Cisco Wireless Control System Configuration Guide

Software Release 7.0
June 2010

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-21743-01

CONTENTS

Preface xxix

Audience xxix

Purpose xxix

Conventions xxix

Related Publications xxx

Obtaining Documentation and Submitting a Service Request xxx

CHAPTER 1 **Overview** 1-1

The Cisco Unified Wireless Network Solution 1-1

The WCS 1-2

WCS Versions 1-3

WCS Base 1-3

WCS Base + Location 1-4

Enabling Mobility Services and HA with WCSPLUS License 1-4

Using WCS Cisco Location Appliances 1-4

Comparison of WCS Base and WCS Location Features 1-6

Embedded Access Points 1-6

Access Point Communication Protocols 1-8

Guidelines and Restrictions for Using CAPWAP 1-8

The Controller Discovery Process 1-8

WCS User Interface 1-9

Cisco WCS Navigator 1-9

CHAPTER 2 **Getting Started** 2-1

Prerequisites 2-1

System Requirements 2-2

High-End Server 2-2

Unified Computing System 2-2

Standard Server 2-3

Unified Computing System 2-3

Low-End Server 2-3

Unified Computing System 2-4

Supported Operating Systems 2-4

Client Requirements 2-5
Supported WLC Releases 2-5
WCS on WLSE 2-5
WCS Navigator 2-5
Installing WCS for Windows 2-5
Before You Begin 2-6
Configuring WCS to Run as a Domain User 2-13
Installing WCS for Linux 2-14
Configuring TFTP as a Network Drive 2-16
Starting WCS 2-16
Starting WCS on Windows 2-16
Starting WCS on Linux 2-17
Logging into the WCS User Interface 2-18
General Tab 2-19
Client Tab 2-20
Security Tab 2-21
Mesh Tab 2-22
CleanAir Tab 2-22
Customizing Home Page Tabs 2-23
Creating a New Tab 2-23
Customizing Home Page Content 2-24
Editing Content 2-25
Additional Edit Content Page Components 2-26
Guest Components for WCS Home Page 2-27
Using the Cisco WCS User Interface 2-28
Icons 2-28
Menu Bar 2-29
Monitor Menu 2-29
Configure Menu 2-29
Administration Menu 2-29
Tools Menu 2-29
Help Menu 2-30
Sidebar Area 2-30
Command Buttons 2-30
Alarm Summary 2-30
Main Data Page 2-31
Administrative Tools 2-31
Using the Search Feature 2-31
Quick Search 2-32

Advanced Search 2-32
Alarms 2-34
Access Points 2-35
Controllers 2-36
Clients 2-37
Chokepoints 2-38
Events 2-38
SE-Detected Interferers 2-39
AP-Detected Interferers 2-39
Wi-Fi TDOA Receivers 2-40
Maps 2-41
Rogue Clients 2-41
Shunned Clients 2-41
Tags 2-42
Controller Licenses 2-43
Saved Searches 2-43
Configuring the Search Results Display 2-44

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 3-2
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 Tab 3-4
Security Index 3-5
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 3-9
Recent Rogue AP Alarms 3-9

Recent Adhoc Rogue Alarm 3-9
Most Recent Security Alarms 3-9
Monitoring Rogue Access Points, Ad hoc Events, and Clients 3-9
Rogue Access Points 3-9
Monitoring Rogue AP Alarms 3-10
Classifying Rogue Access Points 3-11
Rogue Access Point Classification Types 3-13
Viewing Rogue AP Alarm Details 3-14
Viewing Rogue Client Details 3-17
Adhoc Rogue Alarms 3-17
Monitoring Adhoc Rogue Alarms 3-17
Viewing Adhoc Rogue Alarm Details 3-18
Rogue Access Point Location, Tagging, and Containment 3-19
Detecting Access Points 3-20
Working with Alarms 3-21
Monitoring Rogue Alarm Events 3-22
Viewing Rogue AP Event Details 3-23
Monitoring Adhoc Rogue Events 3-24
Viewing Adhoc Rogue Event Details 3-25
Security Overview 3-25
Security Vulnerability Assessment 3-26
Security Index 3-26
Top Security Issues 3-27
Switch Port Tracing 3-33
Integrated Security Solutions 3-34
Using WCS to Convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 Mode 3-34
Configuring a Firewall for WCS 3-35
Access Point Authorization 3-36
Management Frame Protection (MFP) 3-36
Guidelines for Using MFP 3-38
Configuring Intrusion Detection Systems (IDS) 3-38
Viewing IDS Sensors 3-38
Configuring IDS Signatures 3-38
Uploading IDS Signatures 3-41
Downloading IDS Signatures 3-42
Enabling or Disabling IDS Signatures 3-43
Enabling Web Login 3-46
Downloading Customized Web Authentication 3-47

Connecting to the Guest WLAN 3-49
Certificate Signing Request (CSR) Generation 3-49

CHAPTER 4 **Performing System Tasks** 4-1
Adding a Controller to the WCS Database 4-1
Additional Functionality with Location Appliance 4-2
Using WCS to Update System Software 4-2
Downloading Vendor Device Certificates 4-3
Downloading Vendor CA Certificates 4-4
Using WCS to Enable Long Preambles for SpectraLink NetLink Phones 4-5
Creating an RF Calibration Model 4-6

CHAPTER 5 **Adding and Using Maps** 5-1
Monitoring Maps Overview 5-2
Configuring Edit View 5-3
Edit View Command Buttons 5-3
Select a Command for Maps 5-4
Adding a Campus Map 5-4
Adding Buildings 5-5
Adding a Building to a Campus Map 5-5
Adding a Standalone Building 5-9
Managing a Current Campus 5-10
Editing a Current Campus 5-11
Moving Buildings 5-12
Deleting a Map 5-12
Editing Map Properties 5-13
Copying a Map 5-13
Exporting a Map 5-15
Importing a Map 5-15
Managing Location Presence Information 5-16
Enabling Location Presence for Mobility Services 5-18
Adding Outdoor Areas 5-19
Deleting Outdoor Areas 5-21
Searching Maps 5-21
Adding and Enhancing Floor Plans 5-22
Adding Floor Plans to a Campus Building 5-22
Adding Floor Plans to a Standalone Building 5-27
Using the Map Editor 5-29

Map Editor Functions 5-29
Using the Map Editor to Draw Polygon Areas 5-30
Planning Mode 5-36
Accessing Planning Mode 5-36
Using Planning Mode to Calculate Access Point Requirements 5-37
Inspecting VoWLAN Location Readiness 5-43
Troubleshooting Voice RF Coverage Issues 5-44
Adding Access Points 5-44
Placing Access Points 5-49
Guidelines for Placing Access Points 5-49
Import Map and AP Location Data 5-51
Positioning Access Points, Wi-Fi TDOA Receivers, and Chokepoints by Importing or Exporting a File 5-53
Floor Area Map Overview 5-54
Floor Settings 5-54
Viewing Floor Component Details 5-61
Floor View Navigation 5-70
Select a Command for Floor Areas 5-71
Refresh Options 5-72
Creating a Network Design 5-73
Designing a Network 5-73
Changing Access Point Positions by Importing and Exporting a File 5-78
Importing or Exporting WLSE Map Data 5-79

CHAPTER 6 **Monitoring Wireless Devices** 6-1
Rogue Access Point Location, Tagging, and Containment 6-1
Configuring ACS View Server Credentials 6-2
Receiving Radio Measurements 6-2
Monitoring Mesh Networks Using Maps 6-3
Monitoring Mesh Link Statistics Using Maps 6-3
Monitoring Mesh Access Points Using Maps 6-6
Monitoring Mesh Access Point Neighbors Using Maps 6-8
Monitoring Mesh Health 6-11
Mesh Statistics for an Access Point 6-15
Viewing the Mesh Network Hierarchy 6-19
Using Mesh Filters to Modify Map Display of Maps and Mesh Links 6-21
Monitoring Channel Width 6-23
Viewing Google Earth Maps 6-26

Google Earth Settings 6-27
Viewing Clients Identified as WGBs 6-28
Retrieving the Unique Device Identifier on Controllers and Access Points 6-29
Coverage Hole 6-32
Monitoring Pre-Coverage Holes 6-32
Viewing DHCP Statistics 6-34
Guest User Monitoring 6-36
RRM Dashboard 6-36
Channel Change Notifications 6-37
Transmission Power Change Notifications 6-38
RF Grouping Notifications 6-38
Viewing the RRM Dashboard 6-38

CHAPTER 7 **Managing WCS User Accounts** 7-1
Adding WCS User Accounts 7-1
Deleting WCS User Accounts 7-4
Changing Passwords 7-4
Monitoring Active Sessions 7-4
Viewing or Editing User Information 7-6
Setting the Lobby Ambassador Defaults 7-7
Viewing or Editing Group Information 7-8
Editing the Guest User Credentials 7-9
Viewing the Audit Trail 7-9
Creating Guest User Accounts 7-10
Logging in to the WCS User Interface as a Lobby Ambassador 7-11
Managing WCS Guest User Accounts 7-12
Scheduling WCS Guest User Accounts 7-12
Printing or E-mailing WCS Guest User Details 7-14
Saving Guest Accounts on a Device 7-14
Editing the Guest User Credentials 7-14
Adding a New User 7-15
Adding User Names, Passwords, and Groups 7-15
Assigning a Virtual Domain 7-16
Virtual Domain RADIUS and TACACS+ Attributes 7-18
Understanding Virtual Domains as a User 7-18

CHAPTER 8 **Configuring Mobility Groups** 8-1
Overview of 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 8-7
Configuring Mobility Groups 8-8
Prerequisites 8-8
Setting the Mobility Scalability Parameters 8-12
Mobility Anchors 8-13
Configuring Mobility Anchors 8-13
Configuring Multiple Country Codes 8-16
Creating Config Groups 8-19
Adding New Group 8-20
Configuring Config Groups 8-21
Adding or Removing Controllers from Config Group 8-22
Adding or Removing Templates from the Config Group 8-23
Applying or Scheduling Config Groups 8-23
Auditing Config Groups 8-24
Rebooting Config Groups 8-25
Reporting Config Groups 8-26
Downloading Software 8-26
Downloading IDS Signatures 8-27
Downloading Customized WebAuth 8-27

CHAPTER 9 **Configuring Access Points** 9-1
Setting AP Failover Priority 9-1
Configuring Global Credentials for Access Points 9-2
Configuring Ethernet Bridging and Ethernet VLAN Tagging 9-3
Enabling Ethernet Bridging and VLAN Tagging 9-7
Autonomous to Lightweight Migration Support 9-9
Adding Autonomous Access Points to WCS 9-10
Adding Autonomous Access Points by Device Information 9-10
Adding Autonomous Access Points by CSV File 9-10
Viewing Autonomous Access Points in WCS 9-12
Downloading Images to Autonomous Access Points 9-12
Work Group Bridge (WGB) Mode 9-12
Autonomous Access Point to Lightweight Access Point Migration 9-13
Viewing the Migration Analysis Summary 9-14
Upgrading Autonomous Access Points 9-14

Changing Station Role to Root Mode 9-15
Running Migration Analysis 9-15
Generating the Migration Analysis Report 9-15
Adding/Modifying a Migration Template 9-15
Configuring Access Points 9-17
Downloading Images 9-25
Importing Access Point Configuration 9-25
11n Antenna Selection 9-25
Configuring Access Point Radios for Tracking Optimized Monitor Mode 9-33
Scheduling Radio Status 9-34
Viewing Scheduled Tasks 9-34
Viewing Audit Status (for Access Points) 9-35
Searching Access Points 9-35
Viewing Mesh Link Details 9-36
Viewing or Editing Rogue Access Point Rules 9-36
Configuring Spectrum Experts 9-37
Adding a Spectrum Expert 9-37
Monitoring Spectrum Experts 9-38
Spectrum Experts > Summary 9-38
Interferers > Summary 9-38
Spectrum Experts Details 9-39
OfficeExtend Access Point 9-39
Licensing for an OfficeExtend Access Point 9-40
Configuring Link Latency Settings for Access Points 9-40

CHAPTER 10 **Configuring Controllers and Switches** 10-1
Adding Controllers 10-2
Downloading Software to Controllers 10-4
Discovering Templates from Controllers 10-9
Displaying Templates Applied to Controller 10-10
Configuring Controllers and Switches 10-10
Configuring DHCP Scopes 10-10
Configuring DHCP Proxy 10-11
Configuring IGMP Snooping 10-12
Configuring AP Timers 10-12
Configuring Controller WLANs 10-13
Viewing WLAN Details 10-14
General Tab 10-15

Security Tab 10-16
QoS Tab 10-20
Advanced Tab 10-20
Adding a WLAN 10-23
Deleting a WLAN 10-24
Managing WLAN Status Schedules 10-25
Viewing WLAN Configuration Scheduled Task Results 10-26
Mobility Anchors 10-26
Configuring AAA General Parameters 10-27
Configuring Local Network Users 10-28
Configuring New LDAP Bind Requests 10-28
Setting Multiple Country Codes 10-29
Configuring Aggressive Load Balancing 10-30
Configuring Band Selection 10-31
Guidelines for Using Band Selection 10-32
Configuration Steps 10-32
Searching Controllers 10-33
Managing User Authentication Order 10-34
Viewing Audit Status (for Controllers) 10-34
Viewing Latest Network Audit Report 10-37
Configuring 802.3 Bridging 10-37
Setting AP Failover Priority 10-38
Sending Primary Discovery Requests 10-38
Pinging a Network Device from a Controller 10-39
Enabling Load-Based CAC for Controllers 10-39
Configuring CleanAir Parameters (for 802.11a/n or 802.11b/g/n) 10-41
Configuring an RRM Threshold Controller (for 802.11a/n or 802.11b/g/n) 10-42
Configuring 40-MHz Channel Bonding 10-42
Configuring EDCA Parameters for Individual Controller 10-44
Configuring SNMPv3 10-44
Viewing All Current Templates 10-45
Configuring NAC Out-of-Band Integration 10-45
Guidelines for Using NAC Out-of-Band Integration 10-46
Configuring NAC Out-of-Band Integration 10-47
Configuring Wired Guest Access 10-51
Creating an Ingress Interface 10-52
Creating an Egress Interface 10-53

Creating a Wired LAN for Guest Access 10-54
Using Switch Port Tracing 10-57
Switch VLANs 10-60
Removing Switches 10-61
Shutting a Switch Port 10-61
Client Access on 1524SB Dual Backhaul 10-62
Configuring Client Access using WCS 10-62
Backhaul Channel Deselection Using WCS 10-63
Configuring Mesh DCA Flag on Controllers Using WCS 10-63
Changing the Channel List Using Config Groups 10-63
Background Scanning on 1510s in Mesh Networks 10-64
Background Scanning Scenarios 10-64
Enabling Background Scanning 10-65
Configuring QoS Profiles 10-66

CHAPTER 11 **Managing Clients** 11-1
Client Tab 11-1
Client Distribution 11-2
Client Protocol Distribution 11-3
Client Count 11-3
Client Alarm Summary 11-5
Client Traffic 11-6
Client Authentication Type Distribution 11-6
AP Join Taken Time 11-7
AP Threats/Attacks 11-7
Client Detail Page 11-8
Running a Link Test 11-9
Enabling Automatic Client Troubleshooting 11-10
Client Details from Access Point Page 11-11
Running Client Reports 11-11
Client Troubleshooting 11-11
Troubleshooting from the Client Tab Dashboard 11-11
Troubleshooting Using the Search Feature 11-12

CHAPTER 12 **Using Templates** 12-1
Controller Template Launch Pad 12-1
Adding Controller Templates 12-3
Configuring Controller Templates 12-3

Configuring General Templates 12-4
Configuring an NTP Server Template 12-8
Configuring AP 802.1X Supplicant Credentials 12-9
Configuring DHCP Template 12-10
Configuring Dynamic Interface Templates 12-11
Configuring QoS Templates 12-13
Configuring AP Timers 12-15
Configuring a Traffic Stream Metrics QoS Template 12-16
Configuring WLAN Templates 12-18
Security 12-20
QoS 12-28
Advanced 12-29
Configuring WLAN AP Groups 12-32
Adding Access Point Groups 12-33
Deleting Access Point Groups 12-34
Configuring H-REAP AP Groups 12-34
Configuring a File Encryption Template 12-36
Configuring a RADIUS Authentication Template 12-37
Configuring a RADIUS Accounting Template 12-40
Configuring a RADIUS Fallback Template 12-41
Configuring a LDAP Server Template 12-43
Configuring a TACACS+ Server Template 12-45
Configuring a Local EAP General Template 12-46
Configuring a Local EAP Profile Template 12-47
Configuring an EAP-FAST Template 12-49
Configuring Network User Credential Retrieval Priority Templates 12-51
Configuring a Local Network Users Template 12-52
Configuring Guest User Templates 12-54
Configuring a User Login Policies Template 12-56
Configuring a MAC Filter Template 12-57
Configuring an Access Point or MSE Authorization 12-59
Configuring a Manually Disabled Client Template 12-60
Configuring a Client Exclusion Policies Template 12-61
Configuring an Access Point Authentication and MFP Template 12-63
Configuring a Web Authentication Template 12-64
Downloading a Customized Web Authentication Page 12-67
Configuring External Web Auth Server 12-69
Configuring Access Control List Templates 12-69
Configuring a CPU Access Control List (ACL) Template 12-74
Configuring a Rogue Policies Template 12-75

Configuring a Rogue AP Rules Template 12-77
Configuring a Rogue AP Rule Groups Template 12-79
Configuring a Friendly Access Point Template 12-81
Configuring Radio Templates (for 802.11a/n or 802.11b/g/n) 12-83
Configuring a Voice Parameter Template (for 802.11a/n or 802.11b/g/n) 12-86
Configuring a Video Parameter Template (for 802.11a/n or 802.11b/g/n) 12-87
Configuring EDCA Parameters through a Controller Template 12-88
Configuring a Roaming Parameters Template (for 802.11a/n or 802.11b/g/n) 12-90
Configuring an RRM Threshold Template (for 802.11a/n or 802.11b/g/n) 12-91
Configuring an RRM Interval Template (for 802.11a/n or 802.11b/g/n) 12-93
Configuring an 802.11h Template 12-94
Configuring a High Throughput Template (for 802.11a/n or 802.11b/g/n) 12-95
Configuring CleanAir Controller Templates (for 802.11a/n or 802.11b/g/n) 12-96
Editing Existing CleanAir Controller Templates (802.11a/n or 802.11 b/g/n) 12-97
Adding a New CleanAir Controller Template (802.11a/n or 802.11 b/g/n) 12-97
Configuring a Mesh Template 12-98
Configuring a Trap Receiver Template 12-100
Configuring a Trap Control Template 12-101
Configuring a Telnet SSH Template 12-104
Configuring a Legacy Syslog Template 12-105
Configuring a Multiple Syslog Template 12-106
Configuring a Local Management User Template 12-107
Configuring a User Authentication Priority Template 12-108
Applying a Set of CLI Commands 12-109
Configuring Location Settings 12-110
Applying Controller Templates 12-112
Deleting a Controller Template 12-113
Adding Access Point Templates 12-113
Configuring Access Point Templates 12-113
Applying or Scheduling Templates 12-119
Configuring Scheduled Configuration Tasks 12-121
AP Template Tasks 12-121
Config Group Tasks 12-123
WLAN Configuration 12-124
Download Software 12-125
Configuring Radio Templates 12-130
Selecting Access Points 12-132
Applying the Report 12-133

CHAPTER 13 **Mobility Services** 13-1

CAS 13-1

wIPS 13-1

MSE Services Co-Existence 13-2

Adding a Mobility Services Engine to Cisco WCS 13-2

Deleting a Mobility Services Engine from the Cisco WCS 13-4

Keeping the Mobility Services Engines Synchronized 13-4

Synchronizing Cisco WCS and a Mobility Services Engine 13-4

Configuring Automatic Database Synchronization and Out of Sync Alerts 13-6

Smart Controller Assigment and Selection Scenarios 13-8

Out-of-Sync Alarms 13-8

Viewing Synchronization Information 13-9

Viewing Mobility Services Engine Synchronization Status 13-9

Viewing Synchronization History 13-9

Adding and Deleting Event Groups 13-10

Adding Event Groups 13-10

Deleting Event Groups 13-11

Adding Event Definitions 13-11

Planning for and Configuring Context-Aware Software 13-14

wIPS Planning and Configuring 13-16

CHAPTER 14 **Performing Maintenance Operations** 14-1

Verifying the Status of WCS 14-1

Checking the Status of WCS on Windows 14-1

Checking the Status of WCS on Linux 14-2

Stopping WCS 14-2

Stopping WCS on Windows 14-2

Stopping WCS on Linux 14-3

Backing Up the WCS Database 14-3

Scheduling Automatic Backups 14-3

Performing a Manual Backup 14-4

Backing Up the WCS Database (for Windows) 14-4

Backing Up the WCS Database (for Linux) 14-5

Restoring the WCS Database 14-5

Restoring the WCS Database (for Windows) 14-6

Restoring the WCS Database (for Linux) 14-7

Restoring the WCS Database in a High Availability Environment 14-8

Uninstalling WCS 14-8
Uninstalling WCS on Windows 14-8
Uninstalling WCS on Linux 14-9
Upgrading WCS 14-9
Using the Installer to Upgrade WCS for Windows 14-10
Using the Installer to Upgrade WCS for Linux 14-13
Manually Upgrading WCS on Windows 14-14
Manually Upgrading WCS on Linux 14-14
Upgrading WCS in a High Availability Environment 14-15
Upgrading the Network 14-15
Reinitializing the Database 14-15
Recovering the WCS Password 14-16

CHAPTER 15 **Configuring Hybrid REAP** 15-1
Overview of Hybrid REAP 15-1
Hybrid-REAP Authentication Process 15-2
Hybrid REAP Guidelines 15-4
Configuring Hybrid REAP 15-4
Configuring the Switch at the Remote Site 15-4
Configuring the Controller for Hybrid REAP 15-5
Configuring an Access Point for Hybrid REAP 15-9
Connecting Client Devices to the WLANs 15-12
Hybrid REAP Access Point Groups 15-12
Hybrid-REAP Groups and Backup RADIUS Servers 15-13
Hybrid-REAP Groups and CCKM 15-13
Hybrid-REAP Groups and Local Authentication 15-14
Configuring Hybrid-REAP Groups 15-14
Auditing an H-REAP Group 15-16

CHAPTER 16 **Alarms and Events** 16-1
Using the Alarm Summary 16-1
Customizing Alarm Summary Results 16-4
Monitoring Alarms 16-5
Monitoring Alarm Overview 16-5
Select a Command Menu 16-8
Using Edit View for Alarms 16-8
Viewing Alarm Details 16-9
Monitoring Rogue Access Point Alarms 16-10

Select a Command 16-11
Using Advanced Search 16-12
Configuring Alarm Severity 16-14
Viewing Rogue Access Point Details 16-14
Acknowledging Alarms 16-16
Monitoring Air Quality Alarms 16-16
Monitoring CleanAir Security Alarms 16-18
Monitoring Adhoc Rogue Alarms 16-19
Monitoring Adhoc Rogue Details 16-20
Rogue Access Point Location, Tagging, and Containment 16-21
Detecting Access Points 16-21
Monitoring Rogue Alarm Events 16-22
Monitoring E-mail Notifications 16-23
Monitoring Severity Configurations 16-23
Monitoring CleanAir Air Quality Events 16-24
Viewing Air Quality Event Details 16-24
Monitoring Interferer Security Risk Events 16-25
Viewing Interferer Security Risk Event Details 16-26
Alarm and Event Dictionary 16-26
Notification Format 16-26
Traps Added in Release 2.0 16-28
AP_BIG_NAV_DOS_ATTACK 16-28
AP_CONTAINED_AS_ROGUE 16-28
AP_DETECTED_DUPLICATE_IP 16-28
AP_HAS_NO_RADIOS 16-29
AP_MAX_ROGUE_COUNT_CLEAR 16-29
AP_MAX_ROGUE_COUNT_EXCEEDED 16-29
AUTHENTICATION_FAILURE (From MIB-II standard) 16-29
BSN_AUTHENTICATION_FAILURE 16-30
COLD_START (FROM MIB-II STANDARD) 16-31
CONFIG_SAVED 16-31
IPSEC_IKE_NEG_FAILURE 16-31
IPSEC_INVALID_COOKIE 16-32
LINK_DOWN (FROM MIB-II STANDARD) 16-32
LINK_UP (FROM MIB-II STANDARD) 16-32
LRAD_ASSOCIATED 16-32
LRAD_DISASSOCIATED 16-33
LRADIF_COVERAGE_PROFILE_FAILED 16-33
LRADIF_COVERAGE_PROFILE_PASSED 16-33
LRADIF_CURRENT_CHANNEL_CHANGED 16-34

LRADIF_CURRENT_TXPOWER_CHANGED 16-34
LRADIF_DOWN 16-34
LRADF_INTERFERENCE_PROFILE_FAILED 16-35
LRADIF_INTERFERENCE_PROFILE_PASSED 16-35
LRADIF_LOAD_PROFILE_FAILED 16-36
LRADIF_LOAD_PROFILE_PASSED 16-36
LRADIF_NOISE_PROFILE_FAILED 16-36
LRADIF_NOISE_PROFILE_PASSED 16-37
LRADIF_UP 16-37
MAX_ROGUE_COUNT_CLEAR 16-37
MAX_ROGUE_COUNT_EXCEEDED 16-38
MULTIPLE_USERS 16-38
NETWORK_DISABLED 16-38
NO_ACTIVITY_FOR_ROGUE_AP 16-38
POE_CONTROLLER_FAILURE 16-39
RADIOS_EXCEEDED 16-39
RADIUS_SERVERS_FAILED 16-39
ROGUE_AP_DETECTED 16-40
ROGUE_AP_ON_NETWORK 16-40
ROGUE_AP_REMOVED 16-41
RRM_DOT11_A_GROUPING_DONE 16-41
RRM_DOT11_B_GROUPING_DONE 16-41
SENSED_TEMPERATURE_HIGH 16-42
SENSED_TEMPERATURE_LOW 16-42
STATION_ASSOCIATE 16-42
STATION_ASSOCIATE_FAIL 16-43
STATION_AUTHENTICATE 16-43
STATION_AUTHENTICATION_FAIL 16-43
STATION_BLACKLISTED 16-44
STATION_DEAUTHENTICATE 16-44
STATION_DISASSOCIATE 16-44
STATION_WEP_KEY_DECRYPT_ERROR 16-45
STATION_WPA_MIC_ERROR_COUNTER_ACTIVATED 16-45
SWITCH_DETECTED_DUPLICATE_IP 16-45
SWITCH_DOWN 16-46
SWITCH_UP 16-46
TEMPERATURE_SENSOR_CLEAR 16-46
TEMPERATURE_SENSOR_FAILURE 16-47
TOO_MANY_USER_UNSUCCESSFUL_LOGINS 16-47
Traps Added in Release 2.1 16-47

ADHOC_ROGUE_AUTO_CONTAINED 16-47
ADHOC_ROGUE_AUTO_CONTAINED_CLEAR 16-48
NETWORK_ENABLED 16-48
ROGUE_AP_AUTO_CONTAINED 16-48
ROGUE_AP_AUTO_CONTAINED_CLEAR 16-48
TRUSTED_AP_INVALID_ENCRYPTION 16-49
TRUSTED_AP_INVALID_ENCRYPTION_CLEAR 16-49
TRUSTED_AP_INVALID_RADIO_POLICY 16-49
TRUSTED_AP_INVALID_RADIO_POLICY_CLEAR 16-49
TRUSTED_AP_INVALID_SSID 16-50
TRUSTED_AP_INVALID_SSID_CLEAR 16-50
TRUSTED_AP_MISSING 16-50
TRUSTED_AP_MISSING_CLEAR 16-50
Traps Added in Release 2.2 16-51
AP_IMPERSONATION_DETECTED 16-51
AP_RADIO_CARD_RX_FAILURE 16-51
AP_RADIO_CARD_RX_FAILURE_CLEAR 16-51
AP_RADIO_CARD_TX_FAILURE 16-52
AP_RADIO_CARD_TX_FAILURE_CLEAR 16-52
SIGNATURE_ATTACK_CLEARED 16-52
SIGNATURE_ATTACK_DETECTED 16-53
TRUSTED_AP_HAS_INVALID_PREAMBLE 16-53
TRUSTED_HAS_INVALID_PREAMBLE_CLEARED 16-53
Traps Added in Release 3.0 16-54
AP_FUNCTIONALITY_DISABLED 16-54
AP_IP_ADDRESS_FALLBACK 16-54
AP_REGULATORY_DOMAIN_MISMATCH 16-55
RX_MULTICAST_QUEUE_FULL 16-55
Traps Added in Release 3.1 16-56
AP_AUTHORIZATION_FAILURE 16-56
HEARTBEAT_LOSS_TRAP 16-56
INVALID_RADIO_INTERFACE 16-57
RADAR_CLEARED 16-57
RADAR_DETECTED 16-57
RADIO_CORE_DUMP 16-58
RADIO_INTERFACE_DOWN 16-58
RADIO_INTERFACE_UP 16-58
UNSUPPORTED_AP 16-59
Traps Added in Release 3.2 16-59
LOCATION_NOTIFY_TRAP 16-59

Traps Added In Release 4.0 16-60
CISCO_LWAPP_MESH_POOR_SNR 16-60
CISCO_LWAPP_MESH_PARENT_CHANGE 16-60
CISCO_LWAPP_MESH_CHILD_MOVED 16-60
CISCO_LWAPP_MESH_CONSOLE_LOGIN 16-61
CISCO_LWAPP_MESH_AUTHORIZATION_FAILURE 16-61
CISCO_LWAPP_MESH_CHILD_EXCLUDED_PARENT 16-62
CISCO_LWAPP_MESH_EXCESSIVE_PARENT_CHANGE 16-62
IDS_SHUN_CLIENT_TRAP 16-62
IDS_SHUN_CLIENT_CLEAR_TRAP 16-63
MFP_TIMEBASE_STATUS_TRAP 16-63
MFP_ANOMALY_DETECTED_TRAP 16-64
GUEST_USER_REMOVED_TRAP 16-64
Traps Added or Updated in Release 4.0.96.0 16-65
AP_IMPERSONATION_DETECTED 16-65
RADIUS_SERVER_DEACTIVATED 16-65
RADIUS_SERVER_ACTIVATED 16-65
RADIUS_SERVER_WLAN_DEACTIVATED 16-66
RADIUS_SERVER_WLAN_ACTIVATED 16-66
RADIUS_SERVER_TIMEOUT 16-66
DECRYPT_ERROR_FOR_WRONG_WPA_WPA2 16-66
Traps Added or Updated in Release 4.1 16-67
AP_IMPERSONATION_DETECTED 16-67
INTERFERENCE_DETECTED 16-67
INTERFERENCE_CLEAR 16-67
ONE_ANCHOR_ON_WLAN_UP 16-68
RADIUS_SERVER_DEACTIVATED 16-68
RADIUS_SERVER_ACTIVATED 16-68
RADIUS_SERVER_WLAN_DEACTIVATED 16-68
RADIUS_SERVER_WLAN_ACTIVATED 16-69
RADIUS_SERVER_TIMEOUT 16-69
MOBILITY_ANCHOR_CTRL_PATH_DOWN 16-69
MOBILITY_ANCHOR_CTRL_PATH_UP 16-69
MOBILITY_ANCHOR_DATA_PATH_DOWN 16-70
MOBILITY_ANCHOR_DATA_PATH_UP 16-70
WLAN_ALL_ANCHORS_TRAP_DOWN 16-70
MESH_AUTHORIZATIONFAILURE 16-71
MESH_CHILDEXCLUDEDPARENT 16-71
MESH_PARENTCHANGE 16-71
MESH_CHILDMOVED 16-72

MESH_EXCESSIVEPARENTCHANGE 16-72
MESH_POORSNR 16-72
MESH_POORSNRCLEAR 16-73
MESH_CONSOLELOGIN 16-73
LRADIF_REGULATORY_DOMAIN 16-73
LRAD_CRASH 16-74
LRAD_UNSUPPORTED 16-74
Traps Added or Updated in Release 4.2 16-74
GUEST_USER_ADDED 16-74
GUEST_USER_AUTHENTICATED 16-75
IOSAP_LINK_UP 16-75
IOSAP_LINK_DOWN 16-75
IOSAP_UP 16-76
IOSAP_DOWN 16-76
WCS_EMAIL_FAILURE 16-76
AUDIT_STATUS_DIFFERENCE 16-77
LRAD_POE_STATUS 16-77
ROGUE_AP_NOT_ON_NETWORK 16-77
Traps Added or Updated in Release 5.0 16-78
GUEST_USER_LOGOFF 16-78
WCS_NOTIFICATION_FAILURE 16-78
WCS_LOW_DISK_SPACE 16-78
WCS_OK_DISK_SPACE 16-79
WCS_LOW_DISK_SPACE_BACKUP 16-79
STATION_ASSOCIATE_DIAG_WLAN 16-79
WLAN_SHUT_FAILED 16-80
WLAN_SHUT_SUCCESS 16-80
RADIO_SHUT_FAILED 16-81
RADIO_SHUT_SUCCESS 16-81
Traps Added or Updated in Release 5.1 16-82
CONFIGAUDITSET_ENFORCEMENT_SUCCESS 16-82
CONFIGAUDITSET_ENFORCEMENT_FAIL 16-82
Traps Added or Updated in Release 6.0 16-82
STATION_AUTHENTICATED 16-82
WCS_CLIENT_TRAP_DISABLED 16-83
WLC_LICENSE_NOT_ENFORCED 16-83
WLC_LICENSE_COUNT_EXCEEDED 16-83
VOIP_CALL_FAILURE 16-84
MSE_EVAL_LICENSE 16-84
MSE_LICENSING_ELEMENT_LIMIT 16-84

Traps Added or Updated in Release 7.0 16-84
SI_AQ_TRAPS 16-85
SI_SECURITY_TRAPS 16-85
SI_SENSOR_CRASH_TRAPS 16-85
Unsupported Traps 16-85

CHAPTER 17 **Running Reports** 17-1
Report Launch Pad 17-2
Creating and Running a New Report 17-2
Managing Current Reports 17-8
Managing Scheduled Run Results 17-9
Sorting Scheduled Run Results 17-10
Viewing or Editing Scheduled Run Details 17-10
Managing Saved Reports 17-11
Sorting Saved Reports 17-11
Viewing or Editing Saved Report Details 17-12
Running a Saved Report 17-12
Specific WCS Reports 17-13
CleanAir Reports 17-14
Air Quality vs Time 17-14
Security Risk Interferers 17-16
Worst Air Quality APs 17-18
Worst Interferers 17-19
Client Reports 17-21
Busiest Clients 17-22
Client Count 17-24
Client Sessions 17-26
Client Summary 17-29
Client Traffic Stream Metrics 17-33
Throughput 17-35
Unique Clients 17-37
V5 Client Statistics 17-40
Compliance Reports 17-41
Configuration Audit 17-41
Payment Card Industry (PCI) 17-43
Device Reports 17-48
AP Image Predownload 17-48
AP Profile Status 17-49
Busiest APs 17-51

AP Summary 17-53
Inventory Reports 17-55
Uptime 17-58
Utilization 17-60
Guest Reports 17-62
Guest Accounts Status 17-62
Guest Association 17-64
Guest Count 17-65
Guest User Sessions 17-66
WCS Guest Operations 17-67
Mesh Reports 17-68
Alternate Parent 17-69
Link Stats 17-70
Nodes 17-72
Packet Stats 17-73
Packet Error Statistics 17-75
Packet Queue Statistics 17-77
Stranded APs 17-79
Worst Node Hops 17-80
Network Summary 17-82
802.11n Summary 17-82
Executive Summary 17-84
Performance Reports 17-86
802.11 Counters 17-87
Coverage Hole 17-89
Network Utilization 17-91
Traffic Stream Metrics 17-93
Tx Power and Channel 17-96
VoIP Calls Graph 17-97
VoIP Calls Table 17-99
Voice Statistics 17-100
Security Reports 17-102
Adaptive wIPS Alarms 17-103
Adaptive wIPS Top 10 Access Points 17-105
Adhoc Rogue Events 17-107
Adhoc Rogues 17-109
New Rogue Access Points 17-111
New Rogue Access Point Count 17-113
Rogue Access Points Events 17-115
Rogue Access Points 17-117

Security Summary 17-119

CHAPTER 18 **Administrative Tasks** 18-1

Running Background Tasks 18-1

Performing a Task 18-2

Configuration Sync 18-5

Controller License Status 18-6

WCS Historical Data 18-7

Importing Tasks Into ACS 18-8

Adding WCS to an ACS Server 18-8

Adding WCS as a TACACS+ Server 18-9

Adding WCS UserGroups into ACS for TACACS+ 18-10

Adding WCS to ACS server for Use with RADIUS 18-13

Adding WCS UserGroups into ACS for RADIUS 18-14

Adding WCS to a Non-Cisco ACS Server for Use with RADIUS 18-17

Setting AAA Mode 18-18

Auto Provisioning 18-19

Auto Provisioning Device Management (Auto Provisioning Filter List) 18-20

Auto Provisioning Setting (Auto Provisioning Primary Search Key Setting) 18-28

Turning Password Rules On or Off 18-29

Configuring TACACS+ Servers 18-29

Configuring RADIUS Servers 18-31

Establishing Logging Options 18-32

Using Logging Options to Enhance Troubleshooting 18-34

Performing Data Management Tasks 18-34

Alarms 18-35

Audit 18-37

Configuring Audit Parameters 18-38

Client 18-39

CLI Session 18-41

Controller Upgrade Settings 18-41

Data Management 18-42

Guest Account Settings 18-43

Login Disclaimer 18-44

Mail Server Configuration 18-45

Notification Receiver 18-47

MIB to WCS alert/event mapping 18-50

Report 18-52

Server Settings 18-53
Severity Configurations 18-54
SNMP Credentials 18-56
SNMP Settings 18-58
Switch Port Trace 18-60
High Availability 18-62
Failover Scenario 18-62
Prerequisites and Limitations 18-63
Configuring High Availability 18-64
Deploying High Availability 18-65
Adding a New Primary WCS 18-66
Removing a Primary WCS 18-66
Setting User Preferences 18-66
Accessing the License Center 18-67
WCS License Information 18-68
Controller License Information 18-69
MSE License Information 18-70
Controller 18-71
MSE 18-72
Managing Individual Licenses 18-74
Managing Controller Licenses 18-74
Managing WCS Licenses 18-75
Managing MSE Licenses 18-76
Configuring ACS 5.x 18-76
Creating Network Devices and AAA Clients 18-76
Adding Groups 18-77
Adding Users 18-78
Creating Policy Elements or Authorization Profiles 18-78
Creating Policy Elements or Authorization Profiles for RADIUS 18-78
Creating Policy Elements or Authorization Profiles For TACACS 18-79
Creating Authorization Rules 18-80
Creating Service Selection Rules for RADIUS 18-80
Creating Service Selection Rules for TACACS 18-81
Configuring Access Services 18-82
Configuring Access Services for RADIUS 18-82
Configuring Access Services for TACACS 18-83

CHAPTER 19 **Tools Menu** 19-1
Using Voice Audit 19-1

Controller Tab 19-1
Rules Tab 19-2
Reports Tab 19-5
Voice Audit Details 19-5
Voice Audit Report Results 19-5
Verifying Location Accuracy 19-5
Using the Location Accuracy Tool to Test Location Accuracy 19-6
Using Scheduled Accuracy Testing to Verify Accuracy of Current Location 19-6
Using On-Demand Location Accuracy Testing 19-8
Viewing Configuration Audit Summary 19-9
Configuring Migration Analysis 19-10
Upgrading Autonomous Access Points 19-11
Viewing a Firmware Upgrade Report 19-11
Changing Station Role to Root Mode 19-11
Viewing a Role Change Report 19-12
Running Migration Analysis 19-12
Viewing a Migration Analysis Report 19-12

CHAPTER 20 **Virtual Domains** 20-1
Creating a Virtual Domain 20-1
Creating a New Virtual Domain 20-2
Understanding Virtual Domain Hierarchy 20-3
Modifying a Virtual Domain 20-7
Virtual Domain RADIUS and TACACS+ Attributes 20-9
Understanding Virtual Domains as a User 20-9
Viewing Assigned Virtual Domain Components 20-10

CHAPTER 21 **Google Earth Maps** 21-1
Creating an Outdoor Location Using Google Earth 21-1
Understanding Geographical Coordinates for Google Earth 21-1
Creating and Importing Coordinates in Google Earth (KML File) 21-2
Creating and Importing Coordinates as a CSV File 21-4
Importing a File into WCS 21-5
Viewing Google Earth Maps 21-6
Viewing Google Earth Map Details 21-6
Adding Google Earth Location Launch Points to Access Point Pages 21-7
Google Earth Settings 21-8

APPENDIX A **Troubleshooting and Best Practices** A-1

Troubleshooting Cisco Compatible Extensions Version 5 Client Devices A-1

Diagnostic Channel A-1

Configuring the Diagnostic Channel A-2

Web Auth Security on WLANs A-3

Debug Commands A-4

Debug Strategy A-4

Best Practices A-8

APPENDIX B **WCS and End-User Licenses** B-1

WCS Licenses B-1

Types of Licenses B-1

Licensing Enforcement B-2

Product Authorization Key Certificate B-3

Determining Which License To Use B-3

Installing a License B-4

Backup and Restore License B-4

Notices and Disclaimers B-5

Notices B-5

OpenSSL/Open SSL Project B-5

License Issues B-5

Disclaimers B-7

End-User License Agreement B-7

APPENDIX C **Conversion of a WLSE Autonomous Deployment to a WCS Controller Deployment** C-1

Supported Hardware C-2

Cisco WLSE Management Stations C-2

Autonomous Access Points Convertible to LWAPP C-2

Installation and Configuration C-2

Installing Cisco WCS C-2

Upgrading to Red Hat Enterprise Linux 4 or 5 C-3

Minor Upgrades to WCS C-3

Configuring the Converted Appliance C-4

Licensing C-7

WLSE Upgrade License C-7

Preface

The preface provides an overview of the *Cisco Wireless Control System Configuration Guide, Release 7.0*, references related publications, and explains how to obtain other documentation and technical assistance, if necessary. It contains these sections:

- Audience, page xxix
- Purpose, page xxix
- Conventions, page xxix
- Related Publications, page xxx
- Obtaining Documentation and Submitting a Service Request, page xxx

Audience

This guide describes the Cisco Wireless Control System (WCS). It is meant for networking professional who uses WCS to manage a Cisco Unified Wireless Network Solution. To use this guide, you should be familiar with the concepts and terminology associated with wireless LANs.

Purpose

This guide provides the information you need to manage a Cisco Unified Wireless Network Solution using WCS.

Note This guide pertains specifically to WCS Release 7.0. Earlier versions of WCS software may look and operate somewhat differently.

Conventions

This publication uses the following conventions to convey instructions and information:

- Commands and keywords are in **boldface** text.
- Variables are in *italicized* text.

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

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

Related Publications

For more information about WCS and related products, see the following website:

http://www.cisco.com/cisco/web/psa/default.html

Obtaining Documentation and Submitting a Service Request

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

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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

CHAPTER 1

Overview

This chapter describes the Cisco Unified Wireless Network Solution and the Cisco WCS. It contains these sections:

- The Cisco Unified Wireless Network Solution, page 1-1
- The WCS, page 1-2
- WCS Versions, page 1-3
- Embedded Access Points, page 1-6
- WCS User Interface, page 1-9
- Cisco WCS Navigator, page 1-9

The Cisco Unified Wireless Network Solution

The Cisco Unified Wireless Network solution provides 802.11 wireless networking solutions for enterprises and service providers. It simplifies the deployment and management of large-scale wireless LANs and enables a you to create a unique best-in-class security infrastructure. The operating system manages all data client, communications, and system administration functions, performs radio resource management (RRM) functions, manages system-wide mobility policies using the operating system security solution, and coordinates all security functions using the operating system security framework.

The Cisco Unified Wireless Network Solution consists of Cisco Unified Wireless Network Controllers (hereafter called *controllers*) and their associated lightweight access points controlled by the operating system, all concurrently managed by any or all of the operating system user interfaces:

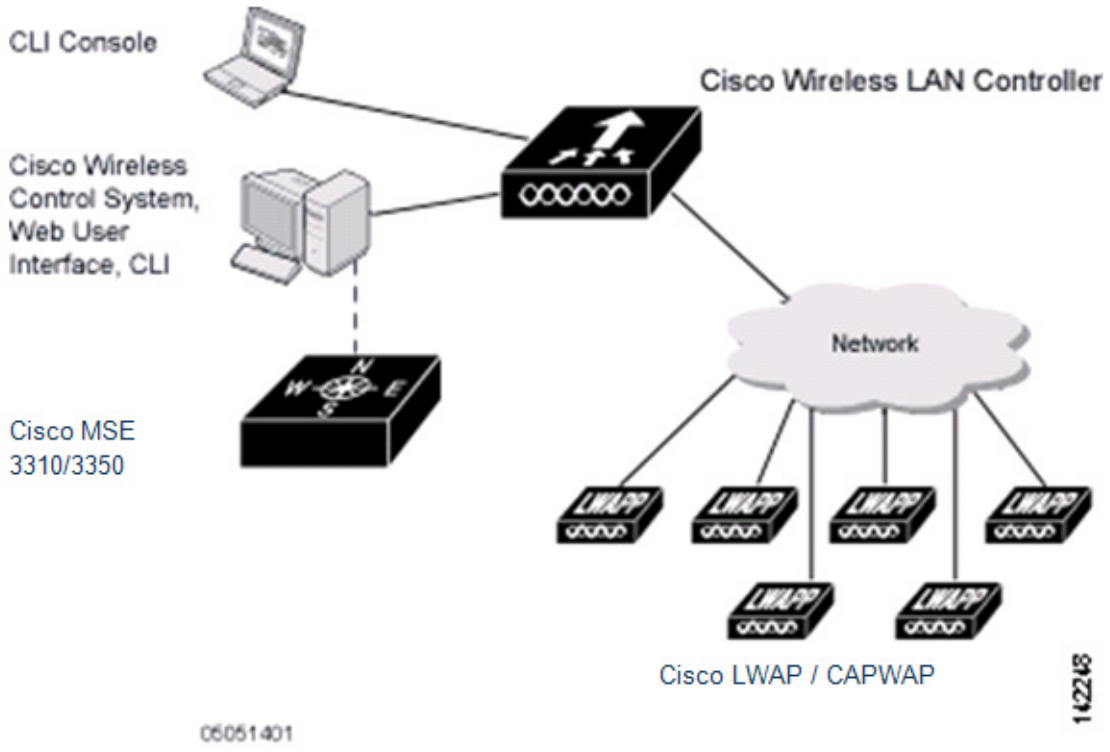
- An HTTPS full-featured web user interface hosted by Cisco controllers can be used to configure and monitor individual controllers.
- A full-featured command-line interface (CLI) can be used to configure and monitor individual controllers.
- WCS can be used to configure and monitor one or more controllers and associated access points. WCS has tools to facilitate large-system monitoring and control. It runs on Windows 2003 and Red Hat Enterprise Linux ES/AS 5.X servers.
- An industry-standard SNMP V1, V2c, and V3 interface can be used with any SNMP-compliant third-party network management system.

The Cisco Unified Wireless Network Solution supports client data services, client monitoring and control, and all rogue access point detection, monitoring, and containment functions. It uses lightweight access points, controllers, and the optional WCS to provide wireless services to enterprises and service providers.

Note Unless specified otherwise, information pertaining to controllers applies to all Cisco Unified Wireless Network Controllers, including but not limited to Cisco 2000 and 2100 Series Unified Wireless Network Controllers, Cisco 4100 Series Unified Wireless Network Controllers, Cisco 4400 Series Unified Wireless Network Controllers, Cisco 5500 Series Wireless LAN Controllers, and controllers within the Cisco Wireless Services Module (WiSM) and Cisco 26/28/37/38*xx* Series Integrated Services Routers.

Figure 1-1 shows the Cisco Unified Wireless Network Solution components, which can be simultaneously deployed across multiple floors and buildings.

Figure 1-1 Cisco Unified Wireless Network Solution



The WCS

WCS enables you to configure and monitor one or more controllers and associated access points. WCS 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.

WCS runs on Windows 2003/SP2, Windows 2003 R2/SP2 32-bit installations, and Red Hat Linux Enterprise Server 5.X 32-bit installations. On both Windows and Linux, WCS runs as a service, which runs continuously and resumes running after a reboot.

You must use Internet Explorer 7.0 or later in order to control all permitted Cisco Unified Wireless Network Solution configuration, monitoring, and control functions through Internet Explorer 7.0 with the Flash plugin, or Mozilla Firefox 3.5 or later. The administrator defines permissions from the Administration menu, which also enables the administrator to manage user accounts and schedule periodic maintenance tasks.

Note You are strongly advised not to enable third-party browser extensions. In Internet Explorer, you can disable third-party browser extensions by choosing Tools > Internet Options and unselecting the Enable third-party browser extensions check box on the Advanced tab.

WCS simplifies controller configuration and monitoring and reduces data entry errors. WCS uses the industry-standard SNMP protocol to communicate with the controllers.

This section contains the following topics:

- WCS Base, page 1-3
- WCS Base + Location, page 1-4
- Enabling Mobility Services and HA with WCSPLUS License, page 1-4

WCS Versions

You can install WCS with one of two capabilities: WCS Base or WCS Location. A license is required for both.

WCS Base

The WCS Base supports wireless client data access, rogue access point detection, and rogue ad hoc detection and containment functions (such as on-demand location of rogue access points that are mapped next to the detecting access point), and Cisco UWN Solution monitoring and control.

It also includes graphical views of the following:

- Autodiscovery of access points as they associate with controllers
- Autodiscovery and containment or notification of rogue access points
- Map-based organization of access point coverage areas, which is helpful when the enterprise spans more than one geographical area
- Ad hoc rogue detection
- User-supplied campus, building, and floor plan graphics, which show the following:
  - Locations and status of managed access points
  - Locations of rogue access points based on the signal strength received by the nearest managed Cisco access points
  - Coverage hole alarm information for access points based on the received signal strength from clients. This information appears in a table rather than map format.
  - RF coverage maps

The WCS Base also provides system-wide control of the following:

- Streamlined network, controller, and managed access point configuration using customer-defined templates
- Network, controller, and managed access point status and alarm monitoring
- Automated and manual data client monitoring and control functions
- Automated monitoring of rogue access points, rogue ad hoc events, coverage holes, security violations, controllers, and access points
- Full event logs for data clients, rogue access points, coverage holes, security violations, controllers, and access points
- Automatic channel and power level assignment by radio resource management (RRM)
- User-defined automatic controller status audits, missed trap polling, configuration backups, and policy cleanups
- Real-time location of rogue access points and rogue ad hoc events to the nearest Cisco access point
- Real-time and historical location of clients to the nearest Cisco access point

WCS Base + Location

WCS Location includes all the features of WCS Base as well as these enhancements:

- On-demand location of rogue access points and rogue ad hoc events to within 33 feet (10 meters)
- On-demand location of clients to within 33 feet (10 meters)
- Ability to use location appliances to collect and return historical location data viewable in the WCS Location user interface

Enabling Mobility Services and HA with WCSPLUS License

A Cisco WCS PLUS license supports Cisco WCS base license features and the following capabilities:

- Location services
- High availability

A Cisco WCS PLUS license is backward compatible to existing Cisco WCS location and enterprise licenses. The process to provision a Cisco WCS PLUS license is the same as provisioning a current Cisco WCS license. A PLUS license is required in order to enable mobility services engines which are launched with the Motion campaign.

Using WCS Cisco Location Appliances

When WCS Location is used, you can also deploy Cisco 2700 Series Location Appliances. The location appliance enhances WCS Location capabilities by computing, collecting, and storing historical location data, which can be displayed in WCS. In this role, the location appliance acts as a server to a WCS server by collecting, storing, and passing on data from its associated controllers.

When WCS is enhanced with a location appliance, it can display historical location data for up to 2,500 laptop clients, palmtop clients, VoIP telephone clients, radio frequency identifier (Wi-Fi tags) asset tags, rogue access points, rogue ad hoc events, and rogue clients for each location appliance in the Cisco Unified Wireless Network Solution. You can configure location appliances to collect this data and statistics at defined intervals.

You can also use WCS to configure location appliance event notification parameters. *Event notification* is a feature that enables you to define conditions that cause the location appliance to send notifications to the listeners that you specify in WCS.

In this way, WCS acts as a notification listener. It receives notifications from the location appliance in the form of the locationNotifyTrap trap as part of the bsnwras.my MIB file. WCS translates the traps into user interface alerts and displays the alerts in the following format:

```
Absence:
- Absence of Tag with MAC 00:0c:cc:5b:e4:1b, last seen at 16:19:45 13 Apr 2010.

Containment:
- Tag with MAC 00:0c:cc:5b:fa:44 is In the Area 'WNBU > WNBU > 4th Floor > wcsDevArea'

Distance:
- Tag with MAC 00:0c:cc:5b:fa:47 has moved beyond the distance configured for the marker
'marker2'.
- Tag with MAC 00:0c:cc:5b:f9:b9 has moved beyond 46.0 ft. of marker 'marker2', located at
a range of 136.74526528595058 ft.
```

Note See the *Cisco Location Application Configuration Guide* for more detailed information about the location appliance and its use with WCS.

The location appliance can be backed up to any WCS server into an operator-defined FTP folder, and the location appliance can be restored from that server at any time and at defined intervals. Also, the location appliance database can be synchronized with the WCS server database at any time. Operators can use the location appliance features and download new application code to all associated appliances from any WCS server.

Comparison of WCS Base and WCS Location Features

Table 1-1 WCS Base and WCS Location Features

Features	WCS Base	WCS Location
Location and tracking		
Low-resolution client location	Yes	—
High-resolution client location	—	Yes
Integration with location appliance	—	Yes
Low-resolution rogue access point location	Yes	—
High-resolution rogue access point location	—	Yes
Client data services, security, and monitoring		
Client access via access points	Yes	Yes
Multiple wireless LANs (individual SSIDs and policies)	Yes	Yes
Rogue access point detection and containment using access points	Yes	Yes
802.11a/b/g/n bands	Yes	Yes
Radio resource management		
Real-time channel assignment and rogue access point detection and containment	Yes	Yes
Real-time interference detection and avoidance, transmit power control, channel assignment, client mobility management, client load distribution, and coverage hole detection	Yes	Yes
Automated software and configuration updates	Yes	Yes
Wireless intrusion protection	Yes	Yes
Global and individual Access Point security policies	Yes	Yes
Controls Cisco Unified Wireless Network Controllers	Yes	Yes
Supported workstations		
Windows 2003	Yes	Yes
Red Hat Enterprise Linux ES 5.1	Yes	Yes
Mozilla Firefox 2.0.0.11 or later	Yes	Yes

Embedded Access Points

WCS software release 5.2 or later 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 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 this CLI command on the router in privileged EXEC mode: **service-module wlan-ap 0 bootimage unified**.

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

After enabling the recovery image, enter this CLI command on the router to shut down and reboot the access point: **service-module wlan-ap 0 reload**. 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.

Note To use the CLI commands mentioned previously, the router must be running Cisco IOS Release 12.4(20)T or later. If you experience any problems, refer to the "Troubleshooting an Upgrade or Reverting the AP to Autonomous Mode" section in the Integrated Services Router configuration guide at this URL:

http://cisco.com/en/US/docs/routers/access/800/860-880-890/software/configuration/guide/admin_ap.html#wp1061143

In order to support CAPWAP or LWAPP, the router must be activated with at least the Cisco Advanced IP Services IOS license-grade image. A license is required in order to upgrade to this Cisco IOS image on the router. See this URL for licensing information:

http://cisco.com/en/US/docs/routers/access/800/860-880-890/software/activation/Software_Activation_on_Cisco_Integrated_Routers.html

After the AP801 boots up with the recovery image for the unified mode, it requires an IP address in order to communicate with the controller and to download its unified image and configuration from the controller. The router can provide DHCP server functionality, the DHCP pool to reach the controller, and setup option 43 for the controller IP address in the DHCP pool configuration. Use the following configuration to perform this task.

```
ip dhcp pool pool_name
    network ip_address subnet_mask
    dns-server ip_address
    default-router ip_address
    option 43 hex controller_ip_address_in_hex
Example:
ip dhcp pool embedded-ap-pool
    network 209.165.200.224 255.255.255.224
    dns-server 209.165.200.225
    default-router 209.165.200.226
    option 43 hex f104.0a0a.0a0f /* single WLC IP address (209.165.201.0) in hex format */
```

The AP801 802.11n radio supports lower power levels than the 802.11n radio in the Cisco Aironet 1250 series access points. The AP801 stores the radio power levels and passes them to the controller when the access point joins the controller. The controller uses the supplied values to limit the user configuration.

The AP801 can be used in hybrid-REAP mode. See "Configuring Hybrid REAP" section on page 15-1 for more information on hybrid REAP.

Note For more information on the AP801, refer to the documentation for the Cisco 800 Series ISRs at this URL:

http://www.cisco.com/en/US/products/hw/routers/ps380/tsd_products_support_series_home.html.

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 Protocol (CAPWAP) 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 these 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 1142 series access point will only associate with CAPWAP controllers needs to be updated to say 1140 and 3500 series, and should go on to state 3500 will only connect with WLC running 7.0 code or above.

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.

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 these 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 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 access point's non-volatile memory. 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.

WCS User Interface

The WCS user interface enables the network operator to create and configure Cisco Unified Wireless Network Solution coverage area layouts, configure system operating parameters, monitor real-time Cisco Unified Wireless Network Solution operation, and perform troubleshooting tasks using an HTTPS web browser window. The WCS user interface also enables the WCS administrator to 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.

Note The Cisco WCS user interface requires Internet Explorer 7.0 or later, or Firefox 3.5 or later. Cisco recommends Firefox 3.5 or later on a Windows workstation for full access to WCS functionality. Internet Explorer 6.0 is not supported.

Cisco WCS Navigator

The Cisco Wireless Control System Navigator (Cisco WCS Navigator) manages multiple Cisco WCSs (running the same version as Navigator) and provides a unified view of the network. It uses SOAP/XML over HTTPs to communicate with individual WCSs. With WCS Navigator, there is monitoring

functionality and reporting capability across all WCSs. In addition, network wide searches are available. In Windows and Linux, Cisco WCS Navigator runs as a service, which runs continuously and resumes running after a reboot.

In order for the WCS Navigator to detect the regional WCSs, you must manually add them to the system using either the IP address or hostname and specify the login credentials for each of the regional WCSs. After being added, WCS Navigator provides summary information and links to the regional WCS systems.

CHAPTER 2

Getting Started

This chapter describes how to prepare Cisco WCS for operation. It contains these sections:

- Prerequisites, page 2-1
- System Requirements, page 2-2
- Installing WCS for Windows, page 2-5
- Installing WCS for Linux, page 2-14
- Starting WCS, page 2-16
- Logging into the WCS User Interface, page 2-18
- Customizing Home Page Tabs, page 2-23
- Using the Cisco WCS User Interface, page 2-28
- Using the Search Feature, page 2-31

Prerequisites

Before installing the Cisco WCS, ensure that you have completed the following:

- Meet the necessary hardware and software requirements as listed in the "System Requirements" section on page 2-2 for Cisco WCS.
- Update your system with the necessary critical updates and service packs.

Note See the latest release notes for information on the service packs and patches required for correct operation of Cisco WCS.

- To receive the expected results, you should run no more than 3 concurrent WCS setups for standard server use (4 GB memory and 3 GHz CPU speed) and no more than 5 concurrent WCS setups for high-end server use (8 GB memory and 3 GHz CPU speed).
- Verify that the following ports are open during installation and startup:
  - HTTP: configurable during install (80 by default)
  - HTTPS: configurable during install (443 by default)
  - 1315
  - 1299

- 6789
- 8009
- 8456
- 8005
- 69
- 21
- 162
- 8457

Note Make sure your firewall rules are not restrictive. You can check the current rules on Linux with the built-in *iptables -L* command or on Windows with the Control Panel > Windows Firewall option.

System Requirements

Cisco WCS can be run on a workstation/server class system and access points can be distributed unevenly across controllers. The following requirements must be met for the different components.

High-End Server

- Up to 3000 Cisco Aironet lightweight access points, 1250 standalone access points, and 750 Cisco wireless LAN controllers.
- 3.16-GHz Intel Xeon or Quad processor.
- 8-GB RAM.
- 200-GB minimum free disk space on your hard drive.

Note The free disk space listed is a minimum requirement but may be different for your system, depending on the number of backups.

Unified Computing System

Cisco UCS C250 M1 Server

The following are the recommended specifications for the Cisco UCS C250 M1 Server, but you can choose higher processing capabilities:

- One Intel Xeon 5500 series processor X5570 (4-core 2.93-GHz).

  Note If your processor speed is less than the one mentioned above, we recommend you to use two processors.

- 8-GB RAM.
- 200-GB minimum free disk space on your hard drive.

Cisco UCS C250 M2 Server

The following are the recommended specifications for the Cisco UCS C250 M2 Server, but you can choose higher processing capabilities:

- One Intel Xeon 5600 series processor X5680 (6-core 3.33-GHz) or one Intel Xeon 5600 series processor X5670 (6-core 2.93-GHz).
- 8-GB RAM.
- 200-GB minimum free disk space on your hard drive.

Standard Server

- Up to 2000 Cisco Aironet lightweight access points, 1000 standalone access points, and 450 wireless LAN controllers.
- 3.2-GHz Intel Dual Core processor.
- 2.13-GHz Intel Quad Core X3210 processor.
- 2.16-GHz Intel Core2 processor.
- 4 GB of RAM.
- 80-GB minimum free disk space on your hard drive.

Unified Computing System

Cisco UCS C250 M1 Server

The following are the recommended specifications for the Cisco UCS C250 M1 Server, but you can choose higher processing capabilities:

- One Intel Xeon 5500 series processor X5570 (4-core 2.93-GHz) or one Intel Xeon 5500 series processor X5550 (4-core 2.66-GHz) or one Intel Xeon 5500 series processor E5540 (4-core 2.53-GHz).
- 4 GB of RAM.
- 80-GB minimum free disk space on your hard drive.

Cisco UCS C250 M2 Server

The following are the recommended specifications for the Cisco UCS C250 M2 Server, but you can choose higher processing capabilities:

- One Intel Xeon 5600 series processor X5650 (6-core 2.66-GHz) or one Intel Xeon 5600 series processor X5670 (6-core 2.93-GHz).
- 4 GB of RAM.
- 80-GB minimum free disk space on your hard drive.

Low-End Server

- Up to 500 Cisco Aironet lightweight access points, 200 standalone access points, and 125 Cisco wireless LAN controllers.

- 3.06-GHz Intel processor.
- 1.86-GHz Intel Dual core processor.
- 2 GB of RAM.
- 50-GB minimum free disk space on your hard drive.

