. If a wireless client attempts to communicate with another wireless client, the Cisco Adaptive Wireless IPS raises an alarm for a potential intrusion attack. This alarm does not apply if your WLAN deploys wireless printers or VoWLAN applications because these applications rely on wireless client-to-client communication.

**Probe Request Fuzzed Frame Detected**

**Alarm Description and Possible Causes**

802.11 Fuzzing is the process of introducing invalid, unexpected or random data into the 802.11 frames and then replaying those modified frames into the air. This can cause unexpected behavior to the destination device including driver crashes, operating system crashes and stack based overflows which would allow execution of arbitrary code on the affected system. The CVE website (http://cve.mitre.org/index.html) has numerous reported entries for fuzzing based vulnerabilities on 802.11 frames.

The system inspects each Probe Request frame looking for signs of fuzzing activity. Most common forms of Probe Request fuzzing involve expanding the SSID field beyond the limit of 32 bytes and changing the supported data rates to invalid rates. The system looks for these anomalies and will generate the Probe Request Fuzzing alarm when the field values are beyond the 802.11 specification.
**wIPS Solution**

The system monitors the wireless network for traffic consistent with Probe Request Fuzzing. It is recommended to locate the device and take it offline.

**Related Topics**

- Security IDS/IPS Overview
- Intrusion Detection—Security Penetration

**Probe Response Fuzzed Frame Detected**

**Alarm Description and Possible Causes**

802.11 Fuzzing is the process of introducing invalid, unexpected or random data into the 802.11 frames and then replaying those modified frames into the air. This can cause unexpected behavior to the destination device including driver crashes, operating system crashes and stack based overflows which would allow execution of arbitrary code on the affected system. The CVE website (http://cve.mitre.org/index.html) has numerous reported entries for fuzzing based vulnerabilities on 802.11 frames.

The system inspects each Probe Response frame looking for signs of fuzzing activity. Most common forms of Probe Response fuzzing involve expanding the SSID field beyond the limit of 32 bytes and changing the supported data rates to invalid rates. The system looks for these anomalies and will generate the Probe Response Fuzzing alarm when the field values are beyond the 802.11 specification.

**wIPS Solution**

The system monitors the wireless network for traffic consistent with Probe Response Fuzzing. It is recommended to locate the device and take it offline.

**Honey Pot AP Detected**

**Alarm Description and Possible Causes**

The addition of WLANs in the corporate environment introduces a whole new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. A rogue access point can put the entire corporate network at risk for outside penetration and attack. Not to understate the threat of the rogue access point, there are many other wireless security risks and intrusions such as mis-configured access points, unconfigured access points, and DoS (denial of service) attacks.

One of the most effective attacks facing enterprise networks implementing wireless is the use of a "honey pot" access point. An intruder uses tools such as NetStumbler, Wellenreiter, and MiniStumbler to discover the SSID of the corporate access point. Then the intruder sets up an access point outside the building premises or, if possible, within the premises and broadcasts the discovered corporate SSID. An unsuspecting client then connects to this "honey pot" access point with a higher signal strength. When associated, the intruder performs attacks against the client station because traffic is diverted through the "honey pot" access point.
**wIPS Solution**

When a "honey pot" access point is identified and reported by the Cisco Adaptive Wireless IPS, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the rogue device.

**Soft AP or Host AP Detected**

Host AP tools: Cquire AP

**Alarm Description and Possible Causes**

A host-based access point (desktop or a laptop computer serving as a wireless access point) represents two potential threats to enterprise security. First, host-based access points are not typically part of the enterprise wireless infrastructure and are likely to be rogue devices which do not conform to the corporate security policy. Second, host-based access points are used by wireless attackers as a convenient platform to implement various known intrusions such as man-in-the-middle, honey-pot access point, access point impersonation, and DoS (denial of service) attacks. Since software tools for turning a desktop or laptop into an access point can be easily downloaded from the Internet, host-based access points are more than just a theoretical threat.

Some laptops are shipped with the Host AP software pre-loaded and activated. When the laptops connect to the enterprise wireless network, they expose the wireless network to the hackers.

**wIPS Solution**

The Cisco Adaptive Wireless IPS detected soft access point should be treated as a rogue access point as well as a potential intrusion attempt. When the soft access point is identified and reported by the Cisco Adaptive Wireless IPS, the WLAN administrator may use integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the rogue device.

**Spoofed MAC Address Detected**

Spoofing tools may include the following: SMAC, macchanger, and SirMACsAlot.

**Alarm Description and Possible Causes**

A wireless intruder can disrupt a wireless network using a wide range of available attack tools, many of which are available as free downloads from the Internet. Most of these tools rely on a spoofed MAC address which masquerades as an authorized wireless access point or as an authorized client. By using these tools, an attacker can launch various denial of service (DoS) attacks, bypass access control mechanisms, or falsely advertise services to wireless clients.

**wIPS Solution**

The Cisco Adaptive Wireless IPS detects a spoofed MAC address by following the IEEE authorized OUI (vendor ID) and 802.11 frame sequence number signature.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MAC spoofing. For more information on MFP, refer to the *Cisco Wireless Control System Configuration Guide*. 
Suspicious After-Hours Traffic Detected

Alarm Description and Possible Causes

One way to detect a wireless security penetration attempt is to match wireless usage against the time when there is not supposed to be any wireless traffic. The wIPS server monitors traffic patterns against the office-hours configured for this alarm to generate alerts when an abnormality is found. Specific suspicious wireless usage sought after by the wIPS server during after-office hours includes the following:

- Client station initiating authentication or association requests to the office WLAN that may indicate security breach attempts.
- Wireless data traffic that may indicate suspicious download or upload over the wireless network.

wIPS Solution

For global wIPS deployment, the configurable office-hour range is defined in local time. The access point or sensor can be configured with a time zone to facilitate management. For the office and manufacturing floor mixed WLAN, one can define one set of office hours for the office WLAN SSID and another set for the manufacturing floor WLAN SSID. If this alarm is triggered, the administrator should look for the devices responsible for the suspicious traffic and remove them from the wireless environment.