Unified Computing System

Cisco UCS C250 M1 Server

The following are the recommended specifications for the Cisco UCS C250 M1 Server, but you can choose higher processing capabilities:

- One Intel Xeon 5500 series processor X5550 (4-core 2.66-GHz).
- 2 GB of RAM.
- 50-GB minimum free disk space on your hard drive.

Cisco UCS C250 M2 Server

The following are the recommended specifications for the Cisco UCS C250 M2 Server, but you can choose higher processing capabilities:

- One Intel Xeon 5600 series processor X5650 (6-core 2.66-GHz).
- 2 GB of RAM.
- 50-GB minimum free disk space on your hard drive.

Supported Operating Systems

The following operating systems are supported:

- Windows 2003/SP2 and Windows 2003 R2/SP2 32-bit installations with all critical and security Windows updates installed.

  Windows 2003/SP2 64-bit installations are not supported.

  Windows 2003 32-bit installations provide support for up to 64 GB of RAM provided Physical Address Extension (PAE) is enabled. See Windows documentation for instructions on enabling this mode.

- Red Hat Linux Enterprise Server 5.X 32-bit operating system installations.

  Red Hat Linux Enterprise Server 5.X 64-bit operating system installations are not supported.

- Microsoft Windows Server 2003 and Red Hat Linux version support on VMware ESX version 3.0.1 and above with either local storage or SAN over fiber channel.

Note Individual operating systems running WCS in VMware must follow the specifications for the size of WCS you intend to use.

Client Requirements

The Cisco WCS user interface requires Internet Explorer 7.0 or later with the 9.0.X or later Flash plugin, or Mozilla Firefox 3 or 3.5. Cisco recommends Mozilla Firefox 3.5 for best performance.

Browsing on Windows 2003 Cisco WCS servers is not recommended because recommended Windows 2003 security settings cause browsing problems.

The client running the browser must have a minimum of 1 GB of RAM and a 2-GHz processor. The client device should not be running any CPU or memory-intensive applications.

Note The screen resolution should be set to 1024 x 768 pixels for both WCS and Navigator.

Supported WLC Releases

Cisco WCS 7.0 can manage the following releases of the WLC as found on various controllers (such as 2106, 4400 series, WiSM, and so on):

- 4.2
- 5.2
- 6.0
- 7.0

Note See the release notes (http://www.cisco.com/en/US/products/ps6305/prod_release_notes_list.html) for the exact version numbers.

WCS on WLSE

- Up to 1500 Cisco Aironet lightweight access points and 100/375 Cisco wireless LAN controllers.
- 3-GHz Intel Pentium4 processor with 3 GB of RAM.
- 38 GB of free space on your hard drive.

WCS Navigator

- Up to 20 WCSs
- Up to 30,000 access points

Installing WCS for Windows

Before installing Cisco WCS, refer to the "Prerequisites" section on page 2-1 and the "System Requirements" section on page 2-2. You must have administrator privileges on Windows. If you receive a message that a previous version of WCS was detected, you must continue with one of two upgrade options. See the "Upgrading WCS" section on page 14-9.

If installing WCS for Linux, see the "Installing WCS for Linux" section on page 2-14.

Before You Begin

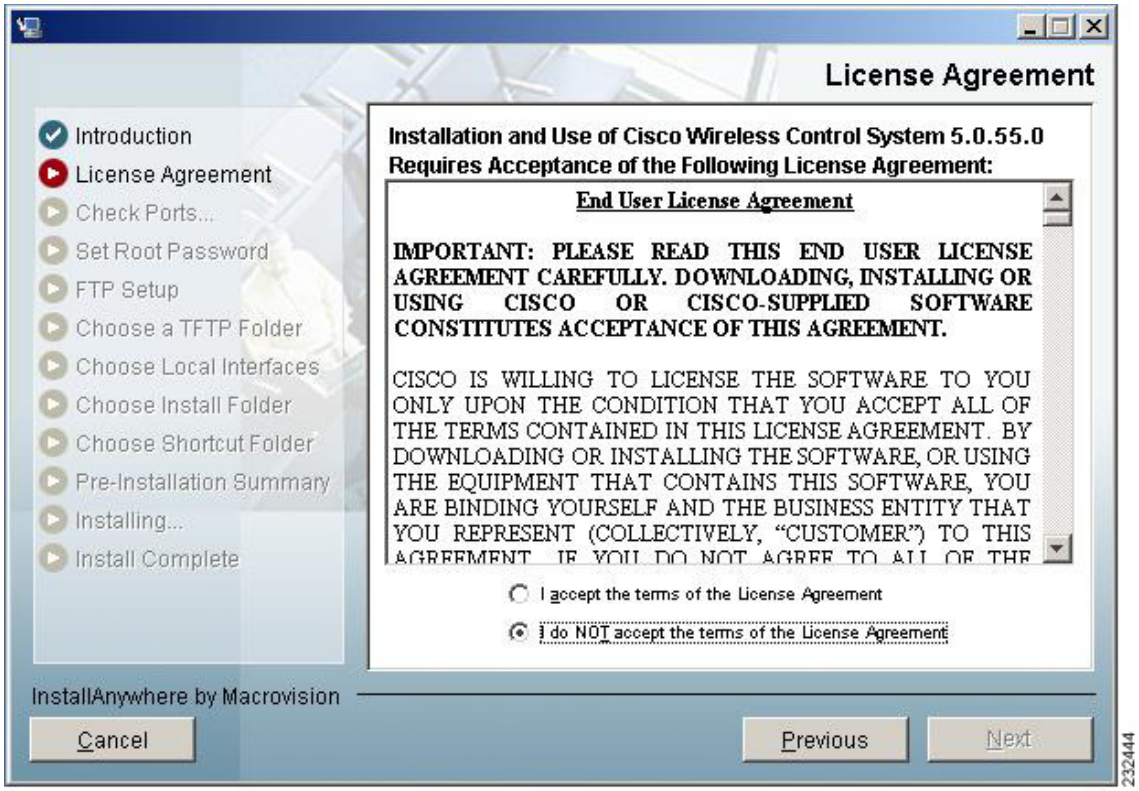
- You cannot install the WCS software if the username used to log into the server contains special characters such as exclamation marks (!). To ensure successful installation, log into the server using a username with no special characters before installing the software.
- Cisco WCS does not support the underscore character (_) in the name of the Windows server running the WCS software. If the server name contains an underscore, you can install the WCS software, but WCS fails to start.
- You must install WCS on a dedicated Windows server with no other services running (including those running as primary or secondary domain controllers) to avoid conflict with WCS.
- No hard-coded limits exist regarding the number of users or the type of user activities, but a heavy memory and CPU load on the server may affect functionality.

To install Cisco WCS, follow these steps:

Step 1 Insert the Windows Cisco WCS CD into the CD-ROM drive and double-click the WCS-STANDARD-K9-7.0.XX.Y.exe file where 7.0.XX.Y is the software build. If you received the installer from Cisco.com, double-click the WCS-STANDARD-K9.7-0.XX.Y.exe file that you downloaded to your local drive.

Step 2 The Install Anywhere page appears and prepares the system for installation. After a few seconds, the Introduction window appears, followed by the license agreement window (see Figure 2-1). You must select the "I accept the terms of the License Agreement" radio button to continue.

Figure 2-1 License Agreement Page



Step 3 If the install wizard detects a previous version of WCS, you see a window similar to Figure 2-2 or Figure 2-3. If a previous version is detected, you must proceed as an upgrade and refer to the "Upgrading WCS" section on page 14-9. For a first-time installation, continue to Step 4.

Figure 2-2 Ineligible for Automated Upgrade

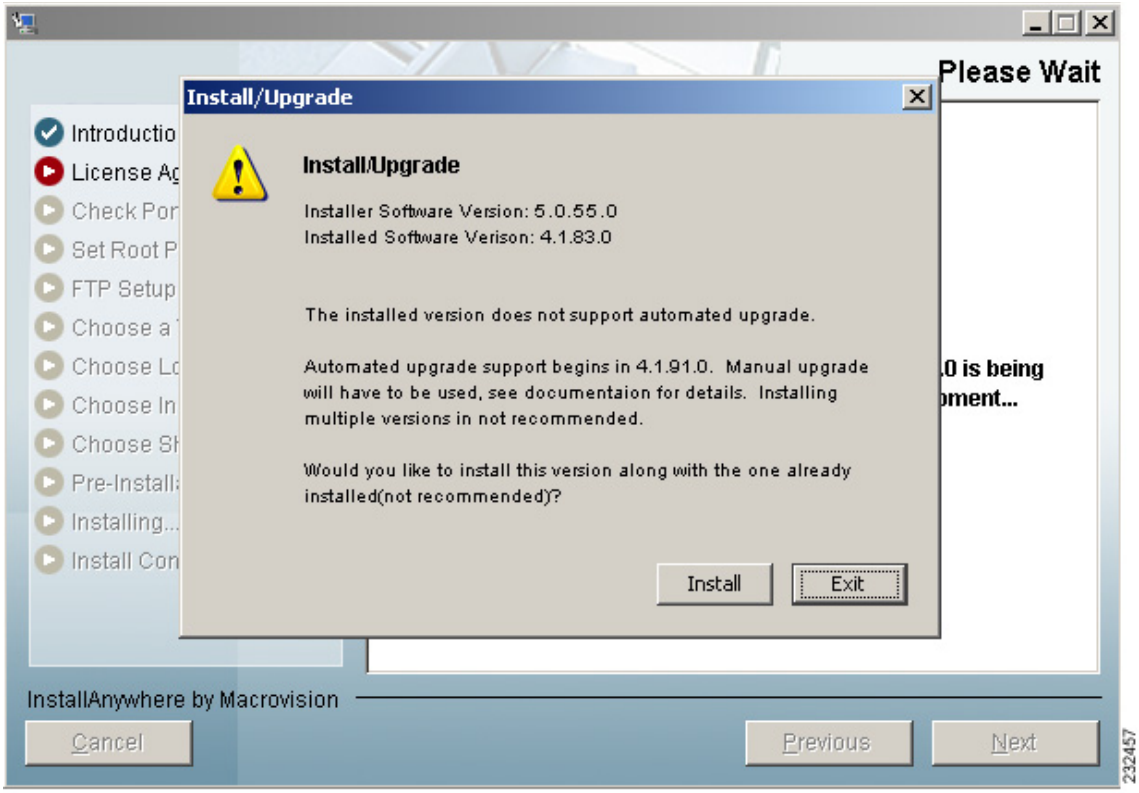
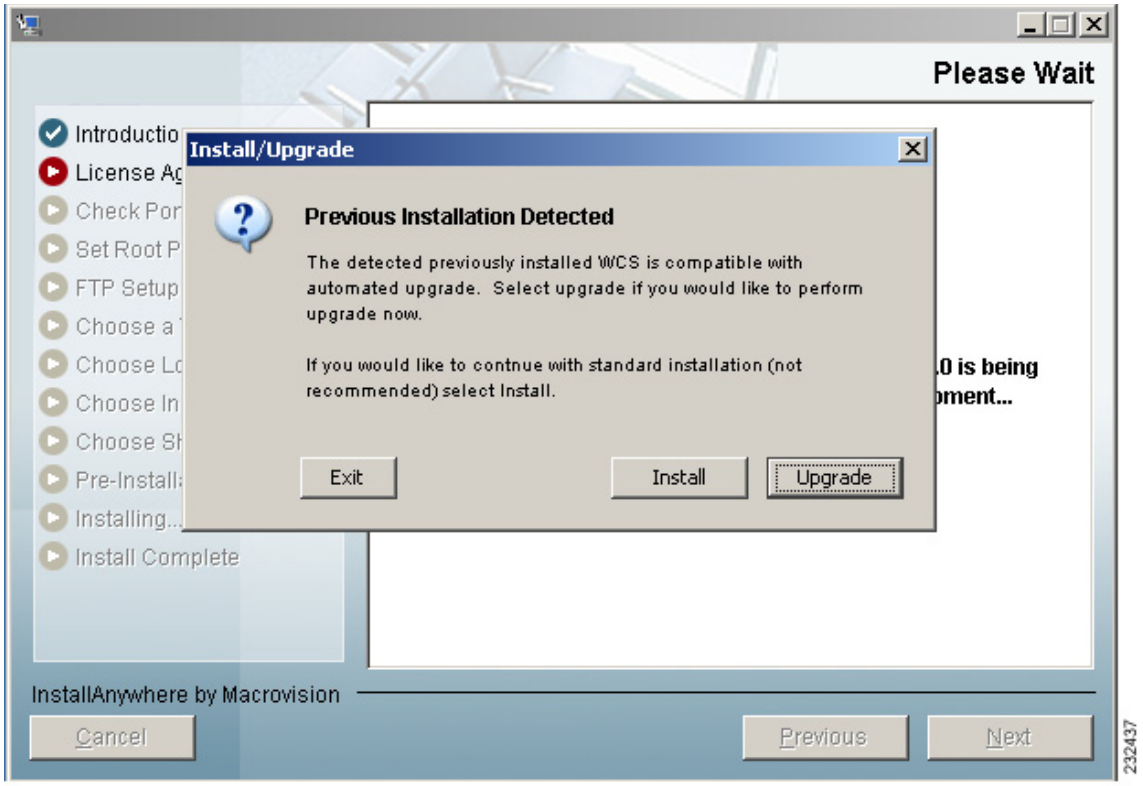
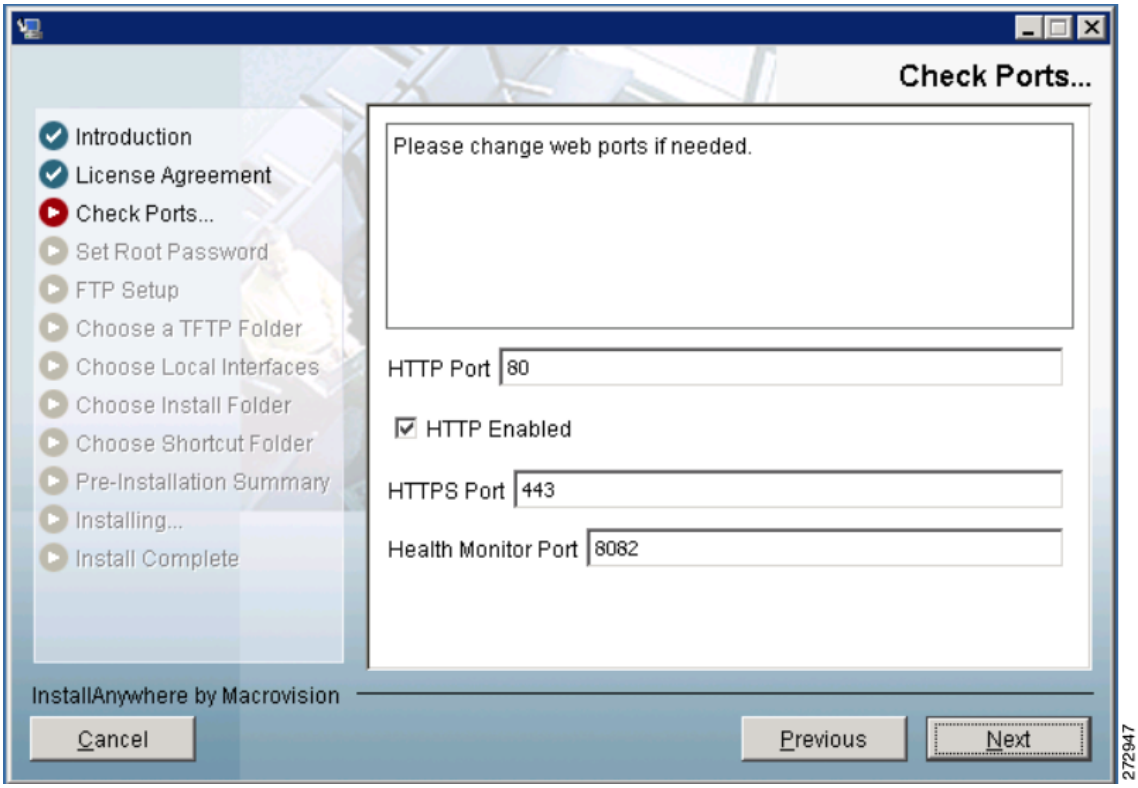


Figure 2-3 Previous Installation Detected



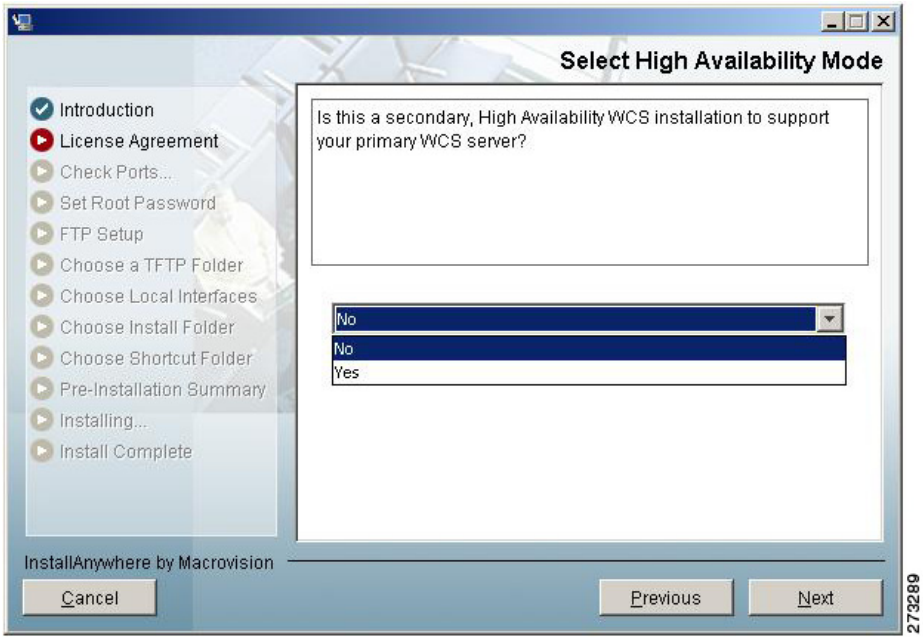
Step 4 The Check Ports window appears (see Figure 2-4). In the Check Ports window, change the default HTTP and HTTPS ports if necessary. The default ports for HTTP and HTTPS are 80 and 443, respectively. HTTP Enabled is selected by default.

Figure 2-4 Check Ports Window



Step 5 Enter a Health Monitor Port. Click **Next**. The Select High Availability Mode window appears (see Figure 2-5).

Figure 2-5 Select HA Mode Window



Step 6 Determine if this is a secondary, high availability WCS installation to support your primary WCS controller. The secondary WCS installation question refers to high availability only. You cannot install two different versions of WCS on the same server. If you are not enabling high availability, choose No (the default) and continue with Step 7. If this is a secondary installation for high availability purposes, choose **Yes** and follow Steps a through c.

a. Enter an authentication key for the primary WCS device and click **Next**.

b. Choose a folder in which to install the secondary WCS in the Choose Install Folder window. Click **Next** to continue.

c. Choose a shortcut location for the secondary WCS.

Step 7 Enter and then re-enter the root password. The rules for a strong password are as follows:

- The minimum password length is 8 characters.
- No character can be used more than three times consecutively in the password.
- The password must contain three of the four following character classes: uppercase, lowercase, numbers, and special characters.

Step 8 Enter the root FTP password.

Step 9 In the FTP Server File page, choose a folder in which to store the FTP server files and click **Next** to open the TFTP File Server window.

Note Store the FTP server files in a folder outside the main installation folder. This ensures that the FTP server files are not deleted if WCS is uninstalled.

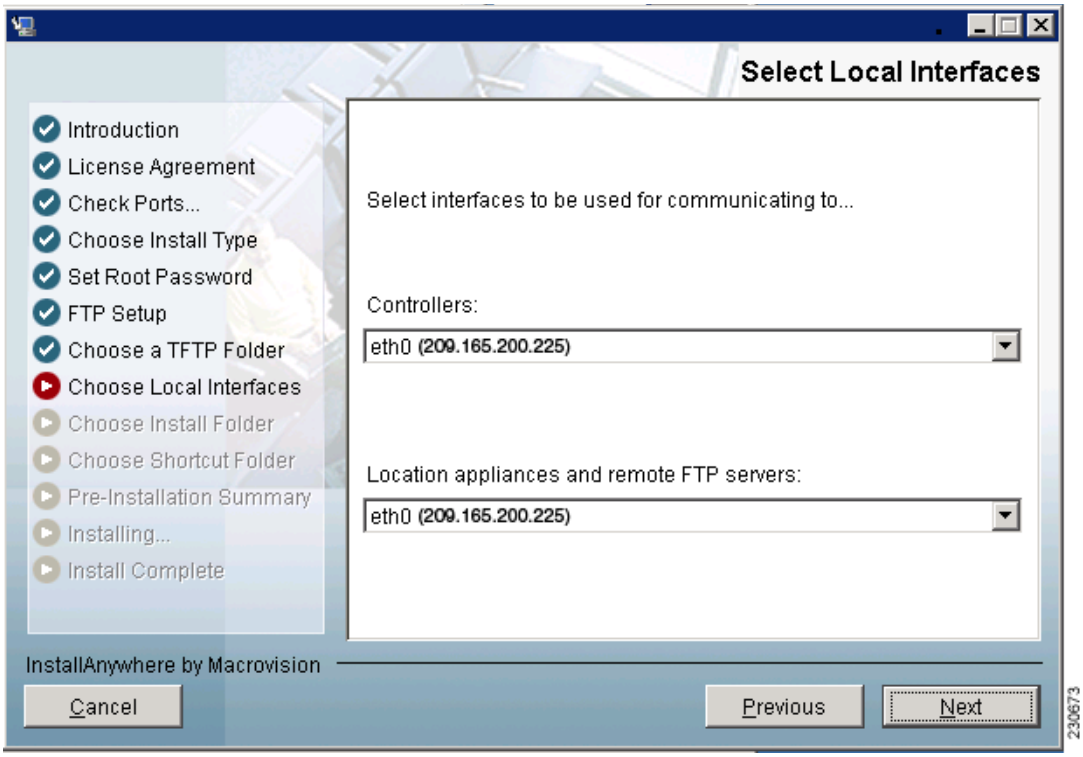
Step 10 In the TFTP Server File window, choose a folder in which to store the TFTP server files and click **Next**.

Note If you want to use a network-mounted drive for the TFTP root, you must configure WCS to run as a domain user (see the"Installing WCS for Windows" section on page 2-5) and then configure the TFTP root (see the "Configuring TFTP as a Network Drive" section on page 2-16).

Note Store the TFTP server files in a folder outside the main installation folder. This ensures that the TFTP server files are not deleted if WCS is uninstalled.

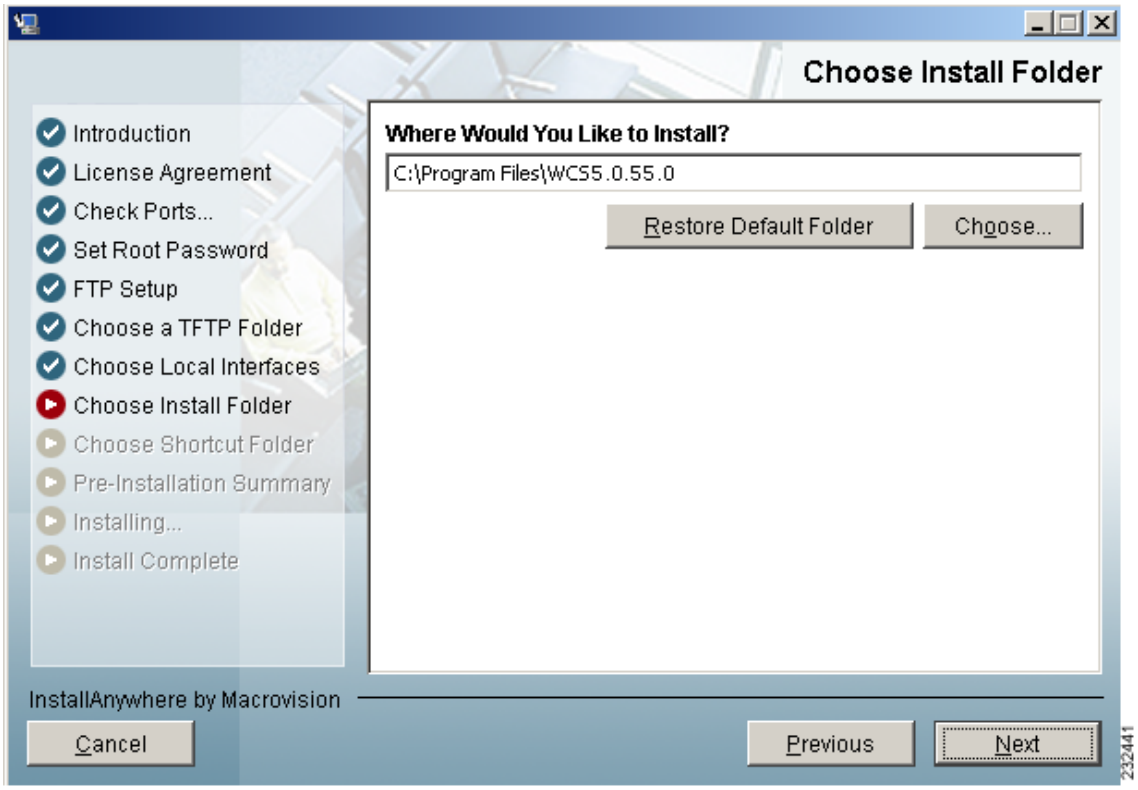
Step 11 If you are installing Cisco WCS on a multi-homed server (a server having multiple interfaces), the installer automatically detects the presence of multiple interfaces. The Select Local Interfaces window appears (see Figure 2-6). Choose the interfaces to be used by the server for communicating with controllers, MSEs and remote FTP servers, and clients. Click **Next**.

Figure 2-6 Select Local Interfaces Window



Step 12 Choose a folder in which to install the Cisco WCS at the Choose Install Folder window (see Figure 2-7). Click **Next** to continue.

Figure 2-7 Choose Install Folder



Step 13 Follow the prompts that appear in the window to complete the installation. After the installation is complete, the Install Complete window appears. Click **Done** to complete the installation.

Note Look at the installation log to verify that nothing went wrong during the installation. The install log resides in the installation root directory if the installation completes. If the installation did not complete, the install log resides in the directory from which the installer was run or the install root directory.

Configuring WCS to Run as a Domain User

To configure WCS to run as a domain user, follow these steps:

Step 1 Stop WCS.

Step 2 Add the domain user that will be used to run the service to the Administrators group of the local machine.

a. Choose **Administrative Tools > Computer Management> Users and Groups > Groups**.

b. Double-click the Administrators group.

c. Add the domain user.

Step 3 Install WCS as instructed in the "Installing WCS for Windows" section on page 2-5.

WCS consists of two services: Cisco Wireless Control System (A.B.C.D) and Nms_Apache_A_B_C_D, where A.B.C.D represents the current release number.

Step 4 Set the WCS service to run as the domain user:

a. Choose Administrative Tools > Services.

b. Right-click **Cisco Wireless Control System (A.B.C.D)** and choose **Properties**.

c. Click the **Log On** tab.

d. Click **This Account**.

e. Enter the domain user with "domain" before the name (such as DOMAIN\username), and the domain user password.

f. Click **OK**.

Step 5 Set the Apache service to run as the domain user:

a. Choose Administrative Tools > Services.

b. Right click **Nms_Apache_A_B_C_D** and choose **Properties**.

c. Click the **Log On** tab.

d. Click **This Account**.

e. Enter the domain user with "domain" before the name (such as DOMAIN\username), and the domain user password.

f. Click **OK**.

Step 6 Start WCS.

Installing WCS for Linux

You must have root privileges on Linux to install WCS.

Step 1 If not already done, log in as root. If you are using the GUI, open a terminal window.

Step 2 Using the command line, perform one of the following:

a. If you are installing from a CD, switch to the /media/cdrom directory. Skip to Step 4.

b. If you are installing from Cisco.com, switch to the directory that the install file was downloaded to. For example, if the install file was placed in /root/Desktop, enter **cd /root/Desktop**. Continue to Step 3.

Step 3 If you downloaded the file from Cisco.com, you need to make it executable using the following command:
chmod +x WCS-STANDARD-K9-7.0.*XX.Y*.bin where *xx.y* represents the current release number.

Step 4 Enter **./WCS-STANDARD-K9-7.0.*XX.Y*.bin** to start the install script.

The install script prepares the install environment and displays the license agreement. You are asked to accept the terms of the license agreement.

Step 5 If the install wizard detects a previous version of WCS, you see a message that states whether the detected version is eligible for an automated upgrade or not. If a previous version is detected, you must proceed as an upgrade and refer to the "Upgrading WCS" section on page 14-9. For a first-time installation, continue to Step 6.

Step 6 Determine if this is a secondary, high availability WCS installation to support your primary WCS controller. Choose 1 for No (the default) or 2 for Yes. You cannot install two different versions of WCS on the same server. If you are not enabling high availability, choose 1 (No). If you are installing a secondary WCS for high availability mode and choose 2 (Yes), you will be prompted for an authentication key and a location for installing the secondary WCS.

Step 7 The Check HTTP Port prompt appears. In the Check HTTP Port window, change the default HTTP and HTTPS ports if necessary. The default ports for HTTP and HTTPS are 80 and 443, respectively.

Step 8 Specify whether you want to enable HTTP redirect. If HTTP redirect is enabled, any requests received on the HTTP port are redirected to the HTTPS port. If it is not enabled, the HTTP port is disabled.

Step 9 Determine whether you want the default Health Monitor port of 8082 or you need to change the port.

Step 10 Enter and then re-enter the root password. The rules for a strong password are as follows:

- The minimum password length is 8 characters.
- The password cannot contain the username or the reverse of the username.
- The password cannot be *Cisco* or *ocsic* (Cisco reversed).
- The root password cannot be *public*.
- No character can be used more than three times consecutively in the password.
- The password must contain three of the four character classes: uppercase, lowercase, numbers, and special characters.

Step 11 Enter the root FTP password.

Step 12 Choose a folder in which to store the FTP server files.

Note If the folder does not already exist, you must enter **mkdir** and create it.

Step 13 Choose a folder in which to store the TFTP server files.

Note Store the TFTP server files in a folder outside the main installation folder. This ensures that the TFTP server files are not deleted if Cisco WCS is uninstalled.

Step 14 If you are installing Cisco WCS on a multi-homed server (a server having multiple interfaces), the installer automatically detects the presence of multiple interfaces. Choose the interfaces to be used by the server for communicating with controllers, MSEs and remote FTP servers, and clients.

Step 15 Choose a folder in which to install the Cisco WCS.

Step 16 Choose to create links from the default location (/opt/WCS5.2.98.0), from your home folder, or another location.

Step 17 Follow the prompts that appear to complete the installation. After the installation is complete, the Install Complete statement appears.

Note Look at the installation log to verify that nothing went wrong during the installation. The install log is located in the installation root directory if the installation completes. If the installation did not complete, the install log resides in the directory from which the installer was run or the install root directory.

Configuring TFTP as a Network Drive

To configure TFTP as a network drive, you must have completed the steps in the "Installing WCS for Linux" section on page 2-14. The desired drive must also be accessible from that domain.

Step 1 Make a backup of installDir/webnms/classes/com/cisco/packaging/PackagingResources.properties.

Step 2 Edit the following line:

TftpRoot=*servername**resourcename*

where your particular *servername* and *resourcename* are entered.

Choose Administration > ServerSettings.

At the TFTP Root setting, enter the desired network resource using the appropriate UNC format (such as \\servername\\resourcename) where your particular servername and resourcename are entered with only one set of backslashes.

Step 3 Restart WCS.

Starting WCS

This section provides instructions for starting WCS on either a Windows or Linux server.

In Windows and Linux, Cisco WCS is installed as a service. The service runs continuously and resumes after a reboot.

Note You can check the status of WCS at any time. To do so, follow the instructions in the "Verifying the Status of WCS" section on page 14-1.

This section includes the following topics:

- Starting WCS on Windows, page 2-16
- Starting WCS on Linux, page 2-17

Starting WCS on Windows

Follow these steps to start WCS when it is installed on Windows.

Note When WCS is installed as a Windows service, WCS runs automatically upon system bootup.

Step 1 Log into the system as administrator.

Step 2 Perform one of the following:

- From the shortcut location (defaulted to Windows Start menu > **Programs > Wireless Control System A.B.C.D) > StartWCS**.
- From the command prompt, navigate to the WCS installation bin directory (the default is C:\Program Files\WCSA.B.C.D\bin) and enter **StartWCS**.

The WCS Admin window appears and displays messages indicating that WCS is starting.

Note If you are starting WCS after a restoration from release 4.0.66.0 or earlier, the startup may take longer than expected. The WCS Admin window may even indicate that starting WCS has failed. See the task viewer to see whether Java is progressively taking CPU space. If so, WCS is running.

Note If WCS is installed as a service, messages also appear to indicate that the Nms_Server service is starting.

Step 3 Close the WCSAdmin window when the Close button becomes active.

Step 4 WCS is ready to host WCS user interfaces (clients). Go to the "Logging into the WCS User Interface" section on page 2-18 to use a web browser to connect to the WCS user interface.

Starting WCS on Linux

Follow these steps to start WCS when it is installed on Linux.

Note To see the version of WCS you currently have installed, enter **nmsadmin.sh version**.

Note When WCS is installed as a Linux service, WCS runs automatically upon system bootup.

Step 1 Log into the system as root.

Step 2 Using the Linux command-line interface (CLI), perform one of the following:

- Navigate to the shortcut location (defaulted to /opt/WCSA.B.C.D directory) and enter **./StartWCS**.
- Navigate to the installation bin directory (the default is opt/WCSA.B.C.D/bin) and enter **./Start WCS**.

The CLI displays messages indicating that WCS is starting.

Step 3 WCS is ready to host WCS user interfaces (clients). Go to the "Logging into the WCS User Interface" section on page 2-18 to use a web browser to connect to the WCS user interface.

Logging into the WCS User Interface

Follow these steps to log into the WCS user interface through a web browser.

Step 1 Launch Internet Explorer 7.0 or later or Mozilla Firefox 3.5 or later on a different computer than the one on which you installed and started WCS.

Note Some WCS features may not function properly if a browser and WCS are running on the same Windows workstation.

Step 2 In the browser's address line, enter **https://***wcs-ip-address***,** where *wcs-ip-address* is the IP address of the computer on which you installed and started WCS.

Step 3 When the WCS user interface displays the Login page, enter the root password you created during installation.

Note If any licensing problems occur, a message appears in an alert box. If you have an evaluation license, the number of days until the license expires is shown. You are also alerted to any expired licenses. You have the option to go directly to the licensing page to address these problems.

Step 4 Click **Submit** to log into WCS. The WCS user interface is now active and available for use. The WCS home page appears. You can predefine what appears on the home page by choosing the monitoring components that are critical for your network. For example, you may want different monitoring components for a mesh network so that you can create a customized tab for a mesh dashboard.

Note If the database or Apache web server does not start, check the launchout.txt file in Linux or the wrapper.log file in Windows. You will see a generic "failed to start database" or "failed to start the Apache web server" message.

This page enables you to choose the information that you want to see. You can organize the information in user-defined tabs. The default view comes with default tabs and pre-selected components for each, and you can arrange them as you like.

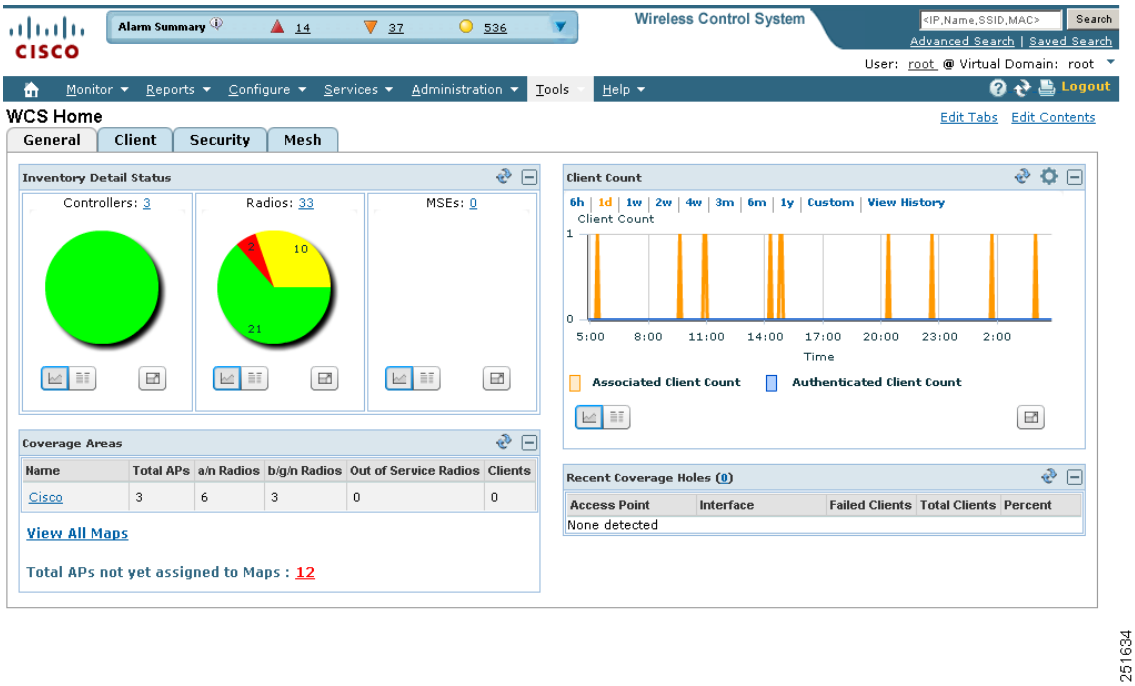
Note When an upgrade occurs, the user-defined tabs arranged by the previous user in the previous version are maintained. Therefore, the latest components may not show. Look at the Edit Components link to find what new components are added.

This page provides a summary of the Cisco Unified Wireless Network Solution, including coverage areas, the most recently detected rogue access points, access point operational data, reported coverage holes, and client distribution over time. Figure 2-8 shows a typical WCS home page.

You should see four tabs on the WCS home page: General, Client, Security, and Mesh.

Note When you use WCS for the first time, the network summary pages show that the Controllers, Coverage Areas, Most Recent Rogue APs, Top 5 APs, and Most Recent Coverage Holes databases are empty. It also shows that no client devices are connected to the system. After you configure the WCS database with one or more controllers, the WCS home page provides updated information.

Figure 2-8 WCS Home



251634

To exit the WCS user interface, close the browser page or click **Logout** in the upper right corner of the page. Exiting a WCS user interface session does not shut down WCS on the server.

When a system administrator stops the WCS server during your WCS session, your session ends, and the web browser displays this message: "The page cannot be displayed." Your session does not reassociate to WCS when the server restarts. You must restart the WCS session.

General Tab

The following are factory default components for the General tab.

Table 2-1 General Tab Components

Component	Description
Inventory Detail Status	Displays the following: • Controllers—Lists the number of controllers that are managed in WCS. Graphically depicts reachable and unreachable controllers. • Radios—Lists the number of radios managed in WCS. Graphically depicts the number of radios in out-of-service (critical), minor, and ok conditions. • MSEs—Lists the number of MSEs that are managed in WCS. Graphically depicts reachable and unreachable servers. Look at the installation log to verify that nothing went wrong while manually adding the servers to WCS. (The trace for MSEs must be turned on.)
Coverage Areas	Displays access points, radios, and client details for each coverage area.
Client Count	Displays the total number of clients in WCS over the selected period of time. **Note** Client count includes autonomous clients.
Recent Coverage Holes	Displays the five most recent coverage alarms.
Total APs not yet assigned to Maps	Indicates the number of unassigned access points. Click the number link to view the list of these access points.

Client Tab

When you click the Client tab from the WCS home page, you see the following factory default components (see Table 2-2).

Table 2-2 Client Tab Components

Component	Description
Client Count	Displays the trend of associated and authenticated client counts in a given period of time.
Client Traffic	Displays the trend of both upstream and downstream client traffic in a given time period.
Client Alarm Summary	Displays the failures and errors of the five most recent client alarms.
Client Protocol Distribution	Displays the distribution of each radio band and the total current client count.
Client Distribution	Displays the distribution of clients by protocol, EAP type, and authentication and the total current client count.

Additionally, refer to "Troubleshooting from the Client Tab Dashboard" section on page 11-11 which describes the Client Troubleshooting portion of the Client tab.

Security Tab

When you click the Security tab from the WCS home page, you see the following factory default components:

Table 2-3 Security Tab Components

Component	Description
AP Threats/Attacks	Displays thread or attacks to access points for the past hour, past 24 hours, and total active.
Attacks Detected	Displays wIPS and signature attacks for the past hour, past 24 hours, and total active.
Recent Rogue AP Alarms	Displays the five most recent rogue alarms. Click the number in parentheses to access the Alarms page. Click an item under MAC Address to view alarm details.
Recent Ad hoc 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.
MFP Attacks	Displays MFP attacks for the past hour, past 24 hours, and total active.
Malicious Rogue APs	Displays malicious rogue access points for the past hour, past 24 hours, and total active.
Cisco Wired IPS Events	Displays Wired IPS events for the past hour, past 24 hours, and total active.
Unclassified Rogue APs	Displays unclassified rogue access points for the past hour, past 24 hours, and total active.
Friendly Rogue APs	Displays friendly rogue access points for the past hour, past 24 hours, and total active.
Ad hoc Rogues	Displays ad hoc rogues for the past hour, past 24 hours, and total active.
Security Index	Indicates the security of the WCS managed network. The security index is calculated by assigning priority to the various security configurations and displaying them in visual form.

Mesh Tab

If you click the Mesh tab from the WCS home page, you see the following factory default components:

Table 2-4 Mesh Tab Components

Component	Description
Most Recent Mesh Alarms	Displays the five most recent mesh alarms. Click the number in parentheses to access the Alarms page.
Worst SNR Link	Displays the worst signal-to-noise ratio (SNR) links. Data includes the Parent AP Name, the Child AP Name, and the Link SNR.
Worst Node Hop Count	Displays the worst node hop counts. Data includes the AP Name, the Hop Count, and the Parent AP Name.
Worst Packet Error Rate	Displays the worst packet error rates. Data includes the Parent AP Name, the Child AP Name, and the Packet Error Rate.

CleanAir Tab

The following factory default components appear on the CleanAir tab:

- 802.11a/n Avg Air Quality—Provides a line chart representing the average air quality for the entire network over a set period of time. Displays the average air quality on the 802.11 a/n band. Data includes time and the average air quality.
- 802.11b/g/n Avg Air Quality—Provides a line chart representing the average air quality for the entire network over a set period of time. Displays the average air quality on the 802.11 b/g/n band. Data includes time and the average air quality.
- 802.11a/n Min Air Quality—Provides a line chart representing the minimum air quality for the entire network over a set period of time. Displays the minimum air quality on the 802.11 a/n band. Data includes time and the minimum air quality.
- 802.11b/g/n Min Air Quality—Provides a line chart representing the minimum air quality for the entire network over a set period of time. Displays the minimum air quality on the 802.11 b/g/n band. Data includes time and minimum air quality.
- Worst 802.11a/n Interferers—Provides a list of active interferers with the worst severity level for the 802.11 a/n band. The graph displays the the top ten worst interferers that are currently active. Data includes InterfererID, Type, Status, Severity, Affected Channels, Duty Cycle(%), Discovered, Last Updated, and Floor.
- Worst 802.11b/g/n Interferers—Provides a list of active interferers with the worst severity level for 802.11 b/g/n band. The graph displays the top ten worst interferers that are currently active. Data includes InterfererID, Type, Status, Severity, Affected Channels, Duty Cycle(%), Discovered, Last Updated, and Floor.
- 802.11a/n Interferer Count—Provides a line chart representing the total number of interferers on all channels over the selected period of time. Displays the number of devices interfering in the 802.11 a/n band. Data includes time and interferer count.

Note The air quality is calculated for all controllers in your network that have CleanAir-enabled access points. The report includes aggregated air quality data across your network.

- 802.11b/g/n Interferer Count—Provides a line chart representing the total number of interferers on all channels over the selected period of time. Displays the number of devices interfering in the 802.11 b/g/n band. Data includes time and interferer count.

Note The information in the worst interferer and interferer count charts is collected from Mobility Services Engines (MSE). If MSEs are not available, this chart will not show any results.

- Recent Security-risk Interferers—Provides a list of active interferers with the worst severity level for each band. Displays the recent security risk interferers on your wireless network. Data includes Type, Severity, Affected Channels, Last Detected, Detected AP.

Note This chart includes information for the interferers for which security alarms are enabled.

You can also view the data presented on this tab in different formats.

Customizing Home Page Tabs

You can customize the predefined set of components depending on your network management needs. This page enables you to choose the displayed information. You can organize the information in user-defined tabs. The default view comes with default tabs and pre-selected components for each. When you click the Edit Tabs link in the WCS home page, the Edit Tabs page appears in which customization can begin (see Figure 2-9).

Note When an upgrade occurs, the arrangement of components in a previous version is maintained. Because of this, components or features added in a new release are not displayed. Click the Edit Contents link to discover new components. See the "Customizing Home Page Tabs" section on page 2-23 for more information.

Creating a New Tab

Follow these steps to create a new tab.

Step 1 Click **Edit Tabs** from the WCS home page. The Edit Tabs page appears (see Figure 2-9).

Figure 2-9 WCS Home > Edit Tabs

251636

Step 2 Enter the name of the new tab you are creating and click **Add**. The tab name you add appears in the Tab Order page.

Note Add is the only function that does not require a Save after its operation. If you click **Delete**, **Rename**, **Move Up**, or **Move Down**, you must click **Save** for the changes to be applied.

Step 3 Click the tab names in the Tab Order page and assign placement by clicking **Move Up** or **Move Down**.

Note If you want to return to the restored factory defaults as shown in Figure 2-8, click **Reset to Factory Default**.

Customizing Home Page Content

Follow these steps to customize WCS home page components. You can add or delete components by selecting from the predefined list.

Also part of the customizable home page are time-based or non-time-based interactive graphs which you can display in graphical or chart form (by clicking the appropriate icon). (Interactive graphs also appear in Monitor > Clients.) These graphs refresh automatically within a predetermined time based on the default polling cycles of dependent tasks, or you can click the Refresh Component icon to get the most current status. When a graph is time based, an additional link bar at the top of the graph page displays the options as follows:

- 6h—the last six hours of data from the current time and current database table

- 1d—the last day of data from the current time and current database table
- 1w—the last week of data from the current time and the hourly aggregated table
- 2w—the last two weeks of data from the current time and hourly aggregated table
- 4w—the last four weeks of data from the current time and hourly aggregated table
- 3m—the last three months of data from the current time and daily aggregated table
- 6m—the last six months of data from the current time and the weekly aggregated table
- 1y—the last year of data from the current time and weekly aggregated table
- custom—the user can set both the days and hours for the start and end date. The appropriate aggregated source (either current, hourly, or daily) is chosen based on the starting date.

After you specify the timeframe, the data for that timeframe is retrieved and the corresponding graph is displayed. The link for which the graph is drawn is shown in a different color (orange) than the other links. The interactive graphs that are available within WCS include line graphs, area graphs, pie graphs, and stacked bar graphs.

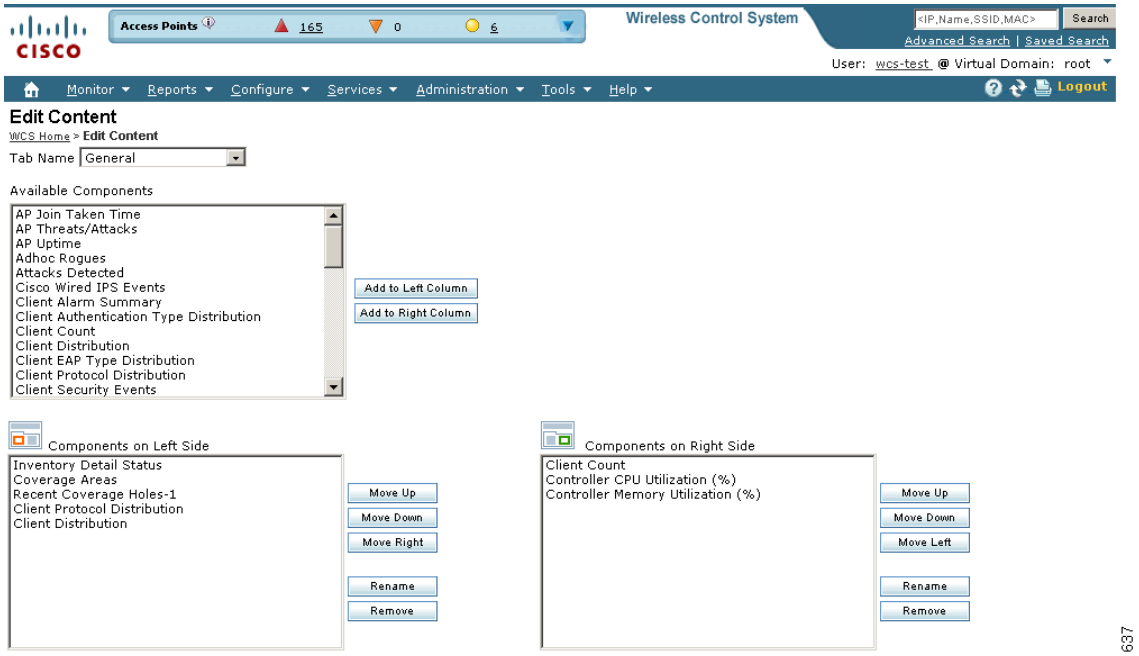
You can click **Enlarge Chart** icon to enlarge the graph in a separate page.

Editing Content

Follow these steps to customize WCS home page components:

Step 1 On the WCS home page, click **Edit Contents**. The Edit Content page appears (see Figure 2-10).

Figure 2-10 Edit Content Page



Step 2 In the Available Components drop-down list, highlight the desired component and choose to add it to the left column or add it to the right column. The component moves to the appropriate column.

Step 3 Click the component in the Left Side or Right Side Column page and move it up, down, or to the right or left.

Note To remove a component, choose it from the Left or Right Column list and click **Remove**.

Step 4 Click **Save**.

Additional Edit Content Page Components

The WCS > Edit Content page lists the following available components:

- AP Join Taken Time—Displays the access point name and the amount of time (in days, minutes, and seconds) that it took for the access point to join.
- AP Threats/Attacks—Displays various types of access point threats and attacks and indicates how many of each type have occurred.
- AP Uptime—Displays each access point name and amount of time it has been associated.
- Ad hoc Rogues—Displays ad hoc rogues for the previous hour, previous 24 hours, and total active.
- Attacks Detected
- Cisco Wired IPS Events—Displays wired IPS events for the previous hour, previous 24 hours, and total active.
- Client Alarm Summary—Displays the five most recent client alarms with client association failures, client authentication failures, client WEP key decryption errors, client WPA MIC errors, and client exclusions.
- Client Authentication Type—Displays the number of clients for each authentication type.
- Client Count—Displays the trend of associated and authenticated client counts in a given period of time.
- Client Distribution—Displays how clients are distributed by protocol, EAP type, and authentication type.
- Client EAP Type Distribution
- Client Protocol Distribution—Displays the current client count distribution by protocols.
- Client Security Events—Displays client security events within the previous 24 hours including excluded client events, WEP decrypt errors, WPA MIC errors, shunned clients, and IPSEC failures.
- Client Traffic—Displays the trend of client traffic in a given time period.
- Client Troubleshooting—Allows you to enter a MAC address of a client and retrieve information for diagnosing the client in the network.
- Clients Detected by Context Aware Service—Displays the client count detected by the context aware service within the previous 15 minutes.
- Controller CPU Utilization (%)— Displays the average, maximum, and minimum CPU usage.
- Controller Memory Utilization—Displays the average, maximum, and minimum memory usage as a percentage for the controllers.
- Coverage Areas
- Friendly Rogue APs—Displays friendly rogue access points for the previous hour, previous 24 hours, and total active.
- Guest Users Count

- Inventory Detail Status
- Inventory Status—Displays the total number of client controllers and the number of unreachable controllers.
- LWAPP Uptime—Displays the access point name and the amount of its uptime in days, minutes, and seconds.
- Latest 5 Logged in Guest Users
- MFP Attacks
- Malicious Rogue APs
- Mesh AP by Hop Count
- Mesh AP Queue Based on QoS
- Mesh Parent Changing AP—Displays the access point name, the parent name, and the number of changes made per minute.
- Mesh Top Over Subscribed AP
- Mesh Worst Node Hop Count
- Mesh Worst Packet Error Rate
- Mesh Worst SNR Link
- Most Recent AP Alarms—Displays the five most recent access point alarms. Click the number in parentheses to open the Alarms page which shows all alarms.
- Most Recent Client Alarms
- Most Recent Mesh Alarms
- Most Recent Security Alarms—Displays the five most recent security alarms. Click the number in parentheses to open the Alarms page.
- Recent 5 Guest User Accounts
- Recent Alarms—Displays the five most recent alarms by default. Click the number in parentheses to open the Alarms page.
- Recent Coverage Holes
- Recent Malicious Rogue AP Alarms
- Recent Rogue Alarms—Displays the five most recent rogue alarms. Click the number in parentheses to open the Alarms page which shows alarms.
- Security Index
- Top APs by Client Count
- Unclassified Rogue APs—Displays unclassified rogue access points for the previous hour, previous 24 hours, and total active.

Guest Components for WCS Home Page

The following guest user components are also available for the WCS home page General tab using the Edit Contents feature:

Table 2-5 Guest User Components

Component	Description
Guest User Accounts	Status of the last five WCS guest accounts configured on the network. Account information includes the guest username, the time and date the account was created, who created or modified the account, the lifetime of the account (days, minutes, and seconds), and the account status (active, scheduled, not active, expired).
Currently Logged Guest Users	List of guest users that are currently logged into the network. Guest user information includes guest username, profile name, date and time the guest user associated with WCS, and the amount of time remaining before the account expires.
Guest Count	Interactive graph showing the number of guest users in the network.

Using the Cisco WCS User Interface

A typical Cisco WCS user interface page consists of these elements:

- Icons, page 2-28
- Menu Bar, page 2-29
- Sidebar Area, page 2-30
- Command Buttons, page 2-30
- Main Data Page, page 2-31
- Alarm Summary, page 2-30
- Administrative Tools, page 2-31
- Using the Search Feature, page 2-31

Icons

The icons on the WCS home page and within the General, Client, Security, and Mesh tabs have the following functions.

Client Tab Icon	Description
	The Component Options icon enables you to filter the data by variables. For example, you can compare client count trends for SSIDs, floor areas, controllers, and so on.
	The Refresh Component icon enables you to automatically adjust the dashboard so that it reflects the current network status.
	The View in Chart icon enables you to view the component in chart rather than table form.
	The View in Grid icon enables you to view the component in a table rather than chart form.

Menu Bar

There are seven menus on each page: **Monitor**, **Reports, Configure**, **Services**, **Administration**, **Tools**, and **Help**. When you move the mouse over any of the heading, a drop-down list appears.

Monitor Menu

The Monitor menu provides you with a top-level description of the devices on your network. You can monitor your network, maps, Google Earth maps, various devices (controllers, access points, clients, tags, chokepoints, Wi-Fi TDOA receivers), RRM, alarms, and events.

Configure Menu

The Configure menu enables you to configure templates, controllers, access points, Ethernet switches, chokepoints, Wi-Fi TDOA receivers, config groups, auto provisioning, scheduled configuration tasks, profiles, ACS view servers, and TFTP servers on your network.

Administration Menu

The Administration menu enables you to schedule tasks like making a backup, checking a device status, auditing your network, synchronizing the MSE, and so on. It also contains Logging to enable various logging modules and specify restart requirements. For user administration such as changing passwords, establishing groups, setting application security settings, and so on, choose AAA. From the Administration Menu, you can also access the licensing information, set user preferences, and establish high availability (a secondary backup device running WCS).

Tools Menu

The Tools Menu covers voice audit, location accuracy, config audit, and migration analysis.

Help Menu

Clicking **Help > Online Help** enables you to view online help. The online help is context sensitive and will open to documentation for the WCS window that you currently have open.

Clicking **Help > Learning Modules** allows you to access short video clips of certain WCS features.

Clicking **Help > Submit Feedback** allows you to access a page where you can enter feedback on the WCS product.

Clicking **Help > About WCS** allows you to verify the version of WCS that you are running. It provides the version, host name, feature, AP limit, and type.

Sidebar Area

The sidebar area enables you to choose a new configuration page under the currently selected menu area. You may choose to display or configure any of the available data. The selector area options vary based on which menu you have chosen.

Some pages contain a group of menus in this area. Click the menu item to reveal a submenu and then click the item to choose it.

Command Buttons

The Cisco WCS user interface uses a number of command buttons throughout its pages. The most common of these are as follows:

- Apply to Controllers: Applies the selected information to the controllers
- Delete: Deletes the selected information
- Cancel: Cancels new information entered on the current page and returns to the previous page
- Save: Saves the current settings
- Audit: Discovers the present status of this access point
- Place AP: Audits the configuration of the selected entity by flagging the differences between WCS database device configurations

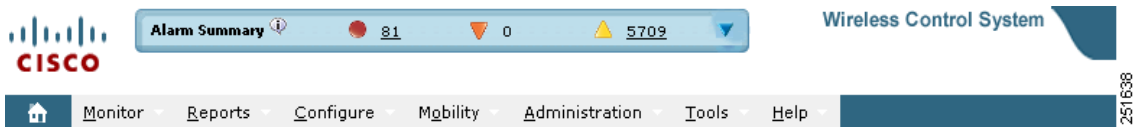
Alarm Summary

When WCS receives an alarm message from a controller, it displays an alarm indicator at the top of the WCS window (see Figure 2-11).

Note The Administration > Settings > Alarms page has a Hide Acknowledged Alarms check box. You must unselect it if you want acknowledged alarms to appear in the WCS Alarm Summary and alarms lists page. By default, acknowledged alarms are not shown.

Critical (red), Major (orange) and Minor (yellow) alarms appear in the alarm dashboard, left to right.

Figure 2-11 WCS Alarm Summary



Alarms indicate the current fault or state of an element that needs attention, and they are usually generated by one or more events. The alarm can be cleared but the event remains.

Note Alarm counts are refreshed every 15 seconds.

Main Data Page

The main data page is determined by the required parameter information. Active areas on the data pages include the following:

- Text boxes into which data may be entered using the keyboard
- Pull-downs from which one of several options may be chosen
- Check boxes in lists allow you to choose one or more items from the displayed list
- Radio buttons allow you to turn a parameter on or off
- Hyperlinks take you to other pages in the Cisco WCS user interface

Input text boxes are black text on a white background. When data is entered or selected, it is not sent to the controller, but it is saved in the text box until you click Go.

Administrative Tools

This area provides shortcuts to administration functions (such as logged in as, logout, refresh, and help) that you use regularly when configuring a controller through the web user interface.

Using the Search Feature

The enhanced WCS Search feature (see Figure 2-12) provides easy access to advanced search options and saved searches. You can access the search options from any page within WCS making it easy to search for a device or SSID (Service Set IDentifier).

Figure 2-12 WCS Search Feature

Quick Search

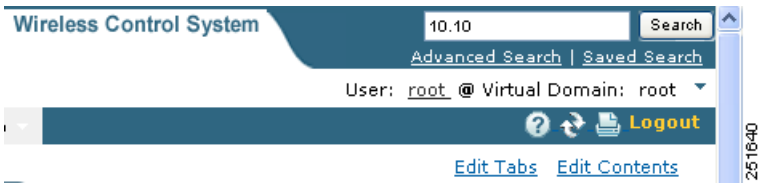
For a quick search, you can enter a partial or complete IP address, MAC address, name, or SSID for clients, alarms, access points, controllers, maps, tags, or rogue clients (see Figure 2-12).

Note You can also enter a username if you are searching for a client.

To quickly search for a device, follow these steps:

Step 1 Enter the complete or partial IP address, device name, SSID, or MAC address of the device in the quick Search text box (see Figure 2-13).

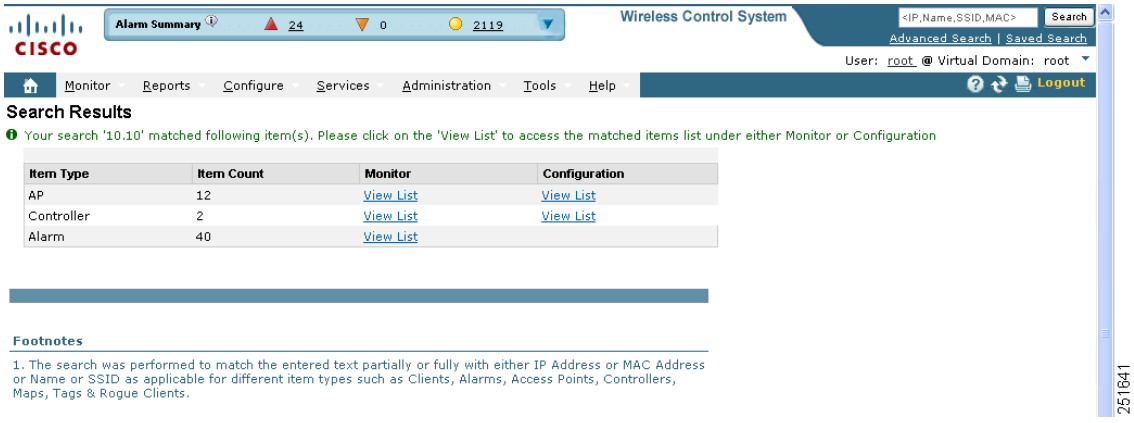
Figure 2-13 Quick Search with Partial IP Address



Step 2 Click **Search** to display all devices that match the Quick Search parameter.

The search results display the matching item type, the number of items that match your search parameter, and links to the list of matching results (see Figure 2-14). Click **View List** to view the matching devices from the Monitor or Configuration pages.

Figure 2-14 Quick Search Results Advanced Search



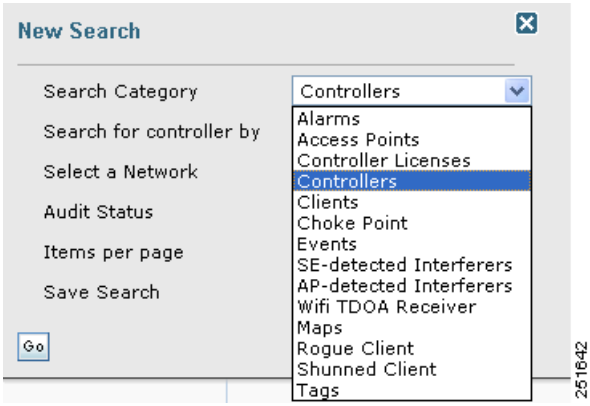
Advanced Search

To perform a more specific search for a device in WCS, follow these steps:

Step 1 Click **Advanced Search** located in the top right corner of WCS (see Figure 2-12).

Step 2 In the New Search page, select a category from the Search Category drop-down list (see Figure 2-15).

Figure 2-15 Search Category Drop-Down List



Note Click each of the following category for more information.