Unauthorized Association by Vendor List

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS enables network administrators to include vendor information in a policy profile to allow the system to effectively detect stations on the WLAN that are not made by approved vendors. When such a policy profile is created, the system generates an alarm whenever an access point is associating with a station by an unapproved vendor. See Figure 18-31.
As the diagram shows, the access points in ACL-1 should only associate with stations made by Cisco and the access points in ACL-2 can only associate with stations manufactured by Intel. This information is entered in the wIPS system policy profile. Any association between the access points and non-Cisco or non-Intel stations is unauthorized and triggers an alarm.

In the enterprise WLAN environment, rogue stations cause security concerns and undermine network performance. They take up air space and compete for network bandwidth. Since an access point can only accommodate a limited number of stations, it rejects association requests from stations when its capacity is reached. An access point laden with rogue stations denies legitimate stations the access to the network. Common problems caused by rogue stations include connectivity problems and degraded performance.

**wIPS Solution**

The Cisco Adaptive Wireless IPS automatically alerts network administrators to any unauthorized access point-station association involving non-conforming stations using this alarm. When the alarm has been triggered, the unauthorized station must be identified and actions must be taken to resolve the issue. One way is to block it using the rogue containment.

**Unauthorized Association Detected**

**Alarm Description and Possible Causes**

In an enterprise network environment, rogue access points installed by employees do not usually follow the network standard deployment practice and therefore compromise the integrity of the network. They are loopholes in network security and make it easy for intruders to hack into the enterprise wired
Intrusion Detection—Security Penetration

Chapter 18 wIPS Policy Alarm Encyclopedia

network. One of the major concerns that most wireless network administrators face is unauthorized associations between stations in an ACL and a rogue access point. Since data to and from the stations flows through the rogue access point, it leaves the door open for hackers to obtain sensitive information. Rogue stations cause security concerns and undermine network performance. They take up air space and compete for bandwidths on the network. Since an access point can only serve a certain number of stations, it rejects association requests from stations once its capacity is reached. An access point laden with rogue stations denies legitimate stations access to the network. Common problems caused by rogue stations include disrupted connections and degraded performance.

wIPS Solution

The Cisco Adaptive Wireless IPS can automatically alert network administrators to any unauthorized access point-station association it has detected on the network through this alarm. When the alarm is triggered, the rogue or unauthorized device must be identified and actions must be taken to resolve the reported issue.

Wellenreiter Detected

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS detects a wireless client station probing the WLAN for an anonymous association (such as association request for an access point with any SSID) using the Wellenreiter tool. See Figure 18-32.

Figure 18-32 War-Chalker Universal Symbols

Wellenreiter is a commonly used tool for war-driving and war-chalking. A wireless hacker uses war-driving tools to discover access points and to publish their information (MAC address, SSID, security implemented, and so on.) on the Internet with the access point geographical location information. War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols as illustrated above. War-walking is similar to war-driving, but the hacker is on foot instead of a car. War-walkers like to use Wellenreiter and similar products to sniff shopping malls and big-box retail stores. War-flying is sniffing for wireless networks from the air. The same equipment is used, but from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up email and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip. See Figure 18-33.
The tool supports Prism2, Lucent, and Cisco-based cards. The tool can discover infrastructure and ad-hoc networks that are broadcasting SSIDs, their WEP capabilities, and can provide vendor information automatically. It also creates an ethereal/tcpdump-compatible dump file and an Application savefile. It also has GPS support. Users can download the tool from http://www.wellenreiter.net/index.html

**wIPS Solution**

To prevent your access points from being discovered by these hacking tools, configure your access points to not broadcast its SSID. You can use the Cisco Adaptive Wireless IPS to see which of your access points is broadcasting an SSID in the beacons.

Prime Infrastructure also provides automated security vulnerability scanning that reports any access points configured to broadcast their SSIDs. For more information on automated security vulnerability scanning, see Prime Infrastructure online help.

**WiFi Protected Setup Pin Brute Force**

**Alarm Description and Possible Causes**

WiFi Protected Setup is a feature on most consumer grade Access Points that allows for easy device setup without the need for complex passwords. The feature allows the user to either use the push button method or enter in the pin found on the bottom of the Access Point to connect. A vulnerability was announced in December 2011 by Stefan Viehböck and independently discovered by Craig Heffner. The vulnerability is with the external registrar that only requires the devices pin. This mode is susceptible to brute force attacks against the pin. There are currently 2 active tools in the wild exploiting this.

The basic idea behind the attack is when a pin authentication fails, the access point sends back an EAP-NACK message to the client. With this EAP-NACK message, the attacker is able to determine if the first half of the pin is correct. The last digit of the pin is known since it is a checksum for the pin. This reduces the attempts to brute force the pin down to 11,000.

It is recommended to disable the external registrar feature of WiFi Protected Setup on your Access Point. Most manufacturers have this feature on by default.
**wIPS Solution**

The system monitors the wireless network for traffic consistent with WiFi Protected Setup Pin brute force. It is recommended to locate the device and take it offline.

**WiFiTap Tool Detected**

**Alarm Description and Possible Causes**

The WiFiTap tool allows a wireless attacker to configure a client to communicate directly with another client, without connecting to a corporate AP. This implementation allows the intruder to target an attack against the individual client, bypassing any security measures configured on the corporate network. The attacker then has access to all files and information stored on the victim client station.

**wIPS Solution**

The wIPS server monitors for use of the WiFiTap tool and triggers an alarm if it is detected. Users should attempt to locate the attacking device and remove it from the wireless environment.
Troubleshooting and Best Practices

This appendix identifies and explains any additional troubleshooting or best practices you might find necessary as you implement a particular function.

This appendix contains the following sections:

- Troubleshooting Cisco-compatible Extensions Version 5 Client Devices, page A-1
- Web Auth Security on WLANs, page A-2
- Troubleshooting RAID Card Configuration, page A-8
- Applying for a Cisco.com Account with Cryptographic Access, page A-9
- Performing Disk Cleanup, page A-9
- Replacing an Old Controller Model with a New Model, page A-10

Troubleshooting Cisco-compatible Extensions Version 5 Client Devices

Two features are designed to troubleshoot communication problems with Cisco-compatible Extension clients: diagnostic channel and client reporting.

**Note**

These features are supported only on Cisco-compatible Extensions Version 5 Client Devices. They are not supported for use with non-Cisco-compatible Extensions Version 5 Client Devices or with clients running an earlier version.

Diagnostic Channel

The diagnostic channel feature enables you to troubleshoot problems regarding client communication with a WLAN. When initiated by a client having difficulties, the diagnostic channel is a WLAN configured to provide the most robust communication methods with the fewest obstacles to communication placed in the path of the client. The client and access points can be put through a defined set of tests in an attempt to identify the cause of communication difficulties experienced by the client.

**Note**

Only one WLAN per controller can have the diagnostic channel enabled, and all of the security on this WLAN is disabled.
Configuring the Diagnostic Channel

Follow these steps to configure the diagnostic channel:

**Step 1** Choose **Configure > Controllers**.

**Step 2** Click an IP address to choose a specific controller.

**Step 3** Choose **WLANs> WLAN Configuration** from the left sidebar menu.

**Step 4** Choose **Add a WLAN** from the Select a command drop-down list to create a new or click the profile name of an existing.

**Note** We recommend that you create a new WLAN on which to run the diagnostic tests.

**Step 5** When the WLANs page appears, click the **Advanced** tab.

**Step 6** If you want to enable diagnostic channel troubleshooting on this WLAN, select the **Diagnostic Channel** check box. Otherwise, leave this check box unselected, which is the default value.

**Step 7** Click **Save** to commit your changes.

Web Auth Security on WLANs

This section describes the troubleshooting and best practices procedures that are useful when implementing web auth security on WLANs.

Web-auth is a Layer 3 security feature which allows web-based authentication to users on a WLAN. It is used mainly in guest networking scenarios, although not restricted to that usage.

When a WLAN is configured with web-auth security, you are redirected to the login page after passing Layer 2 authentications (static WEP, WPA+PSK, MAC filtering, and so on). The login page is stored on the local device or an external web server, and the page can be modified to allow a customized logo, title, and so on.

After the WLAN is configured with a web-auth WLAN, the HTTP get request is sent by the wireless client to the requested website. The controller firewall allows the DNS resolution of the specified URL. After the resolution, the controller interrupts the HTTP packets from the wireless client and redirects to the login page. When the credentials are entered on the login page and submitted, they are authenticated against the local database. If the user is not found in the local database, the configured RADIUS servers are contacted.

**Note** PAP and CHAP authentication are used between the client and authentication agent. Make sure your RADIUS server supports both of these protocols so web-auth login is allowed.

Upon successful authentication, you are allowed to pass traffic. After three unsuccessful authentication attempts, the client is excluded. This excluded client cannot associate until the exclusion timeout limit is surpassed. The exclusion timeout limit is configured with aggressive load balancing, which actively balances the load between the mobile clients and their associated access points.
Web-auth WLAN is also configured with a pre-authentication access control list (ACL). This ACL is configured the same as a normal ACL but permits access to resources that the client needs prior to authentication. An administrator must use the interface section to apply an ACL to the client after authentication.

A web-auth WLAN can be configured with a session timeout value. This value defines the time the client needs to re-authenticate with the device. If the value is set to zero, which means infinity, the client never re-authenticates unless the logged out option is used. You can access the logout URL at http://<VirtualIP>/logout.html.

**Note**  
Disable all pop-up blockers on the client to see the logout page.

Web-auth can be configured in different modes under Layer 3 security. The most commonly used modes of web-auth are as follows:

- Internal Web—Redirection to an internal page using http://<virtual IP /DNS name >/login.html. Customization is available.
- External Web—Redirection to an external URL.

**Debug Commands**

The following debug commands are allowed:

```
debug client <client-mac-address>
debug pm ssh-tcp enable
debug pm ssh-appgw enable
debug pm rules enable
debug pm config enable
show client detail <client-mac-address>
debug pem event enable
```

**Debug Strategy**

Use the following strategy for web-auth configured on a WLAN without guest tunneling:

**Step 1** Identify a mobile client to work with and write down its wireless MAC address. Use the command `prompt > ipconfig /all` for all MS Windows-based systems.