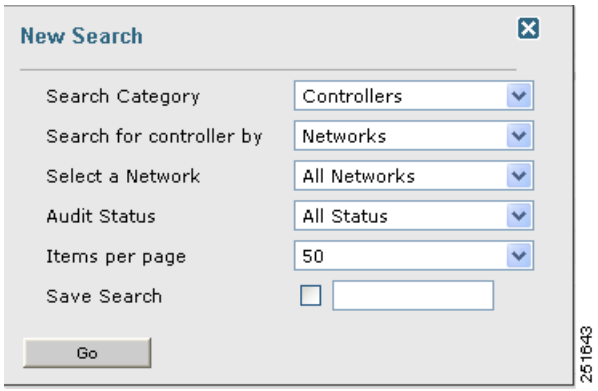
Search categories include:

- Alarms
- Access Points
- Controllers
- Clients
- Chokepoints
- Events
- SE-Detected Interferers
- Wi-Fi TDOA Receivers
- Maps
- Rogue Clients
- Shunned Clients
- Tags
- Controller Licenses

Step 3 Select all applicable filters or parameters for your search (see Figure 2-16).

Note Search parameters change depending on the selected category. The following pre-defined search filters have been added in release 6.0: Associated Clients, Authenticated Clients, Excluded Clients, Probing Clients, All Clients, New Clients detected in last 24 hours, unauthenticated clients, 2.4 GHz clients, and 5 GHz clients.

Figure 2-16 New Search Parameters



Step 4 Choose the number of items to display on the results page.

Step 5 To save this search, select the **Save Search** check box and enter a name for the search in the text box.

Step 6 When all filters and parameters are set, click **Go**.

Alarms

You can configure the following parameters when performing an advanced search for alarms (see Table 2-6):

Table 2-6 Search Alarms Parameters

Parameter	Options
Severity	Choose All Severities, Critical, Major, Minor, Warning, or Clear.
Alarm Category	Choose All Types, Access Points, Controller, Coverage Hole, Config Audit, Mobility Service, Context Aware Notifications, Interference, Mesh Links, Rogue AP, Adhoc Rogue, Security, WCSm or Performance.
Time Period	Choose a time increment from Any Time to Last 7 days. Default is Any Time.

Table 2-6 Search Alarms Parameters (continued)

Parameter	Options
Acknowledged State	Check to search for alarms with an Acknowledged or Unacknowledged state. If this check box is not selected, the acknowledged state is not taken into search criteria consideration.
Assigned State	Check to search for alarms with an Assigned or Unassigned state or by Owner Name. If this check box is not selected, the assigned state is not part of the search criteria. **Note** If you choose Assigned State > Owner Name, type the owner name in the available text box.

Note You can decide what information displays on the alarm search results page. See the "Configuring the Search Results Display" section on page 2-44 for more information.

See the "Monitoring Alarms" section on page 16-5 for more information on alarms.

Access Points

You can configure the following parameters when performing an advanced search for access points (see Table 2-7):

Table 2-7 Search Access Points Parameters

Parameter	Options
Search By	Choose All APs, Base Radio MAC, Ethernet MAC, AP Name, IP Address, Controller Name, Controller IP, All Unassociated APs, Floor Area, Outdoor Area, Unassigned APs, or Alarms. **Note** Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select Floor Area, you also must identify its campus and building. Or, if you select Alarms, you can search for access points based on the severity of the alarm.
AP Type	Choose All Types, LWAPP, or Autonomous.
AP Mode	Choose All Modes, Local, Monitor, H-REAP, Rogue Detector, Sniffer, Bridge, or SE-Connect.
Radio Type	Choose All Radios, 802.11a, or 802.11b/g.

Table 2-7 Search Access Points Parameters (continued)

Parameter	Options
802.11n Support	Check to search for access points with 802.11n support.
OfficeExtend AP Enabled	Check to search for OfficeExtend access points.

Note You can decide what information displays on the access points search results page. See the "Configuring the Search Results Display" section on page 2-44 for more information.

Controllers

You can configure the following parameters when performing an advanced search for controllers (see Table 2-8):

Table 2-8 Search Controllers Parameters

Parameter	Options
Search for controller by	Choose All Controllers, IP Address, Controller Name, or Network. **Note** Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Enter Controller IP Address	This text box appears only if you select IP Address from the Search for controller by text box.
Enter Controller Name	This text box appears only if you select Controller Name from the Search for controller by text box.
Select a Network	Choose All Networks or an individual network.
Audit Status	Choose one of the following from the drop-down list: • All Status • Mismatch—Config differences were found between WCS and controller during the last audit. • Identical—No config differences were found during the last audit. • Not Available—Audit status is unavailable.

Note You can decide what information displays on the controllers search results page. See the "Configuring the Search Results Display" section on page 2-44 for more information.

Clients

You can configure the following parameters when performing an advanced search for clients (see Table 2-9):

Table 2-9 Search Clients Parameters

Parameter	Options
Search By	Choose All Clients, All Excluded Clients, All Wired Clients, All Logged in Guests, IP Address, User Name, MAC Address, Asset Name, Asset Category, Asset Group, AP Name, Controller Name, Controller IP, MSE IP, Floor Area, or Outdoor Area. **Note** Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select IP address, you must enter the specific IP address for this search.
Clients Detected By	Choose WCS or MSEs. Clients detected by WCS—Clients stored in WCS databases. Clients detected by MSE—Clients stored on the mobility services engine that were detected by the MSE through controller polling.
Client States	Choose All States, Idle, Authenticated, Associated, Probing, or Excluded.
Restrict By Radio Band	Select the check box to indicate a specific radio band. Choose 5 GHz or 2.4 GHz from the drop-down list.
Restrict By Protocol	Select the check box to indicate a specific protocol. Choose 802.11a, 802.11b, 802.11g, 802.11n, or Mobile from the drop-down list.
Search on Controllers Now	Select the check box to indicate a search for clients on current controllers. **Note** When selected, the CCX and E2E Compatible check boxes become unavailable.
SSID	Select the check box and choose the applicable SSID from the drop-down list.
Profile	Select the check box to list all of the clients associated to the selected profile. **Note** Once the check box is selected, choose the applicable profile from the drop-down list.

Parameter	Options
CCX Compatible	Select the check box to search for clients that are compatible with Cisco Client Extensions. **Note** Once the check box is selected, choose the applicable version, All Versions, or Not Supported from the drop-down list.
E2E Compatible	Select the check box to search for clients that are End to End compatible. **Note** Once the check box is selected, choose the applicable version, All Versions, or Not Supported from the drop-down list.
NAC State	Select the check box to search for clients identified by a certain Network Admission Control (NAC) state. **Note** Once the check box is selected, choose the applicable state from the drop-down list. Select from Quarantine, Access, Invalid, and Not Applicable.
Include Disassociated	Select to include clients that are no longer on the network but for which WCS has historical records.

Note You can decide what information displays on the client search results page. See the "Configuring the Search Results Display" section on page 2-44 for more information.

Chokepoints

You can configure the following parameters when performing an advanced search for chokepoints (see Table 2-10):

Table 2-10 Search Chokepoint Parameters

Parameter	Options
Search By	Choose MAC Address or Chokepoint Name. **Note** Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select MAC address, you must enter the specific MAC address for this search.

Events

You can configure the following parameters when performing an advanced search for events (see Table 2-11):

Table 2-11 Search Events Parameters

Parameter	Options
Severity	Choose All Severities, Critical, Major, Minor, Warning, Clear, or Info. Color coded.
Event Category	Choose All Types, Access Points, Controller, Security, Coverage Hole, Rogue AP, Adhoc Rogue, Interference, Mesh Links, Client, Mobility Service, Location Notifications, Pre Coverage Hole, or WCS.

See the "Monitoring Rogue Alarm Events" section on page 16-22 for more information on events.

SE-Detected Interferers

You can configure the following parameters when performing an advanced search for interferers detected by access points (see Table 2-12):

Table 2-12 Search SE-Detected Interferers Parameters

Parameter	Options
Search By	Choose All Interferers, Interferer ID, Interferer Category, Interferer Type, Affected Channel, Affected AP, Severity, Power, or Duty Cycle. **Note** Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Detected By	Choose All Spectrum Experts or a specific spectrum expert from the drop-down list.
Detected within the last	Choose the time range for the interferer detections. The times range from 5 minutes to 24 hours to All History.
Active Interferers Only	Select the check box to only include active interferers in your search.

You can decide what information displays on the SE-detected interferers search results page. See the "Configuring the Search Results Display" section on page 2-44 for more information.

AP-Detected Interferers

You can configure the following parameters when performing an advanced search for interferers detected by access points (see Table 2-13):

Table 2-13 Search AP-Detected Interferers Parameters

Parameter	Options
Search By	Choose All Interferers, Interferer ID, Interferer Type, Affected Channel, Severity, Duty Cycle, or Location. **Note** Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Detected within the last	Choose the time range for the interferer detections. The times range from 5 minutes to 24 hours to All History.
Active Interferers Only	Select the check box to only include active interferers in your search.

Note You can decide what information displays on the AP-detected interferers search results page. See the "Configuring the Search Results Display" section on page 2-44 for more information.

Wi-Fi TDOA Receivers

You can configure the following parameters when performing an advanced search for Wi-Fi TDOA receivers (see Table 2-14):

Table 2-14 Search Wi-Fi TDOA Receivers Parameters

Parameter	Options
Search By	Choose MAC Address or Wi-Fi TDOA Receivers Name. **Note** Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.

Maps

You can configure the following parameters when performing an advanced search for maps (see Table 2-15):

Table 2-15 Search Map Parameters

Parameter	Options
Search for	Choose All Maps, Campuses, Buildings, Floor Areas, or Outdoor Areas.
Map Name	Search by Map Name. Enter map name in the text box.

Note You can decide what information displays on the maps search results page. See the "Configuring the Search Results Display" section on page 2-44 for more information.

See the "Monitoring Maps Overview" section on page 5-2 for more information on maps.

Rogue Clients

You can configure the following parameters when performing an advanced search for rogue clients (see Table 2-16):

Table 2-16 Search Rogue Client Parameters

Parameter	Options
Search By	Choose All Rogue Clients, MAC Address, Controller, MSE, Floor Area, or Outdoor Area.
Search In	Choose MSEs or WCS Controllers.
Status	Select the check box and choose Alert, Contained, or Threat from the drop-down list to include status in the search criteria.

See the "Monitoring Rogue Access Points, Ad hoc Events, and Clients" section on page 3-9 for more information on rogue clients.

Shunned Clients

Note When a Cisco IPS sensor on the wired network detects a suspicious or threatening client, it alerts the controller to shun this client.

You can configure the following parameters when performing an advanced search for shunned clients (see Table 2-17):

Table 2-17 Search Shunned Client Parameters

Parameter	Options
Search By	Choose All Shunned Clients, Controller, or IP Address. **Note** Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.

Tags

You can configure the following parameters when performing an advanced search for tags (see Table 2-18):

Table 2-18 Search Tags Parameters

Parameter	Options
Search By	Choose All Tags, Asset Name, Asset Category, Asset Group, MAC Address, Controller, MSE, Floor Area, or Outdoor Area. **Note** Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Search In	Choose MSEs or WCS Controllers.
Last detected within	Choose a time increment from 5 minutes to 24 hours. Default is 15 minutes.
Tag Vendor	Select the check box and choose Aeroscout, G2, PanGo, or WhereNet.
Telemetry Tags only	Check the Telemetry Tags only to search tags accordingly.

Controller Licenses

You can configure the following parameters when performing an advanced search for controller licenses (see Table 2-19):

Table 2-19 Search Controller Licenses Parameters

Parameter	Options
Controller Name	Type the controller name associated with the license search.
Feature Name	Choose All, Plus, or Base depending on the license tier.
Type	Choose All, Demo, Extension, Grace Period, or Permanent.
% Used or Greater	Select the percentage of the license use. The percentages range from 0 to 100.

See the "Accessing the License Center" section on page 18-67 for more information on licenses and the License Center.

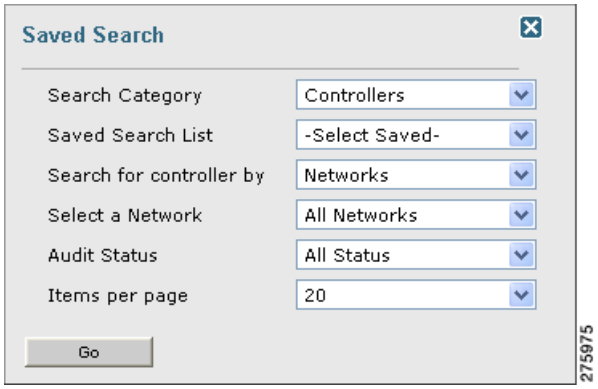
Saved Searches

The Saved Search feature enables you to access and run any previously saved search (see Figure 2-17).

Note When saving a search, you must assign a unique name to the search.

Note Saved searches apply only to the current partition.

Figure 2-17 Saved Search Page



To access and run a saved search, follow these steps:

Step 1 Click **Saved Search**.

Step 2 Select a category from the Search Category drop-down list.

Step 3 Select a saved search from the Saved Search List drop-down list.

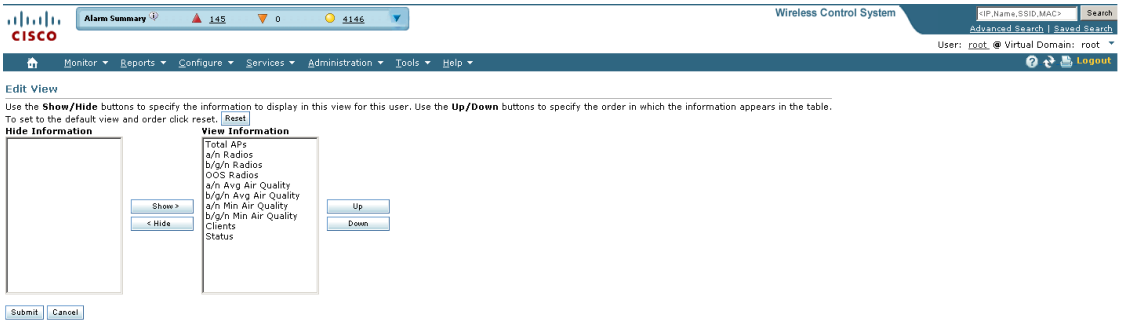
Step 4 If necessary, change the current parameters for the saved search.

Step 5 Click **Go**.

Configuring the Search Results Display

The Edit View page (see Figure 2-18) enables you to choose which columns appear in the Search Results page.

Figure 2-18 Edit View Page



251644

Column names appear in one of the following lists:

- Hide Information—Lists columns that do not appear in the table. The **Hide** button points to this list.
- View Information—Lists columns that do appear in the table. The **Show** button points to this list.

To display a column in a table, click it in the Hide Information list, then click **Show**. To remove a column from a table, click it in the View Information list, then click **Hide**. You can select more than one column by holding down the shift or control key.

To change the position of a column in the View Information list, click it, then click **Up** or **Down**. The higher a column is in the list, the farther left it appears in the table.

Command Buttons

The following command buttons appear in the Edit View page:

- Reset—Sets the table to the default display.
- Show—Moves the highlighted columns from the Hide Information list to the View Information list.

- Hide—Moves the highlighted columns from the View Information list to the Hide Information list.
- Up—Moves the highlighted columns upward in the list (further to the left in the table).
- Down—Moves the highlighted columns downward in the list (further to the right in the table).
- Submit—Saves the changes to the table columns and returns to the previous page.
- Cancel—Undoes the changes to the table columns and returns to the previous page.

CHAPTER 3

Configuring Security Solutions

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

- Cisco Unified Wireless Network Solution Security, page 3-1
- Interpreting the Security Tab, page 3-4
- Monitoring Rogue Access Points, Ad hoc Events, and Clients, page 3-9
- Rogue Access Points, page 3-9
- Adhoc Rogue Alarms, page 3-17
- Rogue Access Point Location, Tagging, and Containment, page 3-19
- Security Overview, page 3-25
- Switch Port Tracing, page 3-33
- Using WCS to Convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 Mode, page 3-34
- Configuring a Firewall for WCS, page 3-35
- Access Point Authorization, page 3-36
- Management Frame Protection (MFP), page 3-36
- Configuring Intrusion Detection Systems (IDS), page 3-38
- Configuring IDS Signatures, page 3-38
- Enabling Web Login, page 3-46
- Certificate Signing Request (CSR) Generation, page 3-49

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

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 Cisco WCS, 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 WCS, errors can be eliminated, and the overall effort is greatly reduced.

Rogue Access Point Solutions

This section describes security solutions for rogue access points.

Rogue Access Point Challenges

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 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.

Tagging and Containing Rogue Access Points

When the Cisco Unified Wireless Network Solution is monitored using WCS, WCS 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

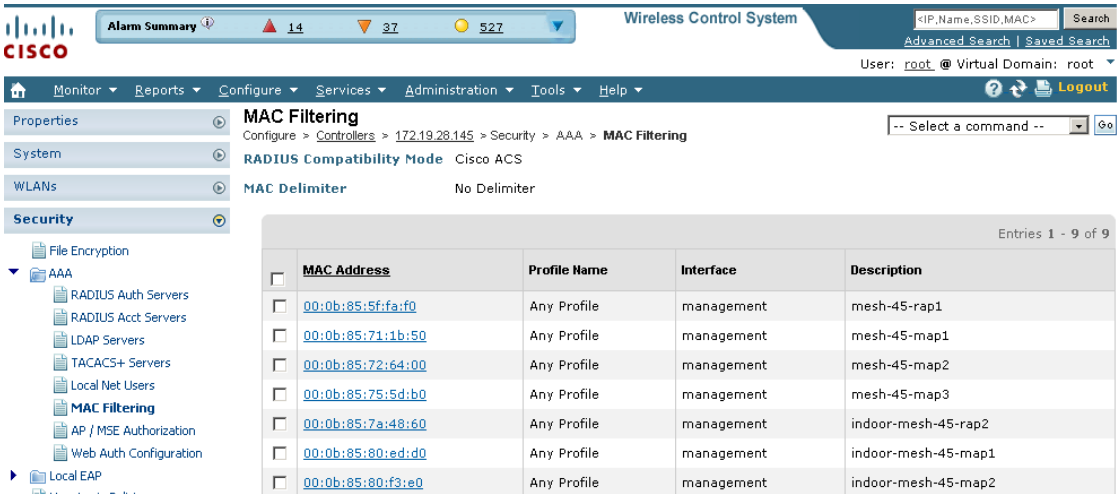
You can secure your network against any rogue access points and disallow access point attacks for those access points not defined in the MAC filter list. Follow these steps to set up MAC filtering.

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address for which you want to enter MAC filters.

Step 3 Choose **Security > AAA> MAC Filtering** from the left sidebar menu. The MAC Filtering page appears (see Figure 3-1).

Figure 3-1 MAC Filtering Page



The RADIUS compatibility mode, MAC delimiter, MAC address, interface, and description appear.

Step 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.

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.

Step 5 To make changes to the profile name, interface, or description, click a specific MAC address in the MAC Address column.

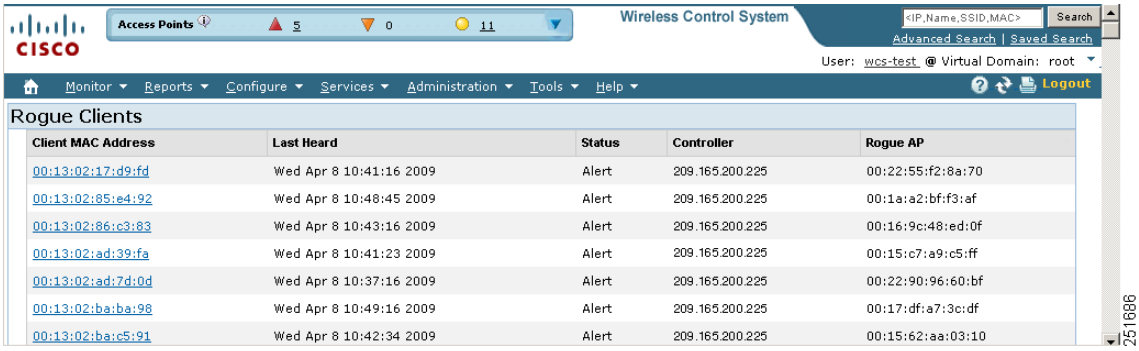
Interpreting the Security Tab

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** tab from the WCS home page. The Rogue Clients page appears (see Figure 3-2).

Figure 3-2 Rogue Clients Page



You can customize the information you want the Security tab to display. Use the Edit Contents link to choose data you want collected and displayed. See the "Editing Content" section on page 2-25 for more information on using the Edit Content link. The default Security tab options are described below.

Security Index

The Security Index indicates the security of the WCS 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 WCS itself. The Security Index of the WCS 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 Guest WLANs are excluded from the WLANs. A WLAN that 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.

Note The configurations stored in WCS may not be current with the ones in the controllers unless the Refresh from Controller command is run from WCS. You can run Security Index calculations from the Configuration Sync task to get the latest configuration data from all the controllers. See the "Configuration Sync" section on page 18-5 for steps on enabling the security index.

Malicious Rogue Access Points

This section 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 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.

Table 3-1 Malicious Rogue AP Details

Parameter	Description
Alert	Indicates the number of rogues in an alert state. **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.
Contained	Indicates the number of contained rogues.
Threat	Indicates the number of threat rogues.
Contained Pending	Indicates the number of contained rogues pending. **Note** Contained Pending indicates that the containment action is delayed due to unavailable resources.

Adhoc Rogues

The Adhoc Rogues section 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 displays as *Alert* when first scanned by the controller or as *Pending* when operating system identification is underway.

Table 3-2 Ad hoc Rogues

Parameter	Description
Alert	Indicates the number of ad hoc rogues in an alert state. **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.
Contained	Indicates the number of contained rogues.
Threat	Indicates the number of threat rogues.
Contained Pending	Indicates the number of contained rogues pending. **Note** Contained pending indicates that the containment action is delayed due to unavailable resources.

CleanAir Security

This section 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 5-43.

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 3-3 Unclassified Rogue Access Points

Parameter	Description
Alert	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.
Contained	Number of contained unclassified rogues.
Contained Pending	Number of contained unclassified rogues pending.

Friendly Rogue Access Points

This section 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 3-4 Friendly Rogue AP Details

Parameter	Description
Alert	Indicates the number of rogues in an alert state. **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.
Internal	Indicates the number of internal access points. **Note** Internal indicates that the detected access point is inside the network and has been manually configured as Friendly - Internal.
External	Indicates the number of external access points. **Note** External indicates that the detected access point is outside of the network and has been manually configured as Friendly - External.

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 3-5 AP Threats/Attacks

Parameter	Description
Fake Attacks	Number of fake attacks
AP Missing	Number of missing access points
AP Impersonation	Number of access point impersonations
AP Invalid SSID	Number of invalid access point SSIDs
AP Invalid Preamble	Number of invalid access point preambles
AP Invalid Encryption	Number of invalid access point encryption
AP Invalid Radio Policy	Number of invalid access point radio policies
Denial of Service (NAV related)	Number of Denial of Service (NAV related) request
AP Detected Duplicate IP	Number of detected duplicate access point IPs

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 and 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.

Monitoring 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 WCS 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.

Rogue Access Points

- Monitoring Rogue AP Alarms
  - Classifying Rogue Access Points
  - Rogue Access Point Classification Types
  - Viewing Rogue AP Alarm Details

- Viewing Rogue Client Details

Monitoring Rogue AP Alarms

Rogue access point radios are unauthorized access points detected by one or more Cisco Managed Series lightweight access points.

To open the Rogue AP Alarms page, do one of the following:

- Search for rogue access points. See the "Using the Search Feature" section on page 2-31 for more information about the search feature.
- In the WCS home page, click the Security tab. 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. See the "Security Tab" section on page 2-21 for more information.
- Click the **Malicious AP** number link in the Alarm Summary box. See the "Using the Alarm Summary" section on page 16-1 for more information.

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.

The Rogue AP Alarms page contains the following parameters:

- Severity—Indicates the severity of the alarm.

  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
- Rogue MAC Address—Indicates the MAC address of the rogue access points. See the "Viewing Rogue AP Alarm Details" section on page 3-14.
- Vendor—Rogue access point vendor name or Unknown.
- Classification Type—Malicious, Friendly, or Unclassified. See the "Rogue Access Point Classification Types" section on page 3-13 for additional information.
- 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 WCS 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.
- Owner
- 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 "Rogue Access Point Classification Types" section on page 3-13 for additional information.
  - Malicious rogue states include: Alert, Contained, Threat, Contained Pending, and Removed. See the "Malicious Rogue Access Points" section on page 3-5 for more information.
  - Friendly rogue states include: Internal, External, and Alert. See the "Friendly Rogue APs" section on page 3-13 for more information.
  - Unclassified rogue states include: Pending, Alert, Contained, and Contained Pending.
- 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. See the "Acknowledging Alarms" section on page 3-22 for more information.

Note The alarm remains in WCS, 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 party's network could have legal consequences.

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 WCS 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.

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

From	To
Friendly (Internal, External, Alert)	Malicious (Alert)
Friendly (Internal, External, Alert)	Unclassified (Alert)
Friendly (Alert)	Friendly (Internal, External)
Malicious (Alert, Threat)	Friendly (Internal, External)
Malicious (Contained, Contained Pending)	Malicious (Alert)
Unclassified (Alert, Threat)	Friendly (Internal, External)
Unclassified (Contained, Contained Pending)	Unclassified (Alert)
Unclassified (Alert)	Malicious (Alert)

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:

- 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 3-13 for more information. For more information on configuring friendly access point rules, see the "Configuring a Friendly Access Point Template" section on page 12-81.
- 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 3-14 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 tab of the WCS 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 "Viewing Alarm Details" section on page 16-9 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 tab of the WCS 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:

- 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.

Click an underlined number in any of the time period categories for detailed information regarding the friendly rogue access points. See the "Viewing Alarm Details" section on page 16-9 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 tab of the WCS 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 "Viewing Alarm Details" section on page 16-9.

Viewing Rogue AP Alarm Details

Rogue access point radios are unauthorized access points detected by Cisco managed lightweight access points. Alarm event details for each rogue access point are available from the Rogue AP Alarms list page.

To view alarm events for a rogue access point radio, follow these steps:

Step 1 In the Monitor > Alarms list page for rogue access point alarms, click the rogue MAC address for the applicable alarm. The Alarm Details page opens.

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.

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. See the "Acknowledging Alarms" section on page 3-22 for more information.
- Classification Type—Malicious, Friendly, or Unclassified. See the "Rogue Access Point Classification Types" section on page 3-13 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 3-13 for additional information.
- 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 on 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)—Provided through polling.

Trap—Provided by the controller.

- Severity—The severity of the alarm.

  You can use the Severity Configuration feature to determine the level of severity for rogue access points.

- Previous Severity—The previous severity of the alarm: Critical, Major, Minor, Clear.
- Event Details—Click to open the Monitor > Rogue AP Alarm > Rogue AP Events page. See the "Monitoring Rogue Alarm Events" section on page 3-22 for more information.
- Switch Port Trace Status—Indicates the switch port trace status. See the "Switch Port Tracing" section on page 3-33 for more information regarding switch port tracing. Potential switch port trace statuses include:

  Not traced—Switch port tracing was never executed.

  Failed—The switch port trace failed. Please check the detail status page in the Switch Port Trace dialog for more information.

  Traced and detected on network—Yes network means "wired" network. This state indicates that the switch port trace was executed, and a rogue access point was found on the wired network.

  Traced but not detected on wire—The switch port trace was executed but no rogue access point was not found on the network.

  Traced and wire contained—The switch port trace was executed, and the switch port to which a rogue access point was connected is now disabled. The rogue access point is now wire contained.

- Switch Port Tracing Details—Provides the most recent switch port tracing details. To view additional trace details, use the **Click here for more details** link. See the "Switch Port Tracing" section on page 3-33 for more information.
- 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 3-17 for more information.

Note The number of rogue clients is the only real-time field on 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.

- 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.

Viewing Rogue Client Details

You can view a list of rogue clients in several ways:

- Perform a search for rogue clients using the WCS Search feature. See the "Using the Search Feature" section on page 2-31 for more information.
- 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, select **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's 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 Information

Adhoc Rogue Alarms

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

- Monitoring Adhoc Rogue Alarms
- Viewing Adhoc Rogue Alarm Details

Monitoring Adhoc Rogue Alarms

The Adhoc Rogue Alarms page displays alarm events for adhoc rogues.

To access the Adhoc Rogue Alarms page, do one of the following:

- Perform a search for adhoc rogue alarms. See the "Using the Search Feature" section on page 2-31 for more information.

- In the WCS home page, select the Security tab. This page displays all the adhoc rogues detected in the past hour and the past 24 hours. Click the adhoc rogue number to view the adhoc 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 parameters:

- Severity—Indicates the severity of the alarm.
- You can use the Severity Configuration feature to determine the level of severity for the following adhoc rogue alarm types:
  - Adhoc Rogue auto contained
  - Adhoc Rogue detected
  - Adhoc Rogue detected on network
  - Adhoc Rogue detected on network
- Rogue MAC Address—Indicates the MAC address of the rogue. See the "Viewing Adhoc Rogue Alarm Details" section on page 3-18 for more information.
- Vendor—Indicates the adhoc 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 on 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.

- 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 adhoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
- SSID—The Service Set Identifier that is being broadcast by the rogue adhoc radio. It is blank if there is no broadcast.
- Map Location—Indicates the map location for this adhoc rogue.
- Acknowledged—Displays whether or not the alarm is acknowledged by the user. See the "Acknowledging Alarms" section on page 3-22 for more information.

Viewing Adhoc Rogue Alarm Details

Alarm event details for each adhoc rogue are available from the Adhoc Rogue Alarms page.

- In the Adhoc Rogue Alarms page, click an item under Rogue MAC Address.

This page displays alarm events for a rogue access point radio. Rogue access point radios are unauthorized access points detected by Cisco managed lightweight access points. The following information is available:

- General
  - Rogue MAC Address—Media Access Control address of the adhoc rogue.
  - Vendor—Adhoc 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.
  - State—Indicates the state of the alarm. Possible states for adhoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
  - SSID—Service Set Identifier being broadcast by the adhoc rogue radio. (Blank if SSID is not broadcast.)
  - Channel Number—Indicates the channel of the adhoc rogue.
  - Containment Level—Indicates the containment level of the adhoc rogue or Unassigned.
  - Radio Type—Lists all radio types applicable to this adhoc rogue.
  - Strongest AP RSSI—Indicates the strongest received signal strength indicator for this WCS (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 adhoc.
  - 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.
  - Severity—Indicates the severity of the alarm.
  - 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 “Monitoring Events” for more information.
- Annotations—Lists existing notes for this alarm.

Rogue Access Point Location, Tagging, and Containment

When the Cisco Unified Wireless Network Solution is monitored using WCS, WCS 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
- 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. See the "Using the Search Feature" section on page 2-31 for more information about the search feature.
- In the WCS home page, select the Security tab. 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 box. See the "Using the Alarm Summary" section on page 16-1 for more information.

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 **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. (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.

Working with Alarms

You can view, assign, and clear alarms and events on access points and mobility services engine using Cisco WCS.

Details on how to have email notifications of alarms sent to you is also described.

- Assigning and Unassigning Alarms
- Deleting and Clearing Alarms
- Acknowledging Alarms

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. See the "Using the Search Feature" section on page 2-31 for more information.

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

Note If you delete an alarm, Cisco WCS removes it from its database. If you clear an alarm, it remains in the Cisco WCS 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, click **Administration > Settings > Alarms**.

Acknowledging Alarms

You may 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 may 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, click 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, WCS will 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.

Any alarms, once acknowledged, will not show up on either the Alarm Summary page or any alarm list page. Also, no emails 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, go to the **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. WCS 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 WCS has already generated an alarm.

Monitoring Rogue Alarm Events

The Events page enables you to review information about rogue alarm events. WCS 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 WCS. See the "Using the Search Feature" section on page 2-31 for more information.
- 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 3-14 for more information.

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 3-23 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 3-13 for more information.
- 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. See the "Rogue Access Point Classification Types" section on page 3-13 for additional information.
- 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.
  - 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 "Rogue Access Point Classification Types" for more information.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point. See "Rogue Access Point Classification Types" 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 adhoc rogue events. WCS generates an event when an adhoc rogue is detected or if you make manual changes to an adhoc rogue (such as changing its state). The Adhoc Rogue Events list page displays all adhoc rogue events.

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

Step 1 Do one of the following:

- Perform a search for adhoc rogues events using the Advanced Search feature of WCS. See the "Using the Search Feature" section on page 2-31 for more information.
- In the Adhoc Rogue Alarms details page, click **Event History** from the Select a command drop-down list. See the "Viewing Adhoc Rogue Alarm Details" section on page 3-18 for more information.

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 3-25 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 adhoc 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 adhoc 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

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

Cisco WCS 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 of an enterprise's overall wireless security posture, 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:

- 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
- 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

The Cisco WCS 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 WCS 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. The WCS displays the vulnerability assessment results through a Security Index on the WCS 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 3-26" 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 will 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 3-27" for more information.

Security Index

Security Index gives an indication of the security of the WCS 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 WCS itself. For example, the security index of the WCS 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 WCS may not be up-to-date with the ones in the controllers unless the Refresh from Controller command is run from WCS. 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
- Security Index Controller Report
- Potential Security Issues

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 may include:

- 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.

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

The following tables describes potential security issues.

Table 3-7 Potential Security Issues

Controller Security Issue	Why is this an Issue?	What is the Solution?
WLAN SSID on the controller has a weak authentication method.	Weak authentication method for a WLAN which can be broken by using tools available online if WLAN packets are sniffed.	Use the most secured authentication method and one that is WPA+WPA2.
WLAN SSID on the controller has a weak authentication method (CKIP) configured.	Weak authentication method for a WLAN.	Use the most secured authentication method and one that is WPA+WPA2.
WLAN SSID on the controller has no user authentication configured.	No authentication method is a clear security risk for a WLAN.	Configure strong authentication methods such as WPA+WPA2.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 40 bits) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 40 bits with Key Permutation) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 40 bits with MMH) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 40 bits with MMH and Key Permutation) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (WEP 104 bits) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 104 bits) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.

Table 3-7 Potential Security Issues (continued)

Controller Security Issue	Why is this an Issue?	What is the Solution?
WLAN SSID on the controller has a weak encryption method (CKIP WEP 104 bits with MMH) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 104 bits with Key Permutation) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 104 bits with MMH and Key Permutation) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (WEP 40 bits) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (WEP 128 bits) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (TKIP) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has no encryption configured.	No encryption method is a clear security risk for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (WEP 104 bits) configured.	Weak encryption method for WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has no key management methods configured (applicable only for WPA+WPA2).	A key management method enhances the security of keys; without one, WLAN is less secure.	Configure at least one key management methods such as CCKM.
WLAN SSID on the controller has MFP Client Protection set to “Optional”.	With MFP Client Protection set to optional for a WLAN, authenticated clients may not be shielded from spoofed frames.	Set MFP Client Protection to “Required” to protect against clients connecting to a rogue access point.
WLAN SSID on the controller has MFP Client Protection set to “Disabled”.	With MFP Client Protection set to disabled for a WLAN, authenticated clients may not be shielded from spoofed frames.	Set MFP Client Protection to “Required” to protect against clients connecting to a rogue access point.
WLAN SSID interface is set to “management” on the controller.	As recommended from SAFE, user traffic should be separated from management traffic.	WLAN interface should not be set to “management” on the controller.

Table 3-7 Potential Security Issues (continued)

Controller Security Issue	Why is this an Issue?	What is the Solution?
Interface set to one which is VLAN for a WLAN.	As recommended from SAFE, user traffic should be separated from VLAN traffic.	WLAN needs its interface to be set to one which is neither management nor one which has a VLAN.
WLAN SSID on the controller has "Client Exclusion" disabled.	With Client Exclusion policies disabled, an attacker is able to continuously try to access the WLAN network.	Enable "Client Exclusion" to secure against malicious WLAN client behavior.
WLAN SSID on the controller has "Broadcast SSID" enabled.		Disable "Broadcast SSID" to secure your wireless network.
WLAN SSID on the controller has "MAC Filtering" disabled.		Enable "MAC Filtering" to secure your wireless network.
Protection Type is set to "AP Authentication" on the controller.	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.	Set Protection Type to "Management Frame Protection (MFP)" on the controller.
Protection Type is set to "None" of the controller.	No security for 802.11 management messages passed between access points and clients.	Set Protection Type to "Management Frame Protection (MFP)" on the controller.
Radio type is configured to detect rogues only on DCA channels.	Rogue detection, if done only on a subset of country/all channels, is less secure than one that is done on country/all channels.	Configure radio types 802.11a/n and 802.11b/g/n to detect rogues on country channels or all channels.
Radio type is configured to detect rogues on neither country channels nor DCA channels.	Rogue detection, if not configured on country nor DCA channels, is less secure than when done on country/all channels.	Configure radio types 802.11a/n and 802.11b/g/n to detect rogues on country channels or all channels.
The rogue policy to detect and report adhoc networks is disabled on the controller.	With detection and reporting of adhoc networks turned off, adhoc rogues go undetected.	Enable the rogue policy to detect and report adhoc networks
"Check for all Standard and Custom Signatures" is disabled on the controller.	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.	Check for all Standard and Custom Signatures needs to be turned on to identify various types of attacks in incoming 802.11 packets.

Table 3-7 Potential Security Issues (continued)

Controller Security Issue	Why is this an Issue?	What is the Solution?
Some of the Standard Signatures are disabled on the controller.	If only some of the Standard Signatures are disabled,	Enable all Standard Signatures on the controller.
The "Excessive 802.11 Association Failures" Client Exclusion Policy is disabled on the controller.	Excessive failed association attempts can consume system resources and launch potential a denial-of-service attack to the infrastructure.	Enable the "Excessive 802.11 Association Failures" Client Exclusion Policy on the controller.
The "Excessive 802.11 Authentication Failures" Client Exclusion Policy is disabled on the controller.	Excessive failed authentication attempts can consume system resources and launch potential Denial-of-Service attack to the infrastructure.	Enable the "Excessive 802.11 Authentication Failures" Client Exclusion Policy on the controller.
The "Excessive 802.1X Authentication Failures" Client Exclusion Policy is disabled on the controller.	Excessive 802.1X failed authentication attempts can consume system resources and launch potential denial-of-service attack to the infrastructure.	Excessive 802.1X Authentication Failures Client Exclusion Policy must be enabled to prevent denial-of-service attack to the infrastructure.
The "Excessive 802.11 Web Authentication Failures" Client Exclusion Policy is disabled on the controller.	If Excessive 802.11 Web failed web authentication attempts can consume system resources and launch potential Denial-of-Service attack to the infrastructure.	Enable the "Excessive 802.11 Web Authentication Failures" Client Exclusion Policy on the controller.
The "IP Theft or IP Reuse" Client Exclusion Policy is disabled on the controller.	If IP Theft or Reuse Client Exclusion Policy is disabled, then an attacker masquerading as another client would not be disallowed.	Enable the "IP Theft or IP Reuse" Client Exclusion Policy on the controller.
No CIDS Sensor configured on the controller.	If no enabled IDS Sensor is configured, then IP-level attacks would not be detected.	Configure at least one CIDS Sensor on the controller.
Controller is configured with default community strings for SNMP v1/v2.	If SNMP V1 or V2 with default Community is configured then it is open to easy attacks since default communities are well known.	Use SNMPv3 with Auth and Privacy Types.
Controller is configured with non-default community strings for SNMP v1/v2.	SNMP V1 or V2 with non-default Community is slightly more secure than default Community but still less secure than SNMP V3.	Use SNMPv3 with Auth and Privacy types.
SNMPv3 is configured with a default user on the controller.	Using a default user makes SNMP V3 connections less secure.	Use a non-default username for SNMPv3 with Auth and Privacy Types.

Table 3-7 Potential Security Issues (continued)

Controller Security Issue	Why is this an Issue?	What is the Solution?
SNMPv3 is configured with either no Auth or Privacy Type on the controller.	SNMP V3 with either Auth or Privacy Type set to none reduces the security of SNMP V3 connection.	Use SNMPv3 with Auth and Privacy Types to secure your wireless network.
HTTP (Web Mode enabled but Secure Web Mode disabled) is enabled on the controller.	HTTP is less secure than HTTPS.	Enable HTTPS (both Web Mode and Secure Web Mode) on the controller.
Telnet is enabled on the controller.	If telnet is enabled, then the controller is at risk of being hacked into.	Disable telnet on the controller.
SSH is disabled and timeout value is set to zero on the controller.	If SSH is enabled and timeout is zero then the controller has risk of being hacked into.	Enable SSH with non-zero timeout value on the controller.
Telnet is enabled on the AP.	If telnet is enabled, then the access point is at risk of being hacked into.	Disable Telnet on all access points.
SSH is enabled on the AP.		Disable SSH on all the access points.
At least one of the APs is configured with default username or password.	If default password is configured, then access points are more susceptible to connections from outside the network.	Configure a non-default username and strong password for all access points associated to the controller.

Table 3-8 Potential Security Issues

Location Server/ Mobility Server Engine Security Issue	Why is this an Issue?	What is the Solution?
HTTP is enabled on the location server.	HTTP is less secure than HTTPS.	Enable HTTPS on the location server.
A location server user has a default password configured.	If default password is configured, then Location Server/ Mobility Server Engine is more susceptible to connections from outside the network.	Configure a strong password for the location server users.
HTTP is enabled on the mobility services engine.	HTTP is less secure than HTTPS.	Enable HTTPS on the mobility services engine.

Table 3-8 Potential Security Issues (continued)

Location Server/ Mobility Server Engine Security Issue	Why is this an Issue?	What is the Solution?
A mobility services engine user has default password configured.	If default password is configured, then Location Server/ Mobility Server Engine is more susceptible to connections from outside the network.	Configure a strong password for the users on the mobility services engine.
wIPS Service is not enabled on the mobility services engine.	Your network is vulnerable to advanced security threats.	Deploy wIPS Service to protect your network from advanced security threats.

Switch Port Tracing

Currently, WCS 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 an CAPWAP Rogue AP Report message. With this method, WCS 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 WCS log and only for rogue access points, not rogue clients.

Note 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.

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

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 WCS home page, click the **Security** tab.

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

Step 3 Choose for which rogue you are setting switch port tracking by clicking the URL in the MAC Address column. The Alarms > Rogue AP details page opens.

Step 4 From the Select a command drop-down list, choose **Trace Switch Port**. The Trace Switch Port page opens, and WCS runs a switch port trace.

When one or more searchable MAC addresses are available, the WCS 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 rogue's switch port.

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 (CIDS/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 WCS to Convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 Mode

Follow these steps to convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 LWAPP transport mode using the WCS user interface.

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 WCS user interface. Then follow these steps to change the LWAPP transport mode from Layer 3 to Layer 2:

a. Click **Configure > Controllers** to navigate to the All Controllers page.

b. Click the desired controller's IP address to display the *IP Address* > Controller Properties page.

c. In the sidebar, click **System > General** to display the *IP Address* > General page.

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

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

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

Step 3 Follow these steps to restart your Cisco Unified Wireless Network Solution:

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 controller's IP address 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 WCS

When a WCS server and a WCS 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)

Open these ports to configure your firewall to allow communications between a WCS server and a WCS user interface.

Access Point Authorization

You can view a list of authorized access points along with the type of certificate that an access point uses for authorization.

Step 1 Choose **Configure > Controllers**.

Step 2 Click one of the URLs in the IP address column.

Step 3 From the left sidebar menu, choose **Security > AP/MSE Authorization**.

Step 4 The AP Policies portion of the page indicates whether the authorization of access points is enabled or disabled. It also indicates whether the acceptance of self-signed certificates (SSC APs) is enabled or disabled. Normally, access points can be authorized either by AAA or certificates. (SSC is only available for 4400 and 200 controllers.)

To change these values, choose **Edit AP Policies** from the Select a command drop-down list, and click **Go**.

Step 5 The AP Authorization List portion shows the radio MAC address of the access point, certificate type, and key hash. To add a different authorization entry, choose **Add AP/MSE Auth Entry** from the Select a command drop-down list, and click **Go**.

Step 6 From the drop-down list, choose a template to apply to this controller and click **Apply**. To create a new template for access point authorization, click the **click here** to get redirected to the template creation page. See the "Configuring an Access Point or MSE Authorization" section on page 12-59 for steps on creating a new template.

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. WCS software release 4.1 and later supports both infrastructure and client MFP while WCS software release 4.0 supports only infrastructure MFP.

- 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 session's data frames. 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 may 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 MC 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. In order 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 12-18.

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 hybrid-REAP modes when the access point is connected to a controller. They support client MFP in local, hybrid-REAP, 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 may associate to a WLAN if client MFP is disabled or optional.

Configuring Intrusion Detection Systems (IDS)

The Cisco intrusion detection system/intrusion protection system (CIDS/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.

Follow these steps to view IDS sensors.

Step 1 Choose **Configure > Controllers**.

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

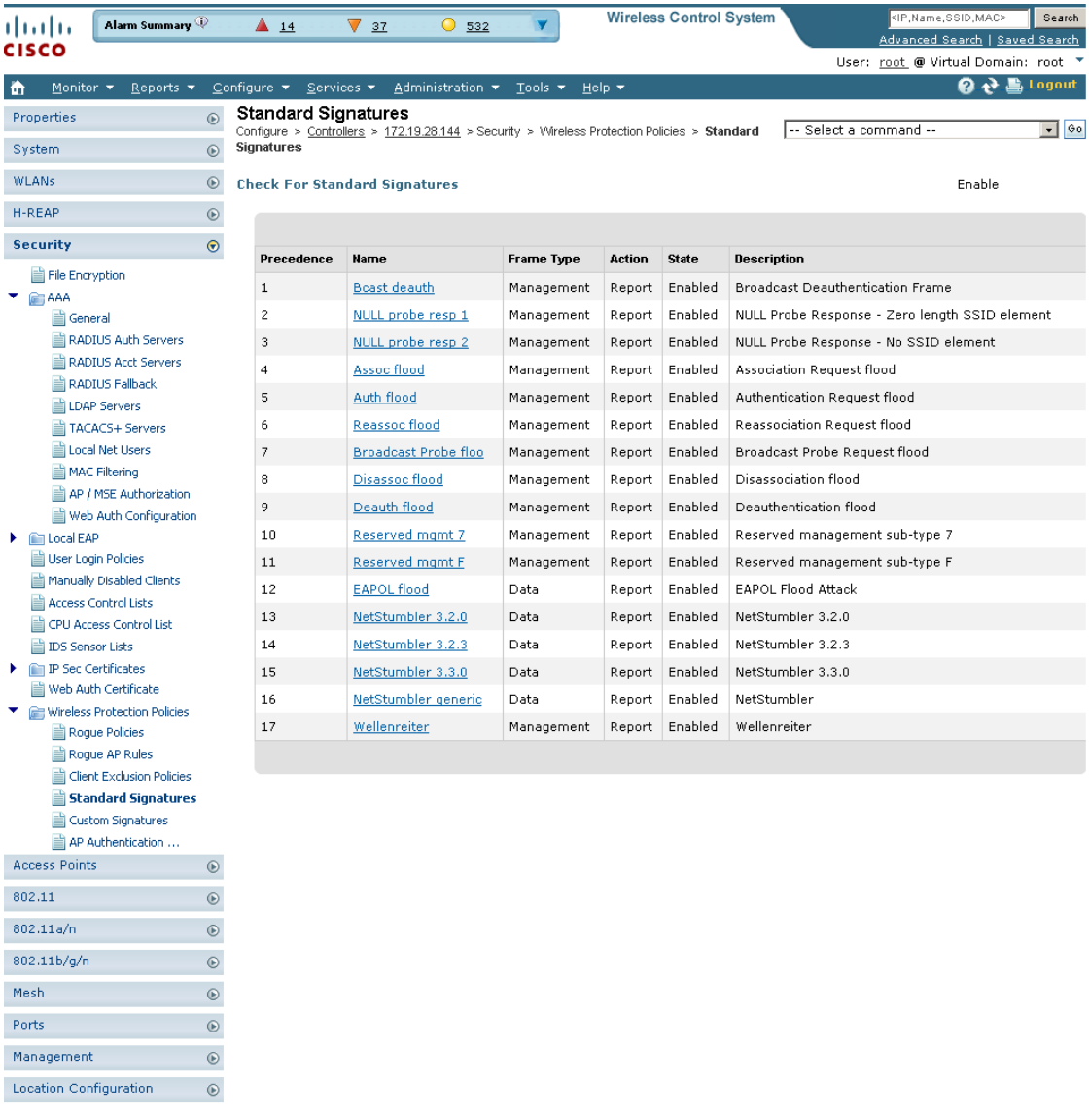
Step 3 From the left sidebar menu, choose **Security > IDS Sensor Lists**. The IDS Sensor page appears. This page lists all of the IDS sensors that have been configured for this controller.

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 (see Figure 3-3). 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.

Figure 3-3 Standard Signatures Page



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:
  - 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 WCS.

  The management frame flood signatures include:
  - 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:

Table 3-9 NetStumbler Versions

Version	String
3.2.0	"Flurble gronk bloopit, bnip Frundletrune"
3.2.3	"All your 802.11b are belong to us"
3.3.0	Sends white spaces

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:

- 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.

Follow these instructions to configure signatures:

- Uploading IDS Signatures, page 3-41
- Downloading IDS Signatures, page 3-42
- Enabling or Disabling IDS Signatures, page 3-43

Uploading IDS Signatures

Follow these steps to upload IDS signatures from the controller.

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 3-42.

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 the Cisco WCS because WCS's built-in TFTP server and third-party TFTP server use the same communication port.

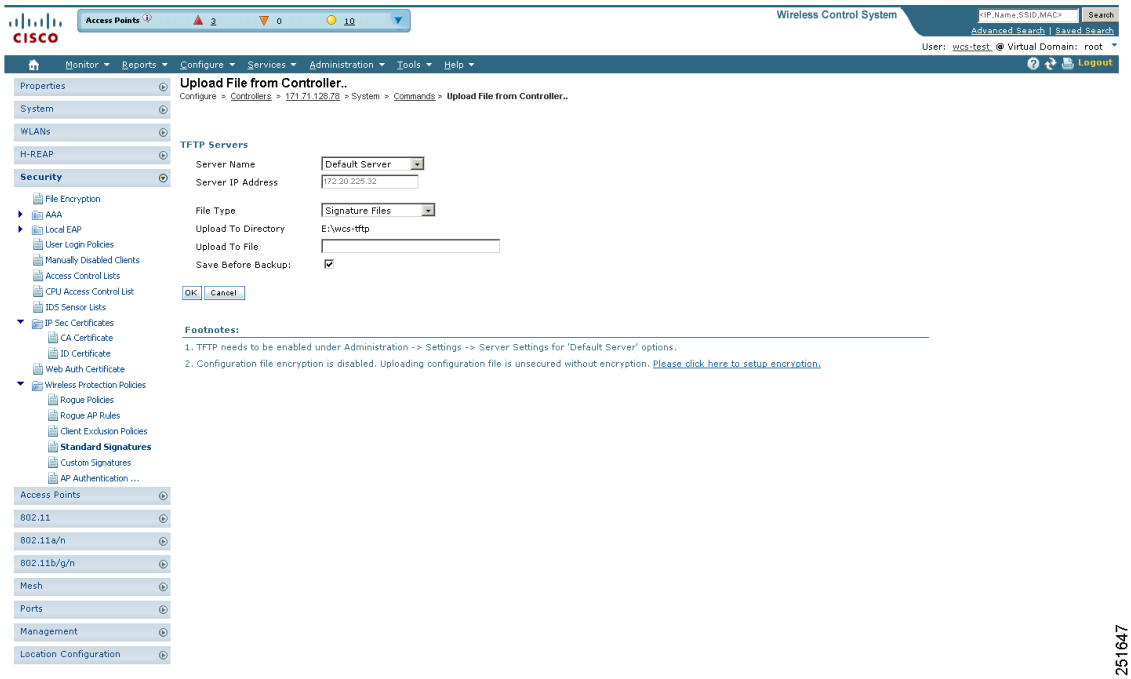
Step 3 Choose **Configure > Controllers**.

Step 4 Choose a controller by clicking on an IP address.

Step 5 From the left sidebar menu, choose **Security** and then **Standard Signatures** or **Custom Signatures**.

Step 6 From the Select a command drop-down list, choose **Upload Signature Files from Controller**. Figure 3-4 shows the page that appears.

Figure 3-4 Uploading Signature File



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 parameter.

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 parameter (this parameter 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 on 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 parameter. If you know the filename and path relative to the server's root directory, 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 parameter.

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 parameter.

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 parameter, and the Server File Name will be populated for you and retried. The local machine option initiates a two-step operation. First, the local file is copied from the administrator's workstation to WCS's own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in the WCS server's TFTP directory, and the download web page now automatically populates the filename.

Step 11 Click **OK**.

Enabling or Disabling IDS Signatures

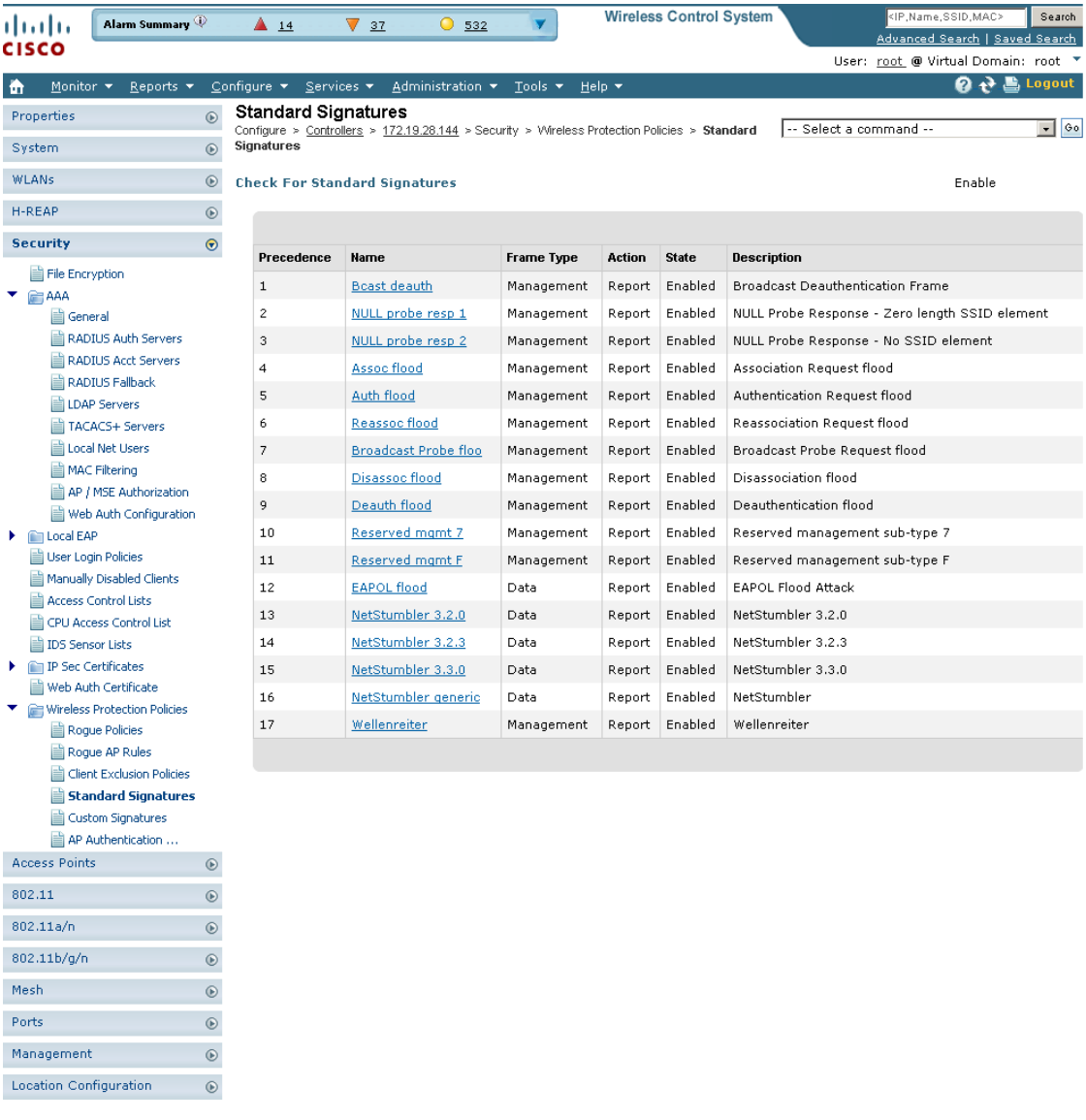
Follow these steps to enable or disable IDS signature.

Step 1 Choose **Configure > Controllers**.

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

Step 3 From the left sidebar menu, choose **Security** and then **Standard Signatures** or **Custom Signatures**. Figure 3-5 shows a sample of the screen that appears.

Figure 3-5 Checking for Standard Signatures



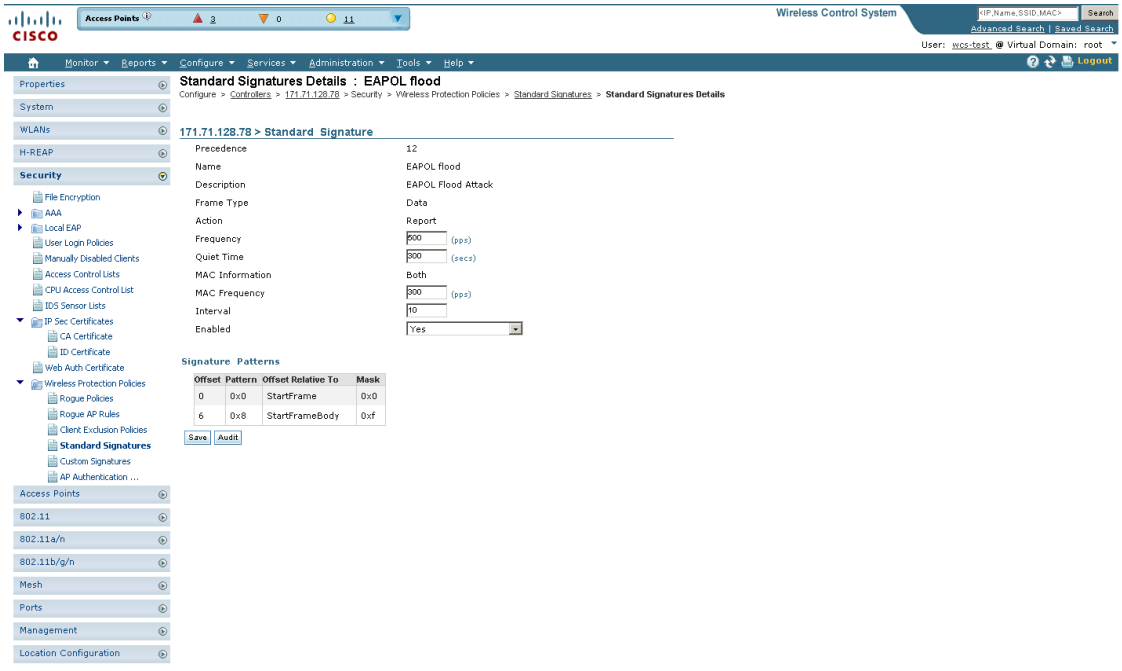
Step 4 To enable or disable an individual signature, click in the **Name** column for the type of attack you want to enable or disable. Figure 3-6 shows a sample of a detailed signature screen.

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 on 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.

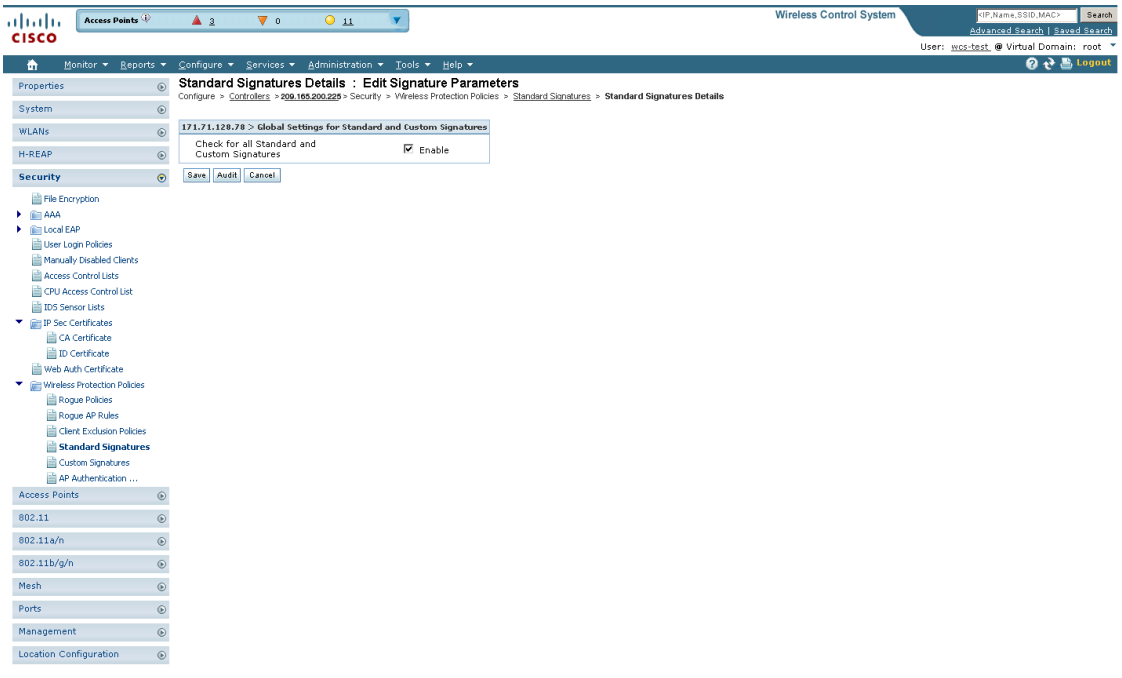
Figure 3-6 Standard Signature



Step 5 In 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 screen in Figure 3-5) from the Select a command drop-down list, and click **Go**. The Edit Signature Parameters page appears (see Figure 3-7).

Figure 3-7 Global Setting for Standard and Custom Signature



Step 7 At the Check for All Standard and Custom Signatures parameter, select the **Enable** check box. This enables all signatures that were individually selected as enabled in Step 5. If this 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 may 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 12-64 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 3-47.
- 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 parameter, 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.company.com, the user is directed to the company home page.

Step 9 Click **Save**.

Downloading Customized Web Authentication

Follow these steps if you chose the customized web authentication option in Step 4 of the previous section. 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, the following steps are required:

Step 1 Click the preview image to download the sample login.html bundle file from the server. See Figure 3-8 for an example of the login.html file. The downloaded bundle is a .TAR file.

Figure 3-8 Login.html

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 the Cisco WCS because WCS's built-in TFTP server and third-party TFTP server use the same communication port.