**Step 2** Disable the radio of the mobile client.

**Step 3** Enter the following debug commands via a serial console set for high speed (115200) or SSH session to the management port of the controller:

```
debug client <client-mac-address>
debug pm ssh-tcp enable
debug pm ssh-appgw enable
debug pm rules enable
debug pm config enable
show client detail <client-mac-address>
```

```debug pem event enable
debug pem state enable```
Step 4  Enable the radio and let the client associate. After the client is associated, enter the `show client detail client-mac-address` command.

$Router1> show client detail 00:0b:85:09:96:10
Client Username ......................... N/A
AP MAC Address................................. 00:0b:85:09:96:10
Client State .................................. Associated
Wireless LAN Id................................. 1
BSSID........................................... 00:0b:85:09:96:1f
Channel......................................... 11
IP Address..................................... 10.50.234.3
Association Id................................. 1
Authentication Algorithm..................... Open System
Reason Code.................................... 0
Status Code.................................... 0
Session Timeout............................... 0
Client CCX version......................... 3
Mirroring........................................ Disabled
QoS Level.................................... Silver
Diff Serv Code Point (DSCP)................. disabled
802.1P Priority Tag........................... disabled
WMM Support.................................. Disabled
Mobility State................................. Local
Internal Mobility State....................... apFMsMmInitial
Mobility Move Count........................... 0
--More-- or (q)uit
Security Policy Completed................ No
Policy Manager State......................... WEBAUTH_REQD =========**
Policy Manager Rule Created............... Yes
NPI Fast Fast Notified....................... Yes
Last Policy Manager State................... WEBAUTH_REQD
Client Entry Create Time.................... 67733 seconds
Policy Type................................... N/A
Encryption Cipher.............................. None
Interface..................................... management
VLAN............................................ 0
Client Capabilities:
  CF Pollable.................................. Not implemented
  CF Poll Request............................. Not implemented
  Short Preamble............................... Implemented
  PBCC......................................... Not implemented
  Channel Agility............................. Not implemented
  Listen Interval............................ 0
Client Statistics:
  Number of Bytes Received................ 188595
  Number of Bytes Sent....................... 19229
  Number of Packets Received.............. 3074
--More-- or (q)uit
  Number of Packets Sent................... 76
  Number of Policy Errors................... 0
  Radio Signal Strength Indicator......... -41 dBm
  Signal to Noise Ratio..................... 59 dB
Nearby AP Statistics:
  TxExcessiveRetries: 0
  TxRetries: 0
  RtsSuccessCnt: 0
  RtsFailCnt: 0
  TxFiltered: 0
  TxRateProfile: [0,0,0,0,0,0,0,0,0,0]
ap:09:96:10(slot 1) ....................
  antenna0: 48 seconds ago -45 dBm................. antenna1: 123 seconds ago -128 dBm
Step 5  Make sure the pemstate of the client is WEBAUTH_REQD. Open the browser page on the client and look for the following messages:

Wed Mar 7 17:59:15 2007: sshpmAddWebRedirectRules: mobile station addr is 10.50.234.3
Wed Mar 7 17:59:15 2007: sshpmAddWebRedirectRules: RuleID for ms 10.50.234.3 is 44
Wed Mar 7 17:59:15 2007: sshpmRuleIndexInsert: adding rule for RuleID 44
Wed Mar 7 17:59:15 2007: sshpmRuleIndexInsert: computed raw hash index 02ad3271 for rule id 0000002c
Wed Mar 7 17:59:15 2007: sshpmRuleIndexInsert: computed adjusted index 00000c32 for rule id 0000002c
Wed Mar 7 17:59:15 2007: sshpmPolicyCommitCallback: called; ContextPtr: 0x2c; Success: 1
Wed Mar 7 18:02:32 2007: SshPmAppgw/pm_appgw.c:1234/ssh_pm_appgw_request: New application gateway request for `alg-http@ssh.com': 10.50.234.3.1153 > 10.50.234.1.80 (nat: 10.50.234.1.80) tcp ft=0x00000000 tt=0x00000000
Wed Mar 7 18:02:32 2007: SshPmAppgw/pm_appgw.c:1239/ssh_pm_appgw_request: Packet attributes: trigger_rule=0x4ecb, tunnel_id=0x0, trd_index=0x00ffffff, prev_trd_index=0x00ffffff
Wed Mar 7 18:02:32 2007: SshPmAppgw/pm_appgw.c:1240/ssh_pm_appgw_request: Packet:
Wed Mar 7 18:02:32 2007: 00000000: 4500 0030 0308 4000 8006 0f57 0a32 ea03
E..0..@....W.2..
Wed Mar 7 18:02:32 2007: 00000010: 0a32 ea01 0481 0050 2f42 e3a4 0000 0000 .2.....P/B......
Wed Mar 7 18:02:32 2007: 00000020: 7002 4000 42fe 0000 0204 05b4 0101 0402 p.@.B...........
Wed Mar 7 18:02:32 2007: SshPmStAppgw/pm_st_appgw.c:403/ssh_pm_st_appgw_start: Calling redirection callback
Wed Mar 7 18:02:32 2007: SshPmAppgw/pm_appgw.c:155/ssh_appgw_redirect: Application gateway redirect: 10.50.234.1.80 -> 10.50.234.1.80
Wed Mar 7 18:02:32 2007: SshPmStAppgw/pm_st_appgw.c:445/ssh_pm_st_appgw_mappings: Creating application gateway mappings: 10.50.234.3.1153 > 10.50.234.1.80 (10.50.234.1.80)
Wed Mar 7 18:02:32 2007: SshPmStAppgw/pm_st_appgw.c:102/ssh_pm_appgw_mappingsCb: appgw connection cached: init flow_index=5967 resp flow_index=5964 event_cnt=718
Wed Mar 7 18:02:32 2007: SshPmStAppgw/pm_st_appgw.c:493/ssh_pm_st_appgw_mappings_done: NAT on initiator side
Wed Mar 7 18:02:32 2007: SshPmStAppgw/pm_st_appgw.c:583/ssh_pm_st_appgw_tcp_responder_stream_done: ssh_pm_st_appgw_tcp_responder_stream_done: conn->context.responder_stream=0x0
Wed Mar 7 18:02:32 2007: SshPmStAppgw/pm_st_appgw.c:624/ssh_pm_st_appgw_tcp_responder_stream_done: Opening initiator stream 10.50.234.1:61611 > 10.76.108.121:2024
Wed Mar 7 18:02:32 2007: SshPmStAppgw/pm_st_appgw.c:154/ssh_pm_appgw_i_flow_enabled: Initiator flow mode has now been set.
Wed Mar 7 18:02:32 2007: SshPmStAppgw/pm_st_appgw.c:646/ssh_pm_st_appgw_tcp_open_initiator_stream: Initiator stream opened
Wed Mar  7 18:02:36 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input: entering state st_wait_input: (r) reading_hdr 1 nmsgs 0
Wed Mar  7 18:02:36 2007: SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:41 2007: 00000000: 4745 5420 2f20 4854 5450 2f31 2e31 0d0a  GET /
Wed Mar  7 18:02:41 2007: 00000010: 4163 6365 7074 3a20 696d 6167 652f 6769  Accept:
Wed Mar  7 18:02:41 2007: 00000020: 662c 2069 6d61 6765 2f78 2d78 6269 746d  f,
Wed Mar  7 18:02:41 2007: 00000030: 6170 2c20 696d 6167 652f 706a 7065 672c  ap,
Wed Mar  7 18:02:41 2007: 00000040: 2061 7070 6c69 6361 7469 6f6e 2f78 2d73  image/pjpeg,
Wed Mar  7 18:02:41 2007: 00000050: 6170 2c20 696d 6167 652f 706a 7065 672c  ap,
Wed Mar  7 18:02:41 2007: 00000060: 696d 6167 652f 706a 7065 672c 2061 7070  image/pjpeg
Wed Mar  7 18:02:41 2007: 00000070: 4d6f 7a 696c 6c61 2f34 2e30  Mozilla/4.0
Wed Mar  7 18:02:41 2007: 00000080: 6465 666c 6174 650d 0a55 7365 722d 4167 decode..User-Agent
Wed Mar  7 18:02:41 2007: 00000090: 656e 743a 204d 6f7a 696c 6c61 2f34 2e30  :en-us..Accept-
Wed Mar  7 18:02:41 2007: 000000a0: 456e 636f 6469 6e67 3a20 6d65 7365 722d en-us..Accept-
Wed Mar  7 18:02:41 2007: 000000b0: 456e 636f 6469 6e67 3a20 6d65 7365 722d encoding: utf-8
If you do not see the HTTP GET message, the HTTP packet has not reached the controller. After the client completes the redirection, enter your login and submit it.
Troubleshooting RAID Card Configuration

Scenario: Due to accidental power interruption, the information about the RAID card configuration that is stored in the NVRAM (non-volatile RAM) gets corrupted or erased. When the configuration information is lost, the RAID card fails to boot in the normal mode. However, the RAID card backs up the configuration information on the hard drives. Though the RAID card recognizes the backup configuration stored on the hard drive, it does not load the configuration information as the default configuration without manual intervention.

Analysis:
When the system tries to boot, the RAID firmware returns an error message that the information about the previous configuration is lost and you need to press C to load the configuration utility. The error message appears on the serial console and the bootup does not proceed without your input.

You must perform the following steps:

Step 7
Look at the entry of the client in NPuDevShell hapiMmcDebugScbInfoShow (‘client mac address’). If the PEM state is not moved from WEBAUTH_REQD to RUN, a credential problem exists. Check the credentials in the local or RADIUS database (where ever they were configured).

Step 8
When the RUN state appears on the client, perform a check from the client to the gateway and see if traffic is being passed.

RF Heatmap Analysis

Scenario: You see some inconsistent heat maps for access points. One part of the access point shows strong heat maps, whereas the other part shows weak heat maps.

Analysis: This might happen when you get the RSSI values of the neighboring access point for one part and not for the other part. Using just one side of the RSSI value to predict the heat map is not suggested, as there can be a thick wall or wired housing which might lead to incorrect heat maps.

Scenario: You are unable to view the dynamic heat map correctly.

Analysis: In case you are unable to view the dynamic heat map correctly, check the following:

• Neighbor AP RSSI values if they are same from both controller and Cisco Prime Infrastructure.
• Wait for 20 minutes for the heat maps to refresh with most latest dynamic heat map data.
• Check AP Positions.

Best Practices

If the client is not redirected to the login page and you want to avoid DNS resolution in the network, enter http://controller-mgmt-ip. If a redirection occur, the issue is not network related.

Enter config network web-auth-port Port to define the ports on the controller other than the standard HTTP port (80). The controller does not interrupt secure HTTP or HTTPS (443) even if the port is configured for interrupt.
Step 1  On the serial console, press C to load the RAID management tool. The RAID firmware indicates that a foreign configuration is available. The foreign configuration is the RAID card configuration that was backed up on the hard drive. But, the RAID firmware does not load this configuration information automatically.

Step 2  In the RAID management tool, type the following command:
-CfgForeign -Import -a0

Step 3  Reboot the server.

---

To apply cryptographic access, follow these steps:

Step 1  If you have a Cisco.com account, skip to Step 2. If you do not have a Cisco.com account, register for one at this URL: http://tools.cisco.com/RPF/register/register.do.

Step 2  Go to this URL: http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y.
The Enter Network Password dialog box appears.

Step 3  Log in with your Cisco.com account.
The Encryption Software Export Distribution Authorization page appears.

Step 4  Select your software from the list box and click Submit.
The Encryption Software Export Distribution Authorization page appears.

Step 5  Review and complete the Encryption Software Export Distribution Authorization form and click Submit.

Note: It takes approximately 4 hours to process your application. You cannot download the software until the entitlement process is complete. You will not receive any notification for this.

---

Performing Disk Cleanup

When Prime Infrastructure is running low on disk space, an alarm is raised in the system. Also, the following error appears as a pop-up dialog box.

The system is running low on disk space, please refer to online help to perform disk cleanup.

To resolve this issue, use the following CLI command:
ncs cleanup

You can use this command to free up and reclaim disk space.
In addition, you can also monitor your system disk usage. For details, see “Checking on System Disk Usage” section on page A-10.

For more details on managing Prime Infrastructure's network data collection and retention, see the following URL:


Checking on System Disk Usage

You can quickly check on the total system disk space usage using the Appliance Status tab in the Administration > Appliance page.

Choose Administration > Appliance > Appliance Status.

Under Disk Usage, Prime Infrastructure displays the current storage allocation and percentage of use for each of the main disk volumes it uses.

Replacing an Old Controller Model with a New Model

When you want to replace an old controller model with a new one without changing the IP address, do the following:

- First delete the old controller from Prime Infrastructure and wait for the confirmation popup that the deletion is complete.
- Replace the controller with the new model in the setup with same IP.
- Re-add the IP address to the Prime Infrastructure.
Cisco Prime Infrastructure Server Hardening

This appendix provides an instructional checklist for hardening a Cisco Prime Infrastructure server. Ideally, the goal of a hardened server is to leave it exposed on the Internet without any other form of protection. This describes the hardening of Prime Infrastructure, which requires some services and processes exposed to function properly. Think of it as Prime Infrastructure best practices. Hardening of Prime Infrastructure involves disabling unnecessary services, removing and modifying registry key entries, and applying appropriate restrictive permissions to files, services, and endpoints.

This appendix contains the following sections:

- Prime Infrastructure Password Handling, page B-1
- Setting Up SSL Certification, page B-1

Prime Infrastructure Password Handling

You can configure additional authentication by configuring the Local Password Policy parameters. Select the check boxes if you want the configurations to be enabled.

The following configurations are added for additional authentication:

- You can configure the minimum length of the password.
- You can configure if you want to allow the username or reverse of the username to be part of the password.
- You can configure if the password can contain 'cisco', 'ocsic', or any capitalized letter variant therein or by substituting 'I', 'l', or '!' for i, '0' for 'o', or '$' for 's'.
- You can configure if the root password can be the word public.
- You can configure if a character can be repeated more than three times consecutively in the password or not.
- You can configure if the password must contain character from three of the character classes: upper case, lower case, digits, and special characters.

Setting Up SSL Certification

The Secure Sockets Layer (SSL) Certification is used to ensure secure transactions between a web server and the browsers. Installing the DoD Certificates allows your web browser to trust the identity and provide secure communications which are authenticated by Department of Defense (DoD).
These certificates are used to validate the identity of the server or website and are used to generate the encryption key used in the SSL. This encryption protects the information being passed between the server and the client.

- Setting Up SSL Client Certification, page B-2
- Setting Up SSL Server Certification, page B-3

## Setting Up SSL Client Certification

To set up the SSL client certificate authentication using a DoD certificate, follow these steps:

**Step 1** Create SSL Client Certificate using the below command.