Step 4 Click **here** in the "After editing the HTML you may 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 parameter. If you know the filename and path relative to the server's root directory, you can also choose TFTP server.

Note For a local machine download, either .zip or .tar file options exists, but the WCS 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 parameter.

Step 7 The WCS Server Files In parameter specifies where the WCS 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 parameter, and the Server File Name is populated. The local machine option initiates a two-step operation. First, the local file is copied from the administrator's workstation to the WCS's own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in the WCS server's TFTP directory, 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 parameter, 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

Follow these steps to connect to the guest central WLAN to complete the web authentication process. See the "Creating Guest User Accounts" section on page 7-10 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 /1.1.1.1/login.html).

Step 2 When the WCS 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 WCS, refer to the following document for instructions on uploading the certificate:

http://www.cisco.com/en/US/products/ps6305/products_configuration_example09186a00808a94ca.shtml.

CHAPTER 4

Performing System Tasks

This chapter describes how to use Cisco WCS to perform system-level tasks. It contains these sections:

- Adding a Controller to the WCS Database, page 4-1
- Using WCS to Update System Software, page 4-2
- Downloading Vendor Device Certificates, page 4-3
- Downloading Vendor CA Certificates, page 4-4
- Using WCS to Enable Long Preambles for SpectraLink NetLink Phones, page 4-5
- Creating an RF Calibration Model, page 4-6

Adding a Controller to the WCS Database

Follow these steps to add a controller to the WCS database.

Note Cisco recommends 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 WCS user interface.

Step 2 Click **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 On the Add Controller page, enter the controller IP address, network mask, and required SNMP settings.

Step 5 Click **OK**. WCS displays a Please Wait dialog box while it contacts the controller and adds the current controller configuration to the WCS database. It then returns you to the Add Controller page.

Step 6 If WCS 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.

- WCS might not have been able to contact the controller. Make sure that you can ping the controller from the WCS server.
- The SNMP settings on the controller might not match the SNMP settings that you entered in WCS. Make sure that the SNMP settings configured on the controller match the settings that you entered in WCS.

Step 7 Add additional controllers if desired.

Additional Functionality with Location Appliance

Cisco 2700 series location appliances operate within the Cisco Wireless LAN Solution infrastructure. Location appliances compute, collect, and store historical location data using Cisco wireless LAN controllers and access points to track the physical location of wireless devices.

The location appliance can track up to 2,500 elements. You can track the following elements: client stations, active asset tags, rogue clients and access points. Updates on the locations of elements being tracked are provided to the location server from the Cisco wireless LAN controller.

Only those elements designated for tracking by the controller are viewable in Cisco WCS maps, queries, and reports. No events and alarms are collected for non-tracked elements, and they are not used in calculating the 2,500 element limit.

You can modify the following tracking parameters using Cisco WCS:

- Enable and disable which element locations (client stations, active asset tags, and rogue clients and access points) you actively track
- Set limits on how many of a specific element you want to track

  You can set limits on how many of a specific element you wish to track. For example, given a limit of 2,500 trackable units, you could set a limit to track only 1,500 client stations. Once the tracking limit is met, the number of elements not being tracked is summarized on the Tracking Parameters page.
- Disable tracking and reporting of ad hoc rogue clients and access points

Note Even though all clients are loaded in the map, the display has a limit of 250 clients per floor to prevent overcrowding. You can do an advanced search of the map to see the items of interest.

Selectable filters enable you to search collected data and display specific elements on a map. For example, a biomedical user may want to display only active Wi-Fi tags that are tracking key medical equipment rather than access points or clients for a given floor.

Using WCS to Update System Software

Follow these steps to update controller (and access point) software using WCS.

Step 1 Enter the **ping** ***ip-address*** command to be sure that the WCS server can contact the controller. If you use an external TFTP server, enter **ping** ***ip-address*** to be sure that the WCS 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 Click the **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**. WCS displays the Download Software to Controller page.

Step 4 If you use the built-in WCS TFTP server, select the **TFTP Server on WCS System** check box. If you use an external TFTP server, unselect this check box and add the external TFTP server IP address.

Step 5 Click **Browse** and navigate to the software update file (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**. WCS downloads the software to the controller, and the controller writes the code to flash RAM. As WCS 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 wish to use your own vendor-specific device certificate, it must be downloaded to the controller.

Follow the instructions below to download a vendor-specific device certificate to the controller.

Step 1 Choose **Configure > Controllers**.

Step 2 You can download the certificates in one of two ways:

a. Click 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 parameter. If the certificate is on the local machine, you must specify the file path in the Local File Name parameter using the Browse button.

Step 5 Enter the TFTP server name in the Server Name parameter. The default is for the WCS 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 may be used by EAP-TLS and EAP-FAST (when not using PACs) to authenticate wireless clients during local EAP authentication. However, if you wish to use your own vendor-specific CA certificate, it must be downloaded to the controller. Follow the instructions in this section to download vendor CA certificate to the controller.

Step 1 Click **Configure > Controllers**.

Step 2 You can download the certificates in one of two ways:

a. Click 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 parameter in Step 9. If the certificate is on the local machine, you must specify the file path in the Local File Name parameter in Step 8 using the Browse button.

Step 4 Enter the TFTP server name in the Server Name parameter. The default is for the WCS 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 WCS 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, follow these steps to use WCS to enable long preambles.

Step 1 Log into the WCS user interface.

Step 2 Click **Configure > Controllers** to navigate to the All Controllers page.

Step 3 Click the IP address of the desired controller.

Step 4 In the sidebar, click **802.11b/g/n > Parameters**.

Step 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.

Step 6 Enable long preambles by unchecking the **Short Preamble** check box.

Step 7 Click **Save** to update the controller configuration.

Step 8 To save the controller configuration, click **System > Commands** in the sidebar, **Save Config To Flash** from the Administrative Commands drop-down list, and **Go**.

Step 9 To reboot the controller, click **Reboot** from the Administrative Commands drop-down list and **Go**.

Step 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 may take some time, during which WCS loses its connection to the controller.

Note You can view the controller reboot process with a CLI session.

Creating an RF Calibration Model

If you would like to further refine WCS 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. See Chapter 5 for calibration instructions.

CHAPTER 5

Adding and Using Maps

This chapter describes how to add maps to the Cisco WCS database and use them to monitor your wireless LAN. With the Cisco WCS database, you can add maps and view your managed system on realistic campus, building, and floor maps.

Additionally, you can enable location presences 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 to 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.

Note A mobility server should be synchronized before Location Presence is enabled. For details on enabling location presence and assigning its parameters, 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.

This configuration guide also covers verifying location accuracy, using chokepoints, using Wi-FI TDOA receivers, applying calibration models and other context-aware planning and verification topics.

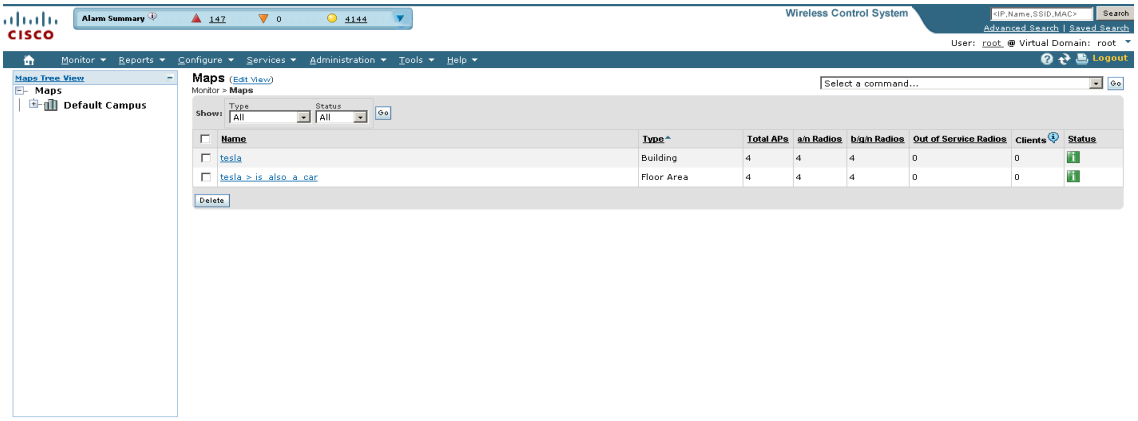
This chapter contains the following sections:

- Monitoring Maps Overview, page 5-2
- Searching Maps, page 5-21
- Adding and Enhancing Floor Plans, page 5-22
- Planning Mode, page 5-36
- Adding Access Points, page 5-44
- Placing Access Points, page 5-49
- Refresh Options, page 5-72
- Creating a Network Design, page 5-73
- Importing or Exporting WLSE Map Data, page 5-79

Monitoring Maps Overview

Note To view or edit current maps, choose **Monitor > Maps** (see Figure 5-1) and select the appropriate map from the list. Use the Select a command drop-down list to access additional functionality.

Figure 5-1 Monitor > Maps Page



251650

The Monitor > Maps page provides a summary of all campuses, buildings, outdoor areas, and floors. The available information includes:

- Total APs—Number of total access points for each map.
- 802.11a/n Radios and 802.11b/g/n Radios—Number of 802.11a/n and 802.11b/g/n radios associated with each map.
- Out of Service (OOS) Radios—Number of 802.11a/n and 802.11b/g/n radios associated with each map.
- Clients—Number of clients associated to access points on the map.

  Note This number is based on the most recent Client Statistics Poll. The number of clients located on the map by MSE may not match this number.

- 802.11a/n and 802.11b/g/n Avg Air Quality—Indicates the average Air Quality (AQ) for 802.11a/n and 802.11b.g.n radios.
- 802.11a/n and 802.11b/g/n Min Air Quality—Indicates the minimum Air Quality (AQ) for 802.11a/n and 802.11b/g/n radios.
- Status—Indicates the current status of the map.
  - Red triangle—Critical fault
  - Yellow triangle—Minor fault
  - Green square—Ok

The left sidebar lists all campuses, buildings, and floors in a tree view. When you click a campus, building, or floor in the Maps Tree View menu, the main area of the page displays corresponding information.

Note Click **Edit View** to change the information displayed for the listed maps. See "Configuring Edit View" section on page 5-3 for more information.

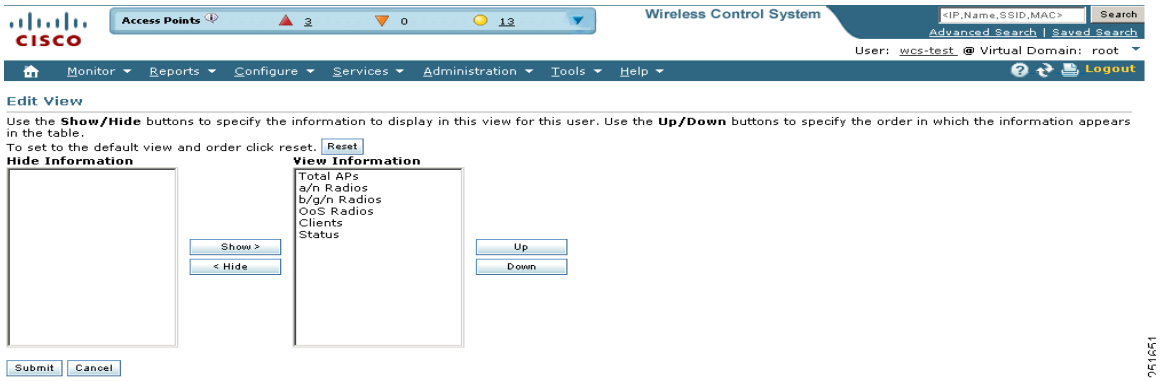
Use the Select a command drop-down list for additional map functionality. See "Select a Command for Maps" section on page 5-4 for more information.

To search for a specific map, use the WCS search feature.

Configuring Edit View

The Edit View page enables you to choose which columns appear in the maps list page (see Figure 5-2).

Figure 5-2 Edit View Page



Column names appear in one of the following lists:

- Hide Information—Lists columns that do not appear in the table. The Hide button points to this list.
- View Information—Lists columns that do not appear in the table. The Show button points to this list.

To display a column in a table, click it in the Hide Information list, then click **Show**. To remove a column from a table, click it in the View Information list, then click **Hide**. You can select more than one column by holding down the Shift or Control key.

To change the position of a column in the View Information list, click it, then click **Up** or **Down**. The higher a column is in the list, the farther left it appears in the table.

Edit View Command Buttons

The following command buttons appear in the Edit View page:

- Reset—Set the table to the default display.
- Show—Move the highlighted columns from the Hide Information list to the View Information list.
- Hide—Move the highlighted columns from the View Information list to the Hide Information list.
- Up—Move the highlighted columns upward in the list (further to the left in the table).

- Down—Move the highlighted columns downward in the list (further to the right in the table).
- Submit—Save the changes to the table columns and return to the previous page.
- Cancel—Undo the changes to the table columns and return to the previous page.

Select a Command for Maps

The Select a Command drop-down list provides access to the following map functionality:

- Adding a Campus Map, page 5-4
- Adding Buildings, page 5-5
- Deleting a Map, page 5-12
- Moving Buildings, page 5-12
- Copying a Map, page 5-13
- Editing Map Properties, page 5-13
- Searching Maps, page 5-21

Adding a Campus Map

Follow these steps to add a single campus map to the Cisco WCS database.

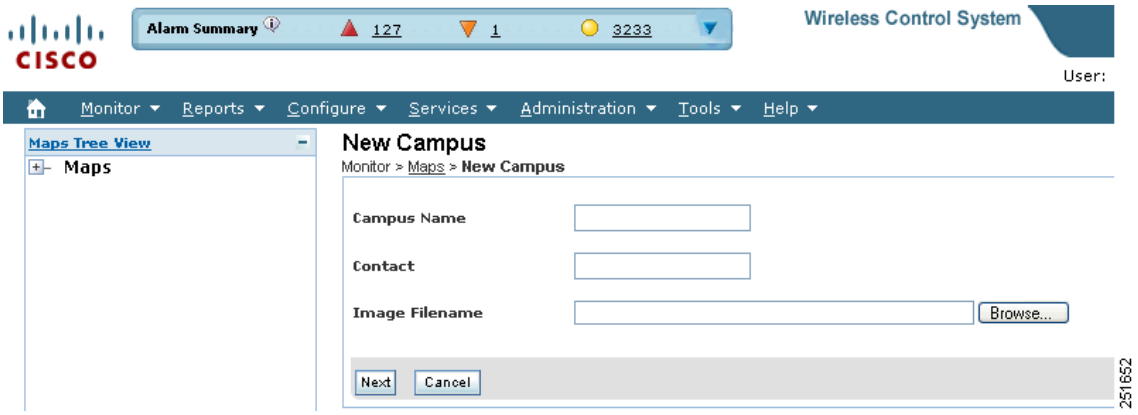
Step 1 Save the map in .PNG, .JPG, .JPEG, or .GIF format.

Note The map can be any size because WCS automatically resizes the map to fit its working areas.

Step 2 Browse to and import the map from anywhere in your file system.

Step 3 Choose **Monitor** > **Maps** to display the Maps page (see Figure 5-3).

Figure 5-3 New Campus Page



Step 4 From the Select a command drop-down list, choose **New Campus**, and click **Go**.

Step 5 On the Maps > New Campus page, enter the campus name and campus contact name.

Step 6 Browse to and choose the image filename containing the map of the campus and click **Open**.

Step 7 Select the **Maintain Aspect Ratio** check box to prevent length and width distortion when WCS resizes the map.

Step 8 Enter the horizontal and vertical span of the map in feet.

Note To change the unit of measurement (feet or meters), select Monitor > Maps and select **Properties** from the Select a command drop-down list.

Note The horizontal and vertical span should be larger than any building or floor plan to be added to the campus.

Step 9 Click **OK** to add this campus map to the Cisco WCS database. WCS displays the Maps page, which lists maps in the database, map types, and campus status.

Step 10 (Optional) To assign location presence information, click the newly created campus link in the Monitor > Maps page. See the "Managing Location Presence Information" section on page 5-16 for more information.

Adding Buildings

You can add buildings to the Cisco WCS database regardless of whether you have added campus maps to the database. This section explains how to add a building to a campus map or a standalone building (one that is not part of a campus) to the Cisco WCS database.

Adding a Building to a Campus Map

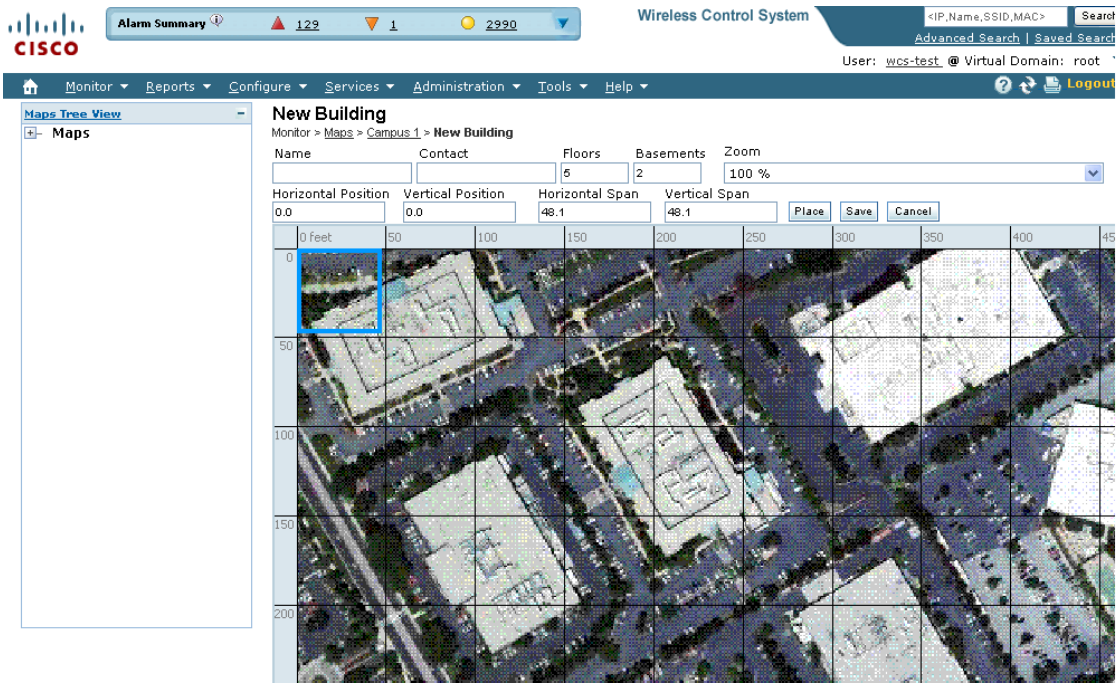
Follow these steps to add a building to a campus map in the Cisco WCS database.

Step 1 Choose **Monitor > Maps** to display the Maps page.

Step 2 Click the desired campus. WCS displays the Maps > *Campus Name* page.

Step 3 From the Select a command drop-down list, choose **New Building**, and click **Go** (see Figure 5-4).

Figure 5-4 Campus > New Building Page



Step 4 On 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), select *Monitor* > *Maps* and select **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 To change the unit of measurement (feet or meters), select *Monitor* > *Maps* and select **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.

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. WCS 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. WCS saves the building name in the building rectangle on the campus map.

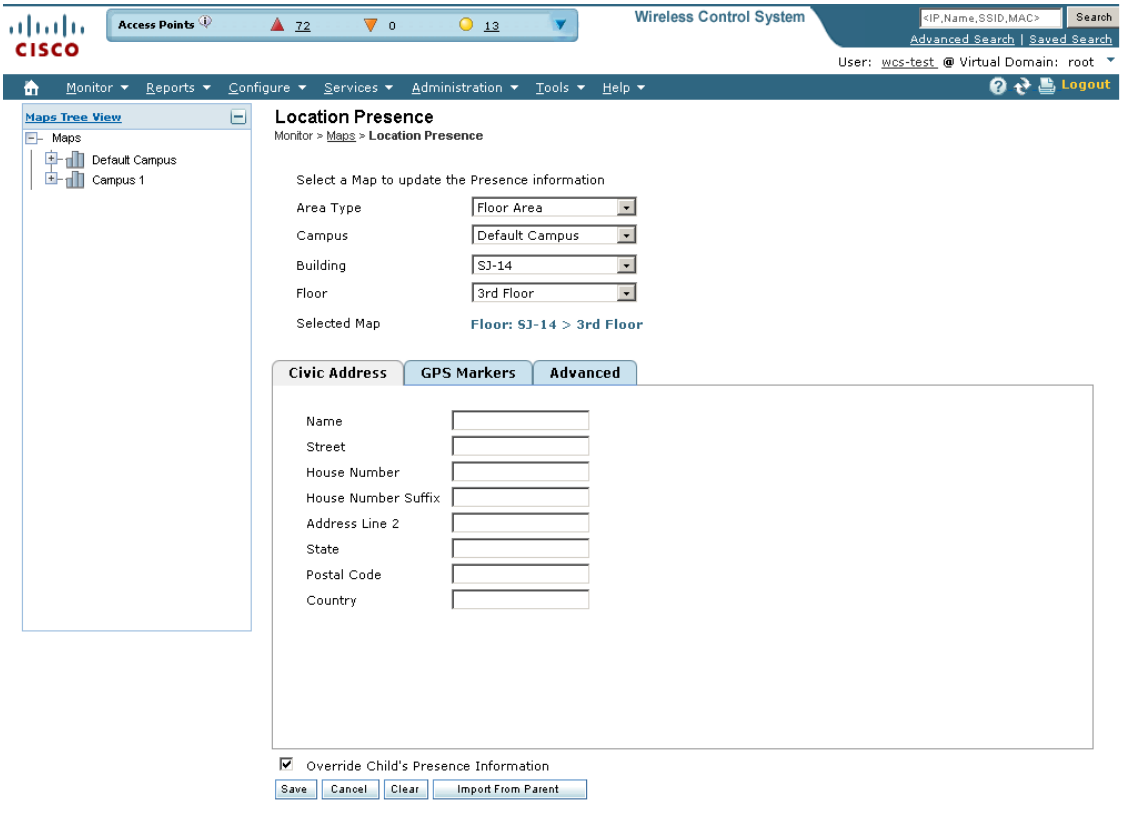
Note A hyperlink associated with the building takes you to the corresponding Map page.

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 (see Figure 5-5).

Note By default, the Override Child Element's Presence Info check box 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 deselected. This option should be deselected if you want to assign building-specific addresses to buildings on its campus rather than one campus address to all.

Figure 5-5 Location Presence Page



b. Choose either the **Civic**, **GPS markers**, or **Advanced** tab.

- Civic Address identifies the campus by name, street, house number, house number suffix, city (address line2), state, postal code, and country.
- GPS Markers identify the campus by longitude and latitude.
- Advanced identifies the campus with expanded civic information such as neighborhood, city division, country, and postal community name.

Note Each selected parameter is inclusive of all of those above it. For example, if you choose Advanced, it can also provide GPS and Civic location information upon client demand. The selected setting must match what is set on the location server level (Services > Mobility Services).

Note If a client requests location information such as GPS Markers for a campus, building, floor, or outdoor area that is not configured for that parameter, an error message is returned.

c. By default, the Override Child Element's Presence Info check box is selected. There is no need to alter this setting for standalone buildings.

Step 6 Click **Save**.

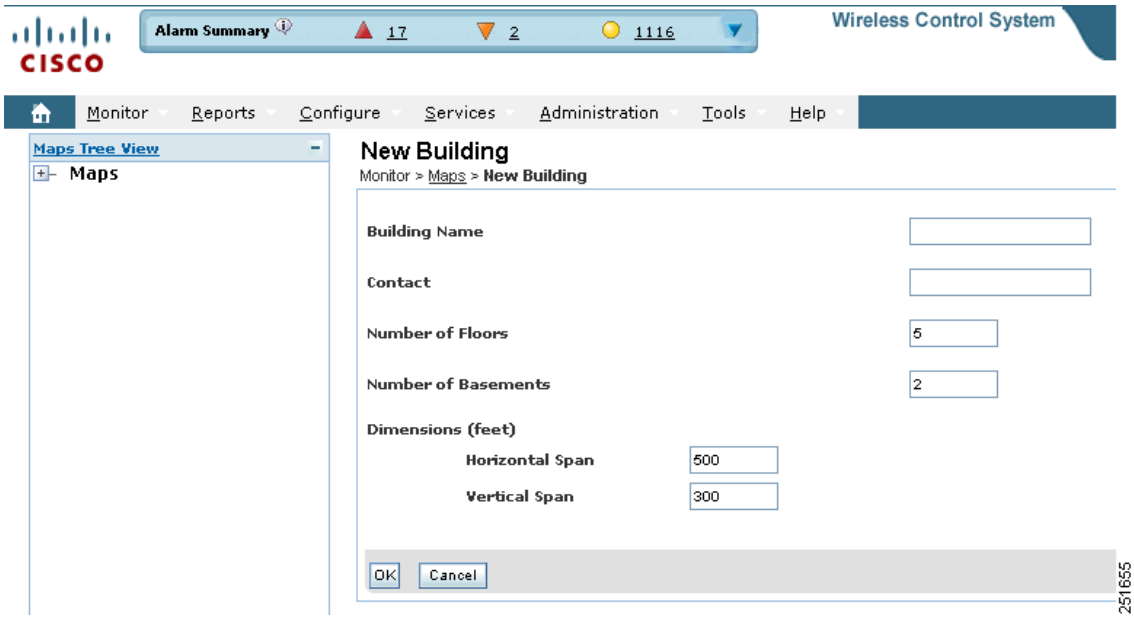
Adding a Standalone Building

Follow these steps to add a standalone building to the Cisco WCS database:

Step 1 Choose **Monitor > Maps** to display the Maps page.

Step 2 From the Select a command drop-down list, choose **New Building**, and click **Go** (see Figure 5-6).

Figure 5-6 New Standalone Building Page



Step 3 On 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), select *Monitor* > *Maps* and select **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 (see Figure 5-5).

b. Choose either the Civic, GPS markers, or Advanced tab.

- Civic Address identifies the campus by name, street, house number, house number suffix, city (address line2), state, postal code, and country.
- GPS Markers identify the campus by longitude and latitude.
- Advanced identifies the campus with expanded civic information such as neighborhood, city division, county, and postal community name.

Note Each selected parameter is inclusive of all of those above it. For example, if you select Advanced, it can also provide GPS and Civic location information upon client demand. The selected setting must match what is set on the location server level (Services > Mobility Services).

Note If a client requests location information such as GPS Markers for a campus, building, floor, or outdoor area that is not configured for that parameter, an error message is returned.

c. By default, the Override Child Element's Presence Info check box 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 location information. The campus address cannot be imported to a building if the check box is deselected. This option should be deselected if you want to assign building-specific addresses to buildings on its campus rather than one campus address to all.

Step 5 Click **Save**.

Note The standalone buildings are automatically placed in a System Campus.

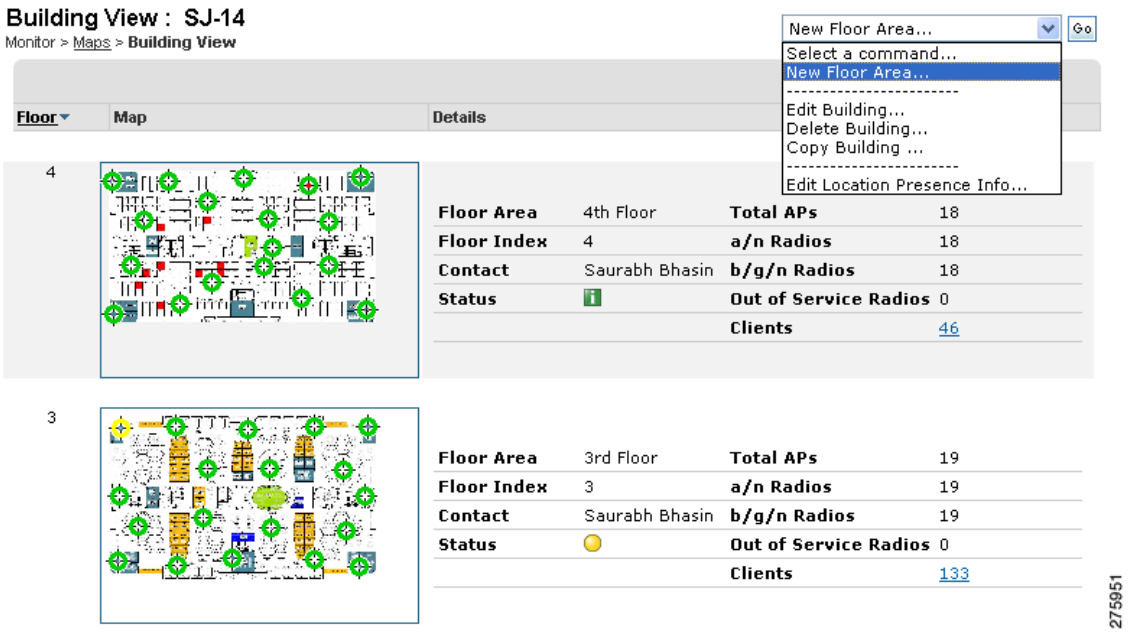
Managing a Current Campus

To view a current campus map, follow these steps:

Step 1 Choose **Monitor > Maps**.

Step 2 Click the name of the campus map to open its details page (see Figure 5-7).

Figure 5-7 Building View Page



Step 3 The Select a command drop-down list provides the following options:

- New Floor Area—See Adding and Enhancing Floor Plans for more information.
- Edit Building—See Editing a Current Campus for more information.
- Delete Building— See Deleting a Map for more information.
- Copy Building—See Copying a Map for more information.
- Edit Location Presence Information—See Managing Location Presence Information for more information.

Note Use the Monitor > Maps > Campus View main navigation bar 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).

Editing a Current Campus

To edit a current campus map, follow these steps:

Step 1 Choose **Monitor > Maps**.

Step 2 Click the name of the campus map to open its details page.

Step 3 From the Select a command drop-down list, choose **Edit Campus**.

Step 4 Make any necessary changes to the Campus Name, Contact, Number of Floors, Number of Basements, and Dimensions (feet).

Note To change the unit of measurement (feet or meters), select *Monitor* > *Maps* and select **Properties** from the Select a command drop-down list.

Step 5 Click **Next**.

Step 6 Make any additional changes to Maintain Aspect Ratio or Dimensions (feet).

Step 7 Click **OK**.

Note System Campus is part of all partitions. Also, you can not edit or delete a system campus.

Moving Buildings

To move a building to a different campus, follow these steps:

Step 1 Choose **Monitor > Maps**.

Step 2 Select the check box of the applicable building.

Step 3 From the Select a command drop-down list, click **Move Buildings**.

Step 4 Click **Go**.

Step 5 Select the Target Campus from the drop-down list.

Step 6 Select the buildings that you want to move. Unselect any buildings that will remain in their current location.

Step 7 Click **OK**.

Deleting a Map

Follow these steps to delete a map.

Step 1 In the Monitor > Maps page, select the check box(es) for the map(s) that you want to delete.

Step 2 Click **Delete** at the bottom of the map list or choose **Delete Maps** from the Select a Command drop-down list, and click **Go**.

Step 3 Click **OK** to confirm the deletion.

Note Deleting a campus or building also deletes all of its container maps. The access points from all deleted maps are moved to an Unassigned state. System Campus can not be deleted, however, buildings or floors in a System Campus can be modified.

Editing Map Properties

To edit your map properties, follow these steps:

Step 1 Choose **Monitor > Maps**.

Step 2 From the Select a command drop-down list, click **Properties**.

Step 3 Click **Go**.

Step 4 Edit the information in Table 5-1.

Table 5-1 Map Properties Parameters

Parameter or Control	Description
Unit of Dimension	Set dimension measurement in feet or meters for all Cisco WCS maps.
Wall Usage Calibration	Choose to use or not use walls, or set to automatic.
Refresh Map From Network	Enable refresh of map data for Cisco WCS to update maps by polling the Cisco WLAN Solution each time an Cisco WLAN Solution operator requests a map update. Select disable for Cisco WCS to update maps from its stored database. **Note** Updates to the database may not be frequent enough to keep the map data current.
Advanced Debug Mode	This option must be enabled on both the location appliance and WCS to allow use of the location accuracy testpoint feature.

Copying a Map

The following guidelines apply to the copying process:

- Only the child elements are copied to the new map.
- The selected map is copied to the current applicable partition.
- Overlapping areas are not selected when buildings are copied. You should edit these after copying the map for proper positioning.
- If the selected map is above ground, the first available floor above ground is used for the copy.
- If the selected map is a basement, the first available basement is used for the copy.
- The following are *not* copied:
  - Access points and their positioning coordinates.
  - Planning mode data.

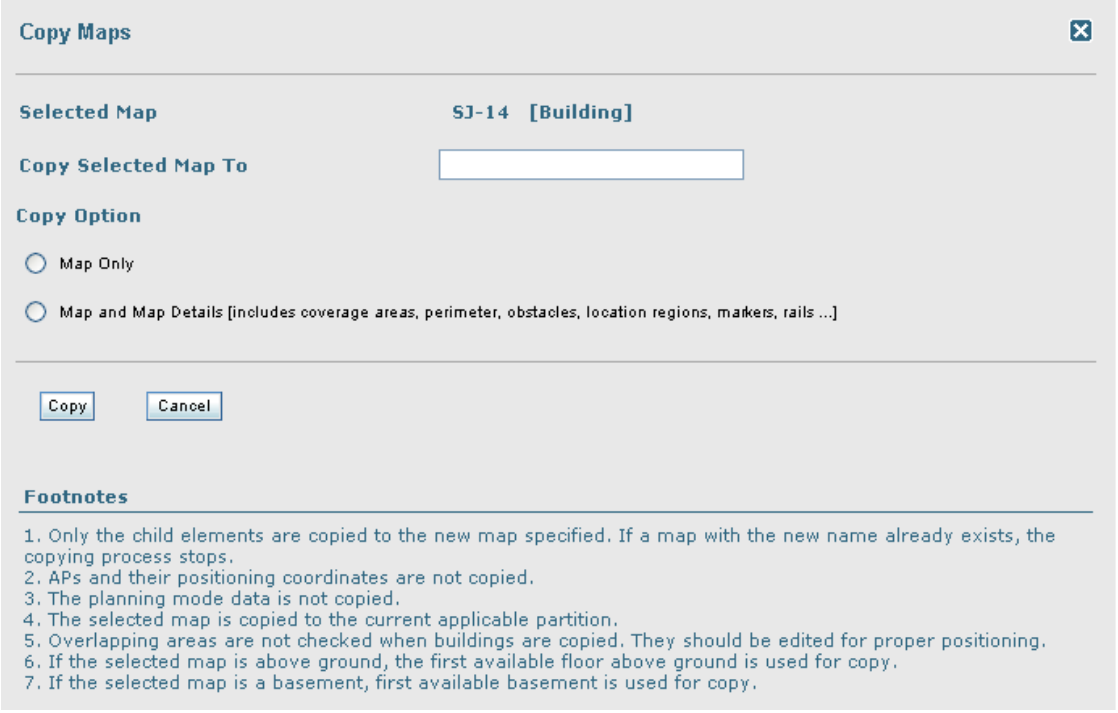
Note You can not copy a System Campus.

To copy a map, follow these steps:

Step 1 In the **Monitor** > **Maps** page, select the check box of the map that you want to copy.

Step 2 From the Select a Command drop-down list, click **Copy Maps**. The Copy Maps page opens (see Figure 5-8).

Figure 5-8 Copy Maps Page



Step 3 Enter the name of the new map to which you want to copy the current map.

Note If a map with the new name already exists, the copying process stops.

Step 4 Select the Copy Option (Map Only or Map and Map Details).

Note Map and Map Details includes coverage areas, perimeters, obstacles, location regions, markers, and rails.

Step 5 Click **Copy** to complete the copying process or **Cancel** to close the page without copying the current map.

Exporting a Map

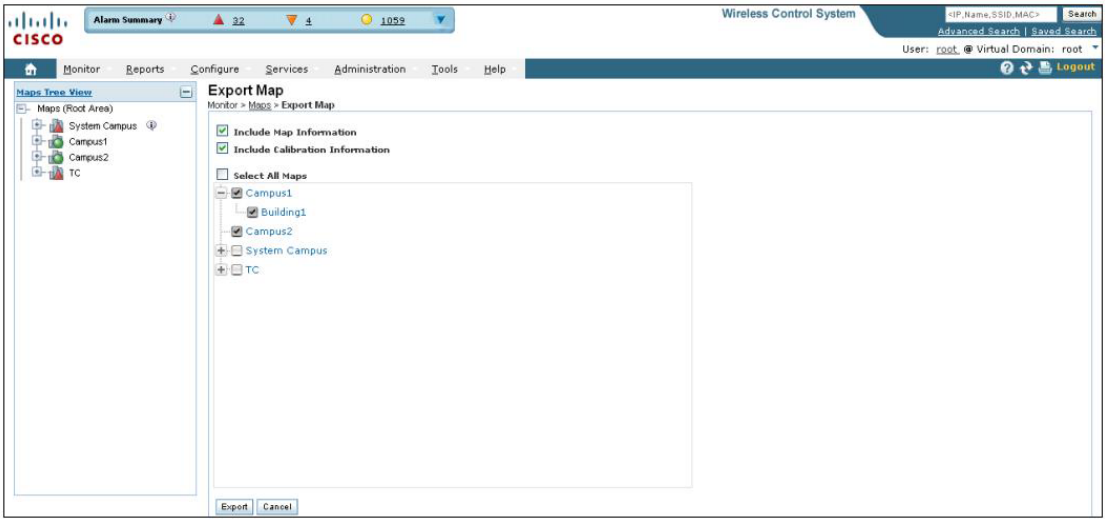
The Export Map feature allows you to export map or calibration information to XML. The exported XML will be in an encrypted format and will not be readable. XML and images are bundled, tarred, and zipped into a file for a successful import into another WCS.

To export a map, follow these steps:

Step 1 Choose **Monitor > Maps**.

Step 2 From the Select a command drop-down list, click **Export Maps**. The Export Map page appears (see Figure 5-9).

Figure 5-9 Export Map Page



Step 3 Select the maps that you want to export.

Step 4 Click **Export** to export the selected map data.

Note An admin user does not have partition privileges and hence can not export maps. This functionality is only available to the root user.

Importing a Map

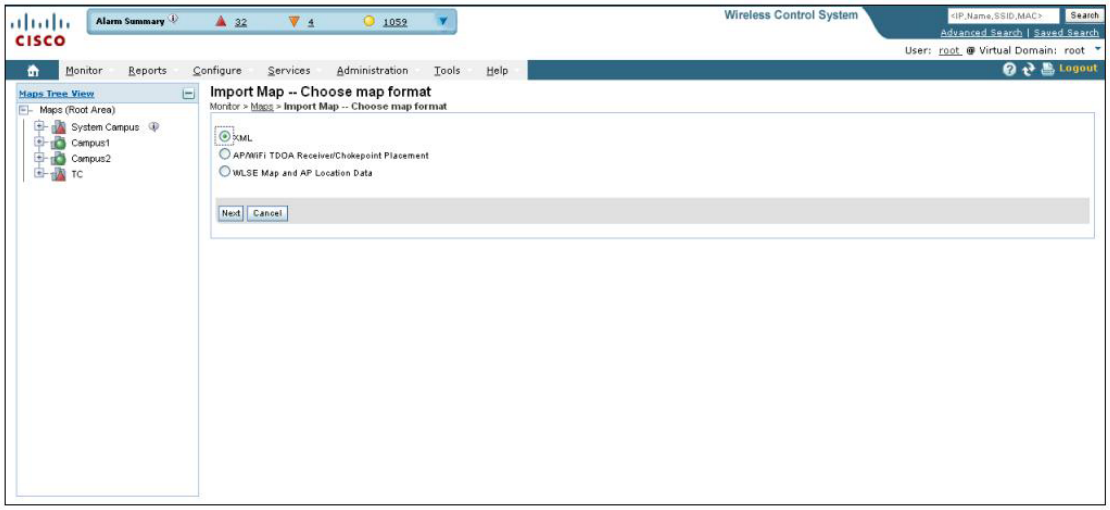
The Import Map feature allows you to import map information from external sources such as XML, WLSE, and CSV. During import, the XML may be encrypted (if exported from WCS) or unencrypted.

To import a map, follow these steps:

Step 1 Choose **Monitor > Maps**.

Step 2 From the Select a command drop-down list, click **Import Maps**. The Import Map page appears (see Figure 5-10).

Figure 5-10 Import Map Page



Step 3 Choose the map format.

Step 4 Select one of the following formats:

- XML
- AP/WiFi TDOA Receiver/Chokepoint Placement
- WLSE Map and AP Location Data

Step 5 Click **Next**.

Step 6 Click **Browse** to select the file that you want to import.

Step 7 Click **Import** to import the selected data.

Managing Location Presence Information

You can enable location presence by 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 Enabling Location Presence for Mobility Services for more information on enabling location presence.

To view or edit current location presence information for a current map, follow these steps:

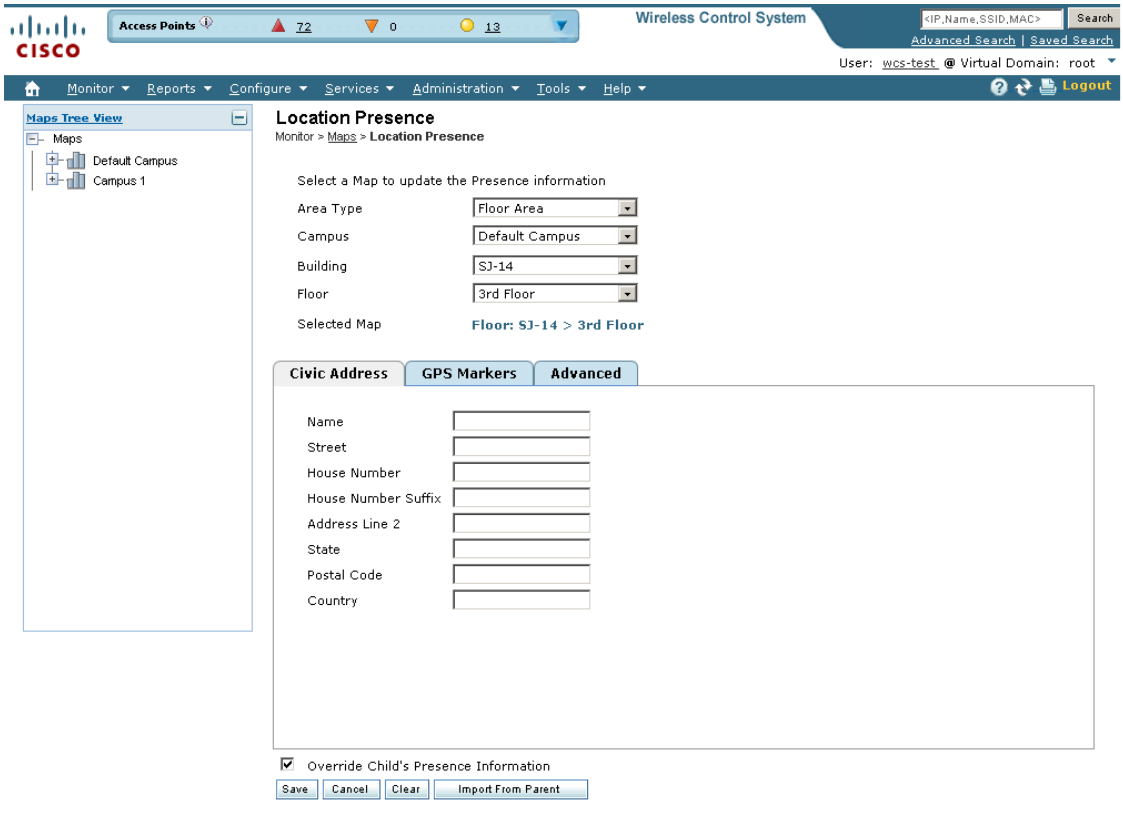
Step 1 In the Monitor > Maps page, select the check box of the map.

Step 2 From the Select a command drop-down list, choose **Location Presence**.

Step 3 Click **Go**. The Location Presence page appears (see Figure 5-11).

Note The current map location information (Area Type, Campus, Building, and Floor) refer to the map you selected from the Monitor > Maps page. To select a different map, use the Select a Map to Update Presence Information drop-down lists to select the new map location.

Figure 5-11 Location Presence Page



Step 4 Choose either the Civic, GPS markers, or Advanced tab.

- Civic Address—Identifies the campus, building, or floor by name, street, house number, house number suffix, city (address line2), state, postal code, and country.
- GPS Markers—Identify the campus, building, or floor by longitude and latitude.
- Advanced—Identifies the campus, building, or floor with expanded civic information such as neighborhood, city division, county, and postal community name.

Note Each selected parameter is inclusive of all of those above it. For example, if you select Advanced, it can also provide GPS and Civic location information upon client demand. The selected setting must match what is set on the mobility services engine level. See the "Enabling Location Presence for Mobility Services" section on page 5-18 for more information.

Note If a client requests location information such as GPS markers for a campus, building, floor, or outdoor area that is not configured for that parameter, an error message appears.

Note By default, the Override Child Element's Presence Info check box is selected.

Enabling Location Presence for Mobility Services

You can enable location presence by 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.

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 location to any requesting Cisco CX v5 client.

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 Click **Services > Mobility Services**.

Step 2 Select the mobility services engine to which the campus or building is assigned.

Step 3 From the Context-Aware Software menu (left sidebar), select **Presence Parameters** from the Administration sub-heading. The Presence page opens.

Step 4 Select the Service Type **On Demand** check box to enable location presence for Cisco CX clients v5.

Step 5 Choose 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 displays.
  - 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 6 Check 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.
- **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 To import a file with multiple Civic listings, refer to Importing Civic Information for Mobility Services.

c. Select the **GEO** check box to provide the longitude and latitude coordinates.

Step 7 By default, the Text check box for Location Response Encoding is selected. It indicates the format of the information when received by the client. There is no need to change this setting.

Step 8 Select the Retransmission Rule **Enable** check box to allow the receiving client to retransmit the received information to another party.

Step 9 Enter a Retention Expiration value in minutes. This determines how long the received information is stored by the client before it is overwritten. Default value is 24 hours (1440 minutes).

Step 10 Click **Save**.

Adding Outdoor Areas

Follow these steps to add an outdoor area to a campus map.

Note You can add outdoor areas to a campus map in the Cisco WCS database regardless of whether you have added outdoor area maps to the database.

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.

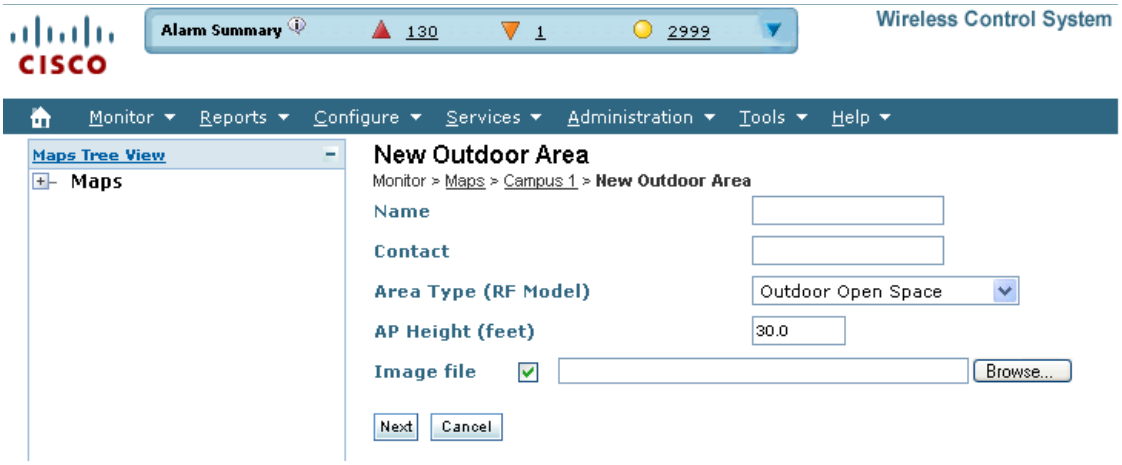
Note You do not need a map to add an outdoor area. You can simply define the dimensions of the area to add it to the database. The map can be any size because WCS automatically resizes the map to fit the workspace.

Step 2 Choose **Monitor > Maps** to display the Maps page.

Step 3 Click the desired campus. WCS displays the Maps > *Campus Name* page.

Step 4 From the Select a command drop-down list, choose **New Outdoor Area**, and click **Go** (see Figure 5-12).

Figure 5-12 Create New Area Page



Step 5 On the *Campus Name* > New Outdoor Area page, follow these steps to create a manageable outdoor area:

a. Name—Enter the outdoor area name.

b. Contact—Enter the outdoor area contact name.

c. Area Type (RF Model)—Cubes and Walled Offices, Drywall Office Only, Outdoor Open Space (default).

d. AP Height (feet)—Enter the height of the access point.

e. Image File—Name of the file containing the outdoor area map. Use the browse button to find the file.

Step 6 Click **Next**.

Step 7 Enter the following information:

- Name—The user-defined name of the outdoor area.
- Contact—The user-defined contact name.
- Zoom—Use to zoom in or zoom out on the map that you are currently viewing.
- Maintain Image Aspect Ratio—Select this check box to maintain the aspect ratio (ratio of horizontal and vertical pixels) of the map image. Maintaining the aspect ratio prevents visual distortion of the map.
- Horizontal Position—Distance from the corner of the outdoor area rectangle to the left edge of the campus map, in feet or meters.
- Vertical Position—Distance from the corner of the outdoor area rectangle to the top edge of the campus map, in feet or meters.
- Horizontal Span—Horizontal measurement (left to right) of the outdoor area rectangle, in feet or meters.
- Vertical Span—Vertical measurement (up and down) of the outdoor area rectangle, in feet or meters.

Tip The horizontal and vertical spans should be larger than or the same size as any floors that may be added later. Use **Ctrl-click** to resize the bounding area in the upper-left corner of the campus map. The horizontal and vertical span parameters change to match.

Note To change the unit of measurement (feet or meters), select *Monitor* > *Maps* and select **Properties** from the Select a command drop-down list.

Step 8 Click **Place** to put the outdoor area on the campus map. WCS 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 Map page.

Step 11 (Optional) To assign location presence information for the new outdoor area, select Edit Location Presence Info, and click Go. See Managing Location Presence Information for more information.

Note By default, the Override Child Element's Presence Info check box is selected. There is no need to alter this setting for outdoor areas.

Deleting Outdoor Areas

To delete a current outdoor area, follow these steps:

Step 1 In the Monitor > Maps page, select the check box for the outdoor area that you want to delete.

Step 2 Click **Delete** at the bottom of the map list (or choose **Delete Maps** from the Select a Command drop-down list, and click **Go**.

Step 3 Click **OK** to confirm the deletion.

Searching Maps

Use the controls in the left sidebar to create and save custom searches:

- New Search drop-down list: Opens the Search Maps page. Use the Search Maps page to configure, run, and save searches.
- Saved Searches drop-down list: Lists the saved custom searches. To open a saved search, choose it from the Saved Searches list.
- Edit Link: Opens the Edit Saved Searches page. You can delete saved searches in the Edit Saved Searches page.
- Audit Status: Allows you to search based on audit status of not available (audit status is not available), identical (no configuration differences were found during the last audit), or mismatch (configuration differences were found during the last audit).

You can configure 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:

Table 5-2 Map Search Results

Parameter	Options
Name	Clicking an item in the Name list gives a map of an existing building with individual floor area maps for each floor.
Type	Campus, building, or floor area.
WCS	WCS name.
Total APs	Displays the total number of Cisco radios detected.
a/n Radios	Displays the number of 802.11a/n Cisco radios.
b/g/n Radios	Displays the number of 802.11b/g/n Cisco radios.
OOS Radios	Displays the number of Out of Service access points associated with this controller.

Adding and Enhancing Floor Plans

This section explains how to add floor plans to either a campus building or a standalone building in the Cisco WCS database. It also provides instructions on using the WCS map editor to enhance floor plans that you have created and the WCS planning mode to calculate the number of access points required to cover an area.

Adding Floor Plans 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. Follow these steps to add floor plans to a campus building.

Step 1 Save your floor plan maps in .PNG, .JPG, or .GIF format.

Note The maps can be any size because WCS automatically resizes the maps to fit the workspace.

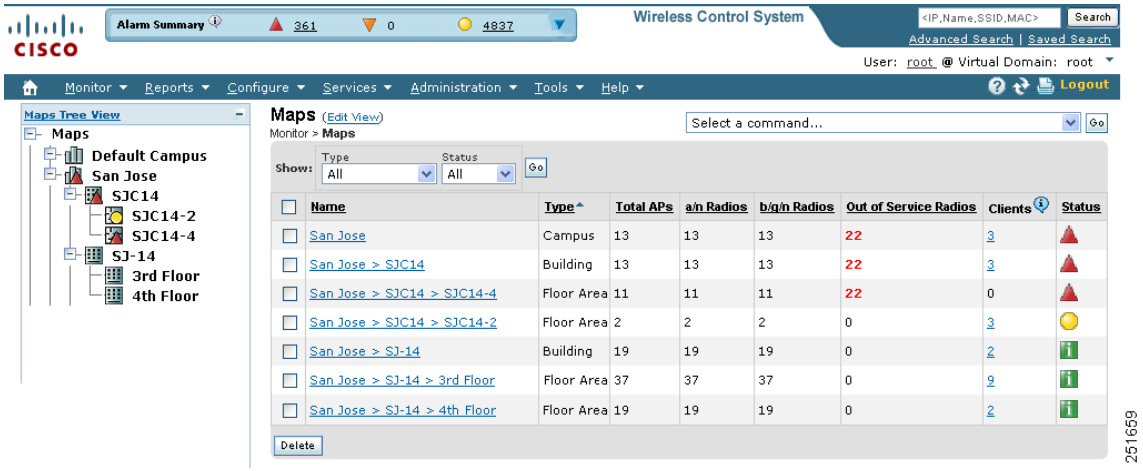
Step 2 Browse to and import the floor plan maps from anywhere in your file system. You can also import CAD image files DXF and DWG.

Note If there are problems converting the auto-cad file, an error message is displayed. WCS uses a native image conversion library to convert auto-cad files into raster formats like PNG. If the native library cannot be loaded, WCS returns the "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 Dependency Walker on Windows platforms or ldd on Linux platforms. The following dlls must be present under the /webnms/rfdlls WCS installation directory: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problems occurred, you may need to install the required libraries and restart WCS.

Note 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.

Step 3 Choose **Monitor > Maps** to display the Maps page (see Figure 5-13).

Figure 5-13 Monitor > Maps Page



Step 4 From the Maps Tree View or the Monitor > Maps list, click the desired campus. WCS displays the Maps > *Campus Name* page.

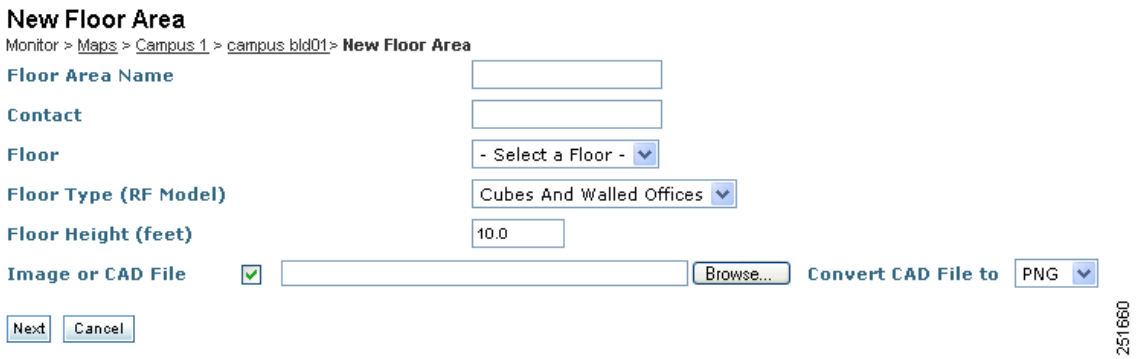
Step 5 Hover your cursor over the name within an existing building rectangle to highlight it.

Note When you highlight the name within a building rectangle, the building description appears in the sidebar.

Note You can also access the building from the Campus View page. In the Campus View page, click the building name to open the Building View page.

Step 6 From the Select a command drop-down list, choose **New Floor Area**, and click **Go** (see Figure 5-14).

Figure 5-14 New Floor Area Page



Step 7 On the *Building Name* > 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 or basement name.

b. Enter the floor or basement contact name.

c. Choose the floor or basement number.

d. Choose the floor or basement type (RF Model).

e. Enter the floor-to-floor height in feet.

Note To change the unit of measurement (feet or meters), select *Monitor* > *Maps* and select **Properties** from the Select a command drop-down list.

f. Select the **Image** or **CAD File** check box; then 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 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.

g. Click **Next**. At this point, if a CAD file was specified, a default image preview is generated and loaded.

Note WCS uses a native image conversion library to convert auto-cad files into raster formats like .PNG. When there are issues loading the native library, WCS throws the following error: "Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library.

If this error displays, make sure all the required dependencies are met for the native library.

On Windows platform, you can use tools such as "Dependency Walker" to find out dependency issues.

Make sure that the following dlls are present under \webnms\rfdlls directory under your WCS installation directory:

\webnms\rfdlls\LIBGFL254.DLL
\webnms\rfdlls\MFC71.DLL
\webnms\rfdlls\MSVCR71.DLL
\webnms\rfdlls\MSVCP71.DLL

On Linux platform, you can use tools such as "ldd" to find out any dependency issues.

If there are any dependency issues, fix them by installing the required libraries for missing dependencies and then restart WCS.

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, WCS displays the image in the building-sized grid.

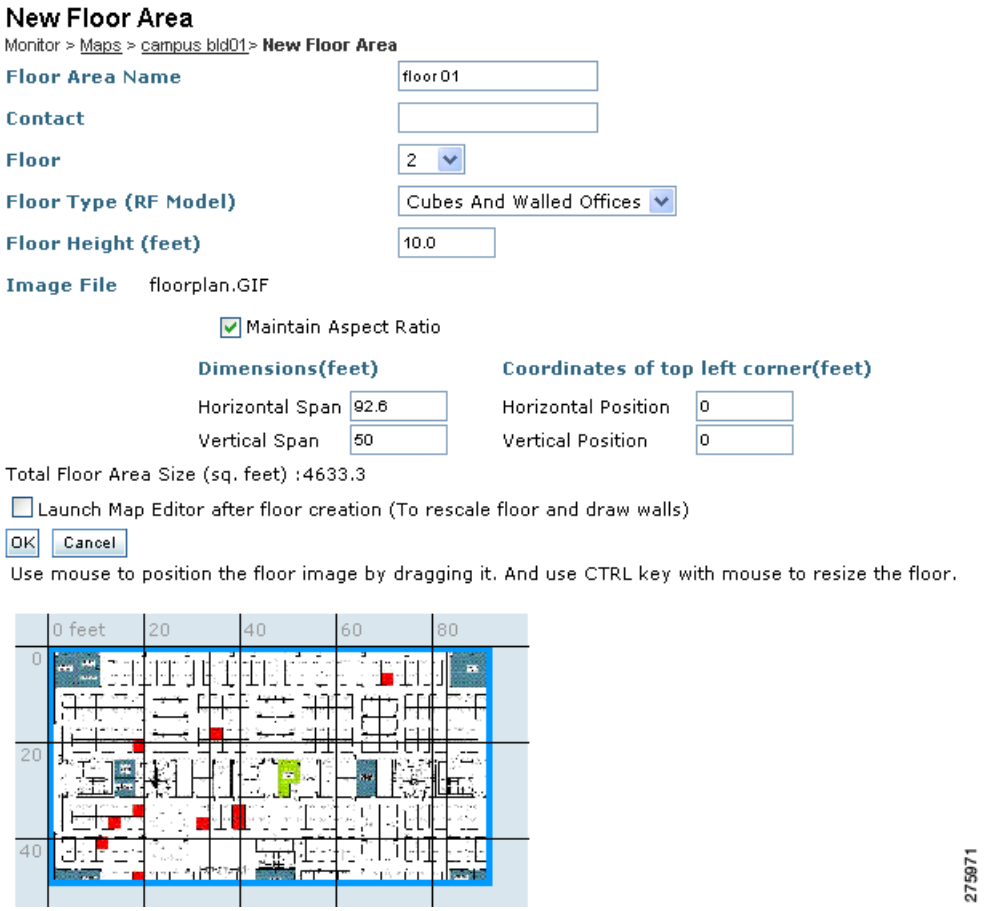
Note The maps can be any size because WCS automatically resizes the maps to fit the workspace.

Note The maps 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.

i. Enter the remaining parameters for the floor area (see Figure 5-15).

Figure 5-15 Floor Area Parameters



j. 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.

k. Enter an approximate floor or basement horizontal span and vertical span (width and depth on the map) in feet.

Note To change the unit of measurement (feet or meters), select *Monitor* > *Maps* and select **Properties** from the Select a command drop-down list.

Note The horizontal and vertical span should be smaller than or the same size as the building horizontal span and vertical span in the Cisco WCS database.

l. If desired, click **Place** to locate the floor or basement image on the building grid.

Tip You can use Ctrl-click to resize the image within the building-sized grid.

m. Click **OK** to save this floor plan to the database. WCS displays the floor plan image on the Maps > *Campus Name* > *Building Name* page.

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 and out to view the map at different sizes, and you can add access points. See the "Inspecting VoWLAN Location Readiness" section on page 5-43 for instructions.

Adding Floor Plans to a Standalone Building

After you have added a standalone building to the Cisco WCS database, you can add individual floor plan maps to the building. Follow these steps to add floor plans to a standalone building.

Step 1 Save your floor plan maps in .PNG, .JPG, or .GIF format.

Note The maps can be any size because WCS 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.

Note If there are problems converting the auto-cad file, an error message is displayed. WCS uses a native image conversion library to convert auto-cad files into raster formats link PNG. If the native library cannot be loaded, WCS returns the "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 Dependency Walker on Windows platforms or ldd on Linux platforms. The following dlls must be present under the /webnms/rfdlls WCS installation directory: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problems occurred, you may need to install the required libraries and restart WCS.

Note 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.

Step 3 Choose **Monitor > Maps** to display the Maps page.

Step 4 From the Maps Tree View or the Monitor > Maps list, click the desired building. WCS displays the Maps > *Building Name* page.

Step 5 From the Select a command drop-down list, choose **New Floor Area**, and click **Go**.

Step 6 On the *Building Name* > 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 or basement name.

b. Enter the floor or basement contact name.

c. Choose the floor or basement number.

d. Choose the floor or basement type.

e. Enter the floor-to-floor height in feet.

Note To change the unit of measurement (feet or meters), select *Monitor* > *Maps* and select **Properties** from the Select a command drop-down list.

f. Select the Image File check box; then browse to and choose the desired floor or basement image filename and click **Open**.

g. Click **Next**.

Note When you choose the floor or basement image filename, WCS displays the image in the building-sized grid.

h. If you imported a CAD file, you are directed to the image conversion page.

Note The length of time for the conversion varies and depends on the file size, file detail, and number of layers in the file.

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 span and vertical span (width and depth on the map) in feet.

Note To change the unit of measurement (feet or meters), select *Monitor* > *Maps* and select **Properties** from the Select a command drop-down list.

Note The horizontal and vertical span should be smaller than or the same size as the building horizontal span and vertical span in the Cisco WCS database.

k. If desired, click **Place** to locate the floor or basement image on the building grid.

Tip You can use Ctrl-click to resize the image within the building-sized grid.

l. Click **OK** to save this floor plan to the database. WCS displays the floor plan image on the **Maps > Building Name** page.

Step 7 Click any of the floor or basement images to view the floor plan or basement map.

Note You can zoom in and out to view the map at different sizes, and you can add access points. See the "Inspecting VoWLAN Location Readiness" section on page 5-43 for instructions.

Using the Map Editor

You can use the WCS map editor to define, draw, and enhance floor plan information. The map editor enables you to create obstacles to consider when you computer RF prediction heat maps for access points. You can also add coverage areas for MSEs that locate clients and tags in that particular area. Follow these general guidelines to use the map editor.

Map Editor Functions

With the map editor, you can perform the following functions:

- Save—Saves the current map image.
- Recompute prediction—Updates the RF prediction heatmap if any changes are made to the existing floor map image.
- Reload Last Saved—Loads the last saved map image.
- Select all—Selects all the obstacles and coverage areas that you have created.
- Unselect—Deselects the obstacles and coverage areas that are selected.
- Move selected Obstacles—Moves the selected obstacles to a different location on the map.
- Duplicate selected Obstacles—Creates a copy of the selected obstacles.
- Zoom in/Zoom out— Zoom in or out on the image you are currently viewing.
- Show floor image—Use this to display the floor image.
- Show obstacles—Use this to display the obstacles.
- Larger resolution/Medium resolution/Smaller resolution—Increase or decrease the resolution of the floor map image.
- SNAP Mode—Use this to snap an obstacle to its nearest obstacle while drawing.
- ORTHO Mode—Use to draw a horizontal or vertical obstacle. This is especially useful when you want to draw all the obstacles at right angles.

General Notes and Guidelines for Using the Map Editor

Consider the following when modifying a building or floor map using the map editor.

- Cisco recommends 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 and 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 may limit the refresh and rendering aspects of WCS.

  - Cisco recommends a practical limit of 400 walls per floor for machines with 1-GB RAM or less.
- All walls are used by WCS when generating RF coverage heatmaps.
  - However, the MSEs use no more than 50 heavy walls in its calculations, and the MSE does not use light walls in its calculations because those attenuations are already accounted for during the calibration process.
- If you have a high resolution image (near 12 megapixels), you may need to scale down the image resolution with an image editing software prior to using map editor.

Follow these steps to use the map editor.

Step 1 Choose **Monitor > Maps** to display the Maps page.

Step 2 Click the desired campus. WCS displays the **Maps > Campus Name** page.

Step 3 Click a campus building.

Step 4 Click the desired floor area. WCS displays the **Maps > Campus Name > Building Name > Floor Area Name** page.

Step 5 From the Select a command drop-down list, choose **Map Editor**, and click **Go**. WCS displays the Map Editor page.

Step 6 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, choose the compass tool from the toolbar.

Step 7 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**.

Step 8 Determine the propogation pattern at the Antenna Mode drop-down list.

Step 9 Make antenna adjustments by sliding the antenna orientation bar to the desired degree of direction.

Step 10 Choose the desired access point.

Step 11 Click **Save**.

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 WCS (refer to the "Adding and Enhancing Floor Plans" section on page 5-22).

Step 2 Choose **Monitor > Maps**.

Step 3 Click the Map Name that corresponds to the outdoor area, campus, building, or floor you want to edit.

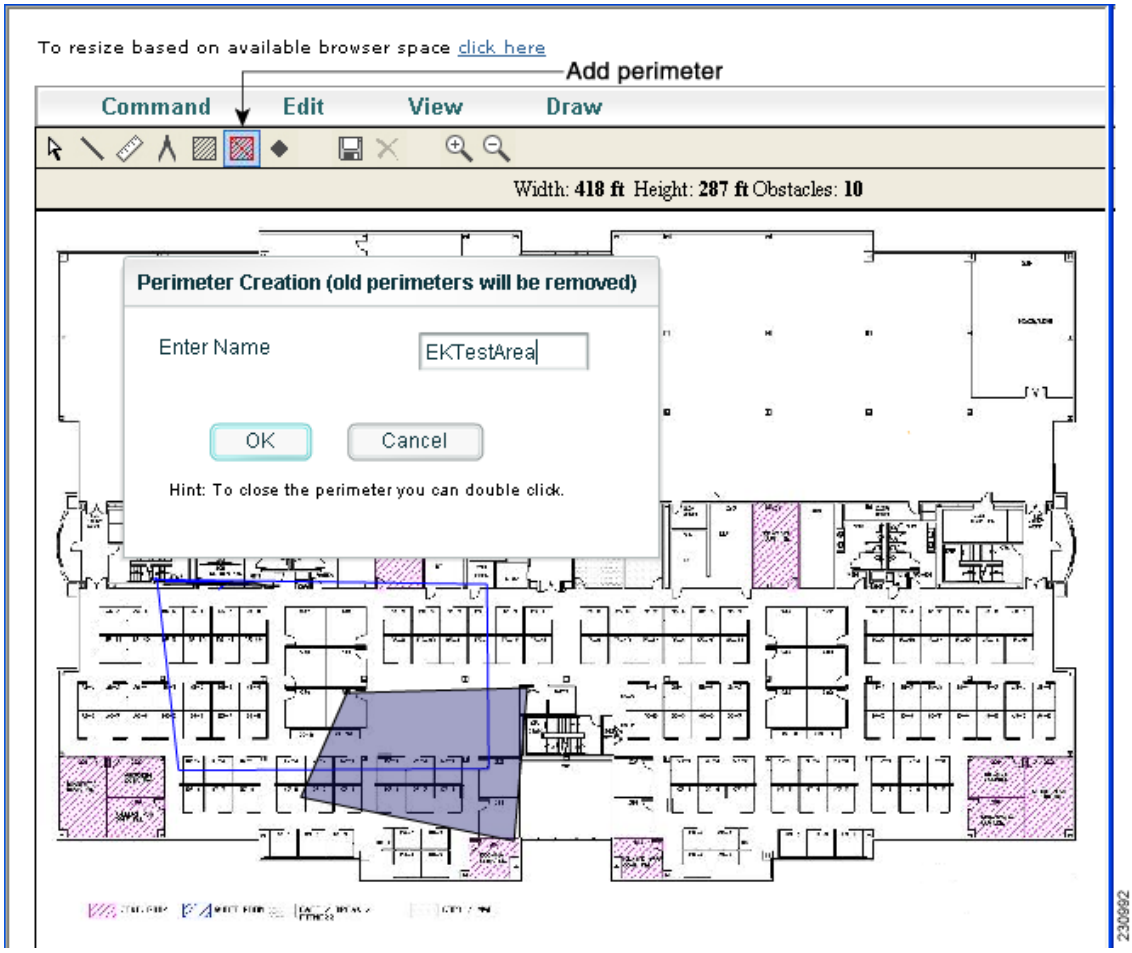
Step 4 From the Select a command drop-down list, choose **Map Editor**, and click **Go**.

Step 5 In the Map Editor page, click the **Add Perimeter** icon on the tool bar (see Figure 5-16).

A dialog box appears.

Note An example of a polygon-shaped area is seen in Figure 5-16.

Figure 5-16 Map Editor Page



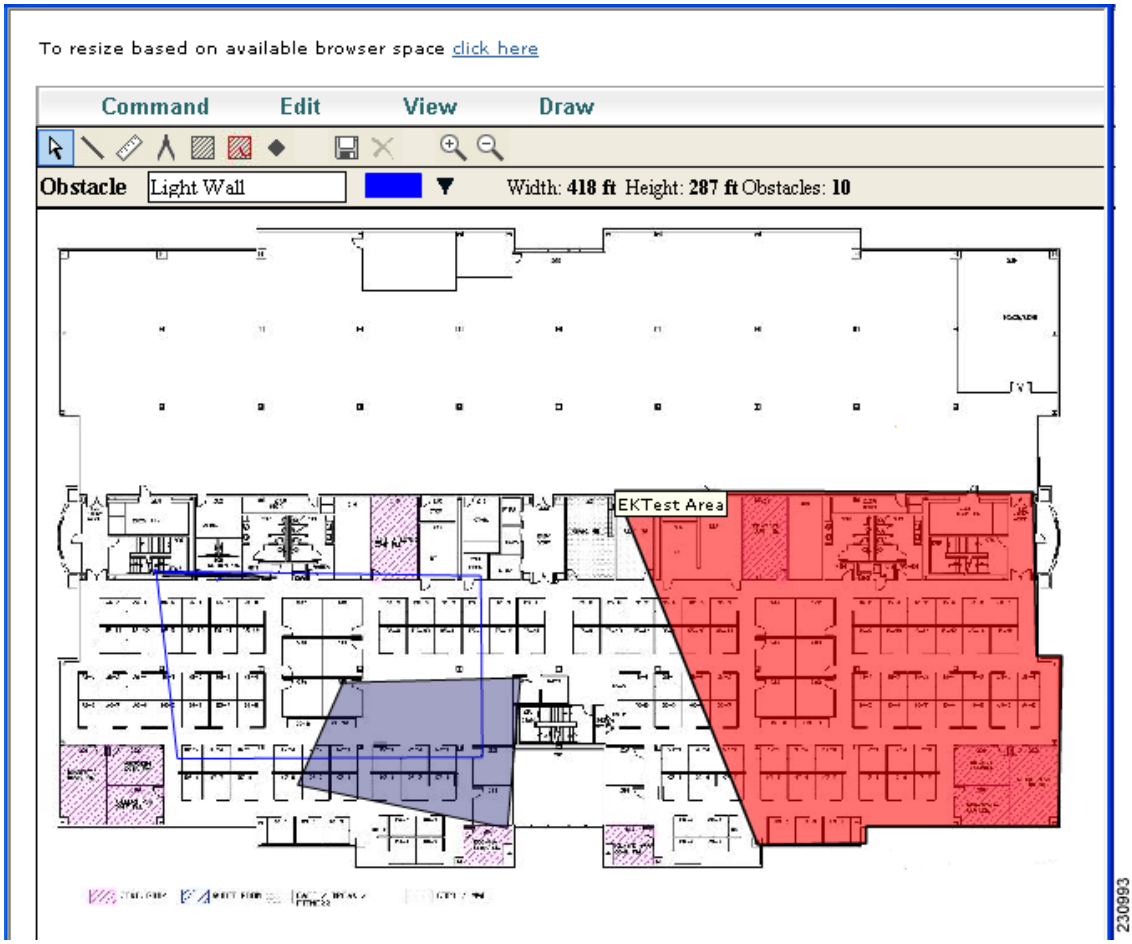
Step 6 Enter the name of the area that you are defining. Click **OK**.

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 on the screen (see Figure 5-17).
- The outlined area must be a closed object to highlight on the map.

Figure 5-17 Polygon Area



Step 8 Click the disk icon on the toolbar to save the newly drawn area.

Step 9 Choose **Command > Exit** to close the page. 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 seen; however, it appears in the Planning Model page when you add elements.

Step 10 Select **Planning Mode** from the Select a command drop-down list to begin adding elements to the newly defined polygon-shaped area.

Table 5-3 explains the color coding of obstacles.

Table 5-3 Obstacle Color Coding

Type of Obstacle	Color Coding	Loss (in dB)
Thick wall		13
Light wall		2

Table 5-3 Obstacle Color Coding (continued)

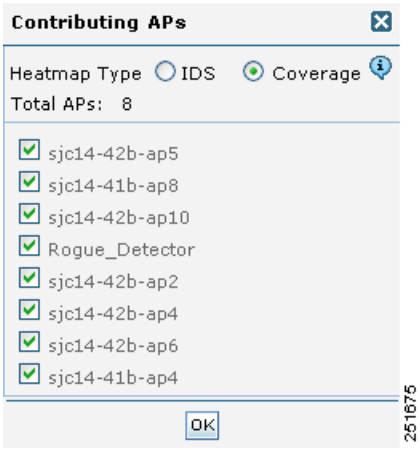
Type of Obstacle	Color Coding	Loss (in dB)
Heavy door		15
Light door		4
Cubicle		1
Glass		1.5

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 may not be enough to contain the RF signal beyond the walls of the heatmap.

Filtering Access Point Heatmap Floor Settings

If you enable the Access Point Heatmap floor setting and click the blue arrow to the right of the Floor Settings, the Contributing APs page opens with heatmap filtering options (Figure 5-18).

Figure 5-18 Access Point Heatmaps Filter



Access point heatmap filtering options include:

- Heatmap Type—Select IDS, Coverage, or Air Quality. If you choose Air Quality, you can further filter the heat map 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.

- Total APs—Displays the number of access points positioned on the map.
- Select the access point check box(es) to determine which heatmaps display on the image map.

Click **OK** when all applicable filtering criteria are selected.

Understanding RF Heatmap Calculation

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 or meters of the obstacle, may or may not account for the obstacle attenuation.

In detail, grid squares partially affected by an obstacle crossing the grid square may or may 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. In example Figure 5-19, the midpoint of the grid square is behind the wall from the access point, so the whole grid square is colored with attenuation, including the top left corner that is actually in front of the wall. Figure 5-21 displays how the attenuation would ideally appear in this situation.

Figure 5-19 Access Point/Grid Example One (Actual Attenuation)

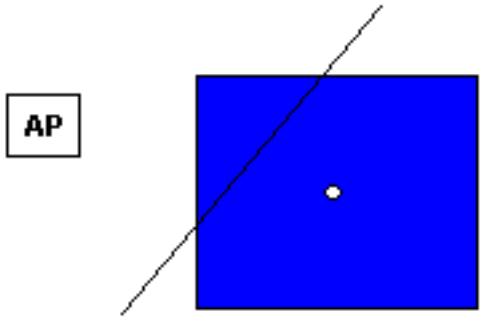
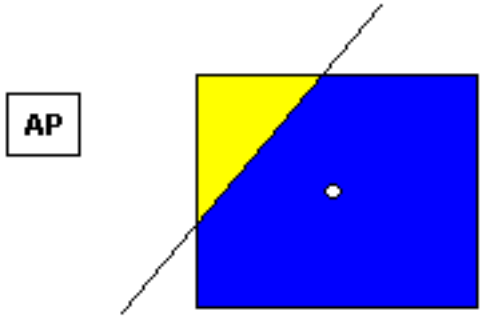


Figure 5-20 Access Point/Grid Example One (Ideal Attenuation)



Conversely, in example Figure 5-21, the midpoint of the grid square is on the same side of the wall as the access point, so the whole grid square is not colored with attenuation, including the bottom right corner that is actually behind the wall from the access point. Figure 5-22 displays how the attenuation would ideally appear in this situation.

Figure 5-21 Access Point/Grid Example Two (Actual Attenuation)

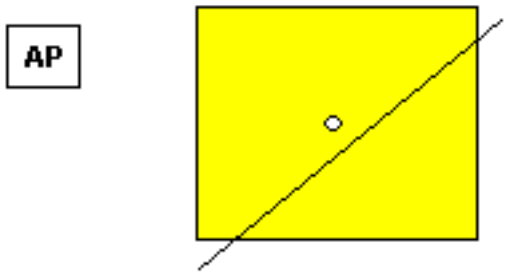
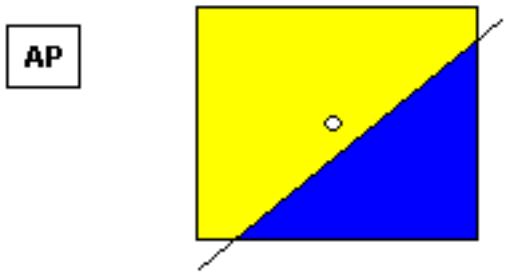


Figure 5-22 Access Point/Grid Example Two (Ideal Attenuation)



Filtering AP Mesh Info Floor Settings

Note The AP Mesh Info option displays only when bridging access points are added to the floor.

When this option is selected, Cisco WCS 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 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 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 opens 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.

Note For a child access point to be visible, its parent must also be selected.

Click **OK** when all applicable filtering criteria are selected.

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.

- Accessing Planning Mode
- Using Planning Mode to Calculate Access Point Requirements
- Inspecting VoWLAN Location Readiness

Accessing Planning Mode

To access the Planning Mode feature, follow these steps:

Step 1 Choose **Monitor > 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, click **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 "Adding Access Points" section on page 5-44 for details.
- Delete APs—Deletes the selected access points.
- Map Editor—Opens the Map Editor page. See the "Using the Map Editor" section on page 5-29 for 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.

Using Planning Mode to Calculate Access Point Requirements

The WCS 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:

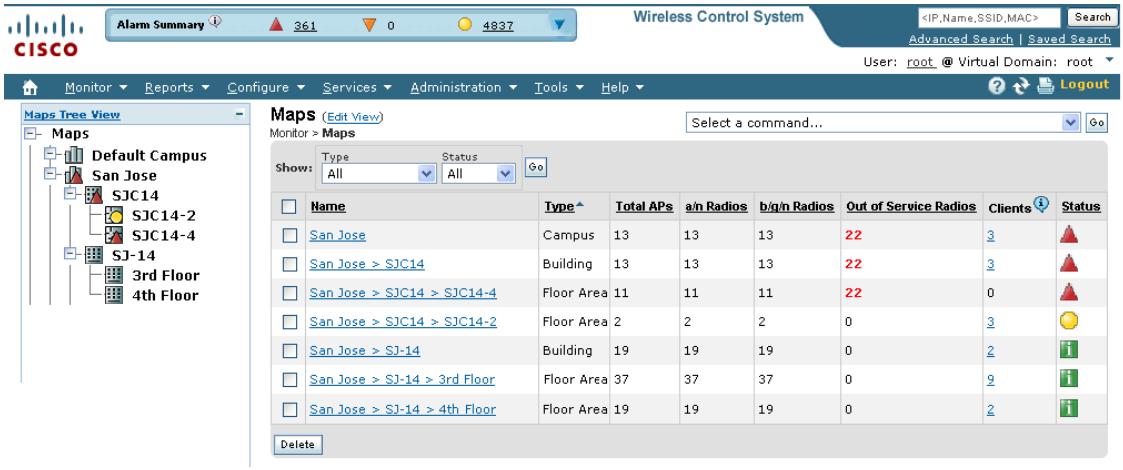
- traffic type active on the network: data or voice traffic or both
- location accuracy requirements
- number of active users
- number of users per square footage

To calculate the recommended number and placement of access points for a given deployment, follow these steps:

Step 1 Choose **Monitor > Maps**.

The page appears (see Figure 5-23).

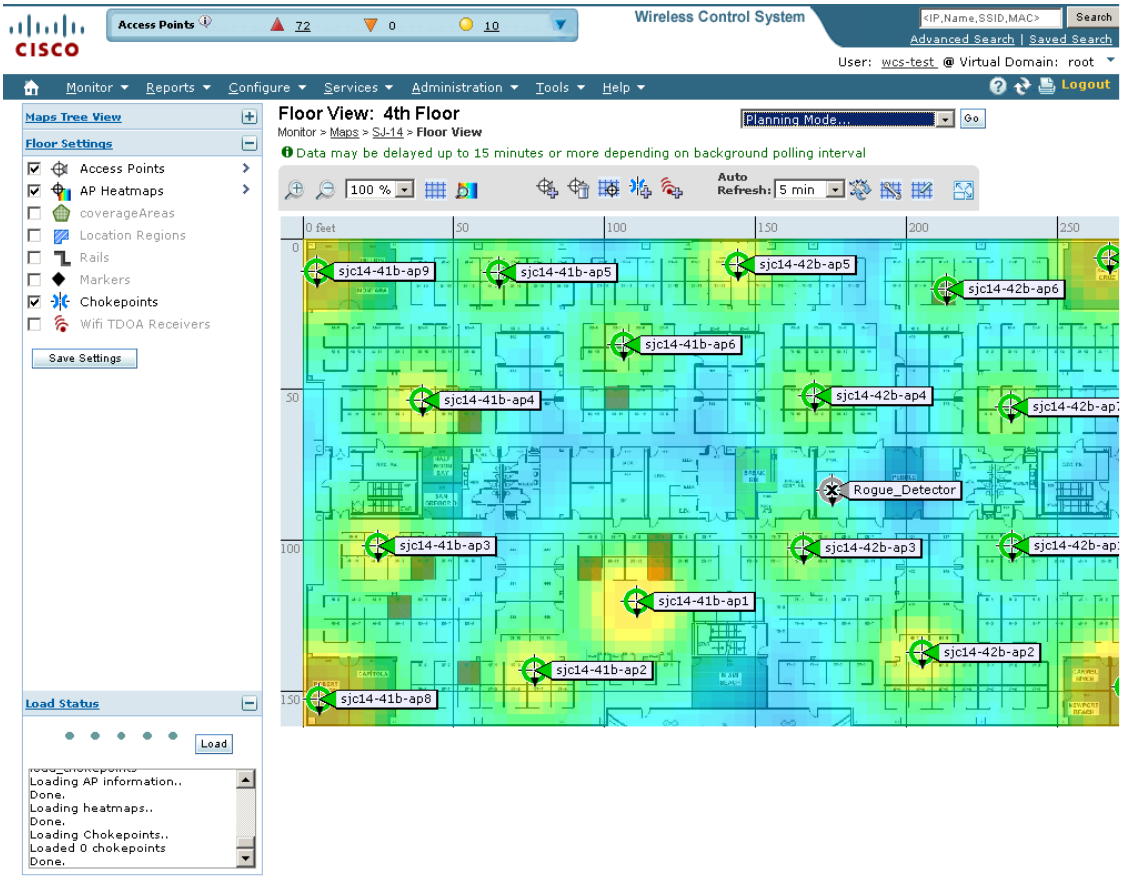
Figure 5-23 Monitor > Maps Page



Step 2 **Click** 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 (see Figure 5-24).

Figure 5-24 Selected Floor Area Showing Current Access Point Assignments



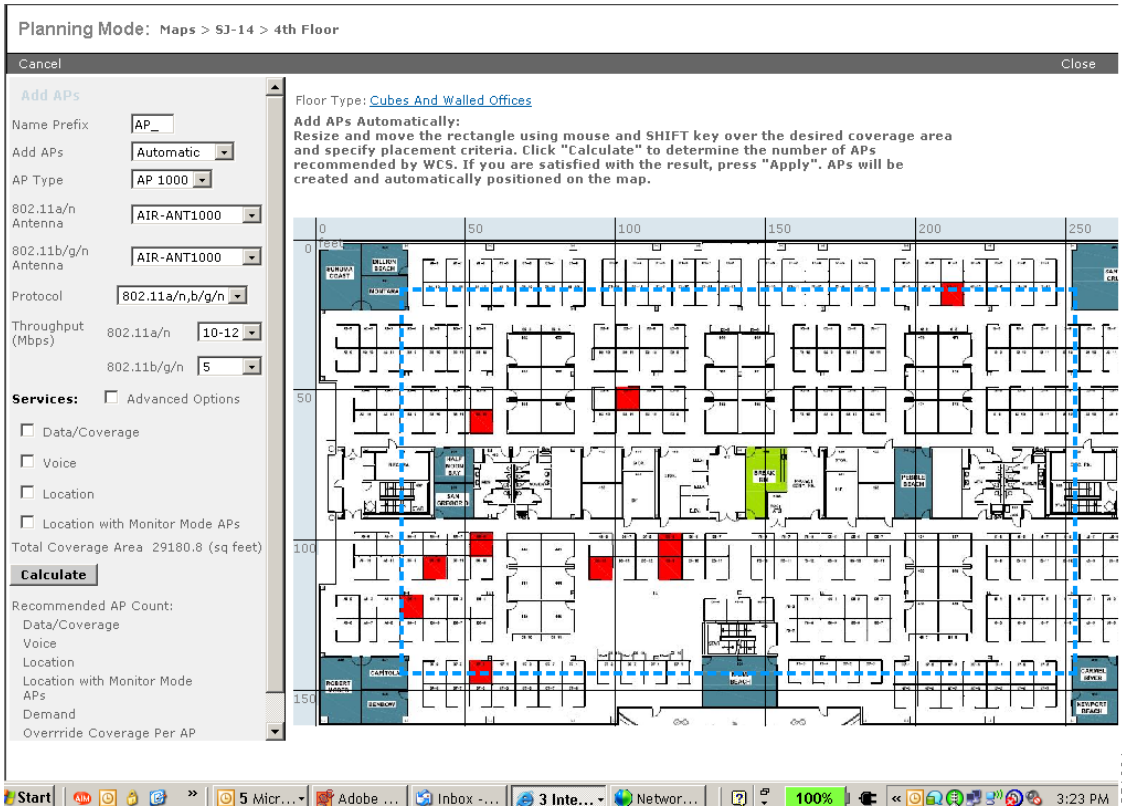
Step 3 Choose **Planning Mode** from the Select a command drop-down list, and click **Go**. A blank floor map appears.

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 (see Figure 5-25).

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.

Figure 5-25 Add APs Page



Step 6 Select **Automatic** from the Add APs drop-down list.

Step 7 Select the **AP Type** and the appropriate antenna and protocol for that access point.

Step 8 Select the target throughput for the access point.

Step 9 Select the box(es) next to the **service(s)** that will be used on the floor. Options are Data/Coverage (default), Voice, Location, and Location with Monitor Mode APs. (see Table 5-5).

Note You must select at least one service or an error occurs.

Note If you select the **Advanced Options** box, two additional access point planning options appear: Demand and Override Coverage per AP. Additionally, a Safety Margin parameter appears for the Data/Coverage and Voice safety margin options (see Table 5-3).

Table 5-4 Definition of Services Option

<table>
<tr><th>Service Options</th><th colspan="4">Description</th></tr>
<tr><td>Data/Coverage</td><td colspan="4">Select 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></td><td>Band</td><td>Path Loss Model (dBm)</td><td>Date Rate (Mb/s)</td><td>Area (Sq. ft.)</td></tr>
<tr><td></td><td>802.11a</td><td>–3.3</td><td>10-12</td><td>6000</td></tr>
<tr><td></td><td>802.11a</td><td>–3.3</td><td>15-18</td><td>4500</td></tr>
<tr><td></td><td>802.11a</td><td>–3.5</td><td>10-12</td><td>5000</td></tr>
<tr><td></td><td>802.11a</td><td>–3.5</td><td>15-18</td><td>3250</td></tr>
<tr><td></td><td>802.11bg</td><td>–3.3</td><td>5</td><td>6500</td></tr>
<tr><td></td><td>802.11bg</td><td>–3.3</td><td>6</td><td>4500</td></tr>
<tr><td></td><td>802.11bg</td><td>–3.5</td><td>5</td><td>5500</td></tr>
<tr><td></td><td>802.11bg</td><td>–3.5</td><td>6</td><td>3500</td></tr>
<tr><td></td><td colspan="4">If you enable Advanced Options (select 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)</td></tr>
<tr><td>Voice</td><td colspan="4">Select if voice traffic is transmitted on the wireless LAN.
If you enable Advanced Options (select 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)]</td></tr>
<tr><td>Location</td><td colspan="4">Select 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.
Note Each service option includes all services that are listed above it. For example, if you select the Location box, the calculation considers data/coverage, voice, and location in determining the optimum number of access points required.</td></tr>
</table>

Table 5-5 Definition of Advanced Services

<table>
<tr><th>Service Options</th><th colspan="4">Description</th></tr>
<tr><td>Data/Coverage</td><td colspan="4">Select 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></td><td>Band</td><td>Path Loss Model (dBm)</td><td>Date Rate (Mb/s)</td><td>Area (Sq. ft.)</td></tr>
<tr><td></td><td>802.11a</td><td>–3.3</td><td>10-12</td><td>6000</td></tr>
<tr><td></td><td>802.11a</td><td>–3.3</td><td>15-18</td><td>4500</td></tr>
<tr><td></td><td>802.11a</td><td>–3.5</td><td>10-12</td><td>5000</td></tr>
<tr><td></td><td>802.11a</td><td>–3.5</td><td>15-18</td><td>3250</td></tr>
<tr><td></td><td>802.11bg</td><td>–3.3</td><td>5</td><td>6500</td></tr>
<tr><td></td><td>802.11bg</td><td>–3.3</td><td>6</td><td>4500</td></tr>
<tr><td></td><td>802.11bg</td><td>–3.5</td><td>5</td><td>5500</td></tr>
<tr><td></td><td>802.11bg</td><td>–3.5</td><td>6</td><td>3500</td></tr>
<tr><td></td><td colspan="4">If you enable Advanced Options (click 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)</td></tr>
<tr><td>Voice</td><td colspan="4">Select if voice traffic is transmitted on the wireless LAN.
If you enable Advanced Options (click 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)]</td></tr>
<tr><td>Location</td><td colspan="4">Select 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.
Note Each service option includes all services that are listed above it. For example, if you select the Location box, the calculation considers data/coverage, voice, and location in determining the optimum number of access points required.</td></tr>
<tr><td>Demand</td><td colspan="4">Select if you want to use the total number of users or user ratio per access point as a basis for the access point calculation.</td></tr>
</table>

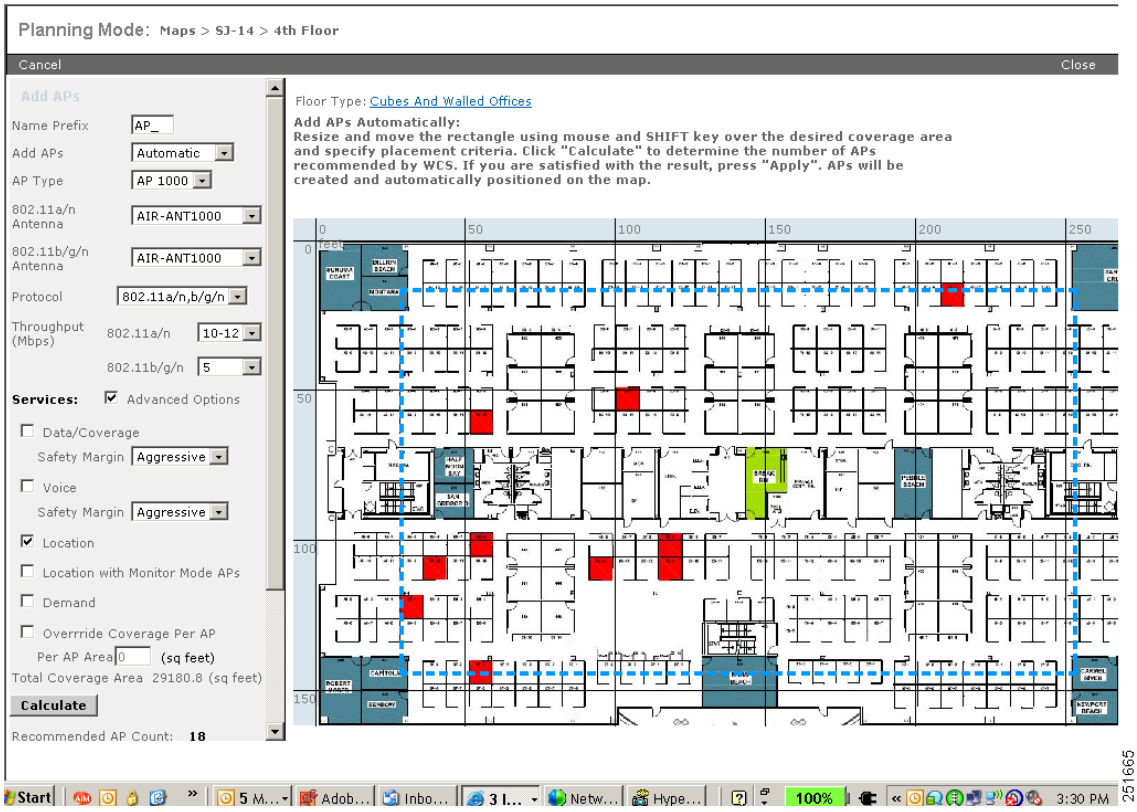
Table 5-5 Definition of Advanced Services (continued)

Service Options	Description
Override Coverage per AP	Select if you want to specify square foot coverage as the basis for access point coverage.
Safety Margin	Select option 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.

Step 10 Click **Calculate**.

The recommended number of access points given the selected services appears (see Figure 5-26).

Figure 5-26 Recommended Number of Access Points Given Selected Services and Parameters

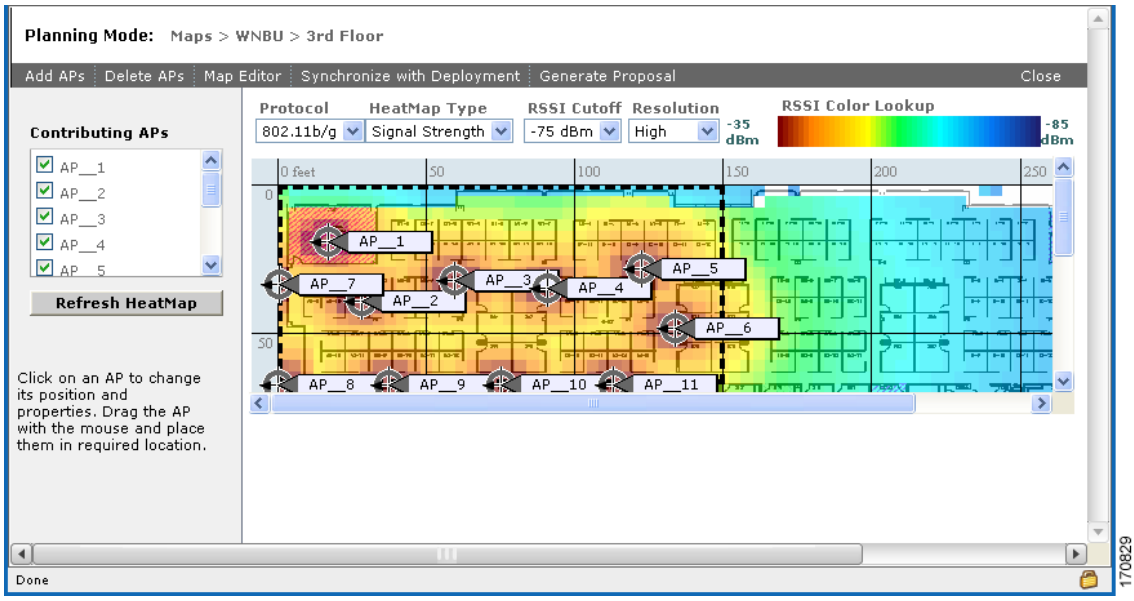


Note Recommended calculations assume the need for consistently strong signals unless adjusted downward by the **safety margin** advanced option. In some cases, the recommended number of access points is higher than what is required.

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 (see Figure 5-27).

Figure 5-27 Recommended Access Point Deployment Given 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.

Inspecting VoWLAN Location Readiness

The Inspect Location Readiness feature is a distance-based predictive tool that can point out problem areas with access point placement. Voice readiness tool (the VoWLAN Readiness tool) allows you to verify that the RF coverage is sufficient for your voice needs. This tool verifies RSSI levels after access points have been installed.

The Inspect Location Readiness tool:

- Displays areas that have the required access point coverage and will provide accurate location results.
- Takes into consideration the placement of each access point along with the inter-access point spacing.
- Assumes that access points and controllers are known to WCS.

A point is defined as “location-ready” if the following is true:

- At least four access points are deployed on the floor.
- At least three access points are within 70 feet of the point-in-question.
- At least one access point is found to be resident in each quadrant surrounding the point-in-question.

To access the Inspect Location Readiness tool, follow these steps:

Step 1 Choose **Monitor > Maps**.

Step 2 Choose the applicable floor area name.

Step 3 From the Select a command drop-down list, click **Inspect VoWLAN Readiness**, and click **Go**.

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 region map for 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 RSSI values may 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

Troubleshooting Voice RF Coverage Issues

Perform the following to troubleshoot voice RF coverage issues:

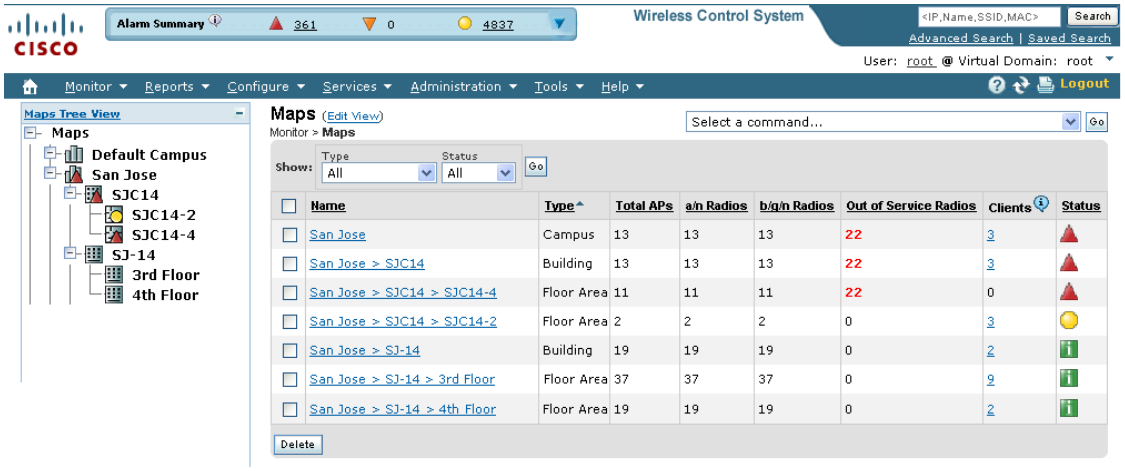
- Set the AP Transmit parameter to **Max** (the maximum downlink power setting). If the map still shows some yellow or red regions, more access points are required to cover the floor.
- Increase the power level of the access points if a calibrated model shows red or yellow regions (where voice is expected to be deployed) while the AP Transmit parameter is set to *Current*.
- Verify the green, yellow, and red regions of the RF environment. These indicators are accurate whether the floor is calibrated or not, but floor calibration improves the accuracy.

Adding Access Points

After you add the .PNG, .JPG, .JPEG, or .GIF format floor plan and outdoor area maps to the Cisco WCS database, you can position lightweight access point icons on the maps to show where they are installed in the buildings. Follow these steps to add access points to floor plan and outdoor area maps.

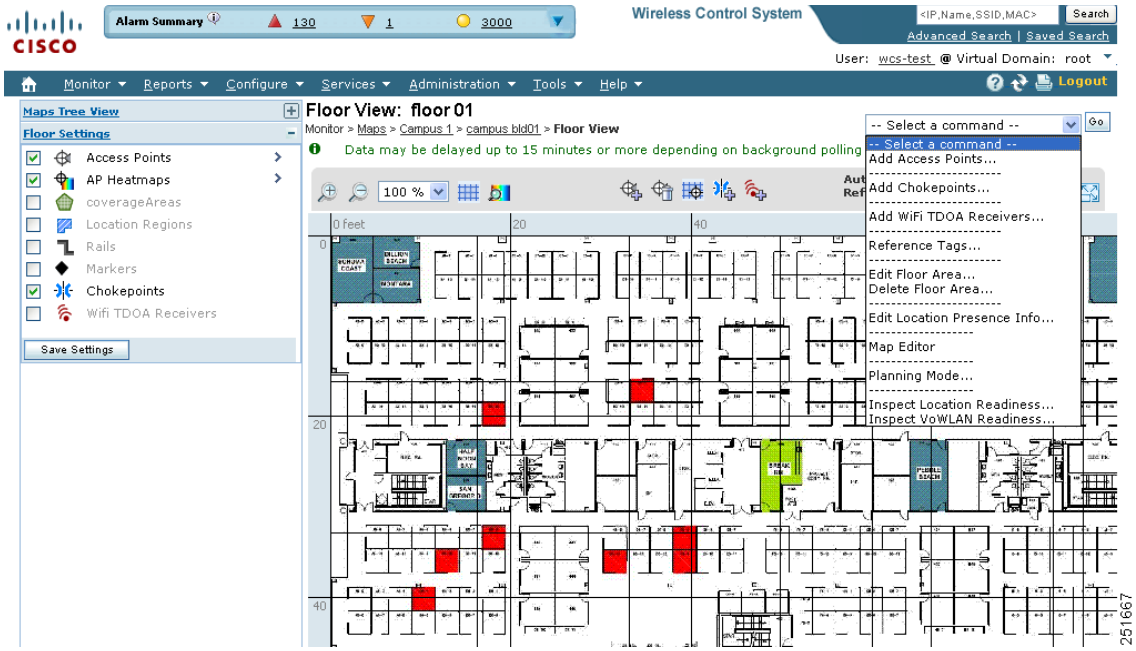
Step 1 Choose **Monitor > Maps**. The Maps page opens (see Figure 5-28).

Figure 5-28 Monitor Maps Page



Step 2 From the Maps Tree View or the Monitor > Maps list, click the applicable floor to open the Floor View page (Figure 5-29).

Figure 5-29 Floor View Page

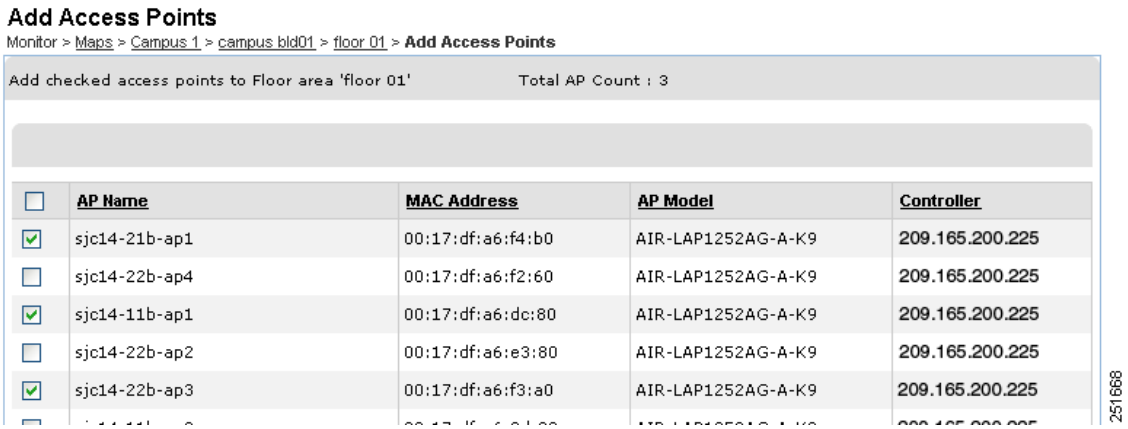


Step 3 From the Select a command drop-down list, choose **Add Access Points**, and click **Go**.

Step 4 On the Add Access Points page, choose the access points to add to the map.

Step 5 Click **OK** to add the access points to the map and display the Position Access Points map (see Figure 5-30).

Figure 5-30 Add Access Point Page

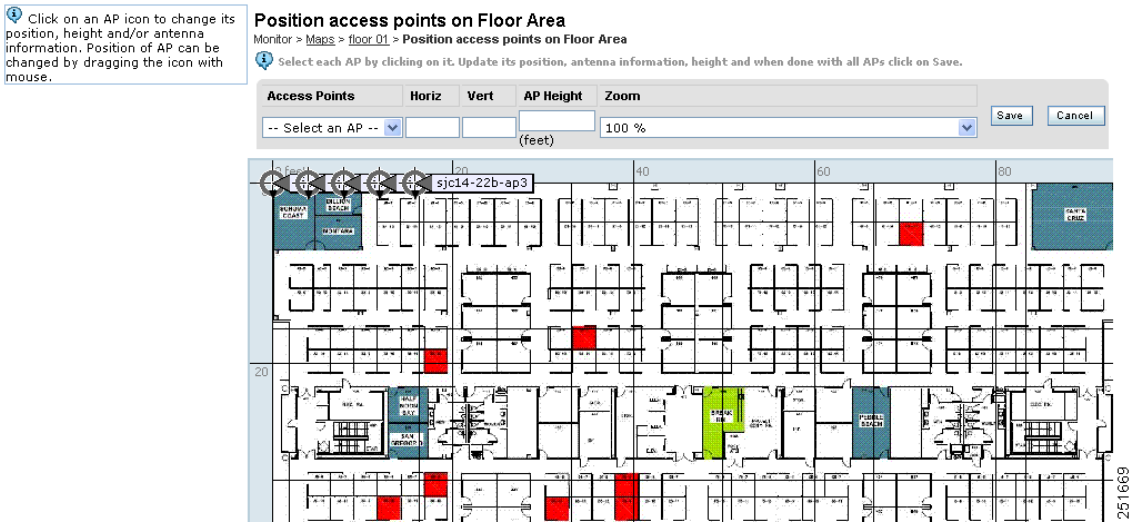


Note The access point icons appear in the upper left area of the map. Select the check box at the top of the list to select all access points.

Step 6 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 opens (see Figure 5-31).

Figure 5-31 Position Access Points Page



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 7 Click and drag each access point to the appropriate locations. Access points turn blue when selected.

Note The small black arrow at the side of each access point represents Side A of each access point, and each access point's 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 in the Antenna Angle drop-down list.

When selected, the access point details display on the left side of the page (see Figure 5-32). Access point details include:

- AP Model—Indicates the model type of the selected access point.
- Protocol—Select the protocol for this access point from the drop-down list.
- Antenna—Select 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 every antenna.

  Note For internal antennas, the same elevation angle applies to both radios.

  The antenna angle is relative to the map's 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.

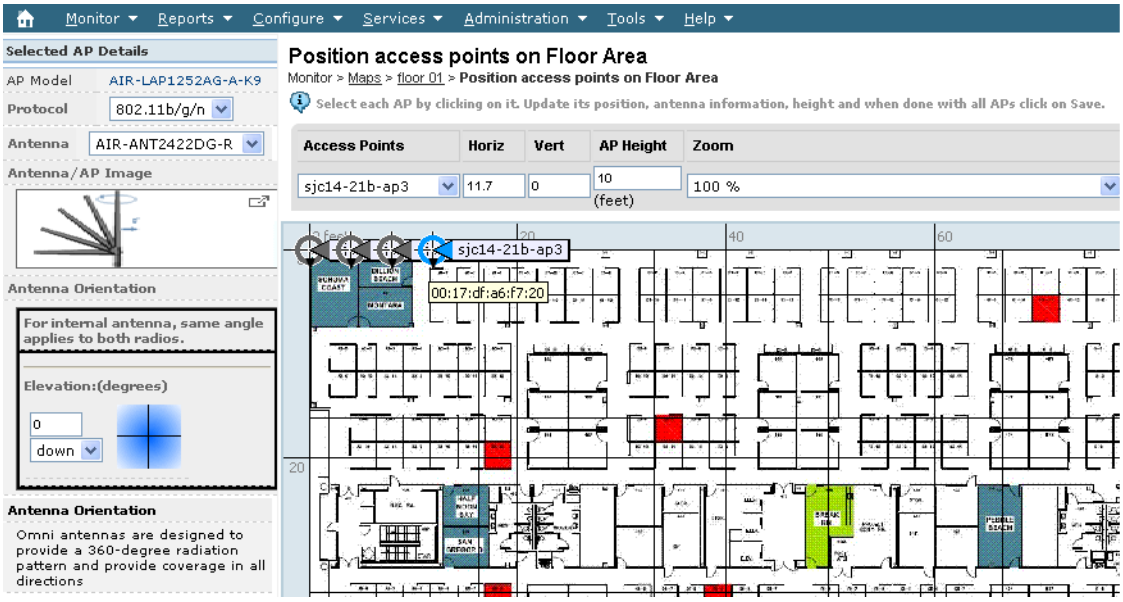
  The antenna elevation is used to move the antenna vertically, up or down, to a maximum of 90 degrees.

Note 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.

See this location for further information about the antenna elevation and azimuth patterns:

http://www.cisco.com/en/US/products/hw/wireless/ps469/tsd_products_support_series_home.html

Figure 5-32 Selected Access Point Details

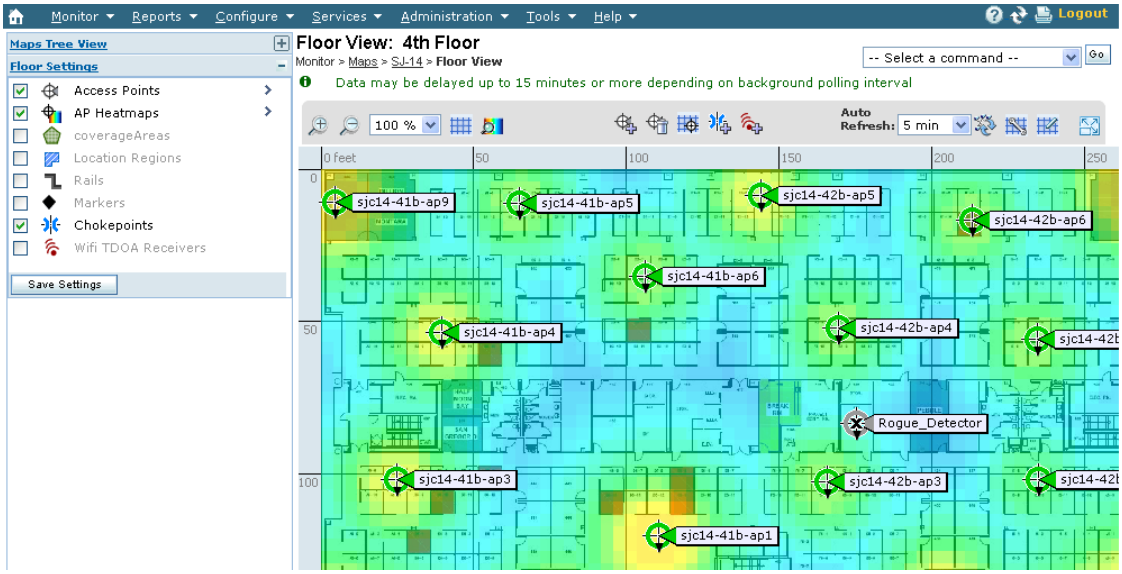


Step 8 When you are finished placing and adjusting each access point, click **Save**.

WCS computes the RF prediction for the coverage area. These RF predictions are popularly known as *heat maps* because they show the relative intensity of the RF signals on the coverage area map. Figure 5-33 shows an RF prediction heat 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.

Figure 5-33 RF Prediction Heatmaps



Note See the "Placing Access Points" section on page 5-49 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 "Changing Access Point Positions by Importing and Exporting a File" section on page 5-78 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.

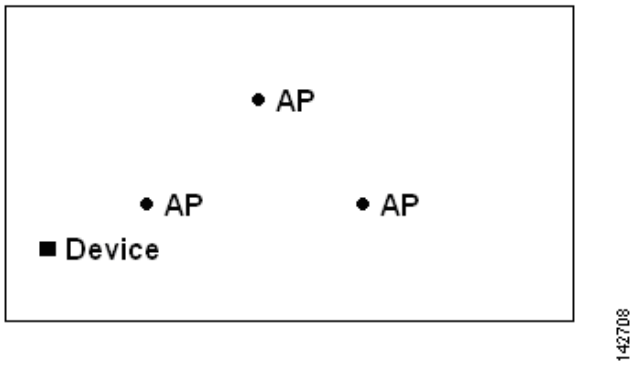
Following these guidelines makes it more likely that access points will detect tracked devices. Rarely do two physical environments have the same RF characteristics. Users may need to adjust those parameters to their specific environment and requirements.

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.

Guidelines for Placing Access Points

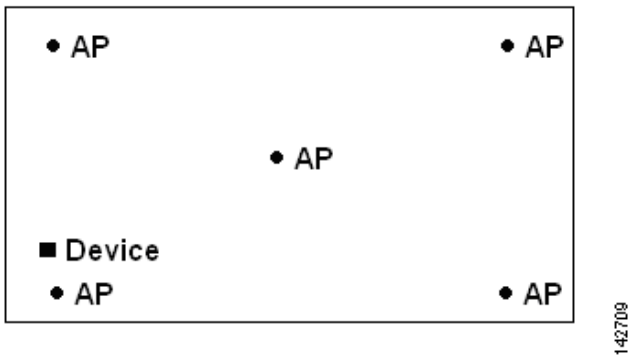
Place access points along the periphery of coverage areas in order to keep devices close to the exterior of rooms and buildings (see Figure 5-34). Access points placed in the center of these coverage areas provide good data on devices that would otherwise appear equidistant from all other access points.

Figure 5-34 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 (see Figure 5-35).

Figure 5-35 Improved Location Accuracy by Increasing Density



In long and narrow coverage areas, avoid placing access points in a straight line (see Figure 5-36). Stagger them so that each access point is more likely to provide a unique snapshot of a device's location.

Figure 5-36 Refrain From Straight Line Placement

Although the design in Figure 5-36 may provide enough access point density for high bandwidth applications, location suffers because each access point's view of a single device is not varied enough; therefore, location is difficult to determine.

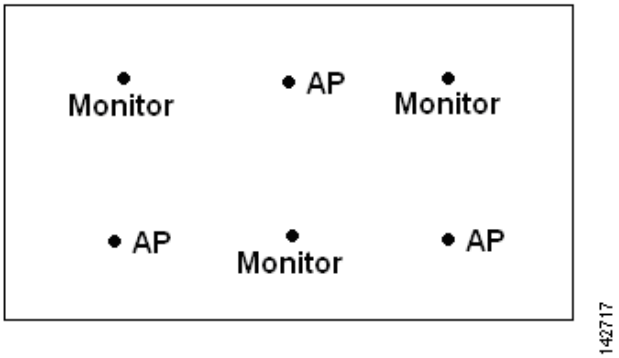
Move the access points to the perimeter of the coverage area and stagger them. Each has a greater likelihood of offering a distinctly different view of the device, resulting in higher location accuracy (see Figure 5-37).

Figure 5-37 Improved Location Accuracy by Staggering Around Perimeter

Designing a location-aware wireless LAN, while planning for voice as well, is better done with a few things in mind. 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 (see Figure 5-38).

Figure 5-38 Less Dense Wireless LAN Installations



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 WCS reports client devices and tags within the specified accuracy range (10 m, 90%).

Import Map and AP Location Data

When converting from autonomous to lightweight access points and from WLSE to WCS, one of the conversion steps is to manually re-enter the access point-related information into WCS. To speed up this process, you can export the information about access points from WLSE and import it into WCS.

Note WCS 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, WCS 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 http://<WLSE_IP_ADDRESS>:1741/debug/export/exportSite.jsp.

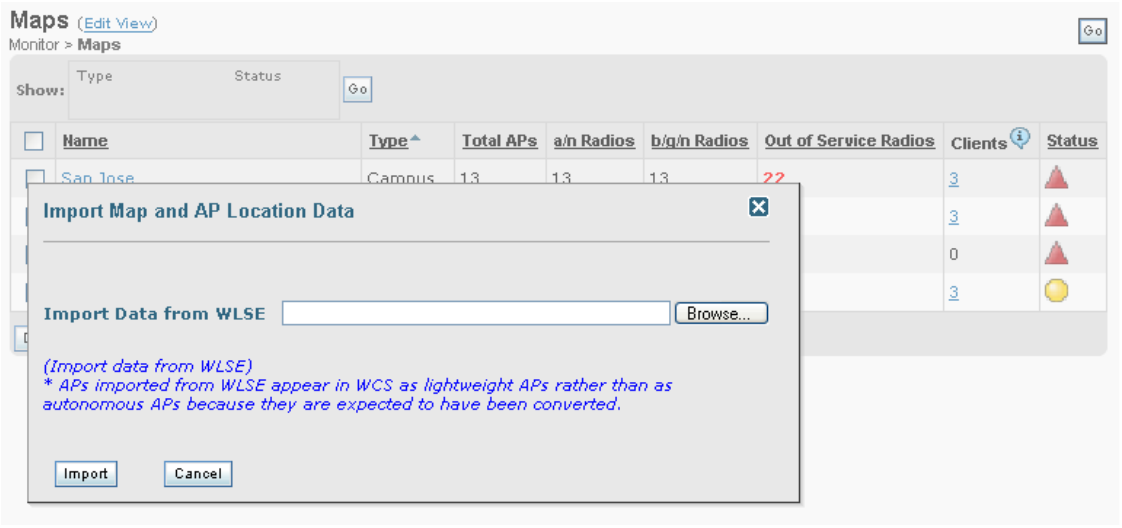
To map properties and import a tar file containing WLSE data using the WCS web interface, follow these steps:

Step 1 Choose **Monitor > Maps**.

Step 2 From the Select a command drop-down list, choose **Import WLSE Map and AP Location Data**.

Step 3 Click **Go**. The Import WLSE Map and AP Location Data page opens (Figure 5-39).

Figure 5-39 Import WLSE Map and AP Location Data Page



Step 4 In the Import Data from WLSE section, click **Browse** to select the file to import.

Step 5 Find and select the .tar file to import and click **Open**.

WCS displays the name of the file in the Import From text box.

Step 6 Click **Import**.

WCS 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, WCS prompts you to correct the problem and retry. Once the file has been loaded, WCS displays a report of what will be added to WCS. The report also specifies what cannot be added and why.

Step 7 If some of the data to be imported already exists, WCS 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 a WCS campus (or top-level building) and building combination, WCS displays a message in the Pre Execute Import Report indicating that it will delete the existing building.

Step 8 Click **Import** to import the WLSE data.

WCS displays a report indicating what was imported.

Step 9 Choose **Monitor > Maps** to view the imported data.

Positioning Access Points, Wi-Fi TDOA Receivers, and Chokepoints by Importing or Exporting a File

You can change an access point, Wi-Fi TDOA receiver, or chokepoint position by importing or exporting a file. The file contains only the lines describing the component you want to move. This option takes less time than manually changing multiple positions. See the *Cisco Context-Aware Services Configuration Guide* for more information on chokepoints and Wi-Fi TDOA receivers.
To change an access point, Wi-Fi TDOA receiver, or chokepoint position, follow these steps:

Step 1 Choose **Monitor > Maps**.

Step 2 From the Select a command drop-down list, choose **Properties**.

Step 3 At the Unit of Dimension drop-down list, choose feet or meters.

Step 4 Select the Advanced Debug Mode **Enable** radio button.

Step 5 Click **OK**.

Step 6 From the Select a command drop-down list, select **Export/Import AP/WiFi TDOA Receiver/Chokepoint Placement**.

Step 7 In the Import/Export AP/WiFi TDOA Receiver/Chokepoint Placement page, click **Browse** to find the file you want to import.

Note The file must already be created and added to WCS.

Note The following is the correct file format:

[BuildingName], [FloorName], [AP/WiFi TDOA Receiver/Chokepoint Name], (aAngle), (bAngle), [X], [Y], ([aAngleElevation, bAngleElevation, Z]), (aAntennaType, aAntennaMode, (aAntennaPattern, (aAntennaGain)), bAntennaType, bAntennaDiversity, (bAntennaPattern, bAntennaGain)))))

The parameters in square brackets are mandatory, and those in parentheses are optional.

Note Angles must be entered in radians (X,Y), and the height is entered in feet. The aAngle and bAngle range is from –2Pi (-6.28...) to 2Pi (6.28...), and the elevation ranges from –Pi (-3.14...) to Pi (3.14...).

Step 8 Click **Import**. The RF calculation takes approximately two seconds per component.

Floor Area Map Overview

- Floor Settings
- Viewing Floor Component Details
- Floor View Navigation
- Select a Command for Floor Areas

Floor Settings

You can modify the appearance of the floor map by selecting or clearing Floor Settings check boxes (Figure 5-40). The selected Floor Settings display in the map image. The Floor Settings options include:

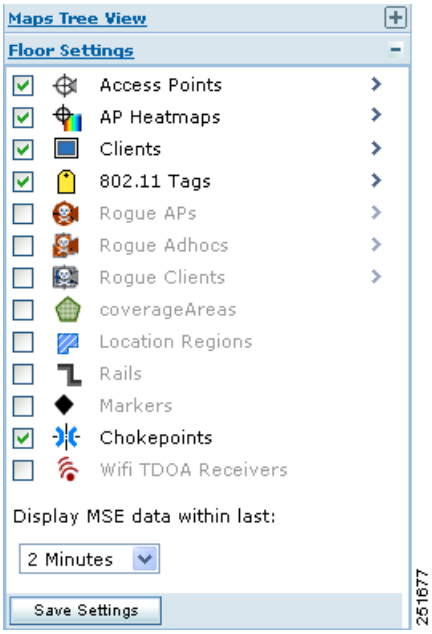
- Access Points—See "Filtering Access Point Floor Settings" for more information.
- AP Heatmaps—See "Filtering Client Floor Settings" for more information.
- AP Mesh Info—Displays only if mesh access points are present in outdoor areas. See "Filtering AP Mesh Info Floor Settings" for more information.
- Clients—Displays data only if an MSE was added in WCS. See "Filtering Client Floor Settings" for more information.
- 802.11 Tags—See "Filtering 802.11 Tag Floor Settings" for more information.
- Rogue APs—Displays data only if an MSE was added in WCS. See "Filtering Rogue AP Floor Settings" for more information.
- Rogue Adhocs—Displays data only if an MSE was added in WCS. See "Filtering Rogue Ad hoc Floor Settings" for more information.
- Rogue Clients—Displays data only if an MSE was added in WCS. See "Filtering Rogue Client Floor Settings" for more information.
- Coverage Areas
- Location Regions
- Rails
- Markers
- Chokepoints—Displays only if chokepoints are added in WCS.
- Wi-Fi TDOA Receivers
- Interferers—Displays details of the interferers on the wireless network. See "Filtering Interferer Settings" for more information.

Use the blue arrows to access Floor Setting filters for access points, access point heatmaps, clients, 802.11 tags, rogue access points, rogue ad hoc events, and rogue clients. When filtering options are selected, click **OK**.

Use the Display MSE data within last drop-down list to select the timeframe for mobility services engine data. This option only appears if an MSE is present on the WCS.

Click **Save Settings** to make the current view and filter settings your new default for all maps.

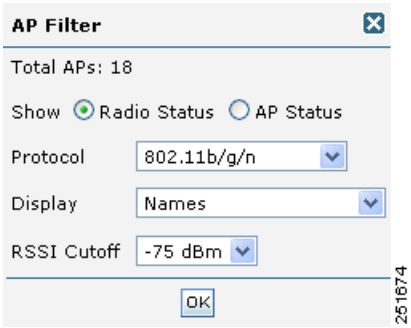
Figure 5-40 Floor Settings Parameters



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 page opens with filtering options (Figure 5-41).

Figure 5-41 Access Point Filter



Access point filtering options include:

- Show—Choose to display the radio status or access point status.
- Protocol—From the drop-down list, which radio types to display (802.11a/n, 802.11b/g/n, or both).
- Display—From the drop-down list, select the identifying information to display for the access points on the map image.
  - Channels—Displays the Cisco Radio channel number or Unavailable (if the access point is not connected).

Note The available channels are defined by the country code setting and are regulated by country:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html.

- 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 See the hardware installation guide for your access point regarding the maximum transmit power levels supported per regulatory domain. Use this URL http://www.cisco.com/en/US/products/ps5678/Products_Sub_Category_Home.html, click the specific access point from the Product Portfolio, and the choose **Install and Upgrade** from the Support page on the right. Also, refer to the data sheet for your access point regarding the number of power levels supported.

Note The power levels are defined by the country code setting and are regulated by country:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html.

- 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 select Load, Noise, Interference, or Coverage.

- 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. 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.

  Note Click the client number to view client details. See "Monitor > Clients" for more information.

- Bridge Group Names

- RSSI Cutoff—From the drop-down list, select the RSSI cutoff level. The RSSI cutoff ranges from -60 dBm to -90 dBm.

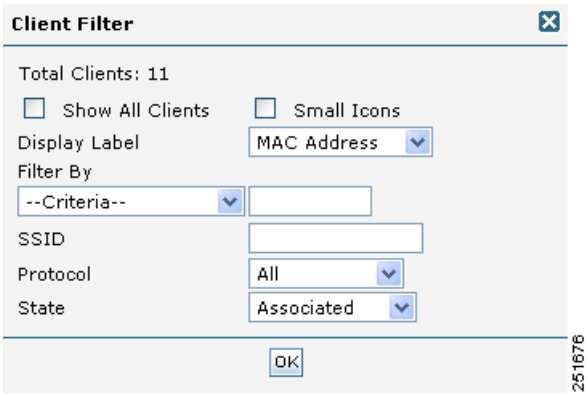
Click **OK** when all applicable filtering criteria are selected.

Filtering Client Floor Settings

Note The Clients option displays only if a mobility server is added in WCS.

If you enable the Clients floor setting and click the blue arrow to the right, the Client Filter page opens (Figure 5-42).

Figure 5-42 Client Filter Page



Client filtering options include:

- 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 click the **Show All Clients** check box and **Small Icons** check box, all other drop-down list options are unavailable.

If you unselect the **Small Icons** check box, you can choose if the want the label to display MAC address, IP address, user name, 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.

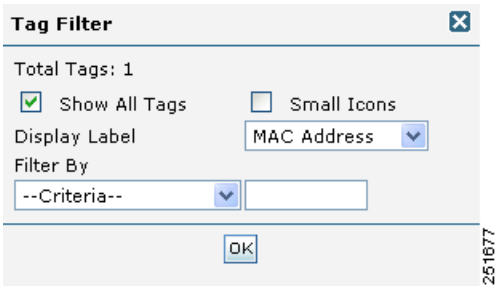
- Display Label—Select the client identifier (IP address, username, MAC address, asset name, asset group, or asset category) to display on the map.
- Filter By—Select the parameter with which you want to filter the clients (IP address, username, MAC address, asset name, asset group, asset category, or controller). Then, type the specific device in the text box.
- SSID—Enter the client SSID in the available text box.
- Protocol—Select 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—Select 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 page opens (Figure 5-43).

Figure 5-43 Tag Filter Page



Tag filtering options include:

- 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 click the **Show All Tags** check box and **Small Icons** check box, all other drop-down list options are grayed out.

If you unselect the **Small Icons** check box, you can choose if the 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 Label—Select the tag identifier (MAC address, asset name, asset group, or asset category) to display on the map.
- Filter By—Select 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 page opens.

Rogue AP filtering options include:

- 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 click the **Show All Rogue APs** check box and **Small Icons** check box, all other drop-down list options are grayed out.

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 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 access points on the network.

Click **OK** when all applicable filtering criteria are selected.

Filtering Rogue Ad hoc Floor Settings

If you enable the Rogue Adhocs floor setting and then click the blue arrow to the right, the Rogue Adhoc filter page opens.

Rogue Adhoc filtering options include:

- Show All Rogue Adhocs—Select the check box to display all rogue ad hoc on the map.
- Small Icons—Select the check box to display icons for each rogue ad hoc on the map.

Note If you click the **Show All Rogue Adhocs** check box and **Small Icons** check box, all other drop-down list options are grayed out.

If you unselect the **Show All Rogue Adhocs** check box, you can specify how you want the rogue ad hocs 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 ad hocs 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 page opens.

Rogue Clients filtering options include:

- 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 click the **Show All Rogue Clients** check box and **Small Icons** check box, all other drop-down list options are grayed out.

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 select 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 settings and then click the blue arrow to the right, the Interferers filter page opens.

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 will likely disrupt Wi-Fi communications, a light pink circle represents a weak interferer.
- Show All Interferer Labels—Select the check box to display all interferer lables detected by the access point.
- Maximum number of Interferers per label—Select the maximum number of interferer to be displayed.

Click **OK** when all applicable filtering criteria are selected.

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 appears displaying detailed information.

The following table (Table 5-6) displays floor map icons.

Table 5-6 Floor Map Icons

Icon	Description
	Access point icon. The color of the circle indicates the alarm status of the Cisco radios. **Note** 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. **Note** A blinking access point icon indicates that an interference, noise, coverage, or load profile failure alarm is pending against this access point. **Note** If a Cisco radio is disabled, a small "x" appears in the middle of the icon.
	Client icon. Hold your mouse cursor over the icon to view client details. See "Client Details" for more information.
	Tag icon. Hold your mouse cursor over the icon to view tag details. See "Tag Details" for more information.

Icon	Description
	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. Hold your mouse cursor over the icon to view rogue access point details. See "Rogue Access Point Details" for more information.
	Rogue ad hoc icon. Hold your mouse cursor over the icon to view rogue ad hoc details. See "Rogue Adhoc Details" for more information.
	Rogue client icon. Hold your mouse cursor over the icon to view rogue client details. See "Rogue Client Details" for more information.
	Chokepoint icon.
	Wi-Fi TDOA receiver icon.
	Interferer device icon. See "Interferer Details" for more information.

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 worst 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 gets whatever color is more severe.

The following table shows the icons used in the Cisco WCS user interface Map displays.

Table 5-7 Access Points Icons Description

Icon	Description
	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.
	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. **Note** 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.

Table 5-7 Access Points Icons Description (continued)

Icon	Description
	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.
	The grayed-out icon with a question mark in the middle represents an unreachable access point. It is gray because its status cannot be determined.
	The grayed-out icon with no question mark in the middle represents an unassociated access point.
	The icon with a red “x” in the center of the circle represents an access point that has been administratively disabled.
	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 worst of the two Cisco Radio colors determines the color of the large triangular pointer.
	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 worst of the two Cisco Radio colors determines the color of the large triangular pointer.
	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 worst of the two Cisco Radio colors determines the color of the large triangular pointer.
	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 worst of the two Cisco Radio colors determines the color of the large triangular pointer.
	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 worst of the two Cisco Radio colors determines the color of the large triangular pointer.

Table 5-7 Access Points Icons Description (continued)

Icon	Description
	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 worst of the two Cisco Radio colors determines the color of the large triangular pointer.
     	The icon with a red “x” on the top half (optional 802.11a) shows that the indicated Cisco Radio has been administratively disabled. The rest of the color coding is as described previously in this table. There are six possibilities as shown.

Each of the access point icons includes a small black arrow that indicates the direction in which the internal Side A antenna points.

The following table shows some arrow examples used in the Cisco WCS user interface map displays.

Table 5-8 Arrows

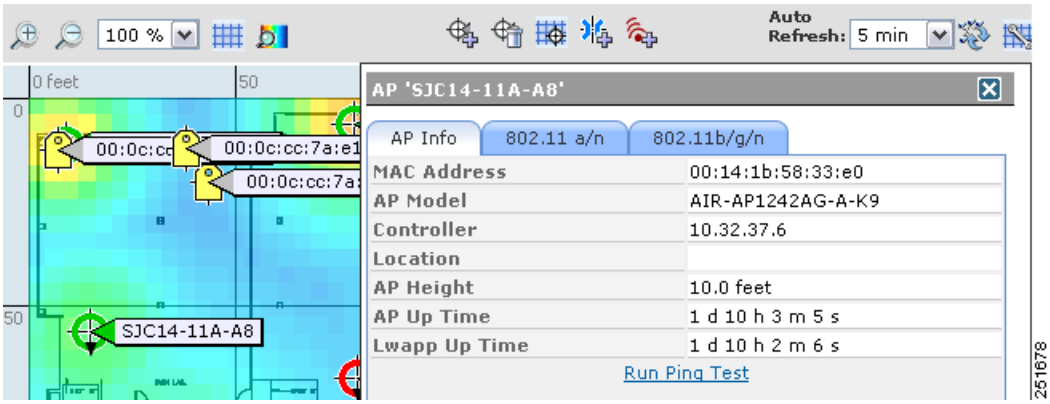
Arrow Examples	Direction
	Zero degrees, or to the right of the map.
	45 degrees, or to the lower right on the map.
	90 degrees, or down on the map.
These examples show the first three 45-degree increments allowed, with an additional five at 45-degree increments.	

Access Point Details

Hold your mouse cursor over an access point icon to view access point details (Figure 5-44). 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.

Figure 5-44 Access Point Details Page



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 (Figure 5-45) 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 may not match the total number of clients.

- Receiving and transmitting utilization percentages
- Channel utilization percentage

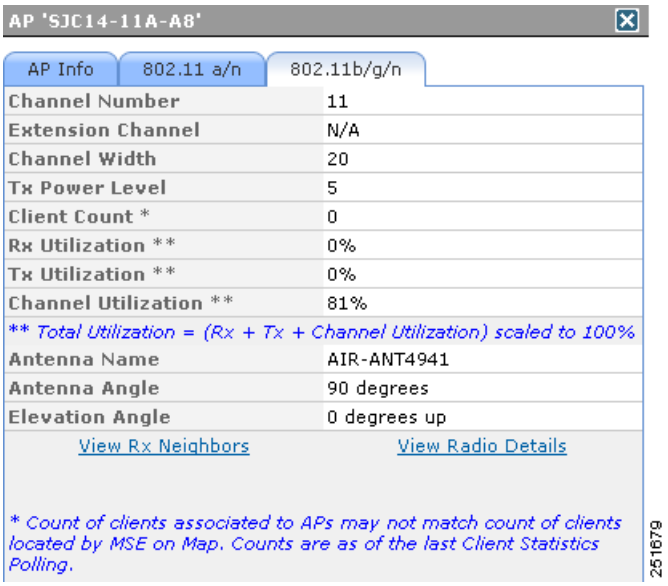
Note Total utilization = (Rx + Tx + Channel utilization) scaled to 100%.

- 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.

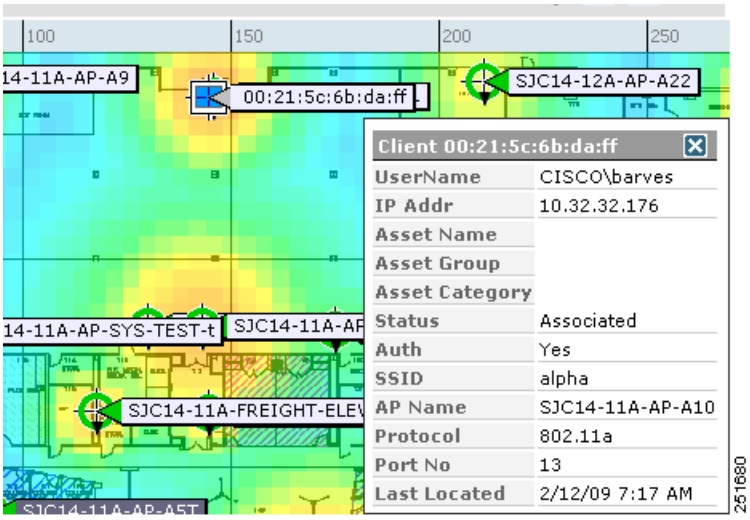
Figure 5-45 802.11 Tabs



Client Details

Hold your mouse cursor over a client icon to view client details (Figure 5-46).

Figure 5-46 Client Details Page



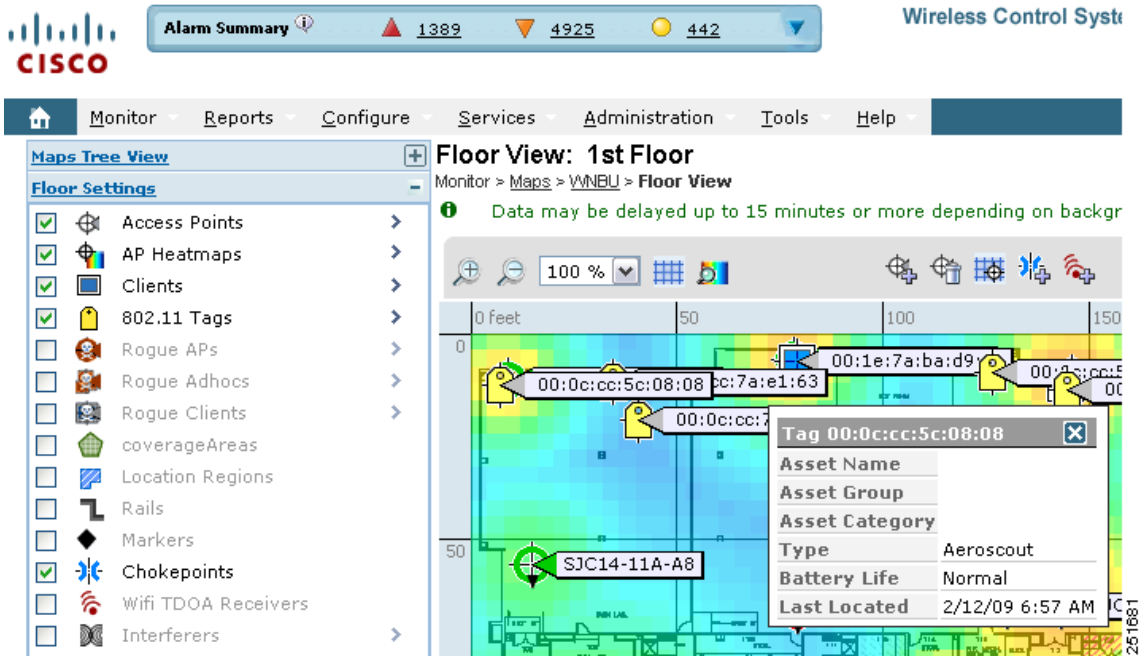
Client details information includes the following:

- Username
- IP address
- Asset name, group, and category
- Status
- Auth
- SSID
- Access point name
- Protocol
- Port number
- Last location

Tag Details

Hold your mouse cursor over a tag icon to view tag details (Figure 5-47).

Figure 5-47 Tag Details Page



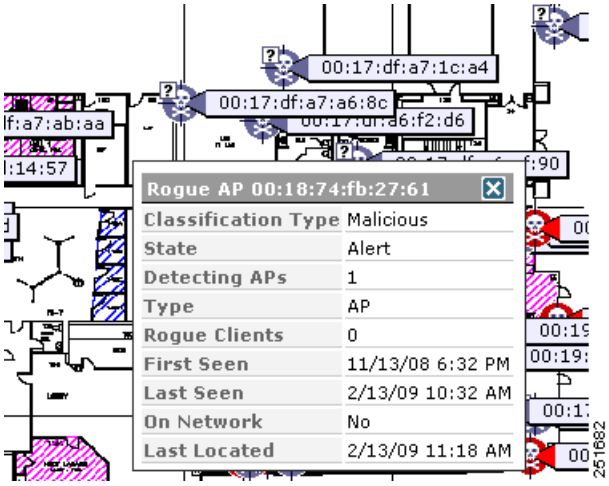
Tag details include:

- Asset name, group, and category
- Type
- Battery life
- Last located

Rogue Access Point Details

Hold your mouse cursor over an access point icon to view rogue access point details (Figure 5-48).

Figure 5-48 Rogue Access Point Details Page



Rogue access point details include:

- Classification type—Friendly, malicious, or unknown.
- State
- Detecting access points
- Type
- Rogue clients
- First seen
- Last seen
- On network
- Last located

Rogue Adhoc Details

Hold your mouse cursor over an access point icon to view rogue ad hoc details.

Rogue Client Details

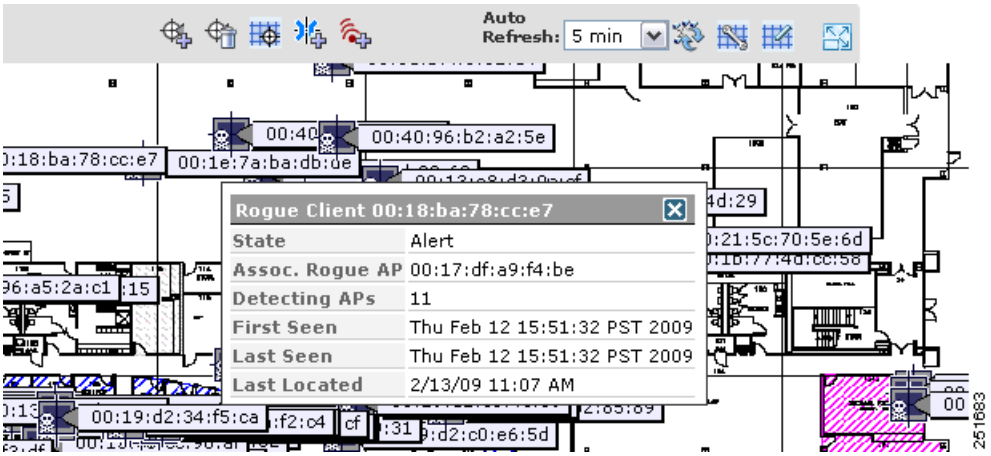
Hold your mouse cursor over an access point icon to view rogue client details (Figure 5-49).

Interferer Details

Hover your mouse cursor over an interferer icon to view its details.
Interferer details include 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.

Figure 5-49 Rogue Client Details Page



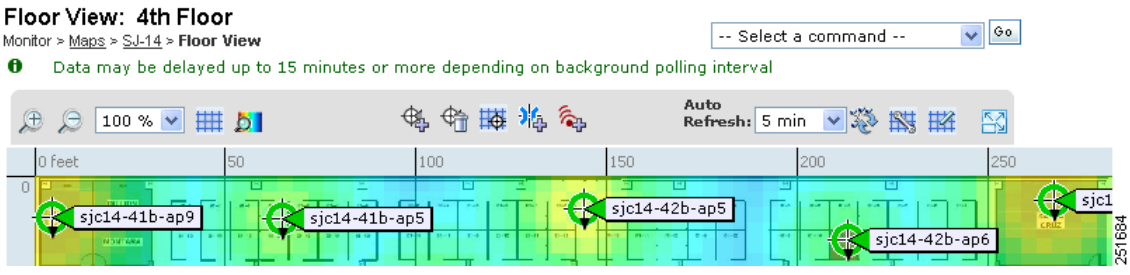
Rogue client details include:

- State
- Associated rogue access point
- Detecting access points
- First seen
- Last seen
- Last located

Floor View Navigation

The main Floor View navigation toolbar (Figure 5-50) provides access to multiple map functions.

Figure 5-50 Floor View Navigation Toolbar



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—Use the map size drop-down list to manually select the map view size (ranging from 50% to 800%).
- Show Grid—Click to show or hide the grid that displays distance in feet on the map.

- RSSI Legend—Hold 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. See the "Adding Access Points" section on page 5-44 for more information.
- 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. See "Placing Access Points" section on page 5-49 for more information.
- Add Chokepoints—Click to open the Add Chokepoints page. See the *Cisco Context-Aware Services Configuration Guide* for more information.
- Add WiFi TDOA Receivers—Click to open the Add Wi-Fi TDOA Receivers page. See the *Cisco Context-Aware Services Configuration Guide* for more information.
- Auto Refresh—From the drop-down list, select 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 page. See the "Understanding RF Heatmap Calculation" section on page 5-34 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.

Select a Command for Floor Areas

The following Floor Map functions are accessible from the Select a Command drop-down list located in the Floor View page of WCS.

- Adding Access Points—Select **Add Access Points**, and click **Go**. In the Add Access Points page, select the check boxes of the access points that you want to add and click **OK**. See the "Adding Access Points" section on page 5-44 for more information.
- Positioning Access Points—Select **Position Access Points**, and click **Go** to open the Position Access Points page. Move the access points to the desired position on the map using the mouse and click **Save**. See "Placing Access Points" section on page 5-49 for more information.
- Removing Access Points—Select **Remove Access Points**, and click **Go**. In the Remove Access Points page, select the check boxes of the access points that you want to remove and click **OK**.
- Adding Chokepoints—See the *Cisco Context-Aware Services Configuration Guide* for more information.
- Adding WiFi TDOA Receivers—See the *Cisco Context-Aware Services Configuration Guide* for more information.
- Reference Tags—Select to open the Reference Tag Calibration Settings page. See the *Cisco Context-Aware Services Configuration Guide* for more information.
- Editing the Floor Area—See the "Editing Floor Areas" section on page 5-72 for more information.
- Deleting the Floor Area—See the "Deleting Floor Areas" section on page 5-72 for more information.
- Editing Location Presence Information—See the "Managing Location Presence Information" section on page 5-16 for more information.
- Recomputing the RF Prediction— Select **Recompute RF Prediction**, and click **Go**.

- Refreshing the Floor Area Map—Select **Refresh from Network**, and click **Go**.
- Map Editor—See the "Using the Map Editor" section on page 5-29 for more information.
- Planning Mode—See the "Understanding RF Heatmap Calculation" section on page 5-34 for more information.
- Inspecting Location Readiness—See "Inspecting VoWLAN Location Readiness" section on page 5-43 for more information.
- Inspecting VoWLAN Readiness—See the "Inspecting VoWLAN Location Readiness" section on page 5-43 for more information.

Editing Floor Areas

To edit a current floor area, follow these steps:

Step 1 Choose **Monitor > Maps**.

Step 2 Click the name of the floor area to open its details page.

Step 3 From the Select a command drop-down list, choose **Edit Floor Area**.

Step 4 Make any necessary changes to Floor Area Name, Contact, Floor, Floor Height (feet), Floor Type (RF Model), Existing Image File, or Import New Image File.

Step 5 Click **OK**.

Deleting Floor Areas

To delete a current floor area, follow these steps:

Step 1 Choose **Monitor > Maps**.

Step 2 Click the check box for the applicable floor area.

Step 3 From the Select a command drop-down list, choose **Delete Maps**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Refresh Options

To prepare for monitoring your wireless LANs, become familiar with the various refresh options for a map.

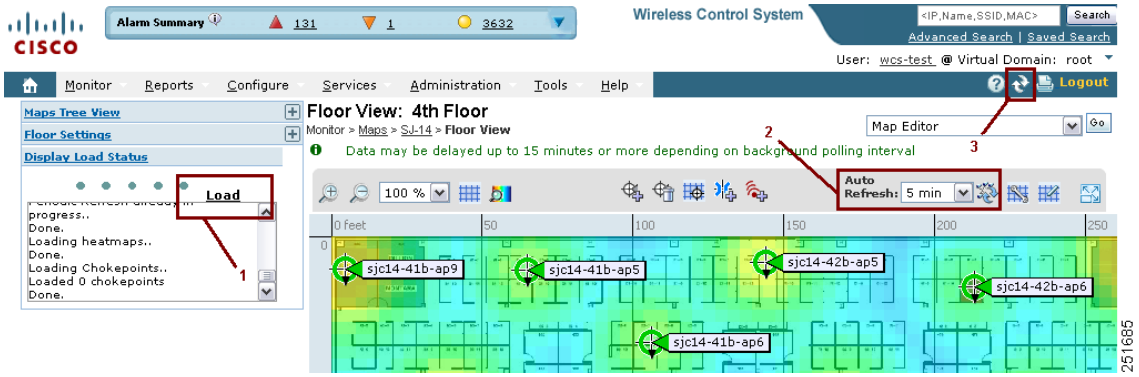
- Load—The Load option in the left sidebar menu refreshes map data from the WCS database on demand (see callout 1 in Figure 5-51).
- Auto Refresh—The Auto Refresh option (see callout 2 in Figure 5-51) provides an interval drop-down list to set how often to refresh the map data from the database.

- Refresh from network—By clicking the **Refresh from network** icon to the right of the Auto Refresh drop-down list (see callout 2 in Figure 5-51), you can refresh the map status and statistics directly from the controller through an SNMP fetch rather than polled data from the WCS 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.

- Refresh browser—Above the map next to the Logout and Print option is another refresh option (see callout 3 in Figure 5-51). Clicking this refreshes the complete page, or the map and its status and statistics if you are on a map page.

Figure 5-51 Refresh Options



Creating a Network Design

After access points have been installed and have joined a controller, and WCS has been configured to manage the controllers, set up a network design. A *network design* is a representation within WCS 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, in order to track devices in that environment. The concept and steps to perform synchronization between WCS and the mobility service engine are explained in the *Cisco 3350 Mobility Services Engine Configuration Guide*.

Designing a Network

Follow these steps to design a network.

Step 1 Open the WCS web interface and log in.

Note To create or edit a network design, you must log into WCS and have SuperUser, Admin, or ConfigManager access privileges.

Step 2 Choose **Monitor** > **Maps**.

Step 3 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.

Step 4 Click **Go**.

Step 5 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.

Note You can use the Browse... button to navigate to the location.

Step 6 Click **Next**.

Step 7 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 image file's aspect ratio. 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.

Step 8 Click **OK**.

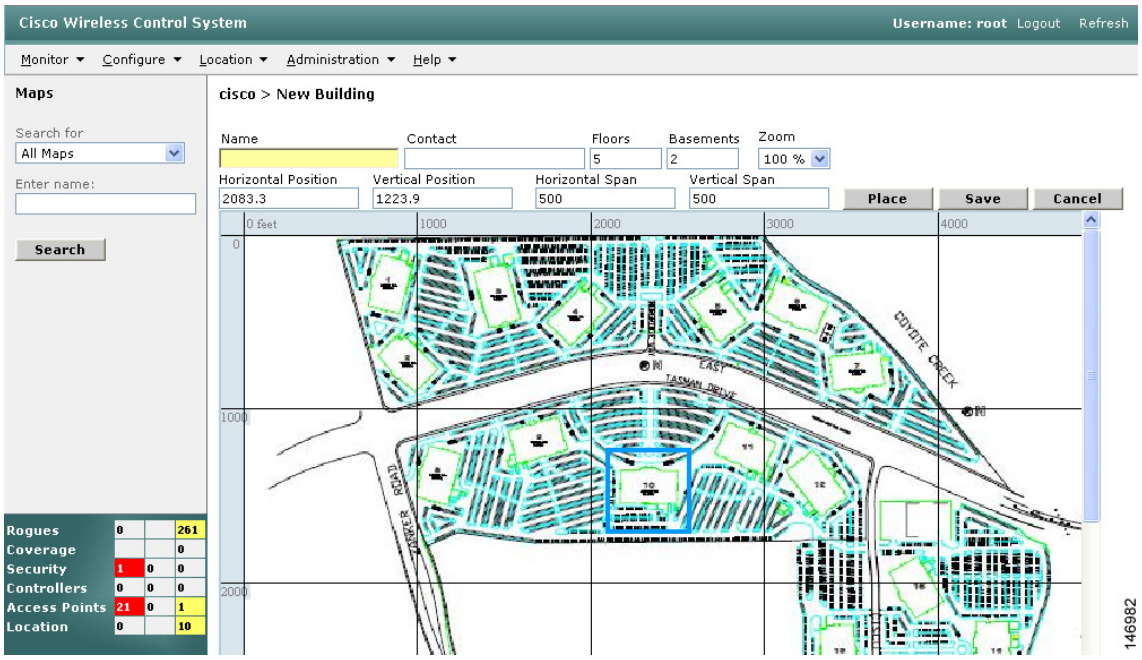
Step 9 On the Monitor > Maps page, click the hyperlink associated with the above-made campus map. A page showing the new campus image is displayed.

Step 10 From the drop-down list on the upper right of the page, select **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**.

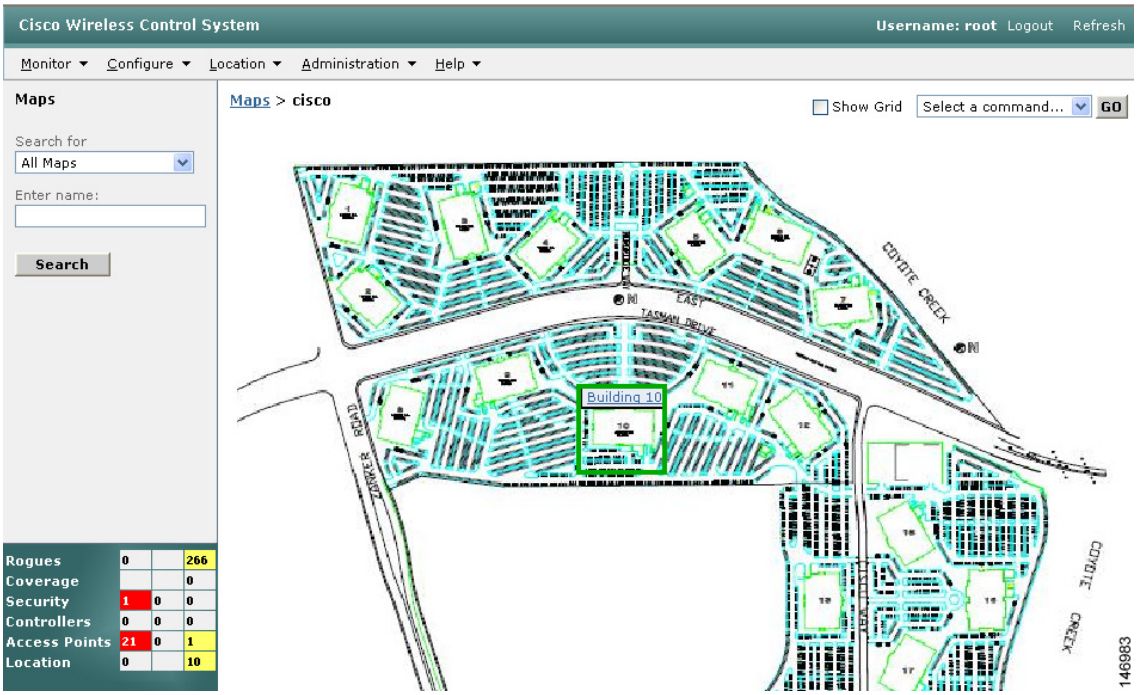
Step 12 Indicate which building on the campus map is the correct building by clicking the blue box in the upper left of the campus image and dragging it to the intended location (see Figure 5-52). To resize the blue box, hold down the **Ctrl** key and click and drag to adjust its horizontal size. You 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 on it and dragging it to the desired location. Click **Save**.

Figure 5-52 Repositioning Building Highlighted in Blue



Step 13 WCS is then returned to the campus image with the newly created building highlighted in a green box. Click the **green box** (see Figure 5-53).

Figure 5-53 Newly Created Building Highlighted in Green



Step 14 To create a building without a campus, choose **New Building**, and click **Go**.

Step 15 Enter the building's name, contact information, number of floors and basements, and dimension information. Click **Save**. WCS is returned to the Monitor > Maps page.

Step 16 Click the hyperlink associated with the newly created building.

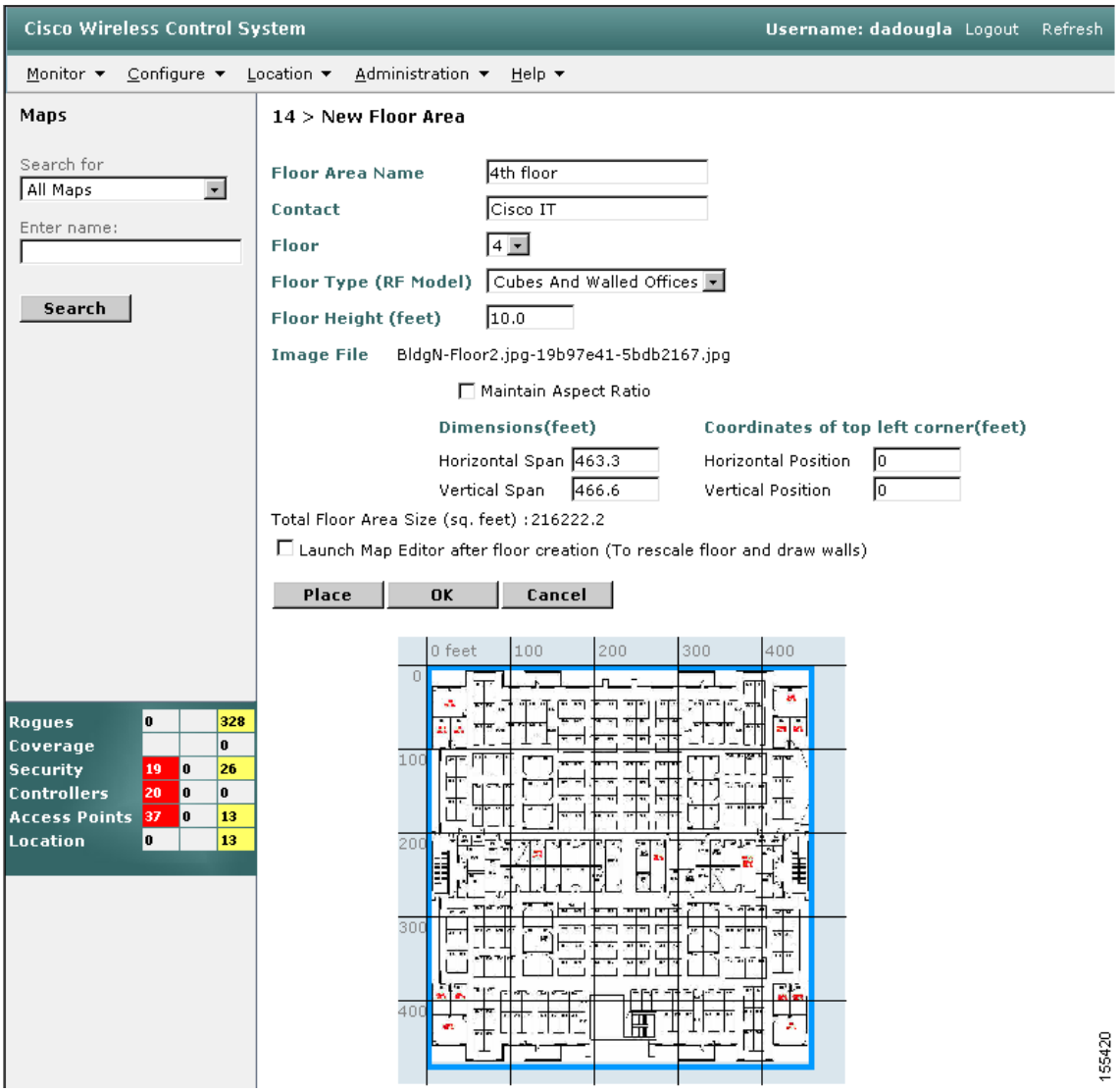
Step 17 On the Monitor > Maps > [Campus Name] > [Building Name] page, go to the drop-down list and choose **New Floor Area**. Click **Go**.

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 boxes 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 (see Figure 5-54). After making changes to any numerical values, click **Place**.

Figure 5-54 Repositioning Using Numerical Value Fields



Step 20 Adjust the floor's characteristics with the WCS map editor by choosing 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 5-29.

Step 21 At the new floor's image page (Monitor > 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 WCS 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 access point's 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.)

Step 24 To adjust the directional arrow, choose the appropriate orientation in the Antenna Angle drop-down list. Click **Save** when you are finished placing and adjusting each access point's direction.

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 the above processes to create campuses, buildings, and floors until each device location is properly detailed in a network design.

Changing Access Point Positions by Importing and Exporting a File

You can change an access point position by importing or exporting a file. The file contains only the lines describing the access point you want to move. This option takes less time than manually changing multiple access point positions. Follow these steps to change access point positions using the importing or exporting of a file.

Step 1 Choose **Monitor > Maps**.

Step 2 From the Select a command drop-down list, choose **Import AP/WiFi TDOA Receiver/Chokepoint Placement or Export AP/WiFi TDOA Receiver/Chokepoint Placement**, and click **Go**.

Step 3 In Import Data from File or Export Data from File, click **Browse** to find the file you want to import. The file in the [BuildingName], [FloorName], [APName], (aAngle), (bAngle), [X], [Y], ([aAngleElevation, bAngleElevation, Z]), (aAntennaType, aAntennaMode, (aAntennaPattern, (aAntennaGain)), bAntennaType, bAntennaDiversity, (bAntennaPattern, bAntennaGain)) format must have already been created and added to WCS. (See the "Inspecting VoWLAN Location Readiness" section on page 5-43.)

Note The parameters in square brackets are mandatory, and those in parentheses are optional.

Note Angles must be entered in radians (X,Y), and the height is entered in feet. The aAngle and bAngle range is from –2Pi (-6.28...) to 2Pi (6.28...), and the elevation ranges from –Pi (-3.14...) to Pi (3.14...).

Step 4 Click **Import**. The RF calculation takes approximately two seconds per access point.

Importing or Exporting WLSE Map Data

When you convert an access point from autonomous to CAPWAP and from WLSE to WCS, one of the conversion steps is to manually re-enter the access point information into WCS. This can be a time-consuming step. To speed up the process, you can export the information about access points from WLSE and import it into WCS.

Note WCS 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, WCS 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 WCS 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 > 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 section, click **Browse** to select the file to import.

Step 4 Find and select the .tar file to import and click **Open**.

WCS displays the name of the file in the Import From field.

Step 5 Click **Import**.

WCS 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, WCS prompts you to correct the problem and retry. After the file has been loaded, WCS displays a report of what will be added to WCS. The report also specifies what cannot be added and why.

If some of the data to be imported already exists, WCS 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 a WCS campus (or top-level building) and building combination, WCS 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.

WCS displays a report indicating what was imported.

Note Since a WLSE file has no floor number information, the structure of the floor index calculation after WLSE is imported into WCS is in descending order. You can click the floor image to go directly to the appropriate floor screen.

Step 7 Choose **Monitor > Maps** to verify the imported data.

CHAPTER 6

Monitoring Wireless Devices

This chapter describes how to use Cisco WCS to monitor your wireless LANs. It contains these sections:

- Rogue Access Point Location, Tagging, and Containment, page 6-1
- Configuring ACS View Server Credentials, page 6-2
- Receiving Radio Measurements, page 6-2
- Monitoring Mesh Networks Using Maps, page 6-3
- Mesh Statistics for an Access Point, page 6-15
- Viewing the Mesh Network Hierarchy, page 6-19
- Monitoring Channel Width, page 6-23
- Viewing Clients Identified as WGBs, page 6-28
- Retrieving the Unique Device Identifier on Controllers and Access Points, page 6-29
- Coverage Hole, page 6-32
- Viewing DHCP Statistics, page 6-34
- Guest User Monitoring, page 6-36
- RRM Dashboard, page 6-36

Rogue Access Point Location, Tagging, and Containment

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.

Configuring ACS View Server Credentials

In order to facilitate communication between WCS and the ACS View Server and to access the ACS View Server tab, you must add a view server with credentials. Follow these steps to configure the ACS View Server Credentials.

Note WCS only supports ACS View Server 5.1 or above.

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 that will be attempted.

Step 5 Click **Submit**.

Receiving Radio Measurements

On 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.

Step 1 Choose **Monitor > Clients**.

Step 2 Choose a client from the Client User Name column.

Step 3 From the Select a command drop-down list, choose **Radio Measurement**.

Note Only associated Cisco Compatible Extension clients using version 2.0 or greater have this option.

Step 4 Click the check box to indicate if you want to specify beacon measurement, frame measurement, channel load, or noise histogram. The different measurements produce differing results:

- 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 the serving access point's 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 present 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
  - CCA busy fraction—The fractional duration over which CCA indicated the channel was busy during the measurement duration defined as ceiling (255 times the duration the CCA indicated channel was busy divided by measurement duration)
- Noise Histogram
  - Channel—The channel number for this measurement
  - RPI density in each of the eight power ranges

Step 5 Click **Perform Measurement** to initiate the measurement.

The measurements take about 5 msec to perform. A message from WCS indicates the progress. If the client chooses not to perform the measurement, that is also communicated.

Monitoring Mesh Networks Using Maps

You can access and view details for the following elements from a mesh network map in Cisco WCS:

- Mesh Link Statistics
- Mesh Access Points
- Mesh Access Point Neighbors

Details on how this information is accessed and the information displayed for each of these items is detailed in the following sections.

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 from the Monitor > Maps display.

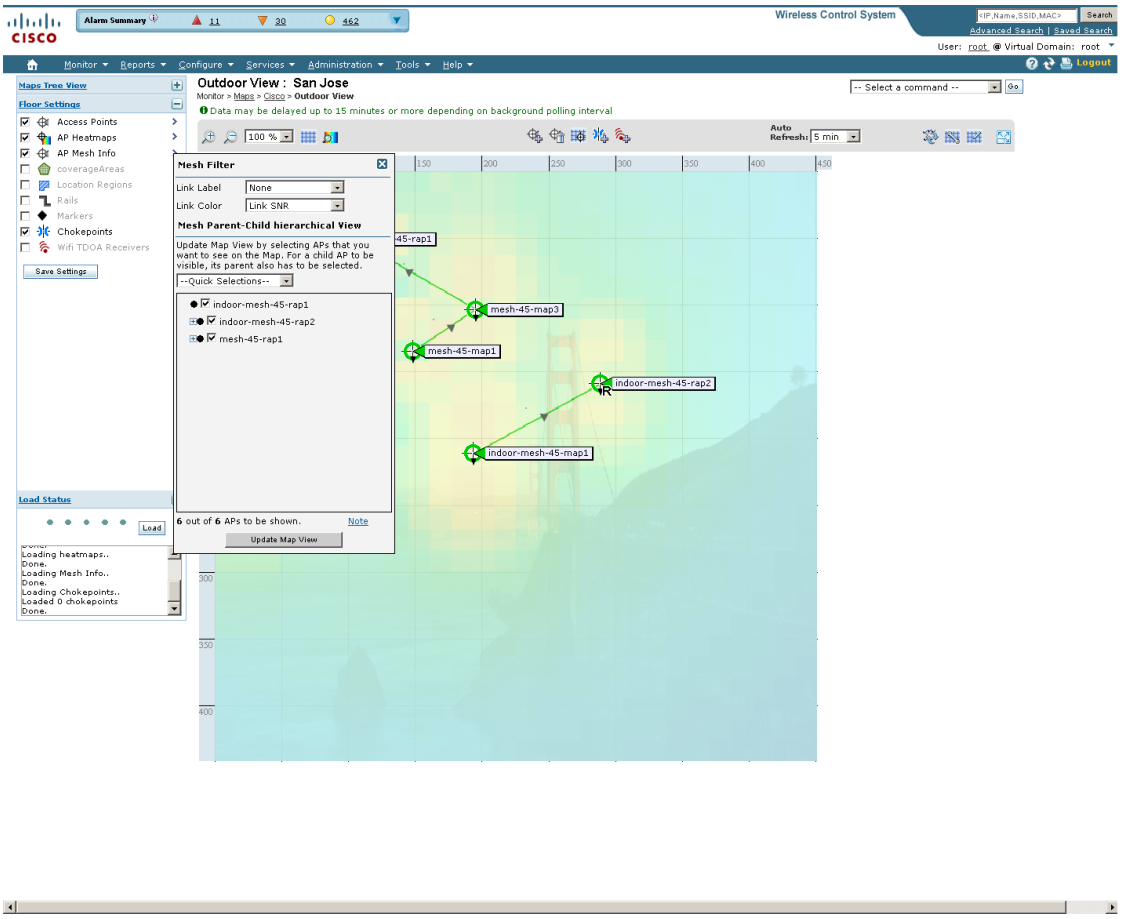
To view details on a specific mesh link between two mesh access points or a mesh access point and a root access point, do the following:

Step 1 Choose **Monitor > Maps**.

Step 2 Click the **Map Name** that corresponds to the outdoor area, campus, building, or floor you want to monitor.

Step 3 Click the arrow to the right of AP Mesh Info in the left sidebar menu (see Figure 6-1). A Mesh Filter dialog box appears.

Figure 6-1 Mesh Filter Page



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 6-1 summarizes the parameters that display.

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.

The following Bridging Link information displays:

Table 6-1 Bridging Link Information

Parameter	Description
Information fetched on	Date and time that information was compiled.
Link SNR	Link signal-to-noise ratio (SNR).
Link Type	Hierarchical link relationship.
SNR Up	Signal-to-noise radio for the uplink (dB).
SNR Down	Signal-to-noise radio for the downlink (dB).
PER	The packet error rate for the link.
Tx Parent Packets	The TX packets to a node while acting as a parent.
Rx Parent Packets	The RX packets to a node while acting as a parent.
Time of Last Hello	Date and time of last hello.

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.

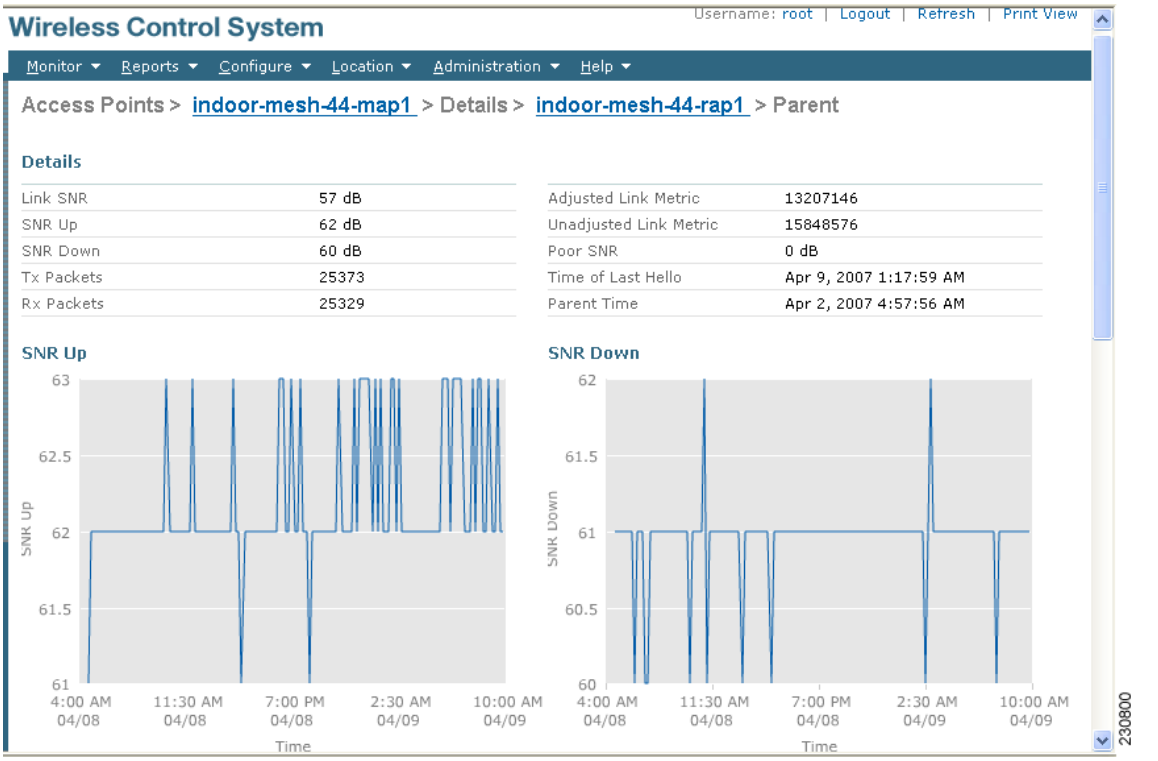
Note You cannot run link tests for both links (child-to-parent and parent-to-child) at the same time.

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 (see Figure 6-2).

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 is the ease to get to 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.

Figure 6-2 Mesh SNR Graphs Page (Top)



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
- Channel

Note This information is in addition to the information shown for all access points (MAC address, access point model, controller IP address, location, height of access point, access point up time, and LWAPP up time).

Note You can also view detailed configuration and access alarm and event information from the map. For detailed information on the Alarms and Events displayed, refer to the "Alarm and Event Dictionary" section on page 16-26.

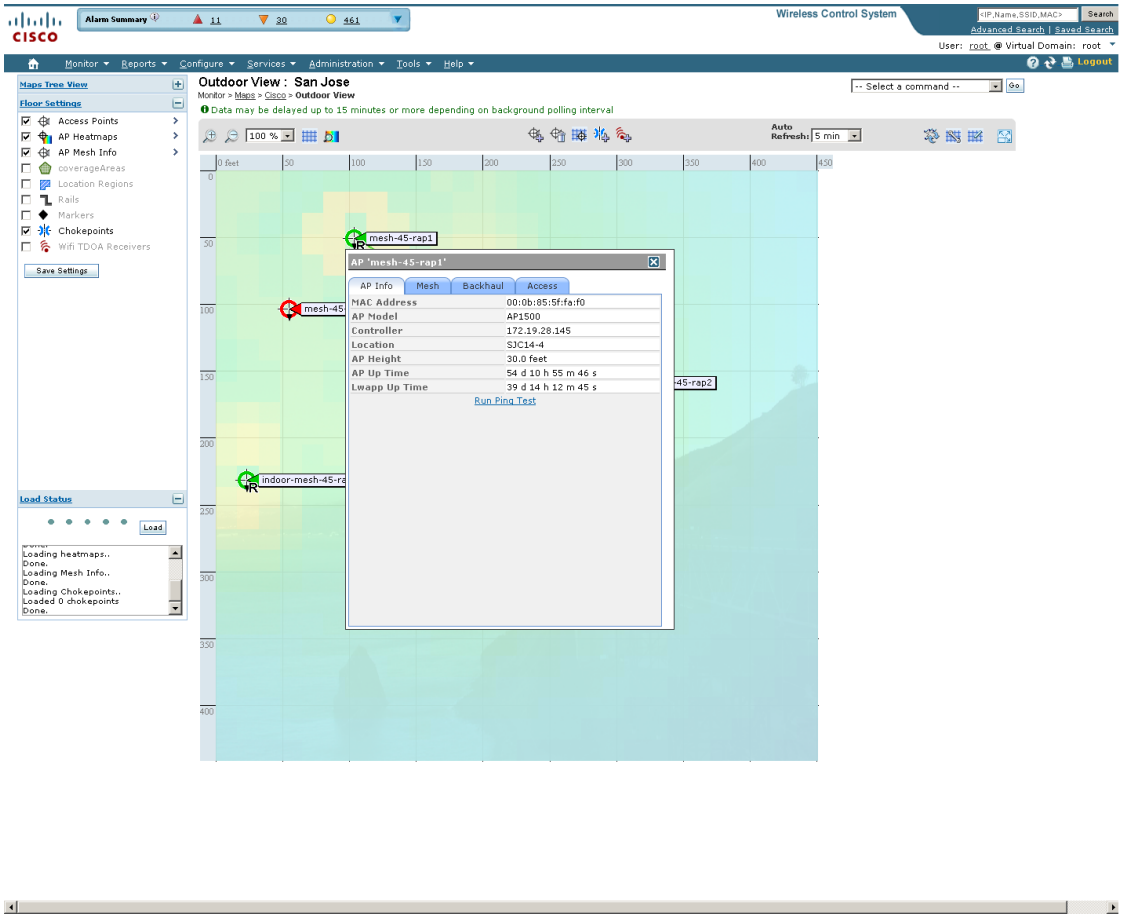
To view summary and detailed configuration information for a mesh access point from a mesh network map, do the following:

Step 1 In Cisco WCS, choose **Monitor > 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, move the cursor over the access point that you want to monitor. A dialog box page with configuration information for the selected access point appears (see Figure 6-3).

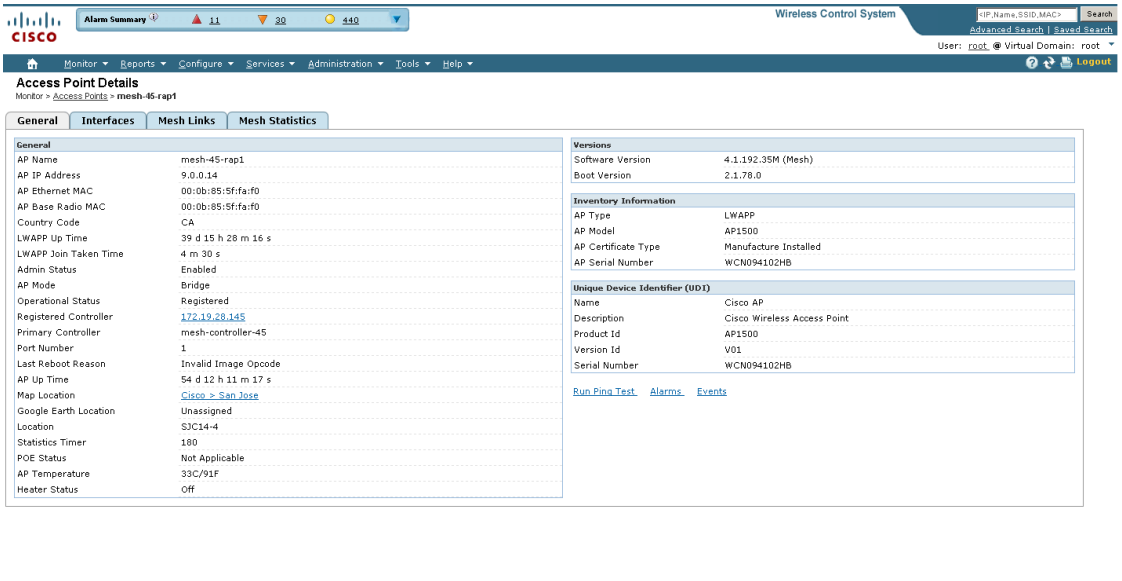
Figure 6-3 Mesh AP Summary Dialog Box



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 appears (see Figure 6-4).

Note For more details on the View Mesh Neighbors link in the access point dialog box (see Figure 6-3), see the "Monitoring Mesh Access Point Neighbors Using Maps" section on page 6-8. If the access point has an IP address, a Run Ping Test link is also visible at the bottom of the mesh access point panel.

Figure 6-4 Mesh AP Detail Page



251691

Step 5 In the Access Point configuration page, follow these steps to view configuration details for the mesh access point.

a. Choose the **General** tab to view the overall configuration of the mesh access point such as 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 the letter *m* and the word *mesh* in parentheses.

b. Choose the **Interface** tab to view configuration details for the interfaces supported on the mesh access point. Interface options are radio and Ethernet.

c. Choose the **Mesh Links** tab to view parent and neighbors' 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. Choose 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, refer to the "Mesh Statistics for an Access Point" section on page 6-15.

Monitoring Mesh Access Point Neighbors Using Maps

To view details on neighbors of a mesh access point from a mesh network map, do the following:

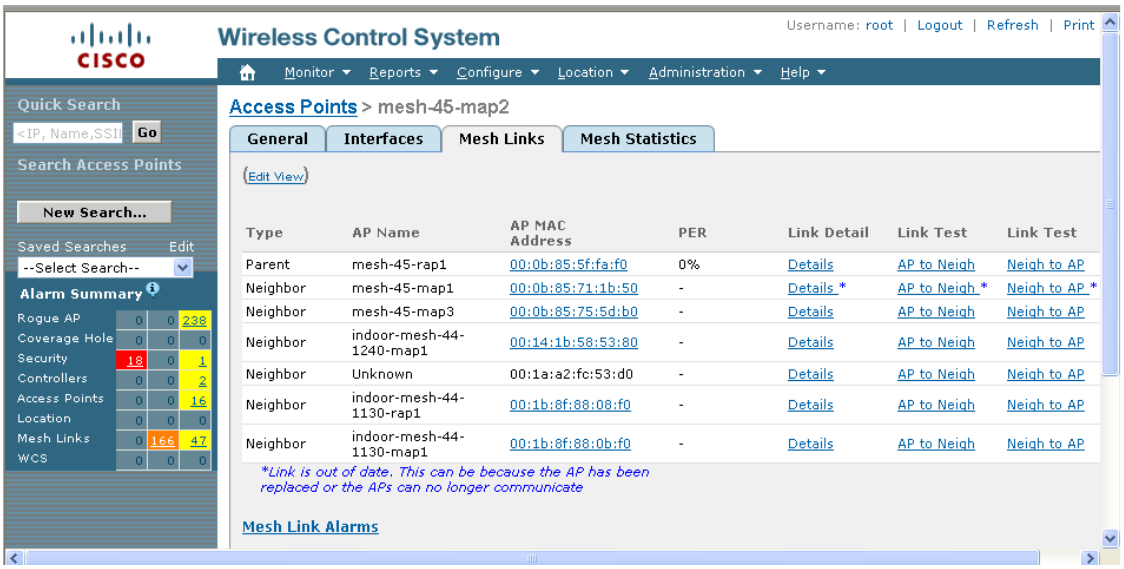
Step 1 Choose **Monitor > Maps**.

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 screen appears.

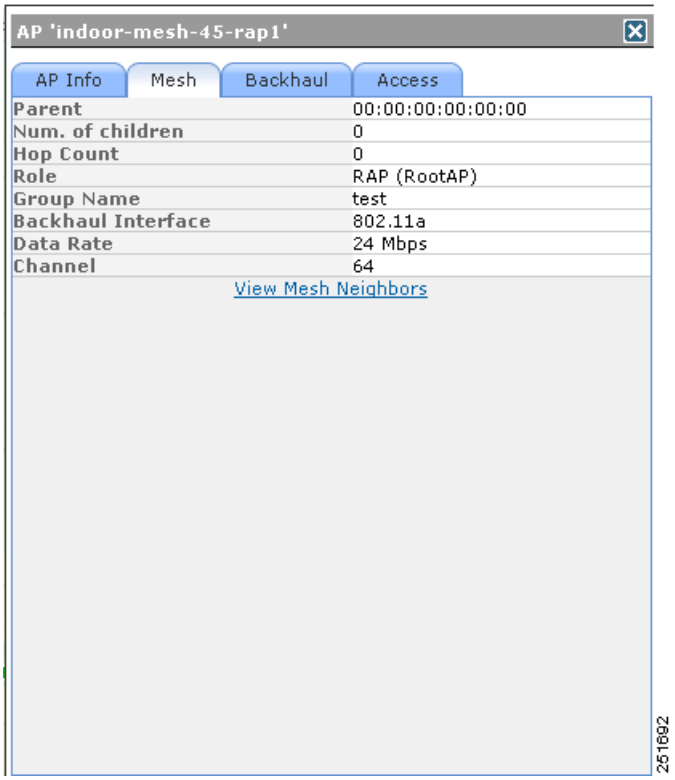
Step 4 Click the **Mesh Links** tab (see Figure 6-5).

Figure 6-5 Access Points > Mesh Links Page



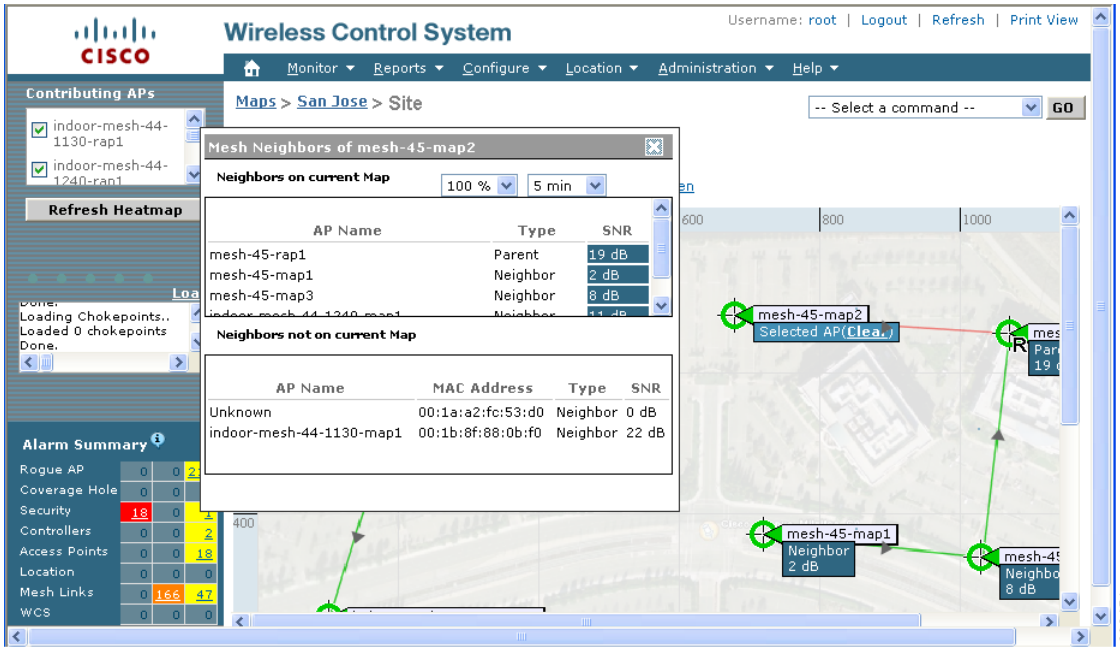
Note You can also view mesh link details for neighbors of a selected access point by clicking on the **View Mesh Neighbors** link from the Mesh tab of the access point configuration summary page, which displays when you mouse over an access point on a map (see Figure 6-6).

Figure 6-6 Access Point Configuration Summary Dialog Box



Note Signal-to-noise (SNR) appears on the View Mesh Neighbors page (see Figure 6-7).

Figure 6-7 View Mesh Neighbors Dialog Box



Note In addition to listing the current and past neighbors in the panel that displays, 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. Select 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 (5 mins). You can modify these default values.

Monitoring Mesh Health

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.

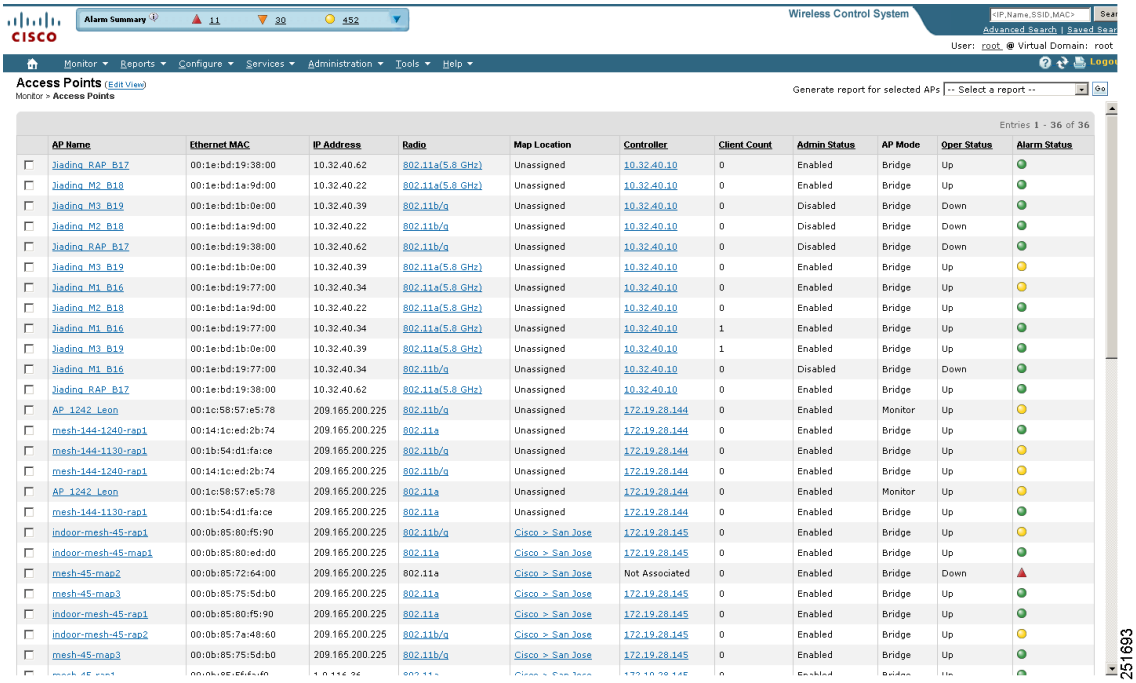
To view the mesh health details for a specific mesh access point, follow these steps.

Step 1 Choose **Monitor > Access Points**. A listing of radios belonging to access points appears (see Figure 6-8).

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 shown below. With the New Search option, you can further define the criteria of the access points that display. Search criteria include AP Type, AP Mode, Radio Type, and 802.11n Support.

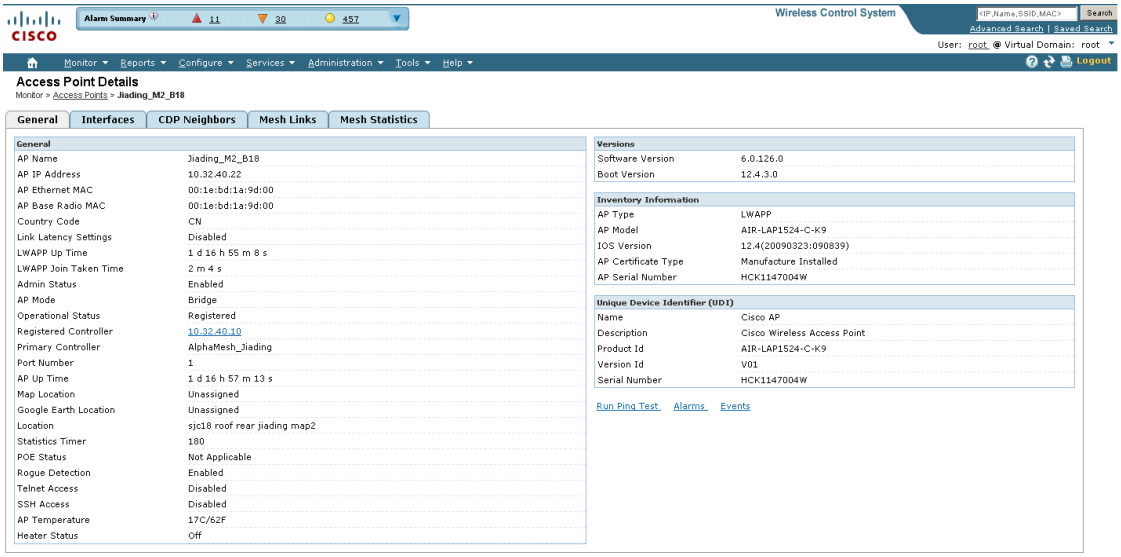
Figure 6-8 Monitor > Access Points



Step 2 Click the AP Name link to display details for that mesh access point. The General tab for that mesh access point appears (see Figure 6-9).

Note You can also access the General tab for a mesh access point from a Cisco WCS 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.

Figure 6-9 AP Name > General Properties Tab



To add, remove, or reorder columns in the table, click the Edit View link In the Monitor > Access Points page. Table 6-2 displays optional access point parameters available from the Edit View page.

Table 6-2 Monitor Access Points Additional Search Results Parameters

Column	Options
AP Model	Indicates the model of the access point.
AP Type	Indicates the type of access point (unified or autonomous).
Antenna Azim. Angle	Indicates the horizontal angle of the antenna.
Antenna Diversity	Indicates if antenna diversity is enabled or disabled. Antenna diversity refers to the access point sampling the radio signal from two integrated antenna ports in order to choose the preferred antenna.
Antenna Elev. Angle	Indicates the elevation angle of the antenna.
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.
Antenna Mode	Indicates the antenna mode such as omni, directional, or non-applicable.
Antenna Name	Indicates the antenna name or type.
Antenna Type	Indicates whether the antenna is internal or external.

Table 6-2 Monitor Access Points Additional Search Results Parameters (continued)

Column	Options
Audit Status	Indicates one of the following audit statuses: • Mismatch—Config differences were found between WCS and controller during the last audit. • Identical—No config differences were found during the last audit. • Not Available—Audit status is unavailable.
Base Radio MAC	Indicates the radio's MAC address.
Bridge Group Name	Indicates the name of the bridge group used to group the access points, if applicable.
CDP Neighbors	Indicates all directly connected Cisco devices.
Channel Control	Indicates whether the channel control is automatic or custom.
Channel Number	Indicates the channel on which the Cisco radio is broadcasting.
Controller Port	Indicates the number of controller ports.
Google Earth Location	Indicates whether a Google Earth location is assigned.
Location	The physical location of the access point.
Node Hops	Indicates the number of hops between access point.
OfficeExtend AP	Specifies if OfficeExtend AP is enabled or disabled. If it is disabled, the access point is remotely deployed, which increases the security risk.
POE Status	Indicates the Power-over-Ethernet status of the access point. The possible values include: • Low—The access point draws low power from the Ethernet. • Lower than 15.4 volts—The access point draws lower than 15.4 volts from the Ethernet. • Lower than 16.8 volts—The access point draws lower than 16.8 volts from the Ethernet. • Normal—The power is high enough for the operation of the access point. • Not Applicable—The power source is not from the Ethernet.
Primary Controller	Indicates the name of the primary controller for this access point.
Reg. Domain Supported	Indicates whether or not the regulatory domain is supported.
Serial Number	Indicates the access point's serial number.
Slot	Indicates the slot number.
Tx Power Control	Indicates whether the transmission power control is automatic or custom.
Tx Power Level	Indicates the transmission power level.
Up Time	Indicates how long the access point has been up in days, hours, minutes, and seconds.

Table 6-2 Monitor Access Points Additional Search Results Parameters (continued)

Column	Options
WLAN Override Names	Indicates the WLAN override profile names.
WLAN Override	Indicates whether WLAN Override is enabled or disabled. Each access point is limited to sixteen 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.

Mesh Statistics for an Access Point

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 (see Figure 6-8).

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 access point summary. With the New Search option, you can further define the criteria of the access points that display. Search criteria include AP Name, IP address, MAC address, Controller IP or Name, Radio type, and Outdoor area.

Step 2 Click the **AP Name** link of the target mesh access point.

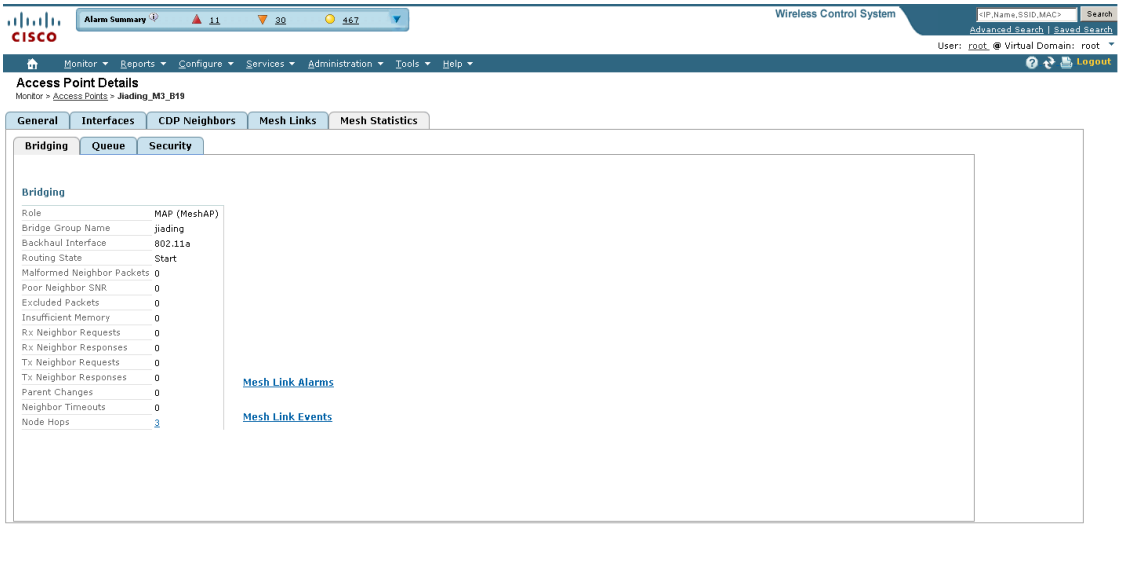
A tabbed page appears and displays the General Properties page for the selected access point.

Step 3 Click the **Mesh Statistics** tab (see Figure 6-10). 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.

Note You can also access the Mesh Securities page for a mesh access point from a Cisco WCS map. To display the page, double-click the mesh access point label.

Figure 6-10 Monitor > Access Points > AP Name > Mesh Statistics



Summaries of the Bridging, Queue and Security Statistics and their definitions are provided in Table 6-3, Table 6-4 and Table 6-5 respectively.

Table 6-3 Bridging Mesh Statistics

Parameter	Description
Role	The role of the mesh access point. Options are mesh access point (MAP) and root access point (RAP).
Bridge Group Name	The name of the bridge group to which the MAP or RAP is a member. Assigning membership in a bridge group name is recommended. If one is not assigned, a MAP is by default assigned to a default bridge group name.
Backhaul Interface	The radio backhaul for the mesh access point.
Routing State	The state of parent selection. Values that display are seek, scan and maint. Maint displays when parent selection is complete.

Table 6-3 Bridging Mesh Statistics (continued)

Parameter	Description
Malformed Neighbor Packets	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.
Poor Neighbor SNR	The number of times the signal-to-noise ratio falls below 12 dB on the backhaul link.
Excluded Packets	The number of packets received from excluded neighbor mesh access points.
Insufficient Memory	The number of insufficient memory conditions.
RX Neighbor Requests	The number of broadcast and unicast requests received from the neighbor mesh access points.
RX Neighbor Responses	The number of responses received from the neighbor mesh access points .
TX Neighbor Requests	The number of unicast and broadcast requests sent to the neighbor mesh access points.
TX Neighbor Responses	The number of responses sent to the neighbor mesh access points.
Parent Changes	The number of times a mesh access point (child) moves to another parent.
Neighbor Timeouts	The number of neighbor timeouts.
Node Hops	The number of hops between the MAP and the RAP. Click the value link to display a sub-panel 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.

Table 6-4 Queue Mesh Statistics

Parameter	Description
Silver Queue	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.
Gold Queue	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.
Platinum Queue	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.

Table 6-4 Queue Mesh Statistics (continued)

Parameter	Description
Bronze Queue	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.
Management Queue	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.

Table 6-5 Security Mesh Statistics

Parameter	Description
Packets Transmitted	Summarizes the total number of packets transmitted during security negotiations by the selected mesh access point.
Packets Received	Summarizes the total number of packets received during security negotiations by the selected mesh access point.
Association Request Failures	Summarizes the total number of association request failures that occur between the selected mesh access point and its parent.
Association Request Timeouts	Summarizes the total number of association request time outs that occur between the selected mesh access point and its parent.
Association Request Success	Summaries the total number of successful association requests that occur between the selected mesh access point and its parent.
Authentication Request Failures	Summarizes the total number of failed authentication requests that occur between the selected mesh access point and its parent.
Authentication Request Timeouts	Summarizes the total number of authentication request timeouts that occur between the selected mesh access point and its parent.
Authentication Request Success	Summarizes the total number of successful authentication requests between the selected mesh access point and its parent mesh node.
Reassociation Request Failures	Summarizes the total number of failed reassociation requests between the selected mesh access point and its parent.
Reassociation Request Timeouts	Summarizes the total number of reassociation request timeouts between the selected mesh access point and its parent.

Table 6-5 Security Mesh Statistics (continued)

Parameter	Description
Reassociation Request Success	Summarizes the total number of successful reassociation requests between the selected mesh access point and its parent.
Reauthentication Request Failures	Summarizes the total number of failed reauthentication requests between the selected mesh access point and its parent.
Reauthentication Request Timeouts	Summarizes the total number of reauthentication request timeouts that occurred between the selected mesh access point and its parent.
Reauthentication Request Success	Summarizes the total number of successful reauthentication requests that occurred between the selected mesh access point and its parent.
Invalid Association Request	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.
Unknown Association Requests	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.
Invalid Reassociation Request	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.
Unknown Reassociation Request	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.

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 display on the Map view, by selecting only access points of interest.

To view the mesh network hierarchy for a selected network, do the following:

Step 1 Choose **Monitor > Maps**.

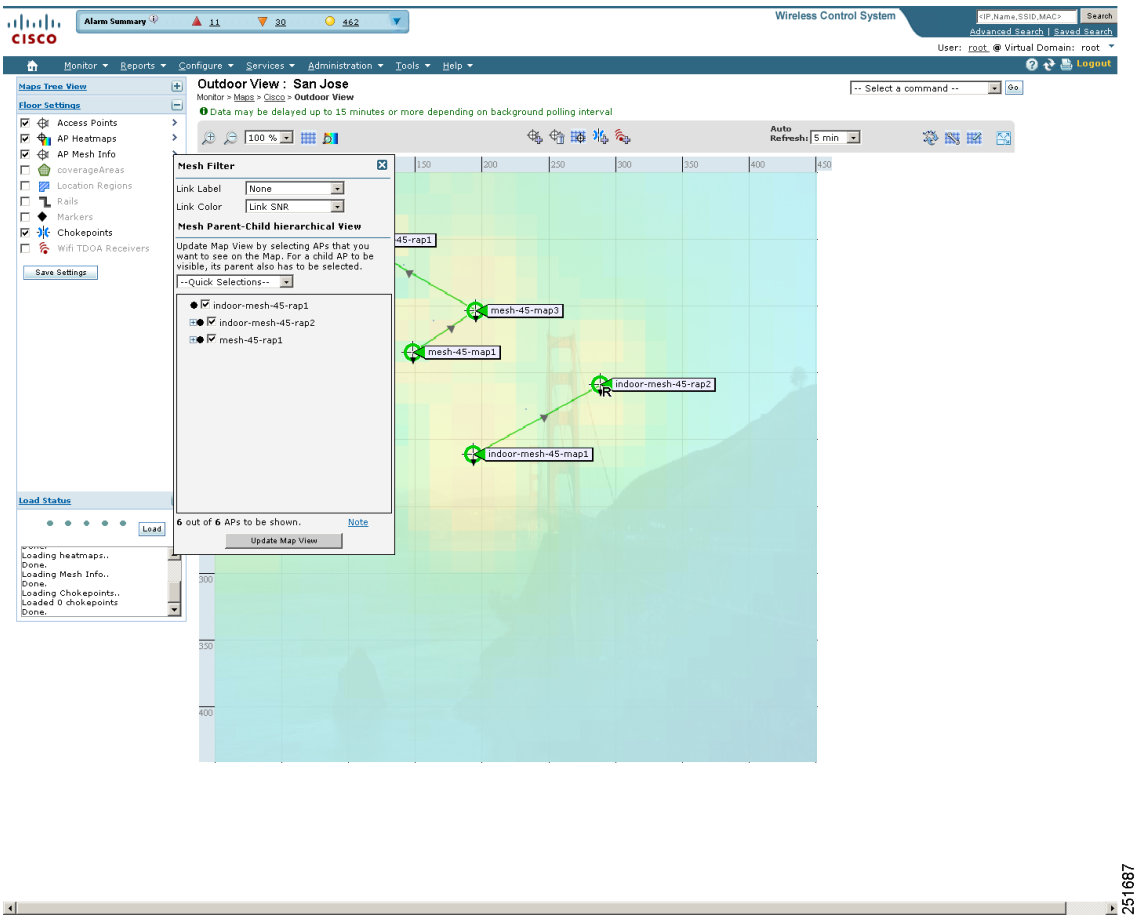
Step 2 Select the map you want to display.

Step 3 Select the **AP Mesh Info** check box in the left sidebar menu if it is not already checked.

Note The AP Mesh Info check box is only selectable if mesh access points are present on the map. It must be checked to view the mesh hierarchy.

Step 4 Click the **AP Mesh Info** arrow to display the mesh parent-child hierarchy (see Figure 6-11).

Figure 6-11 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 displays next to the parent mesh access point entry. For example, in Figure 6-11, the access point, *indoor-mesh-45-rap2*, has only one child, *indoor-mesh-44-map2*.

Step 6 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 6-6 summarizes the parameters that display.

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 6-6 Bridging Link Information

Parameter	Description
Information fetched on	Date and time that information was compiled.
Link SNR	Link signal-to-noise ratio (SNR).
Link Type	Hierarchical link relationship.
SNR Up	Signal-to-noise radio for the uplink (dB).
SNR Down	Signal-to-noise radio for the downlink (dB).
PER	The packet error rate for the link.
Tx Parent Packets	The TX packets to a node while acting as a parent.
Rx Parent Packets	The RX packets to a node while acting as a parent.
Time of Last Hello	Date and time of last hello.

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, select 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, select 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 6-7 defines the different link colors.

Table 6-7 Definition for SNR and Packet Error Rate Link Color

Link Color	Link SNR	Packet Error Rate (PER)
Green	Represents a SNR above 25 dB (high value)	Represents a PER of one percent (1%) or lower
Amber	Represents a SNR between 20 and 25 dB (acceptable value)	Represents a PER that is less than ten percent (10%) and greater than one percent (1%)
Red	Represents a SNR below 20 dB (low value)	Represents a PER that is greater than ten percent (10%)

Note The Link label and color settings are reflected on the map immediately (see Figure 6-12). 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, click the **Quick Selections** drop-down list.

b. Select the appropriate option from the menu. A description of the options is provided in Table 6-8.

Table 6-8 Quick Selection Options

Parameter	Description
Select only Root APs	Choose this setting if you want the map view to display root access points only.
Select up to 1st hops	Choose this setting if you want the map view to display 1st hops only.
Select up to 2nd hops	Choose this setting if you want the map view to display 2nd hops only.
Select up to 3rd hops	Choose this setting if you want the map view to display 3rd hops only.
Select up to 4th hops	Choose this setting if you want the map view to display 4th hops only.
Select All	Select this setting if you want the map view to display all access points.

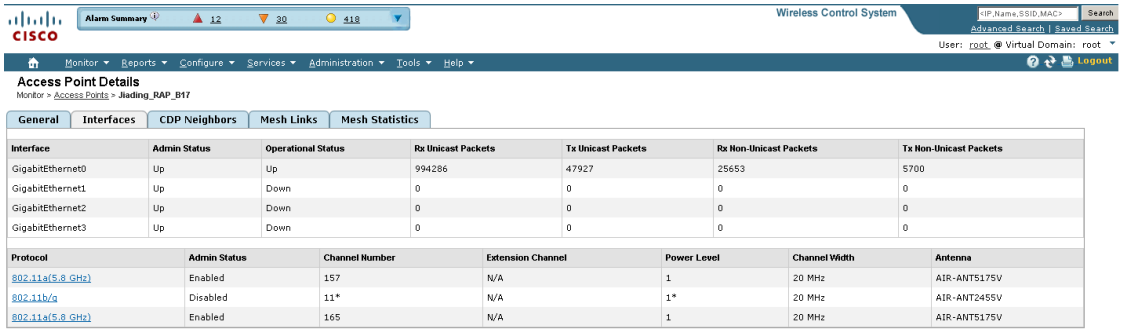
c. Click **Update Map View** to refresh the screen and redisplay the map view with the selected options.

Note Map view information is retrieved from the WCS database and is updated every 15 minutes.

Note You can also select or unselect the check boxes of access points in the mesh hierarchical view to modify which mesh access points are displayed. For a child access point to be visible, the parent access point to root access point must be selected.

Note If you want to have the MAC address appear with the client logo in the Monitor > Maps page, follow these steps:
a) Go to the Maps Tree View.
b) Click the > beside Clients.
c) Click to unselect the Small Icons check box.

Figure 6-12 Mesh Filter and Hope Count Configuration Page



251697

Monitoring Channel Width

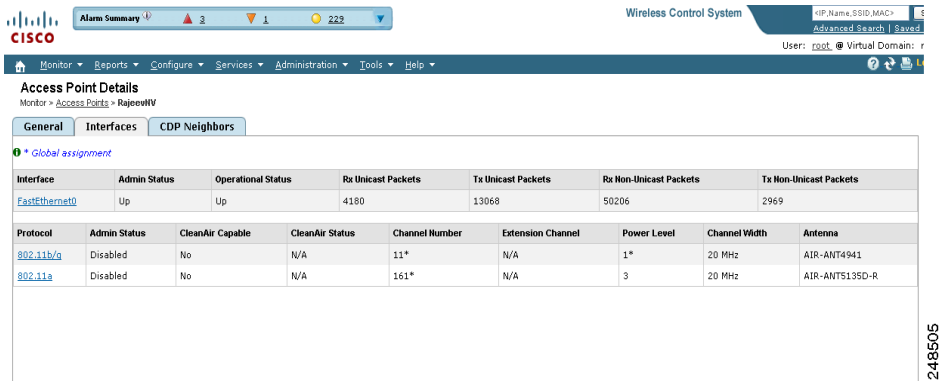
Follow these steps to view the channel width.

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

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. Click an access point in the AP Name column.

Step 2 Click the **Interfaces** tab. The interfaces tab is shown in Figure 6-13.

Figure 6-13 Interfaces Tab



248505

Table 6-9 Interfaces Tab Parameters

Parameter	Description
Interface	
Admin Status	Indicates whether the Ethernet interface is enabled.
Operational Status	Indicates whether the Ethernet interface is operational.
Rx Unicast Packets	Indicates the number of unicast packets received.
Tx Unicast Packets	Indicates the number of unicast packets sent.
Rx Non-Unicast Packets	Indicates the number of non-unicast packets received.
Tx Non-Unicast Packets	Indicates the number of non-unicast packets sent.
Radio Interfaces	
Protocol	802.11a or 802.11b/g.
Admin Status	Indicates whether the access point is enabled or disabled.
Channel Number	Indicates the channel on which the Cisco Radio is broadcasting.
Extension Channel	Indicates the secondary channel on which the Cisco radio is broadcasting.
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.
Channel Width	Indicates the channel width for this radio interface. See "Configuring 40-MHz Channel Bonding" section on page 10-42 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.
Antenna	Identifies the type of antenna.

Step 3 Click an interface name to view its properties (see Figure 6-14).

Figure 6-14 Interface Properties

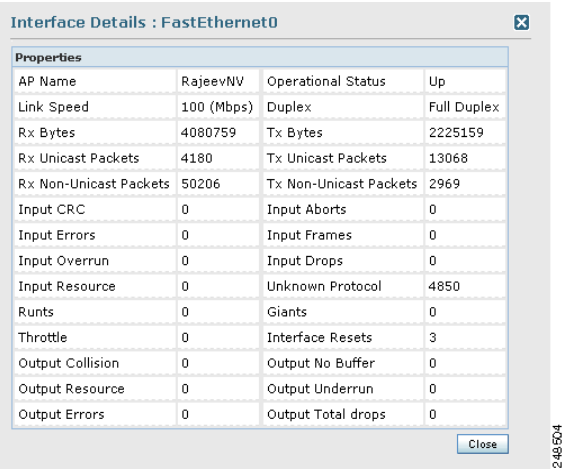


Table 6-10 Interface Properties

Parameters	Description
AP Name	Name of the Access Point.
Link speed	Indicates the speed of the interface in Mbps.
RX Bytes	Indicates the total number of bytes in the error-free packets received on the interface.
RX Unicast Packets	Indicates the total number of unicast packets received on the interface.
RX Non-Unicast Packets	Indicates the total number of non-unicast or mulitcast packets received on the interface.
Input CRC	Indicates the total number of CRC error in packets received on the interface.
Input Errors	Indicates the sum of all errors in the packets while receiving on the interface.
Input Overrun	Indicates the number of times the receiver hardware was incapable of handing received data to a hardware buffer because the input rate exceeded the capability of a receiver to handle the data.
Input Resource	Indicates the total number of resource errors in packets received on the interface.
Runts	Indicates the number of packets that are discarded because they are smaller than the minimum packet size of the medium.
Throttle	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.
Output Collision	Indicates the total number of packet retransmitted due to an Ethernet collision.
Output Resource	Indicates the total number of resource errors in packets transmitted on the interface.

Table 6-10 Interface Properties (continued)

Parameters	Description
Output Errors	Indicates the sum of all errors that prevented the final transmission of packets out of the interface.
Operational Status	Indicates the operational state of the physical Ethernet interface on the AP.
Duplex	Indicates the duplex mode of an interface.
TX Bytes	Indicates the total number of bytes in the error-free packets transmitted on the interface.
TX Unicast Packets	Indicates the total number of unicast packets transmitted on the interface.
TX Non-Unicast Packets	Indicates the total number of non-unicast or mulitcast packets transmitted on the interface.
Input Aborts	Indicates the total number of packet aborted while receiving on the interface.
Input Frames	Indicates the total number of packet received incorrectly having a CRC error and a non-integer number of octets on the interface.
Input Drops	Indicates the total number of packets dropped while receiving on the interface because the queue was full.
Unknown Protocol	Indicates the total number of packet discarded on the interface due to an unknown protocol.
Giants	Indicates the number of packets that are discarded because they exceed the medium's maximum packet size.
Interface Resets	Indicates the number of times that an interface has been completely reset.
Output No Buffer	Indicates the total number of packets discarded because there was no buffer space.
Output Underrun	Indicates the number of times the transmitter has been running faster than the router can handle.
Output Total Drops	Indicates the total number of packets dropped while transmitting from the interface because the queue was full.

Viewing Google Earth Maps

Follow these steps to view Google Earth maps. See Chapter 21, "Google Earth Maps," for further information.

Step 1 Log in to WCS.

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 Google's website.

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 page 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.

Step 2 Click **Cancel** to close the details page.

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—Choose 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, the length of time it takes to collect data depends on 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 the **>** to open the filter page.

  Note These settings apply when Google Earth sends the request for the next refresh.

  - Access Points—From the Display drop-down list, select 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**. Choose the cutoff from the RSSI Cutoff drop-down list (- 60 to - 90 dBm).

Note If both 802.11a/n and 802.11b/g/n protocols are chosen, the heat maps are generated for both and overlaid 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 WCS.

- 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** to confirm these changes or **Cancel** to close the page without saving the changes.

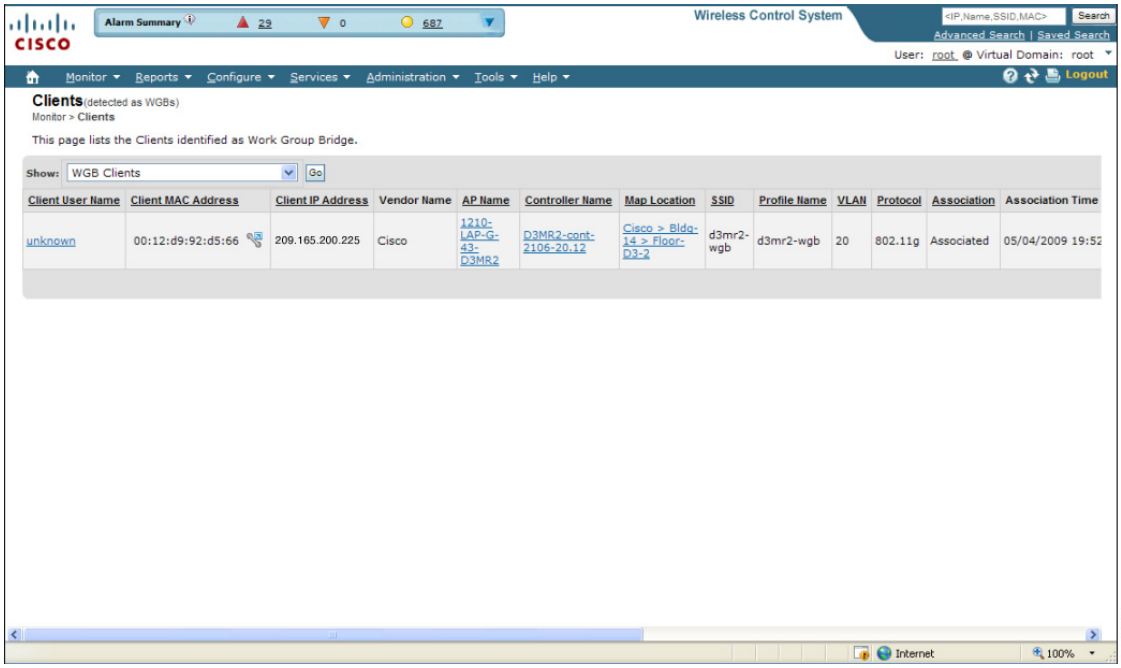
Viewing Clients Identified as WGBs

If an access point is bridge capable, and the AP mode was 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 propogated to the controller and appears as a client in both WCS and WLC. To see a list of all clients identified as a workgroup bridges, follow these steps:

Step 1 Choose **Monitor > Clients**.

Step 2 At the Show drop-down list, choose **WGB Clients**. The Clients (detected as WGBs) page appears (see Figure 6-15).

Figure 6-15 Monitor > WGBs



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:

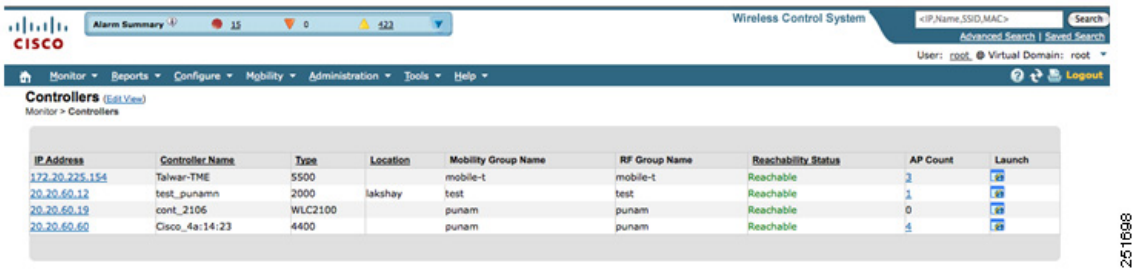
- The orderable product identifier (PID)
- The version of the product identifier (VID)
- The serial number (SN)
- The entity name
- The product description

The UDI is burned into the EEPROM of controllers and lightweight access points at the factory and can be retrieved through the GUI.

Follow these steps to retrieve the UDI on controllers and access points.

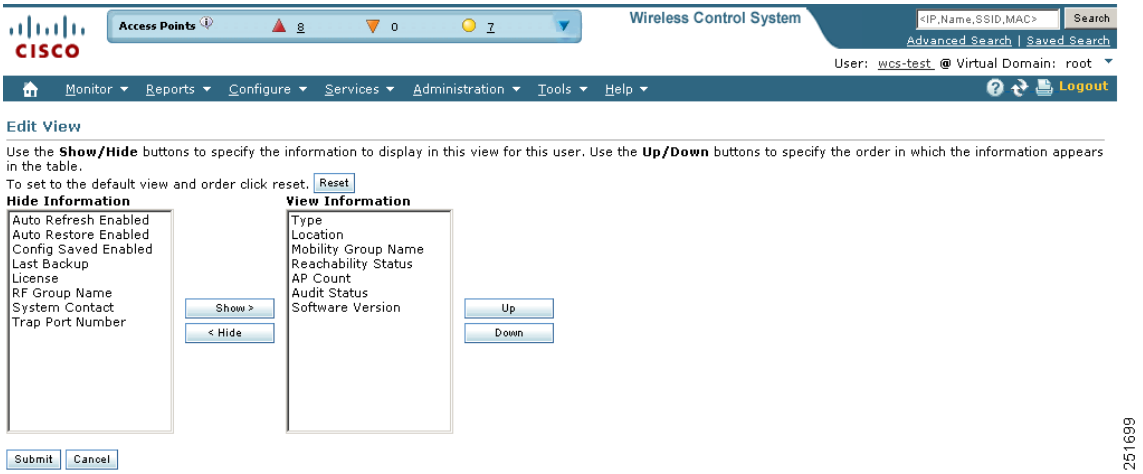
Step 1 Click **Monitor > Controllers**. The Monitor > Controllers page displays (see Figure 6-16).

Figure 6-16 Monitor > Controllers Page



Step 2 (Optional) If you want to change how the controller search results are displayed, click **Edit View**. The Edit View page appears (see Figure 6-17). In the left-hand page, highlight the areas you want to view and click **Show** to move them to the right-hand page. You can then highlight the areas in the right-hand menu and click **Up** or **Down** to rearrange the order.

Figure 6-17 Edit View Page



Step 3 Click the IP address of the controller (seen in Figure 6-16) whose UDI information you want to retrieve. Data elements of the controller UDI display. These elements are described in Table 6-11 and Table 6-12:

Table 6-11 Controllers Summary

Parameter	Description
General Portion	
IP Address	Local network IP address of the controller management interface.
Name	User-defined name of the controller.
Type	The type of controller. **Note** For WiSM, the slot and port numbers are also given.
UP Time	Time in days, hours, and minutes since the last reboot.
System Time	Time used by the controller.

Table 6-11 Controllers Summary (continued)

Internal Temperature	The current internal temperature of the unit (in Centigrade).
Location	User-defined physical location of the controller.
Contact	The contact person for this controller, their textual identification, and ways to contact them. If no contact information is known, this is an empty string.
Total Client Count	Total number of clients currently associated with the controller.
Current LWAPP Transport Mode	Lightweight Access Point Protocol transport mode. Communications between controllers and access points. Selections are Layer 2 or Layer 3.
Power Supply One	Indicates the presence or absence of a power supply and its operations state.
Power Supply Two	Indicates the presence or absence of a power supply and its operation state.
Inventory Portion	
Software Version	The operating system release, version.dot.maintenance number of the code currently running on the controller.
Emergency Image Version	
Description	Description of the inventory item.
Model No.	Specifies the machine model as defined by the Vital Product Data.
Serial No.	Unique serial number for this controller.
Burned-in MAC Address	The burned-in MAC address for this controller.
Number of APs supported	The maximum number of access points supported by the controller.
Gig Ethernet/Fiber Card	Displays the presence or absence of the optional 1000BASE-T/1000BASE-SX GigE card.
Crypto Card One	Displays the presence or absence of an enhanced security module which enables IPSec security and provides enhanced processing power. See Table 6-12 for information on the maximum number of crypto cards that can be installed on a controller. **Note** By default, enhanced security module is not installed on a controller.
Crypto Card Two	Displays the presence or absence of a second enhanced security module.
GIGE Port(s) Status	
Port 1	Up or Down
Port 2	Up or Down
Unique Device Identifier (UDI)	
Name	Product type. Chassis for controller and Cisco AP for access points.

Table 6-11 Controllers Summary (continued)

Description	Description of controller and may include number of access points.
Product Id	Orderable product identifier.
Version Id	Version of product identifier.
Serial Number	Unique product serial number.

Table 6-12 Maximum Number of Crypto Cards That Can Be Installed on a Cisco Wireless LAN Controller

Type of Controller	Maximum Number of Crypto Cards
Cisco 2000 Series	None
Cisco 4100 Series	One
Cisco 4400 Series	Two

Coverage Hole

Coverage holes are areas where clients cannot receive a signal from the wireless network. The Cisco Unified Wireless Network Solution radio resource management (RRM) identifies these coverage hole areas and reports them to the WCS, enabling the IT manager to fill holes based on user demand.

WCS is informed about the reliability-detected coverage holes by the controllers. WCS 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

Coverage holes are displayed as alarms. Pre-coverage holes are displayed as events.

Monitoring Pre-Coverage Holes

While coverage holes are displayed as alarms, pre-coverage holes are displayed as events.

Follow these steps to view pre-coverage hole events.

Step 1 Choose **Monitor > Events** to display all current events.

Step 2 To view pre-coverage hole events only, click the **Advanced Search** link in the upper right.

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 the following table:

Table 6-13 Pre-Coverage Hole Parameters

Parameter	Description
Severity	Pre-coverage hole events are always considered informational (Info).
Client MAC Address	MAC address of the client affected by the pre-coverage hole.
AP MAC Address	MAC address of the applicable access point.
AP Name	The name 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, and 5 = 0.195 to 6.25% power.
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)
WLAN Coverage Hole Status	Determines if the current coverage hole state is enabled or disabled.
WLAN	The name for this WLAN.
Date/Time	The date and time the event occurred. Click the title to toggle between ascending and descending order.

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
  - 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.

Viewing DHCP Statistics

WCS 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 last request timestamp.

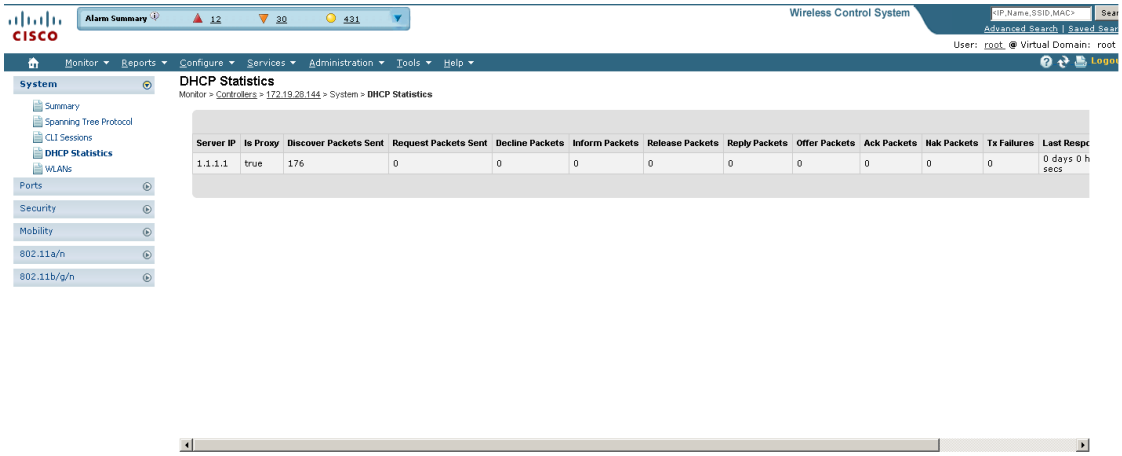
Follow these steps to view DHCP statistics.

Step 1 Choose **Monitor > Controllers**.

Step 2 Click one of the IP addresses in the IP Address column.

Step 3 From the left sidebar menu, choose **System > DHCP Statistics**. The DHCP Statistics page appears (see Figure 6-18).

Figure 6-18 DHCP Statistics Page



251700

The DHCP Statistics screen provides the following information:

Table 6-14 DHCP Statistics

Parameter	Description
Server IP	Identifies the IP address of the server.
Is Proxy	Identifies whether or not this server is proxy.
Discover Packets Sent	Identifies the total number of packets sent with the intent to locate available servers.
Request Packets Sent	Identifies the total number of packets sent from the client requesting parameters from the server or confirming the correctness of an address.
Decline Packets	Identifies the number of packets indicating that the network address is already in use.
Inform Packets	Identifies the number of client requests to the DHCP server for local configuration parameters because the client already has an externally configured network address.
Release Packets	Identifies the number of packets that release the network address and cancel the remaining lease.
Reply Packets	Identifies the number of reply packets.
Offer Packets	Identifies the number of packets that respond to the discover packets with an offer of configuration parameters.
Ack Packets	Identifies the number of packets that acknowledge successful transmission.
Nak Packets	Identifies the number of packets that indicate that the transmission occurred with errors.
Tx Failures	Identifies the number of transfer failures that occurred.

Table 6-14 DHCP Statistics

Parameter	Description
Last Response Received	Provides a timestamp of the last response received.
Last Request Sent	Provides a timestamp of the last request sent.

Guest User Monitoring

WCS provides monitoring and reporting capabilities in regards to guest user accounts. See the "Guest Reports" section on page 17-62 for a description of the reporting capabilities. The guest user components on the WCS home page provide a summary of guest users' deployment and network use. Guest users can also be monitored from the Monitor Controllers > Guest Users page.

The Monitor > Controllers > Guest Users page provides a list of all guest user accounts currently present on the controller. Follow these steps to monitor guest users.

Step 1 Choose **Monitor > Controllers** to access this page.

Step 2 Choose the IP address of the applicable controller.

Step 3 Click **Guest Users** located under Security on the left sidebar menu. The Guest User(s) page appears.

The following information displays for guest users currently present on the controller:

- Guest Username
- Profile—Indicates the profile to which the guest user is connected.
- Lifetime—Indicates the length of time that the guest user's account is active. Length of time displays in days, hours, and minutes or as Never Expires.
- Start Time—Indicates when the guest user's account was activated.
- Remaining Lifetime—Indicates the remaining time for the guest user's account.
- Role—Indicates the designated user role.
- First Logged in at—Indicates the date and time of the user's first login.
- Number of logins—Indicates the total number of logins for this guest user.
- Description—User-defined description of the guest user account for identification purposes.

RRM Dashboard

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

Lightweight access points can simultaneously scan all valid 802.11a/b/g channels for the country of operation as well as for channels available in other locations. The access points go "off-channel" for a period not greater than 60 ms to monitor these channels for noise and interference. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and interfering access points.

Note In the presences of voice traffic (in the last 100 ms), the access points defer off-channel measurements and do not change channels.

Each access point spends only 0.2 percent of its time off-channel. This activity is distributed across all access points so that adjacent access points are not scanning at the same time, which could adversely affect wireless LAN performance. In this way, administrators gain the perspective of every access point, thereby increasing network visibility.

Prior to WCS software release 5.1, WCS 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 WCS events as informational and were maintained by the event dispatcher. The reason for the transmit power or channel changes (such as signals from neighboring access points, interference, noise, load balancing, and so on) were not evident. You could not view these events and statistics to then perform troubleshooting practices.

A snapshot of the Radio Resource Management (RRM) statistics (delivered in 5.1) helps 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 (access point performance, configuration mismatch between controllers in the same RF group, coverage holes that were detected by access points based on threshold, coverage holes that were detected by controllers, ratios of access points operating at maximum power, and so on).

Note The RRM dashboard information is only available for lightweight access points.

Channel Change Notifications

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

The controller’s dynamic channel assignment (DCA) capabilities are also useful in minimizing adjacent channel interference between access points. For example, two overlapping channels in the 802.11b/g band, such as 1 and 2, cannot both simultaneously use 11/54 Mb/s. By effectively reassigning channels, the controller keeps adjacent channels separated, thereby avoiding this problem.

Notifications are sent to the WCS 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 upon request. If the DCA is static, no dynamic channel assignments occur, and values are set to their global default.

In WCS software releases prior to 5.1, only radios using 20-MHz channelization are supported by DCA. In WCS software release 5.1, DCA is extended to support 802.11n 40-MHz channels in the 5-GHz band. 40-MHz channels allow radios to achieve higher instantaneous data rates (potentially 2.25 times higher than 20-MHz channels.) In WCS software release 5.1, you can choose between DCA working at 20 or 40 MHz.

Note Radios using 40-MHz channels in the 2.4-GHz band are not supported by DCA.

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

The controller dynamically controls access point transmit power based on real0time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the access points' transmit power according to how the access points are seen by their third strongest neighbor.

The transmit power control algorithm reduces or increases an access point's power. However, the coverage hole algorithm can only increase access point power, thereby filling a coverage hole. For example, if a failed access point is detected, the coverage hole algorithm can automatically increase power on surrounding access points to fill the gap created by the loss in coverage.

Notifications are sent to the WCS 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.

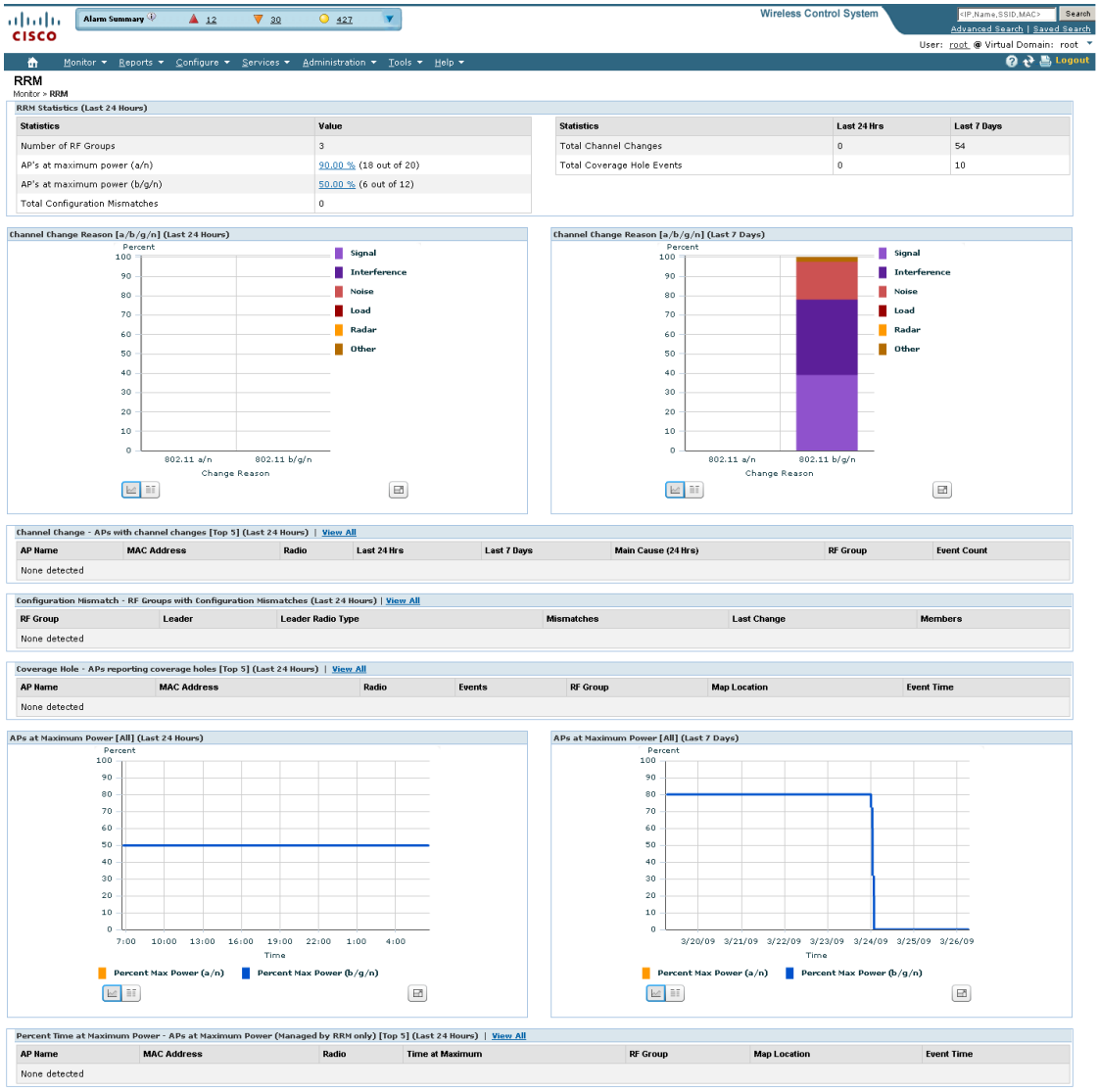
RF Grouping Notifications

When RRM is run on the controller, dynamic grouping is done, and a new group leader is chosen. Dynamic grouping has two modes: on and off. When the grouping is off, no dynamic grouping occurs, and each switch optimizes only its own lightweight access point parameters. When the grouping is on, switches form groups and elect leaders to perform better dynamic parameter optimization. With grouping on, 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

The RRM dashboard is accessed by choosing Monitor > RRM (see Figure 6-19).

Figure 6-19 RRM Statistics Dashboard



The dashboard is made up of the following parts:

- 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.
- The Channel Change shows all events complete with causes.
- The Configuration Mismatch portion shows comparisons between the leaders and members.
- The Coverage Hole portion rates how severe the coverage holes are and gives their location.
- The APs at Maximum Power
- 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 screen with details for that access point only appears.
- Total Configuration Mismatches—The total number of configuration mismatches detected over a 24-hour.
- 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 currently managed by WCS.
- Configuration Mismatch—The configuration mismatch over a 24-hour period by RF group with details on the group leader.
- Percent of 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 present maximum power of the access point.

  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—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 Events APs—The top five access points filtered by IF Type 11 a/n which triggered a coverage hole event 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 and 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. The power is polled 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.

  Note This maximum power portion shows the value from the last 24 hours and is only event driven.

CHAPTER 7

Managing WCS User Accounts

This chapter describes how to configure global e-mail parameters and manage Cisco WCS user accounts. It contains these sections:

- Adding WCS User Accounts, page 7-1
- Viewing or Editing User Information, page 7-6
- Viewing or Editing Group Information, page 7-8
- Viewing the Audit Trail, page 7-9
- Creating Guest User Accounts, page 7-10
- Managing WCS Guest User Accounts, page 7-12
- Saving Guest Accounts on a Device, page 7-14

Adding WCS User Accounts

This section describes how to configure a WCS 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. WCS 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, the user must run a utility to reset the password to another user-defined password.

Follow these steps to add a new user account to WCS.

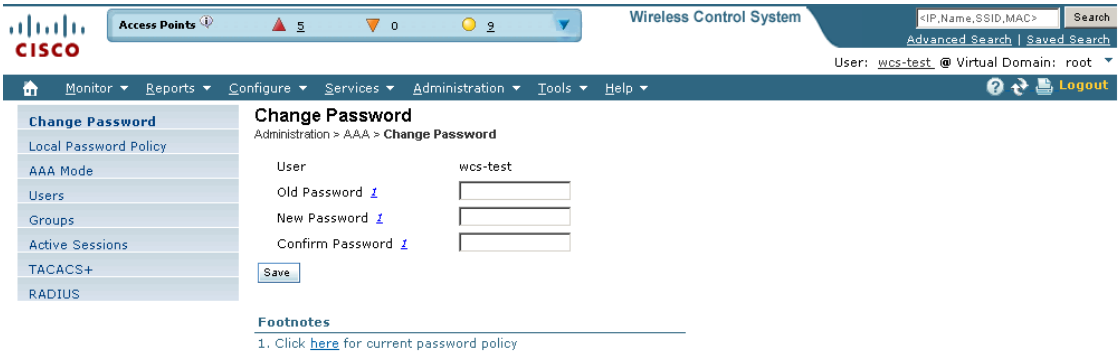
Step 1 Start WCS by following the instructions in the "Starting WCS" section on page 2-16.

Step 2 Log into the WCS user interface as *Super1*.

Note Cisco recommends that you create a new superuser assigned to the SuperUsers group and delete Super1 to prevent unauthorized access to the system.

Step 3 Click **Administration > AAA** and the Change Password page appears (see Figure 7-1).

Figure 7-1 Change Password Page



251702

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 WCS user account. You must enter the password twice.

Note These entries are case sensitive.

Step 6 Click **Groups** from the left sidebar menu. The All Groups page displays the following group names (see Figure 7-2).

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 WCS operations.
- ConfigManagers—Allows users to monitor and configure WCS operations.
- Admin—Allows users to monitor and configure WCS operations and perform all system administration tasks except administering WCS user accounts and passwords.

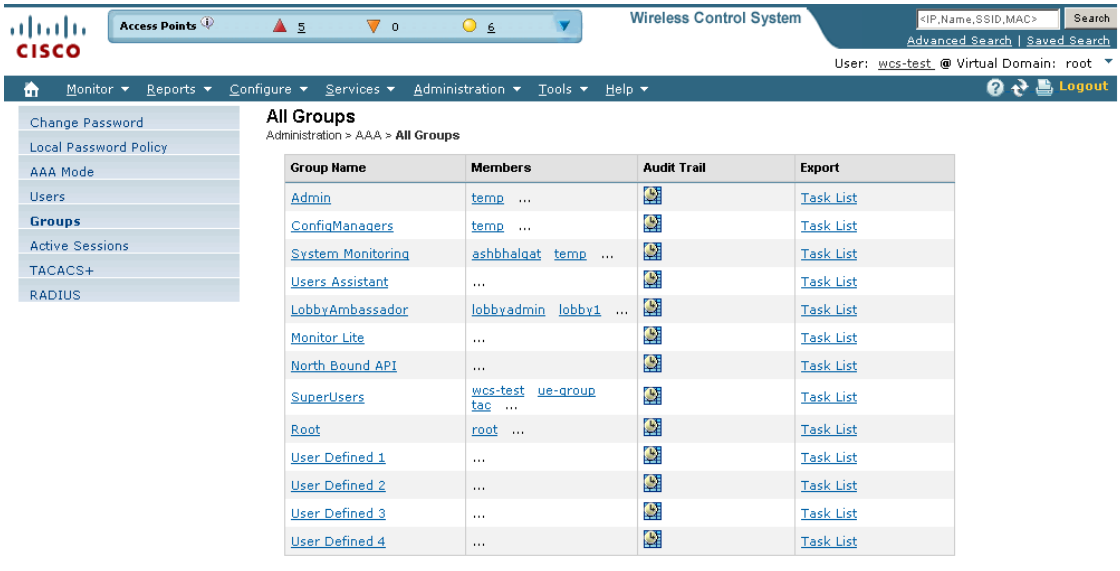
  Note If you choose admin account and log in as such on the controller, you can also see the guest users under Local Net Admin.

- SuperUsers—Allows users to monitor and configure WCS operations and perform all system administration tasks including administering WCS user accounts and passwords. Superusers tasks can be changed.
- North bound API—A user group used only with WCS Navigator.
- Users Assistant—Allows only local net user administration. User assistants cannot configure or monitor controllers. They must access the Configure > Controller path to configure these local net features.

Note If you create a user assistant user, login as that user, and choose Monitor > Controller, you receive a permission denied message as expected behavior.

- Lobby Ambassador—Allows guest access for only configuration and managing of user accounts.
- Monitor lite—Allows monitoring of assets location.
- Root—Allows users to monitor and configure WCS 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.

Figure 7-2 All Groups Page



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 group's permitted operations.

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 checking or unchecking the appropriate check boxes for task permissions and members.

Note Any changes you make will affect all members of this user group.

Note To view complete details on the Monitor > Client details screen 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 WCS User Accounts

Follow these steps to delete a WCS user account.

Step 1 Start WCS by following the instructions in the "Starting WCS" section on page 2-16.

Step 2 Log into the WCS user interface as a user assigned to the SuperUsers group.

Step 3 Click **Administration > AAA**.

Step 4 Click **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

Follow these steps to change the password for a WCS user account.

Step 1 Start WCS by following the instructions in the "Starting WCS" section on page 2-16.

Step 2 Log into the WCS user interface as a user assigned to the SuperUsers group.

Step 3 Click **Administration > AAA** to display the Change Password page.

Step 4 Enter your old password, unless you are the root user. (A root user can change any password without entering the 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.

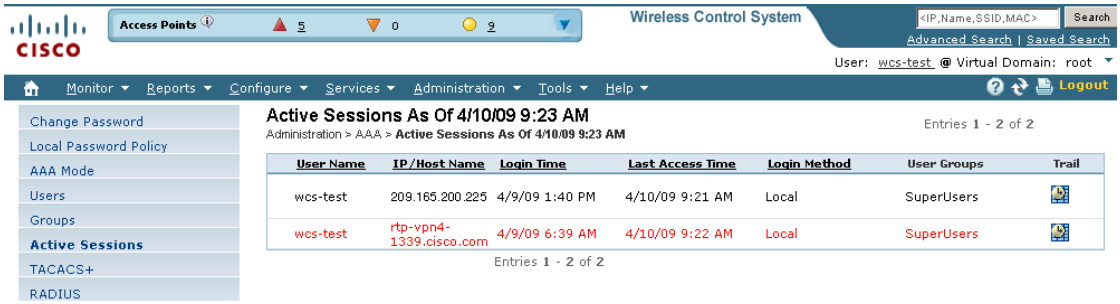
Monitoring Active Sessions

Follow the steps below to view a list of active users.

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Active Sessions**. The Active Sessions page appears (see Figure 7-3).

Figure 7-3 Active Sessions Page



251704

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:

- 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 WCS. All times are based on the WCS server machine time.
- Last Access Time: The time at which the user's browser accessed WCS. All times are based on the WCS 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 panel. However, if a user navigates to a non-WCS Navigator web page in the same browser, the disparity in time is greater upon returning to WCS Navigator. This disparity results because alarm counts are not updated while the browser is visiting non-WCS Navigator web pages.

- Login Method:
  - Web Service: Internal session needed by Navigator to manage WCS.
  - Regular: Sessions created for users who log into WCS directly through a browser.
  - Navigator Redirect: Sessions created for Navigator uses who are redirected to WCS from Navigator.
- User Groups: The list of groups to which the user belongs. (North bound API is a user group used only with WCS Navigator.)
- Audit trail icon: Link to page that displays the audit trail (previous login times) for that user.

Viewing or Editing User Information

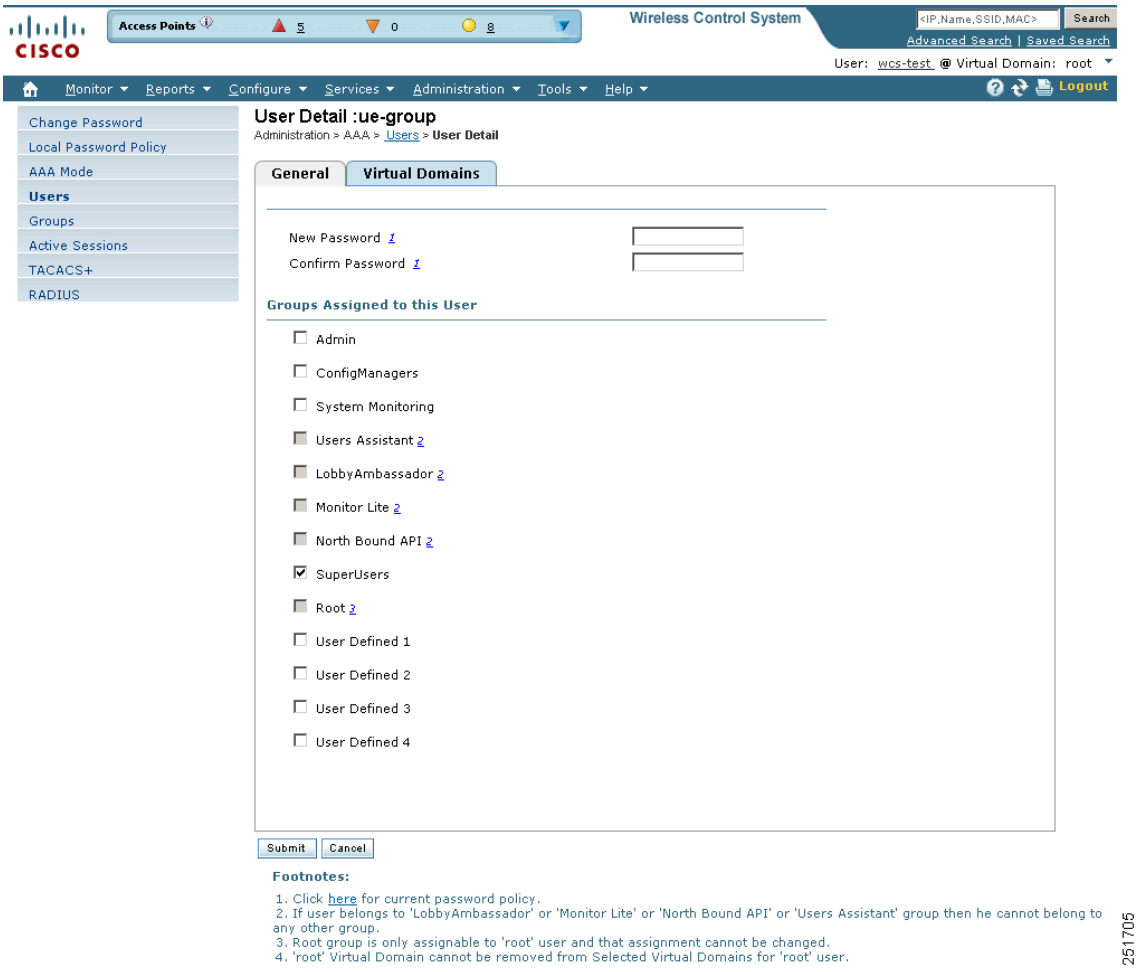
Follow these steps to see the group the user is assigned to or to adjust a password or group assignment for that user.

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Users**.

Step 3 Click in the User Name column. The User Detail : *User Group* page appears (see Figure 7-4).

Figure 7-4 Detailed Users Page



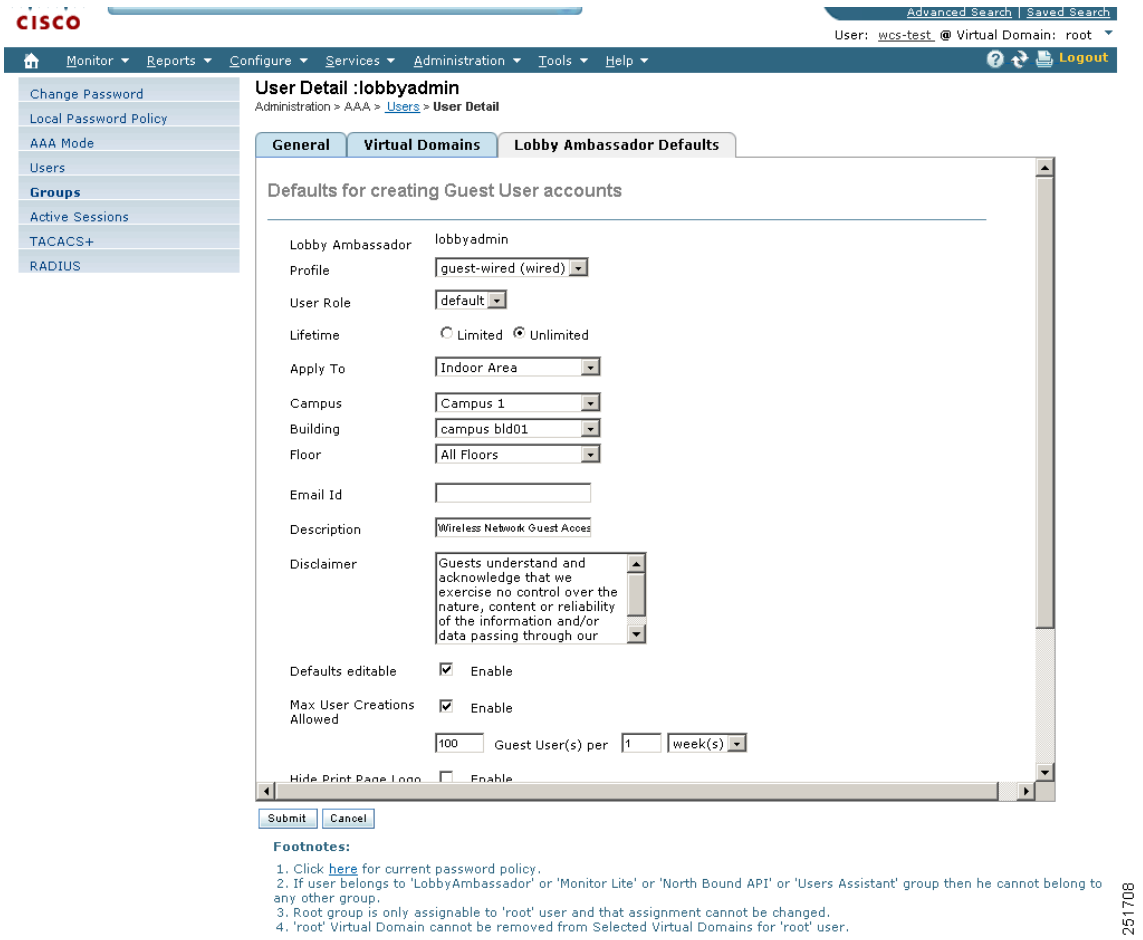
You can see which group is assigned to this user or change a password or group assignment.

Setting the Lobby Ambassador Defaults

If you choose a Lobby Ambassador from the User Name column, a Lobby Ambassador Defaults tab appears (see Figure 7-5). 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.

Figure 7-5 Lobby Ambassador Default Tab



Step 4 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 10-51.

Step 5 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 6 Choose **Limited** or **Unlimited** at the Lifetime parameter.

- 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 7 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 WCS.

Step 8 Enter the e-mail ID of the host to whom the guest account credentials are sent.

Step 9 Provide a brief description of the account.

Step 10 If you want to supply disclaimer text, enter it.

a. 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 11 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 12 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 13 If you want additional page header text, you can enter it at the Print Page Header Text parameter.

Step 14 Click **Submit**.

Viewing or Editing Group Information

Follow these steps to see specific tasks the user is permitted to do within the defined group or make changes to the tasks.

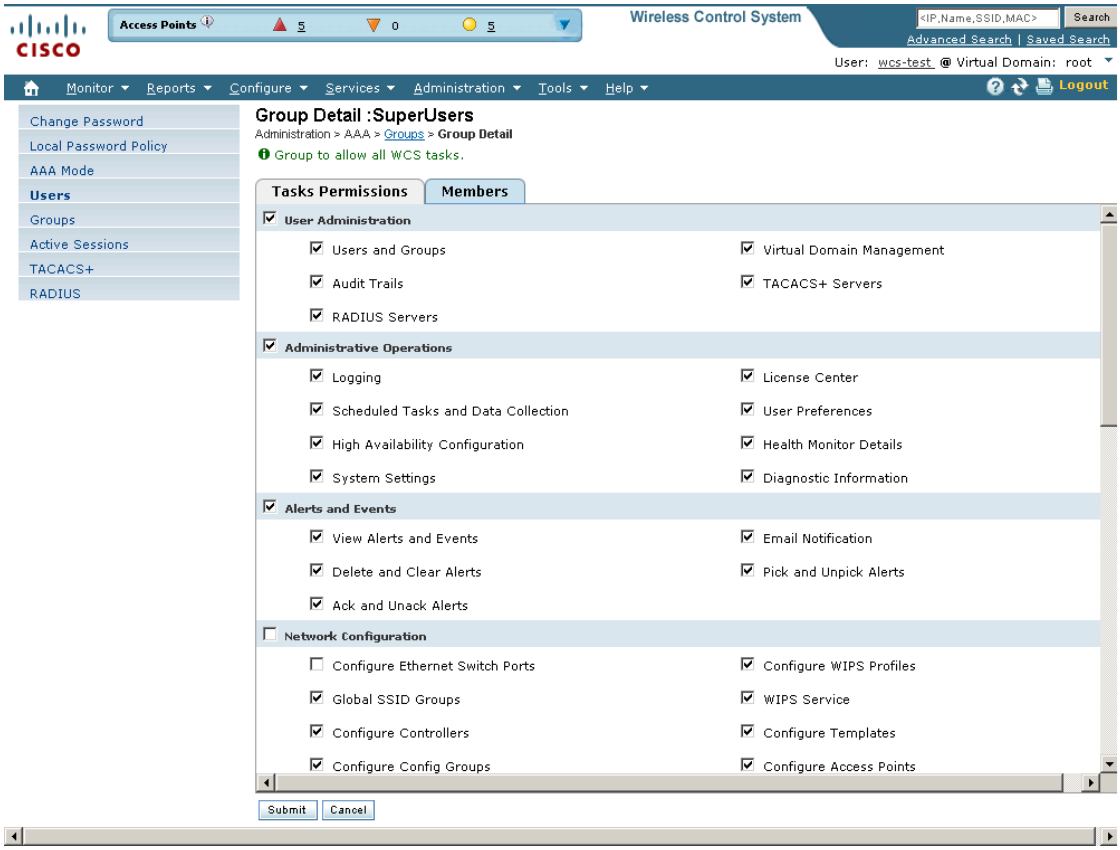
Step 1 Choose **Administration > AAA**.

Step 2 Choose **Users** from the left sidebar menu.

Step 3 Click in the **Member Of** column. The Group Detail: *User Group* page appears (see Figure 7-6).

Note The detailed page varies based on what group you choose. Figure 7-6 shows the detailed page of the superuser.

Figure 7-6 Detailed Group Page



You can see the specific tasks the user is permitted to do within the defined group or make changes to the tasks.

Editing the Guest User Credentials

Click the WCS user name of the guest user whose credentials you want to edit. The Lobby Ambassador Default tab appears, and you can modify the credentials.

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.

Viewing the Audit Trail

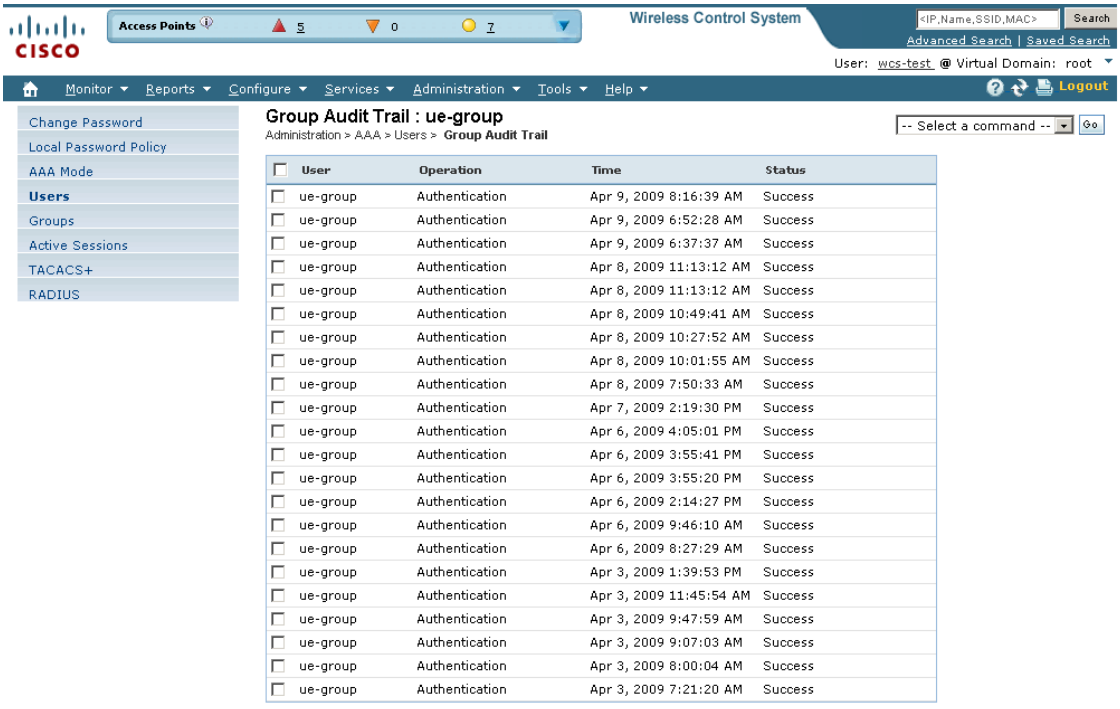
Click the **Audit Trail** icon in the Users page to view a log of authentication attempts. The Audit Trail page appears (see Figure 7-7).

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

Figure 7-7 Audit Trail



Creating Guest User Accounts

You can use the Cisco Lobby Ambassador to create guest user accounts in WCS. 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.
- 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.

This section describes how to perform the following procedures:

- Logging in to the WCS User Interface as a Lobby Ambassador, page 7-11
- Managing WCS Guest User Accounts, page 7-12

Follow these steps to create guest user accounts in WCS.

Note You should have SuperUser privilege (by default) to create a lobby ambassador account and not administration privileges. Multiple lobby ambassador accounts can be created by the administrator with varying profiles and permissions.

Note A root group, which is created during installation, has only one assigned user, and no additional users can be assigned after installation. This root user cannot be changed. Also, unlike a super user, no task changes are allowed.

Step 1 Log into the WCS user interface as an administrator.

Step 2 Click **Administration > AAA**.

Step 3 From the left sidebar menu, choose **Users**.

Step 4 From the Select a Command drop-down list, choose **Add User**, and click **Go**. The Users page appears.

Step 5 Enter the username.

Step 6 Enter the password. The minimum is six characters. Reenter and confirm the password.

Note The password must include at least three of the following four types of elements: lowercase letters, uppercase letters, numbers, and special characters.

Step 7 In the *Groups Assigned to this User* section, select the **LobbyAmbassador** check box to access the **Lobby Ambassador Defaults** tab.

Step 8 Follow the steps in the "Setting the Lobby Ambassador Defaults" section on page 7-7.

Logging in to the WCS User Interface as a Lobby Ambassador

When you log in as a lobby ambassador, you have access to the guest user template page in WCS. You can then configure guest user accounts (through templates).

Follow these steps to log into the WCS user interface through a web browser.

Step 1 Launch Internet Explorer 7.0 or later on your computer.

Note Some WCS features may not function properly if you use a web browser other than Internet Explorer 7.0 or later on a Windows workstation.

Step 2 In the browser's address line, enter **https://*wcs-ip-address*** (*such as* https://1.1.1.1/login.html), where *wcs-ip-address* is the IP address of the computer on which WCS is installed. Your administrator can provide this IP address.

Step 3 When the WCS user interface displays the Login page, 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 WCS. The WCS 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 WCS user interface, close the browser page or click **Logout** in the upper right corner of the page. Exiting a WCS user interface session does not shut down WCS on the server.

Note When a system administrator stops the WCS server during a WCS session, the session ends, and the web browser displays this message: "The page cannot be displayed." Your session does not reassociate to WCS when the server restarts. You must restart the WCS session.

Managing WCS Guest User Accounts

WCS guest user accounts are managed with the use of templates. This section describes how to manage WCS user accounts. It includes the following:

- Adding WCS Guest User Accounts (refer to the "Configuring Guest User Templates" section on page 12-54)
- Scheduling WCS Guest User Accounts, page 7-12
- Printing or E-mailing WCS Guest User Details, page 7-14
- Saving Guest Accounts on a Device, page 7-14

Scheduling WCS 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 using 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.

Follow these steps to schedule a recurring guest user account in WCS.

Step 1 Log in to the WCS 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 On the Guest Users > Scheduling page, enter the guest user name. 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 35 weeks.
  - 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.
- 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 WCS 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.

Follow these steps to print guest user details from the Guest Users List page.

Step 1 Log into the WCS user interface as lobby ambassador.

Step 2 On the Guest User page, select the check box next to User Name and 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-mai**l and from the e-mail page, enter the subject text and the recipient's e-mail address. Click **Send** or **Cancel**.

Note You can also print or email user details from the Configure > Controller Template Launch Pad > Security > Guest User option.

Saving Guest Accounts on a Device

Click the **Save Guest Accounts on Device** check box to save guest accounts to a WLC flash so that they are maintained across WLC reboots.

Note In the Configure > Controller Template Launch Pad > Security > Guest page, you choose **Save Guest Accounts on device** from the Select a command drop-down page.

Editing the Guest User Credentials

Click the WCS user name of the guest user whose credentials you want to edit. The Lobby Ambassador Default tab appears, and you can modify the credentials.

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.

Adding a New User

The Add User page allows the administrator to set up a new user login including user name, 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.

Note You must have SuperUser status to access this page.

This section includes the following topics:

- Adding User Names, Passwords, and Groups
- Assigning a Virtual Domain

Adding User Names, Passwords, and Groups

To add a new user, follow these steps:

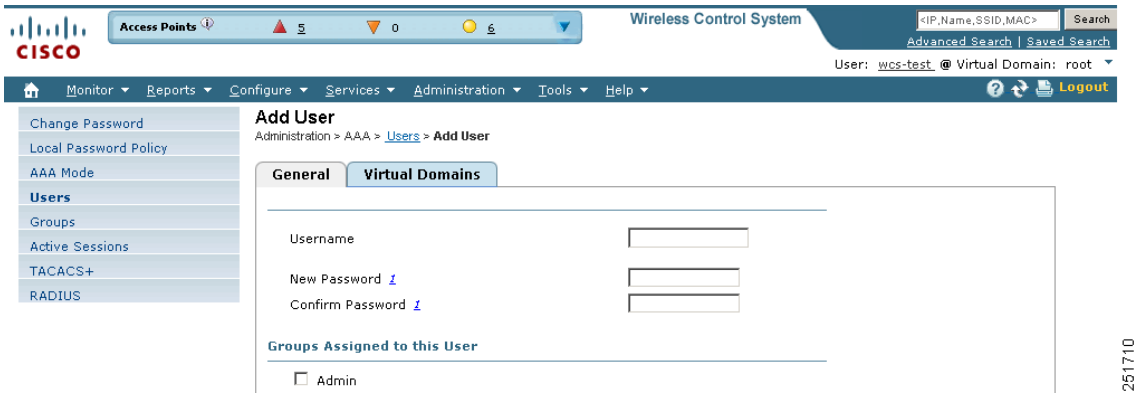
Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, select **Users**.

Step 3 From the **Select a command** drop-down list, choose **Add User**.

Step 4 Click **Go**. The Users page appears (see Figure 7-8).

Figure 7-8 Users Page



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 will be 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 WCS operations and perform all system administration tasks except administering WCS user accounts and passwords.
- ConfigManagers—Allows users to monitor and configure WCS operations.
- System Monitoring—Allows users to monitor WCS 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 only with WCS Navigator and WCS Web Service consumers.

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.

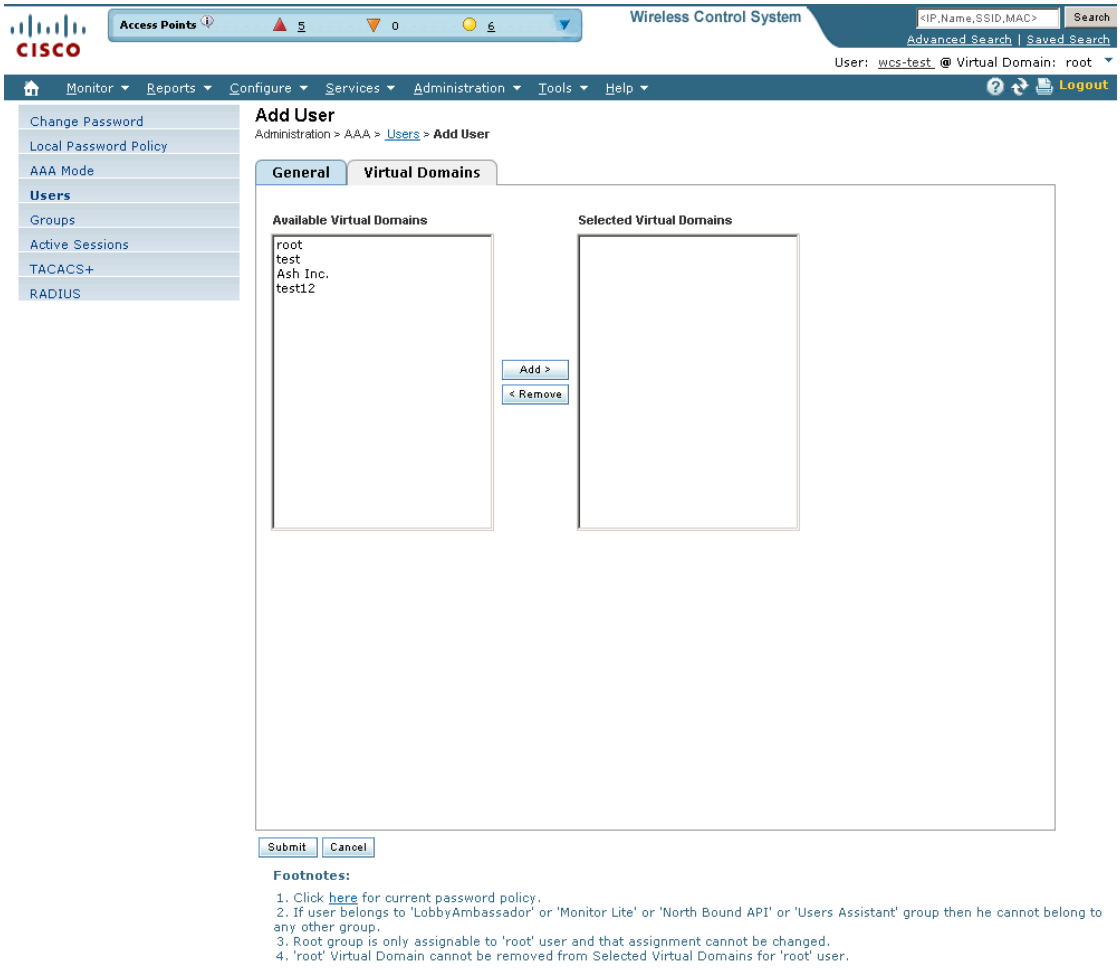
- SuperUsers—Allows users to monitor and configure WCS operations and perform all system administration tasks including administering WCS user accounts and passwords. Superuser tasks can be changed.
- Root—This group is only assignable to 'root' user and that assignment cannot be changed.
- User Defined

Assigning a Virtual Domain

Follow these steps to assign a virtual domain to this user:

Step 1 Click the **Virtual Domains** tab. This page displays all virtual domains available and assigned to this user (see Figure 7-9).

Figure 7-9 Users Virtual Domains Tab



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.

To remove a virtual domain from the Selected Virtual Domains list, click to highlight the domain in the Selected Virtual Domains list, and click **< Remove**. The virtual domain moves from the Selected Virtual Domains to the Available Virtual Domains list.

Step 4 Choose **Submit** to or **Cancel** to close the page without adding or editing the current user.

Virtual Domain RADIUS and TACACS+ Attributes

The Virtual Domain Custom Attributes page allows you to indicate the appropriate protocol-specific data for each virtual domain. The Export button on the Virtual Domain Hierarchy sidebar pre-formats the virtual domain's RADIUS and TACACS+ attributes. You can copy and paste these attributes into the ACS server. This allows you to copy only the applicable virtual domains into the ACS server screen and ensures that the users only have access to these virtual domains.

To apply the pre-formatted RADIUS and TACACS+ attributes to the ACS server, follow these steps:

Step 1 Choose **Administration > Virtual Domains**.

Step 2 From the left Virtual Domain Hierarchy sidebar menu, select to highlight the virtual domain for which you want to apply the RADIUS and TACACS+ attributes.

Step 3 Click **Export**.

Step 4 Highlight the text inside of the RADIUS or TACACS+ Custom Attributes (depending on which one you are currently configuring), go to your browser's menu, and choose **Edit > Copy**.

Step 5 Log in to ACS.

Step 6 Go to User or Group Setup.

Note If you want to specify virtual domains on a per user basis, then you need to make sure you add ALL the custom attributes (for example, tasks, roles, virtual domains) information into the User custom attribute screen.

Step 7 For the applicable user or group, click **Edit Settings**.

Step 8 Use your browser's Edit > Paste feature to place the RADIUS or TACACS+ custom attributes into the applicable text box.

Step 9 Click the check boxes to enable these attributes.

Step 10 Click **Submit**.

Step 11 Click **Restart**.

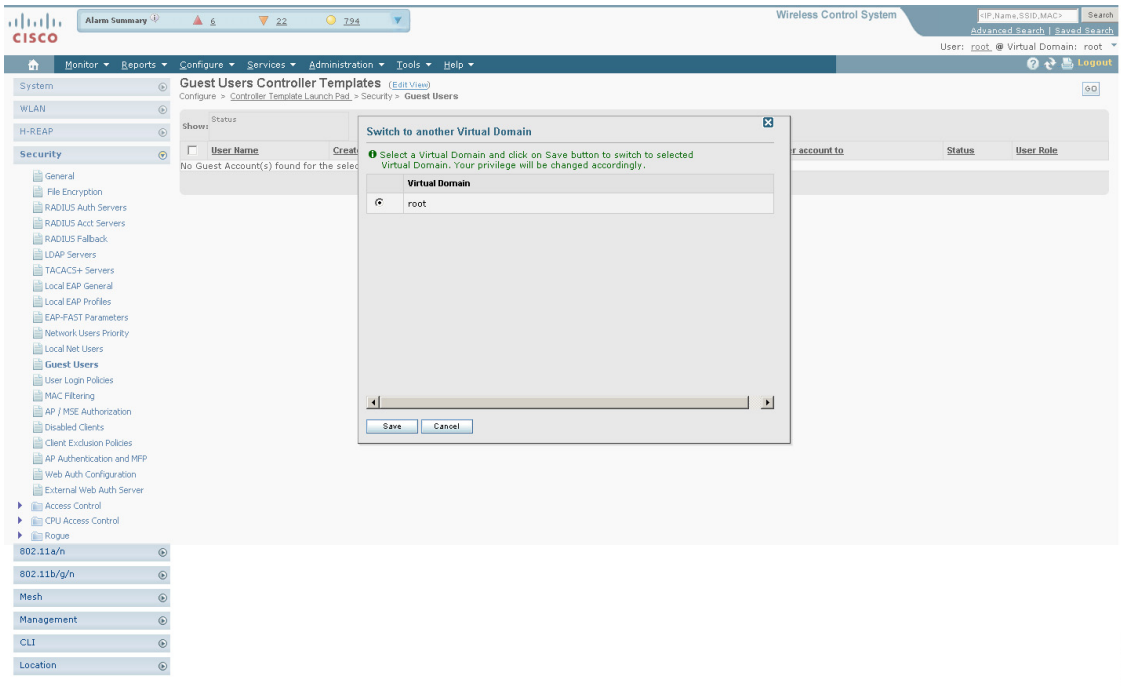
Note For more information on adding RADIUS and TACACS+ attributes to the ACS server, see the "Adding WCS UserGroups into ACS for TACACS+" section on page 18-10 or the "Adding WCS UserGroups into ACS for RADIUS" section on page 18-14.

Understanding Virtual Domains as a User

When you log in, you can access any of the virtual domains that the administrator assigned to you.

Only one virtual domain can be active at login. You can change the current virtual domain by using the Virtual Domain drop-down list in the top of the WCS main page (see Figure 7-10). Only virtual domains that have been assigned to you are available in the drop-down list.

Figure 7-10 Virtual Domains Summary Tab



Select a virtual domain and click Save to switch to the selected virtual domain. The privilege is changed accordingly.

Limited Menu Access

Non-root virtual domain users do not have access to the following WCS menus:

- Monitor > RRM
- Configure > Auto Provisioning
- Configure > ACS View Servers
- Mobility > Mobility Services
- Mobility > Synchronize Servers
- Administration > Background Tasks
- Administration > Settings
- Administration > User Preferences
- Tools > Voice Audit
- Tools > Config Audit

CHAPTER 8

Configuring Mobility Groups

This chapter describes mobility groups and explains how to configure them on Cisco WCS. It contains these sections:

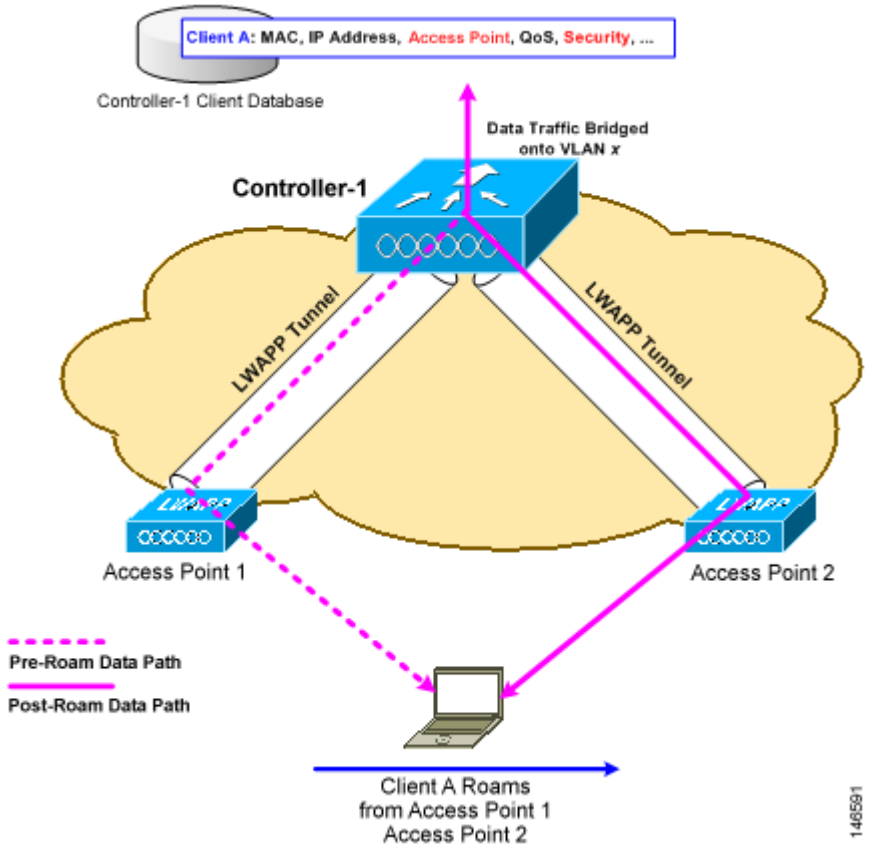
- Overview of Mobility, page 8-1
- Symmetric Tunneling, page 8-5
- Overview of Mobility Groups, page 8-5
- Configuring Mobility Groups, page 8-8
- Mobility Anchors, page 8-13
- Configuring Multiple Country Codes, page 8-16
- Creating Config Groups, page 8-19
- Reporting Config Groups, page 8-26
- Downloading Software, page 8-26

Overview of Mobility

Mobility, or *roaming*, is a wireless LAN client's ability 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 access point's controller places an entry for that client in its client database. This entry includes the client's MAC and IP addresses, 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.

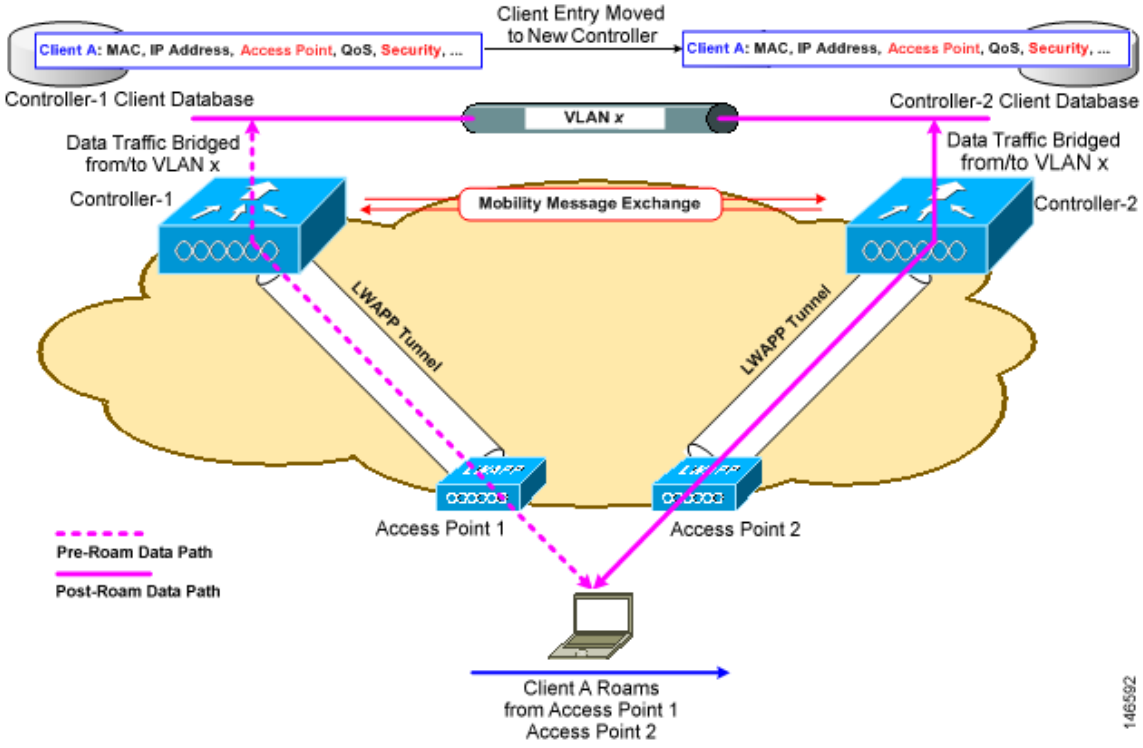
Figure 8-1 Intra-Controller Roaming



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 controllers' wireless LAN interfaces are on the same IP subnet.

Figure 8-2 Inter-Controller Roaming

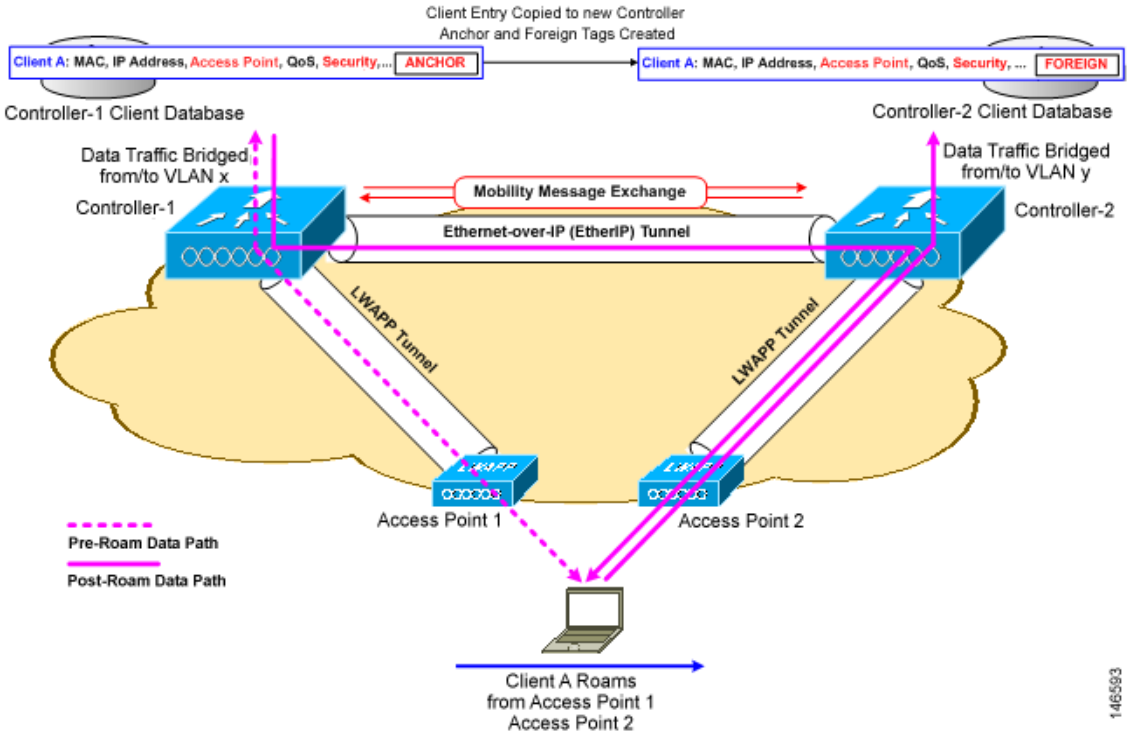


When the client associates to an access point joined to a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database 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 in order to comply with the IEEE standard.

Figure 8-3 illustrates *inter-subnet roaming*, which occurs when the controllers' wireless LAN interfaces are on different IP subnets.

Figure 8-3 Inter-Subnet Roaming



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 may 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 12-3 for instructions on configuring this feature within a template.

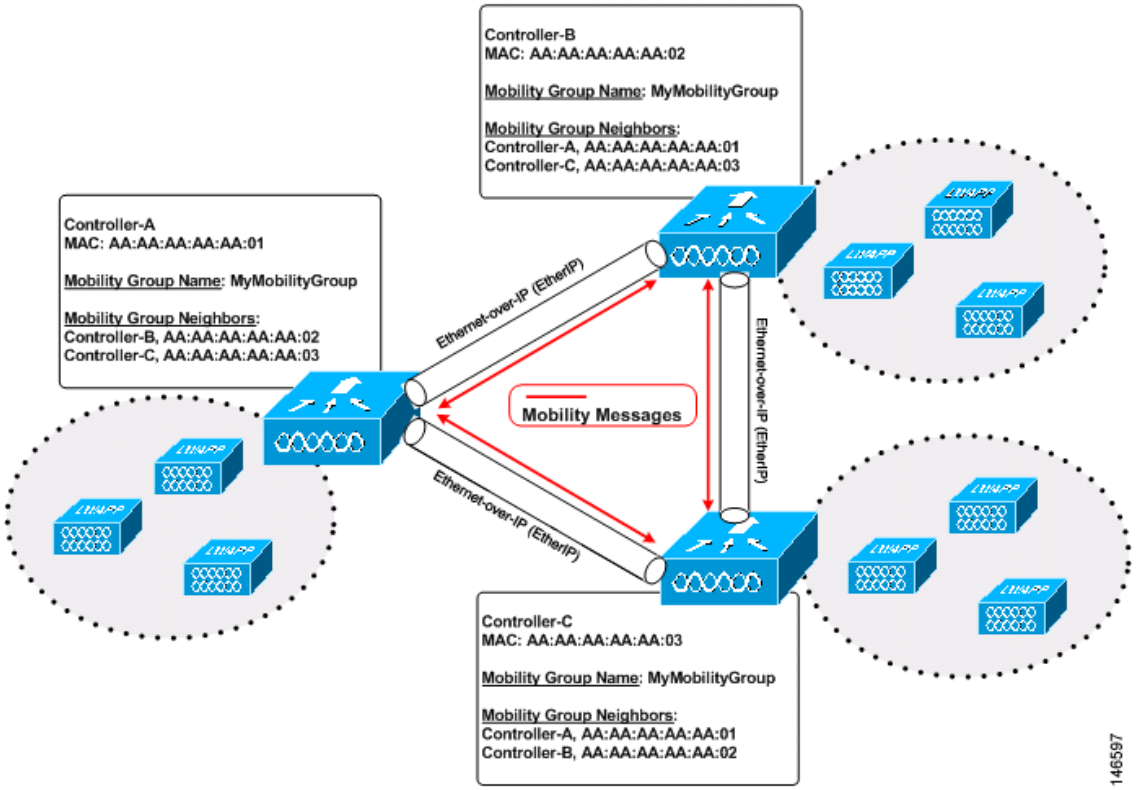
Overview of Mobility Groups

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.

Figure 8-4 A Single Mobility Group



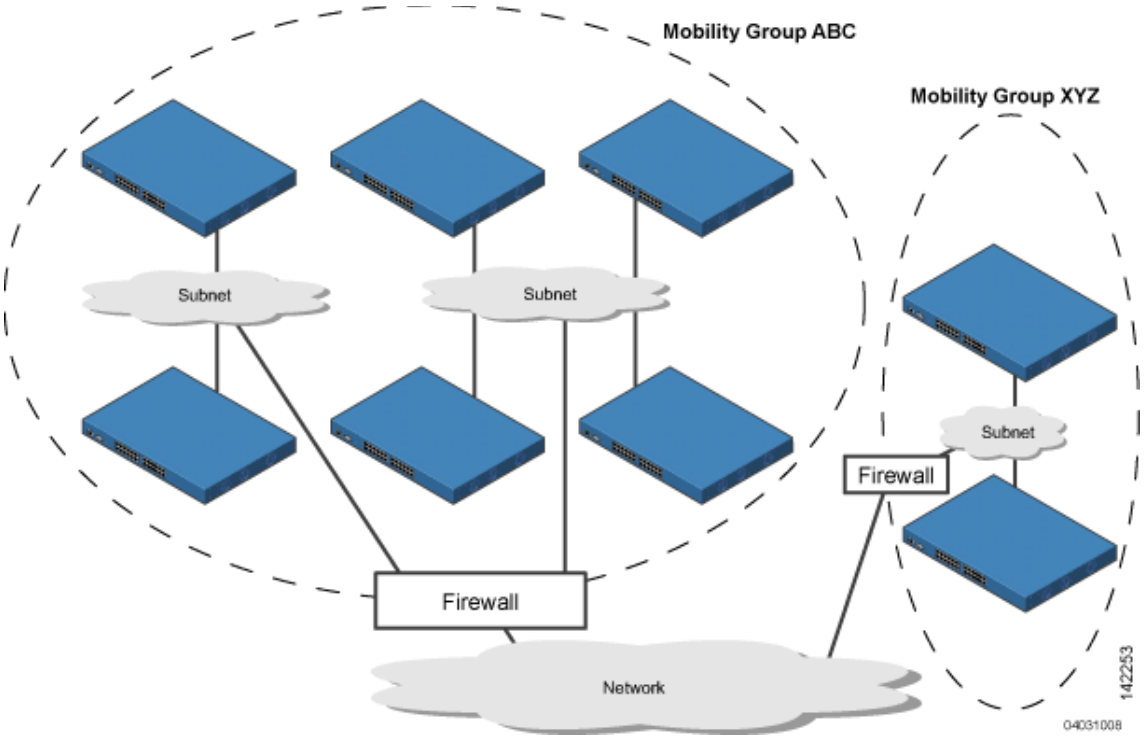
As shown in Figure 8-4, each controller is configured with a list of the other members of the mobility group. Whenever a new client joins a controller, the controller sends out a unicast message to all of the controllers in the mobility group. The controller to which the client was previously connected 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.

Figure 8-5 Two 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 may 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.

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 WCS 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 WCS 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 WCS and controller software releases prior to 5.0, the controller may 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 WCS 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, Cisco recommends 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 on 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 may appear to work, but the hand-off does not complete, and the client loses connectivity for a period of time.

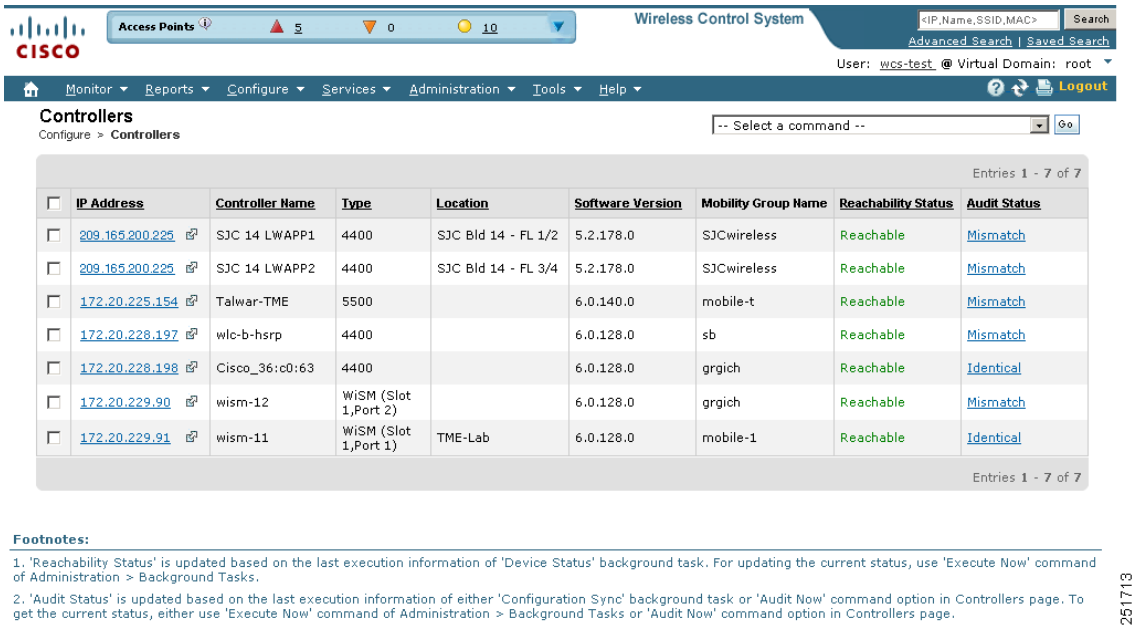
- You must have gathered the MAC address and IP address of every controller that is to be included in the mobility group. This information is necessary because you will be configuring all controllers with the MAC address and IP address of all the other mobility group members.

Note You can find the MAC and IP addresses of the other controllers to be included in the mobility group on the Configure > Controllers page.

Follow these steps to add each WLC controller into mobility groups and configure them.

Step 1 Choose **Configure > Controllers** (see Figure 8-6).

Figure 8-6 Configure > Controllers

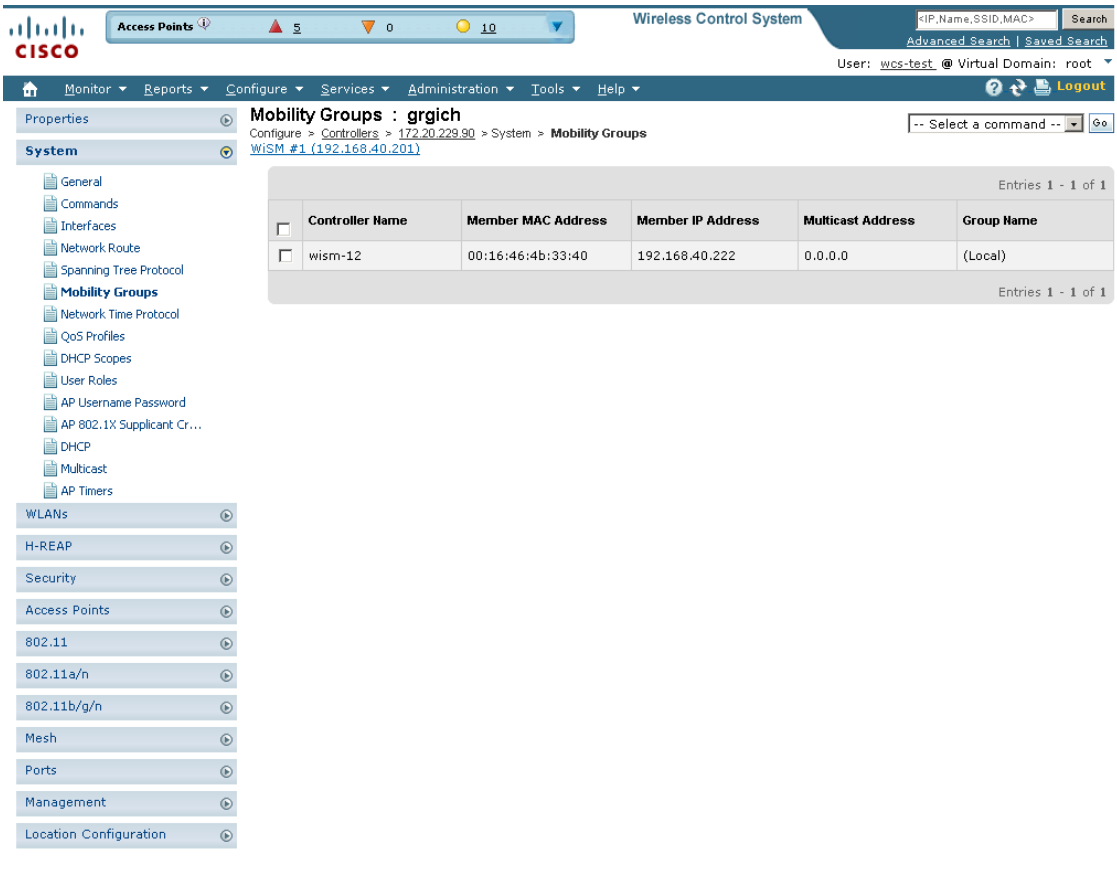


This page shows the list of all the controllers you added in Step 1. The mobility group names and the IP address of each controller that is currently a member of the mobility group is listed.

Step 2 Choose the first controller by clicking on the WLC IP address. You will 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 (see Figure 8-7).

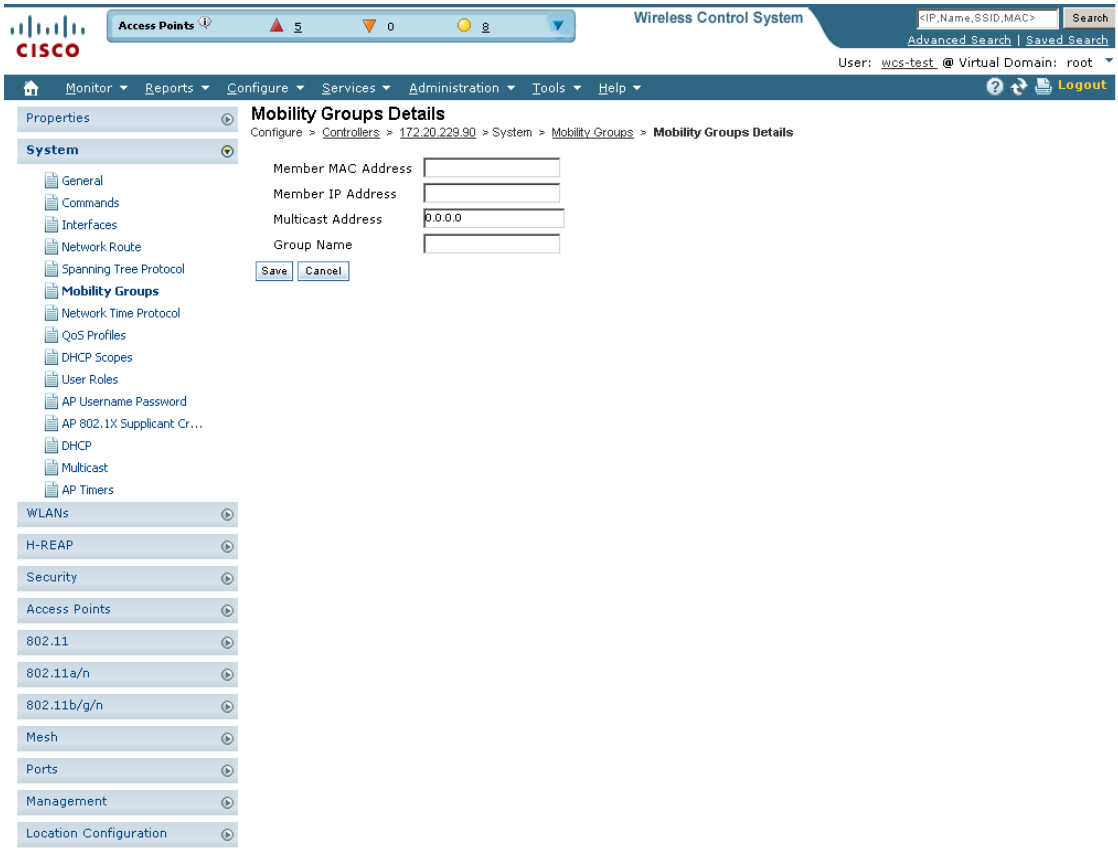
Figure 8-7 Existing Mobility Groups



Step 4 You will 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" message. The Mobility Group Member page appears (see Figure 8-8).

Figure 8-8 Mobility Group Member Page



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 controller's management interface IP address. Otherwise, mobility will fail 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 local mobility member's group address must be the same as the local controller's group address.

Step 9 In the Group Name text box, enter the name of the mobility group.

Step 10 Click **Save**.

Step 11 Repeat the above steps for the remaining WLC devices.

Setting the Mobility Scalability Parameters

Follow these steps to set the mobility message parameters.

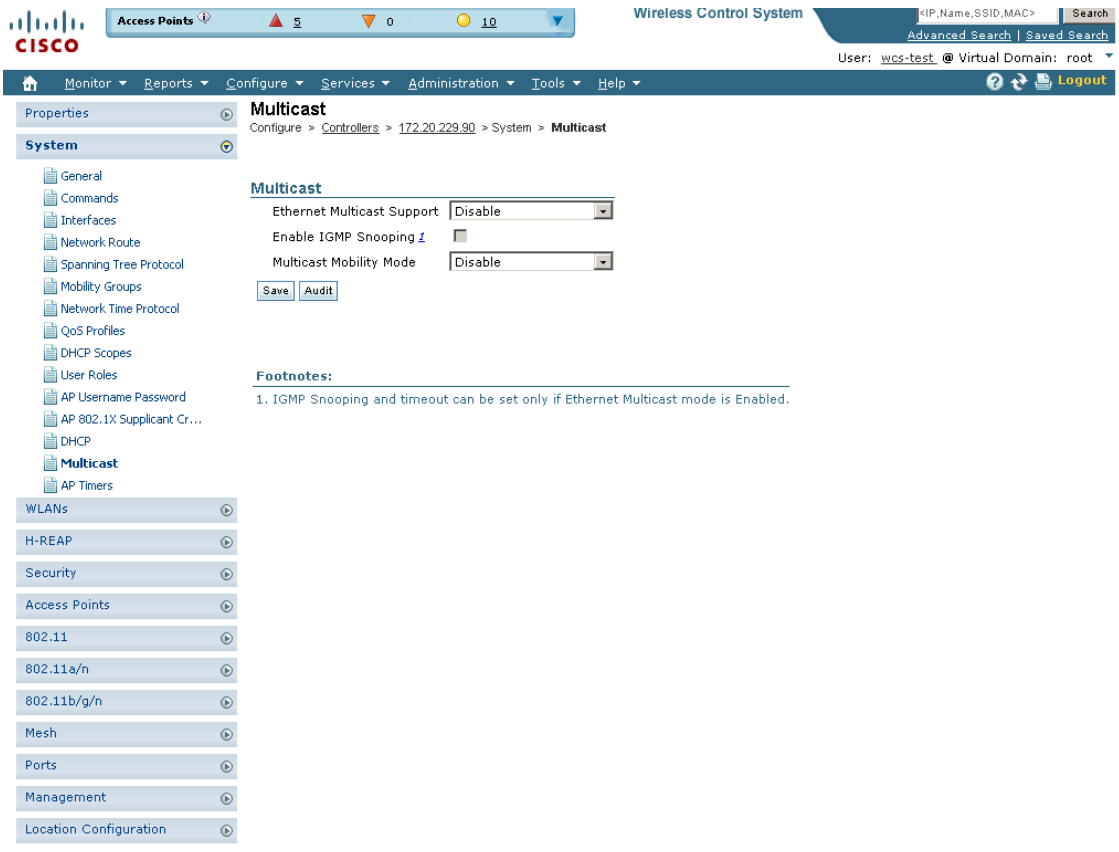
Note You must complete the steps in the "Configuring Mobility Groups" section on page 8-8 prior to setting the mobility scalability parameters.

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 (.Figure 8-9).

Figure 8-9 Multicast Page



Step 4 At the Ethernet Multicast Support parameter, 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.

Step 5 If you chose multicast in Step 4, you must enter the group IP address at the Multicast Group Address parameter 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 to enable IGMP snooping.

Step 7 Select **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 8 If you enabled the Multicast Mobility Mode, enter the mobility group multicast address.

Step 9 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 client's entry point 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).

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 through a mobility tunnel using EtherIP and sent to the anchor controller, where they are decapsulated 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 EtherIP. 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 controller 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.

Configuring Mobility Anchors

Follow these steps to create a new mobility anchor for a WLAN.

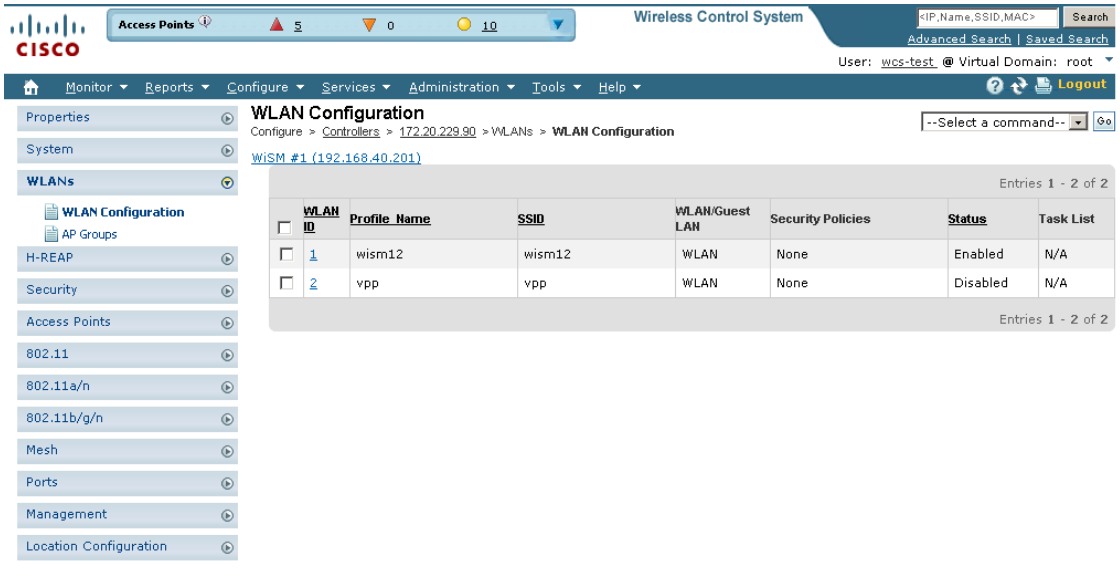
Step 1 Click **Configure > Controllers**.

Step 2 Choose a controller by clicking an IP address.

Step 3 Choose **WLANs > WLAN Configuration** from the left sidebar menu.

Step 4 Select the check box of the desired WLAN ID URL (see Figure 8-10).

Figure 8-10 WLAN Page

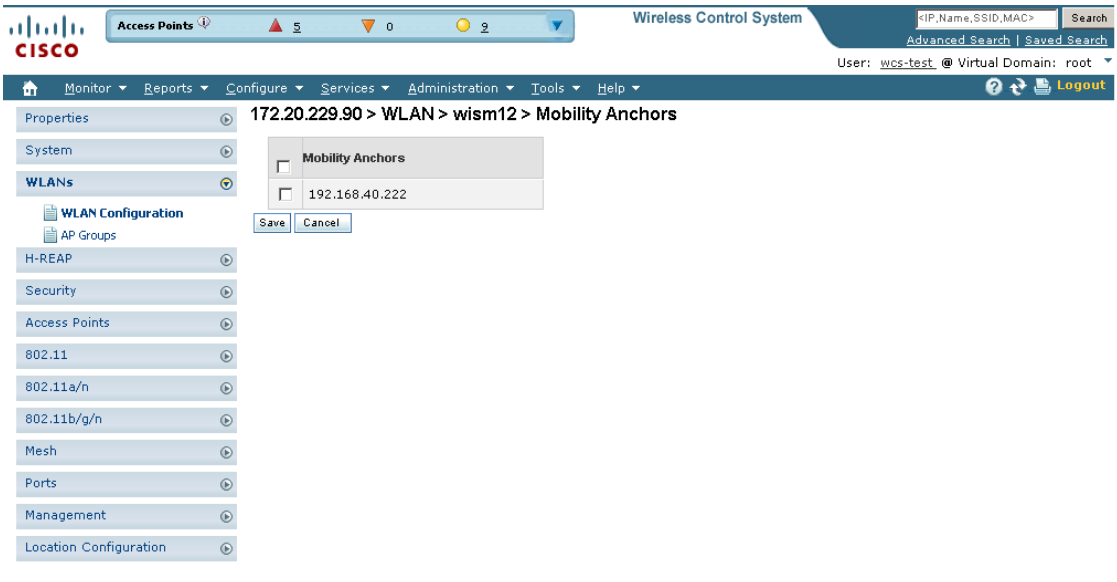


Step 5 After choosing a WLAN ID, a tabbed page appears (see Figure 8-11). Click the **Advanced** tab.

Figure 8-11 Advanced Page

Step 6 Click the **Mobility Anchors** link at the bottom of the page. The Mobility Anchors page appears (see Figure 8-12).

Figure 8-12 Mobility Anchors



Step 7 Select the IP address check box of the controller to be designated a mobility anchor and click **Save**.

Step 8 Repeat Step 6 and Step 7 to set any other controllers as anchors for this WLAN.

Step 9 Configure the same set of anchor controllers on every controller in the mobility group.

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, 1) choose Configure > Controllers, 2) select the desired controller you want to disable, 3) choose 802.11a/n or 802.11b/g/n from the left sidebar menu, and then 4) choose Parameters. The Network Status is the first check box.

Follow these steps to add multiple controllers that are defined in a configuration group and then set the DCA channels. To configure multiple country codes outside of a mobility group, refer to the "Setting Multiple Country Codes" section on page 10-29.

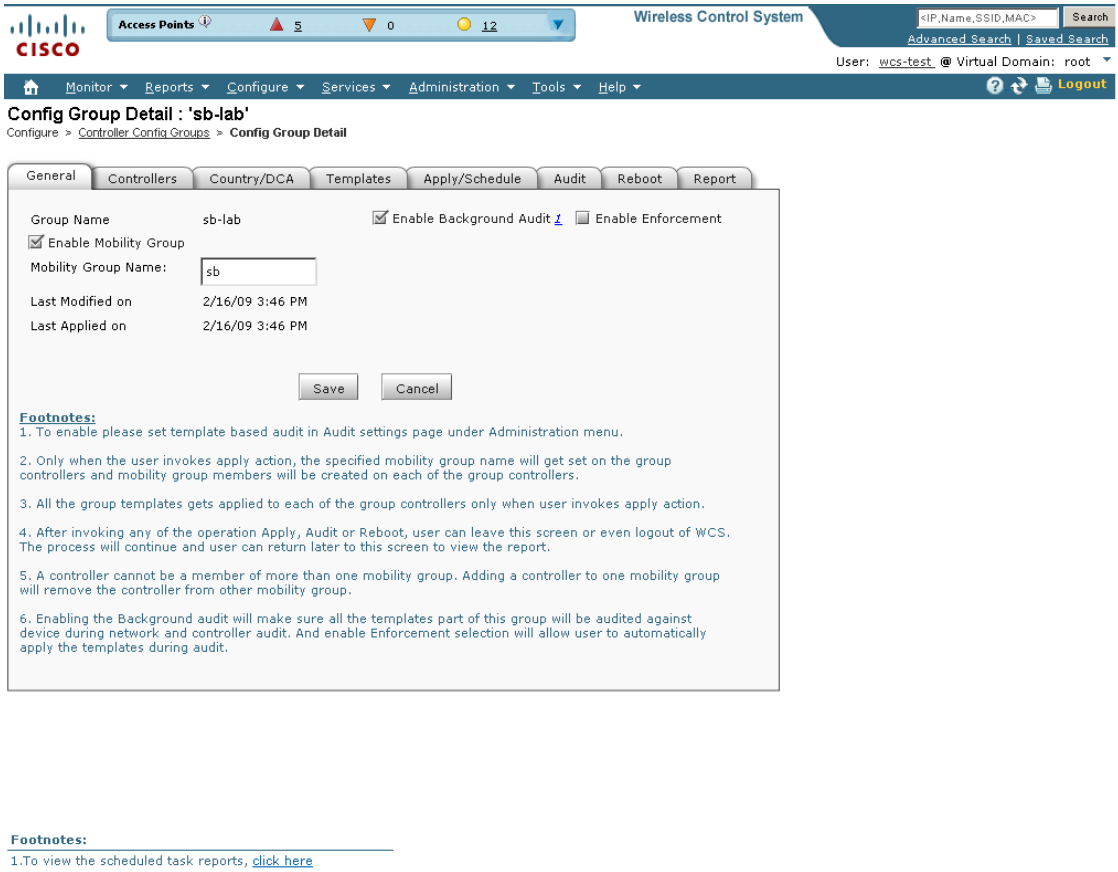
Step 1 Choose **Configure > Controller Config Groups**.

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.

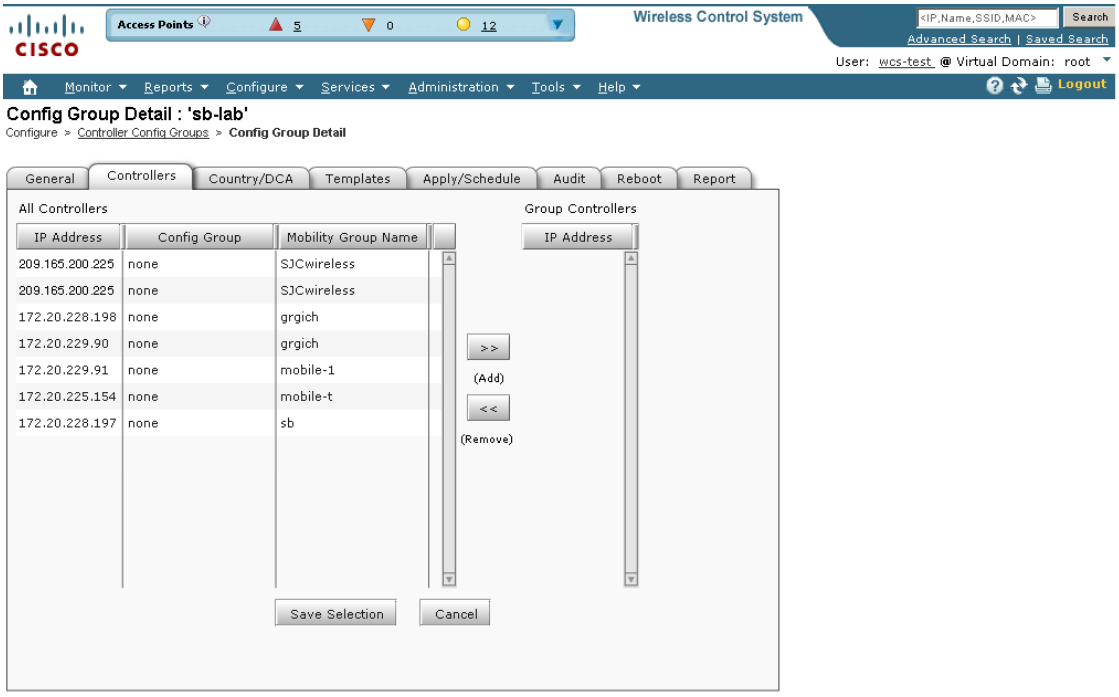
Step 4 Click **Save**. The Config Groups page appears (see Figure 8-13).

Figure 8-13 Config Groups Page



Step 5 Click the **Controllers** tab. The Controllers page appears (see Figure 8-14).