```bash
% keytool -genkey -keystore nmsclientkeystore -storetype pkcs12 -keyalg RSA -keysize 2048 -alias nmsclient -dname "CN=nmsclient, OU=WNBU, O=Cisco, L=San Jose, ST=CA, C=US" -storepass nmskeystore
```

**Note** Provide the Key Algorithm as RSA and KeySize as 1024 or 2048.

**Step 2** Generate the Certificate Signing Request (CSR) using the below command.

```bash
% keytool -certreq -keyalg RSA -keysize 2048  -alias nmsclient -keystore nmsclientkeystore -storetype pkcs12 -file <csrfilename>
```

**Note** Provide the Key Algorithm as RSA and KeySize as 1024 or 2048 and provide a certificate file name.

**Step 3** Send the generated CSR file to DoD. The DoD issues the corresponding signed certificates.

**Note** The CSR reply is through dod.p7b file. In addition you should also receive the root CA certificates.

**Note** Please makes sure to retrieve the PKCS7 encoded certificates; Certificate Authorities provide an option to get the PKCS7 encoded certificates.

**Step 4** Import the CSR reply in the Keystore using the command:

```bash
% keytool -import dod.p7b -keystore nmsclientkeystore -storetype pkcs12 -storepass nmskeystore
```

**Step 5** Check the formats of root CA certificates received, they must be base 64 encoded. If they are not base 64 encoded, use the OpenSSL command to convert them to base 64 encoded format.

```bash
% openssl x509 -in rootCA.cer -inform DER -outform PEM -outfile rootCA.crt
% openssl x509 -in DoD-sub.cer -inform DER -outform PEM -outfile rootCA.crt
```
Note: Convert both root CA certificate and sub-ordinate certificates received.

In case you received both root CA certificate and the sub-ordinate certificate, you have to bundle them together using the below command:

```
% cat DoD-sub.crt > ca-bundle.crt
% cat DoD-rootCA.crt >> ca-bundle.crt
```

**Step 6**

To setup SSL Client Authentication using these certificates, enable SSL Client Authentication in Apache in the `ssl.conf` file located in `<NCS_Home>/webnms/apache/ssl/backup/` folder.

- `SSLCACertificationPath conf/ssl.crt`
- `SSLCACertificationFile conf/ssl.crt/ca-bundle.crt`
- `SSLVerifyClient require`
- `SSLVerifyDepth 2`

**Note:**

SSLVerifyDepth depends on the level of Certificate Chain. In case you have only 1 root CA certificate, this should be set to 1. In case you have a certificate chain (root CA and subordinate CA), this should be set to 2.

**Step 7**

Install the DoD root CA certificates in Prime Infrastructure.

**Step 8**

Import the nmsclientkeystore in your browser.

---

**Setting Up SSL Server Certification**

To set up the SSL server certificate using a DoD certificate, follow these steps:

**Step 1**

Generate the Certificate Signing Request (CSR).

```
% keyadmin -newdn genkey <csrfilename>
```

**Step 2**

Send the generated CSR file to DoD. The DoD issues the corresponding signed certificates.

**Note:**

The CSR reply is through dod.p7b file. In addition you should also receive the root CA certificates.

**Note:**

Please make sure to retrieve the PKCS7 encoded certificates; Certificate Authorities provide an option to get the PKCS7 encoded certificates.

**Step 3**

Import the Signed Certificate using the below command in the Keytool:

```
% keyadmin -importsignedcert <dod.p7>
```
Note
Prime Infrastructure stores the self-signed certificate at /opt/CSCOncs/httpd/conf/ssl.crt. The imported certificates/keys are stored at /opt/CSCOncs/migrate/restore.
Certificate Signing Request (CSR) Generation for a Third-Party Certificate on Cisco Prime Infrastructure

This appendix describes how to generate a Certificate Signing Request (CSR) to obtain a third-party certificate with Cisco Prime Infrastructure and how to import the certificate into Prime Infrastructure. It contains the following sections:

- Prerequisites, page C-1
- Certificate Signing Request (CSR), page C-2
- Generating a Certificate Signing Request (CSR) File, page C-2
- Get a Signed Certificate for CSR from Microsoft Certificate Authority (CA), page C-3
- Importing a Certificate Authority (CA) Certificate and Key, page C-4
- Viewing the list of Certificates, page C-4
- Deleting Certificates, page C-5
- Related Publications, page C-5

Prerequisites

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of how to install and configure Prime Infrastructure for basic operation
- Knowledge of self-signed and digital certificates, and other security mechanisms related to Public Key Infrastructure (PKI)

For more information about the supported hardware, see the Prime Infrastructure release notes at the following URL:


The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.
Certificate Signing Request (CSR)

A certificate is an electronic document that you use to identify a server, a company, or some other entity and to associate that identity with a public key.

A self-signed certificate is an identity certificate that is signed by its own creator. That is, the person who created the certificate also signed off on its legitimacy.

Certificates can be self-signed or can be attested by a digital signature from a certificate authority (CA). CAs are entities that validate identities and issue certificates. The certificate issued by the CA binds a particular public key to the name of the entity that the certificate identifies, such as the name of a server or device. Only the public key that the certificate certifies works with the corresponding private key possessed by the entity that the certificate identifies. Certificates help prevent the use of fake public keys for impersonation.

A CSR is a message that an applicant sends to a CA to apply for a digital identity certificate. Before a CSR is created, the applicant first generates a key pair, which keeps the private key secret. The CSR contains information that identifies the applicant, such as a directory name in the case of an X.509 certificate, and the public key chosen by the applicant. The corresponding private key is not included in the CSR, but is used to digitally sign the entire request.

The CSR can be accompanied by other credentials or proofs of identity required by the certificate authority, and the certificate authority can contact the applicant for further information. For the most part, a third-party CA company, such as Entrust or VeriSign, requires a CSR before the company can create a digital certificate.

CSR generation is independent of the device on which you plan to install an external certificate. Therefore, a CSR and a private key file can be generated on any individual machine which supports CSR generation. CSR generation is not switch-dependent or appliance-dependent in this case.

This appendix describes how to generate a CSR for a third-party certificate using the Cisco Prime Infrastructure.

Generating a Certificate Signing Request (CSR) File

An SSL certificate can be obtained from a third party. To set up this support, you must:

2. Submit the signing request to a Certificate Authority you choose.
3. Apply the signed Security Certificate file to the server.

Step 1 Generate a Certificate Signing Request (CSR) file for the Prime Infrastructure server:

a. At the Prime Infrastructure appliance, exit to the command line.

b. At the command line, log in using the administrator ID and password used to install Prime Infrastructure.

c. Enter the following command to generate the CSR file in the default backup repository:

- `ncs key genkey -newdn -csr CertName.csr repository RepoName`

where:

- `CertName` is an arbitrary name of your choice (for example: MyCertificate.csr).
- `RepoName` is any previously configured backup repository (for example: defaultRepo).
Step 2  Copy the CSR file to a location you can access. For example:

\texttt{copy disk:/RepoName/CertName.csr ftp://your.ftp.server}

Step 3  Send the CSR file to a Certificate Authority (CA) of your choice.

\textbf{Note}  Once you have generated and sent the CSR file for certification, do not use the \texttt{genkey} command again to generate a new key on the same Prime Infrastructure server. If you do, importing the signed certificate file will result in mismatches between keys in the file and on the server.

Step 4  You will receive a signed certificate file with the same filename, but with the file extension CER, from the CA. Before continuing, ensure:
- There is only one CER file. In some cases, you may receive chain certificates as individual files.
- Any blank lines in the CER file are removed.

Step 5  At the command line, copy the CER file to the backup repository. For example:

\texttt{- copy ftp://your.ftp.server/CertName.cer disk:RepoName}

Step 6  Import the CER file into the Prime Infrastructure server using the following command:

\texttt{- ncs key importsignedcert CertName.cer repository RepoName}

Step 7  Restart the Prime Infrastructure server by issuing the following commands in this order:

- \texttt{ncs stop}
- \texttt{ncs start}

Step 8  If the Certificate Authority who signed the certificate is not already a trusted CA: Instruct users to add the certificate to their browser trust store when accessing the Prime Infrastructure login page.

---

\section*{Get a Signed Certificate for CSR from Microsoft Certificate Authority (CA)}

You must take the CSR, load it into the Microsoft CA, and have it signed as an Internet certificate. Once you do this, you get a new *.csr file that shows a path where the Microsoft CA is the trusted root and not the Prime Infrastructure. Complete these steps in order to submit the CSR to CA if your CA is a Windows 2008 Server.

\begin{itemize}
  \item \textbf{Step 1}  Open the CSR file you downloaded in to Notepad and copy the entire contents including the \texttt{---BEGIN CERTIFICATE ---} and \texttt{---END CERTIFICATE --} lines.
  \item \textbf{Step 2}  Go to http://\textless certificate server address\textgreater /certsrv in order to open the Certificates Server web page.
  \item \textbf{Step 3}  Enter your username and password.
  \item \textbf{Step 4}  Click \texttt{Request a certificate}.
    The Request a Certificate web page appears.
  \item \textbf{Step 5}  Click the \texttt{advanced certificate request} link.
    The Submit a Certificate Request or Renewal Request web page appears.
\end{itemize}
Step 6 Paste the content you copied in Step1 into the Saved Request field, choose Web Server in the Certificate Template drop-down list, and click Submit.

Step 7 On the Certificate Issued web page, click the DER encoded radio button, and then click Download certificate.

Step 8 Save the file to your local computer.

---

**Importing a Certificate Authority (CA) Certificate and Key**

**Step 1** At the command line, log in using the administrator ID and password and enter the following command:

```plaintext
ncs key importcacert aliasname ca-cert-filename repository repositoryname
```

where

- `aliasname` is a short name given for this CA certificate.
- `ca-cert-filename` is the CA certificate file name.
- `repositoryname` is the repository name configured in Prime Infrastructure where the ca-cert-filename is hosted.

**Step 2** To import an RSA key and signed certificate to Prime Infrastructure, enter the following command in admin mode:

```plaintext
ncs key importkey key-filename cert-filename repository repositoryname
```

where

- `key-filename` is the RSA private key file name.
- `cert-filename` is the certificate file name.
- `repositoryname` is the repository name configured in Prime Infrastructure where the key-file and cert-file are hosted.

**Step 3** Restart the Prime Infrastructure server by issuing the following commands in this order:

- `ncs stop`
- `ncs start`

---

**Viewing the list of Certificates**

To list all the CA certificates that exist in Prime Infrastructure trust store, use Prime Infrastructure `key listcacerts` command.

```plaintext
ncs key listcacerts
```

This example shows how to list all the CA certificates exist in Prime Infrastructure trust store:

```
admin# ncs key listcacerts
Certificate utnuserfirsthardwareca from CN=UTN-USERFirst-Hardware, OU=http://www.example.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US
```
Certificate gtecybertrust5ca from CN=GTE CyberTrust Root 5, OU="GTE CyberTrust Solutions, Inc.", O=GTE Corporation, C=US
Certificate equifaxsecurebusinessca1 from CN=Equifax Secure eBusiness CA-1, O=Equifax Secure Inc., C=US
Certificate thawtepersonalfreemailca from EMAILADDRESS=email@example.com, CN=Thawte Personal Freemail CA, OU=Certification Services Division, O=Thawte Consulting, L=Cape Town, ST=Western Cape, C=ZA
Certificate addtrustclass1ca from CN=AddTrust Class 1 CA Root, OU=AddTrust TTP Network, O=AddTrust AB, C=SE
Certificate aolrootca1 from CN=America Online Root Certification Authority 1, O=America Online Inc., C=US
Certificate geotrustuniversalca from CN=GeoTrust Universal CA, O=GeoTrust Inc., C=US
Certificate digicertglobalrootca from CN=DigiCert Global Root CA, OU=www.example.com, O=DigiCert Inc, C=US
Certificate certumtrustednetworkca from CN=Certum Trusted Network CA, OU=Certum Certification Authority, O=Unizeto Technologies S.A., C=PL
Certificate swisssignsilverg2ca from CN=SwissSign Silver CA - G2, O=SwissSign AG, C=CH

Deleting Certificates

To delete CA certificates that exist in Prime Infrastructure trust store, use Prime Infrastructure key deletecert command.

`ncs key deletecert aliasname`

This example shows how to delete CA certificates exist in Prime Infrastructure trust store:

`admin# ncs key deletecert certumtrustednetworkca`
Deleting certificate from trust store

Related Publications

For more information about Prime Infrastructure, see the following URL:
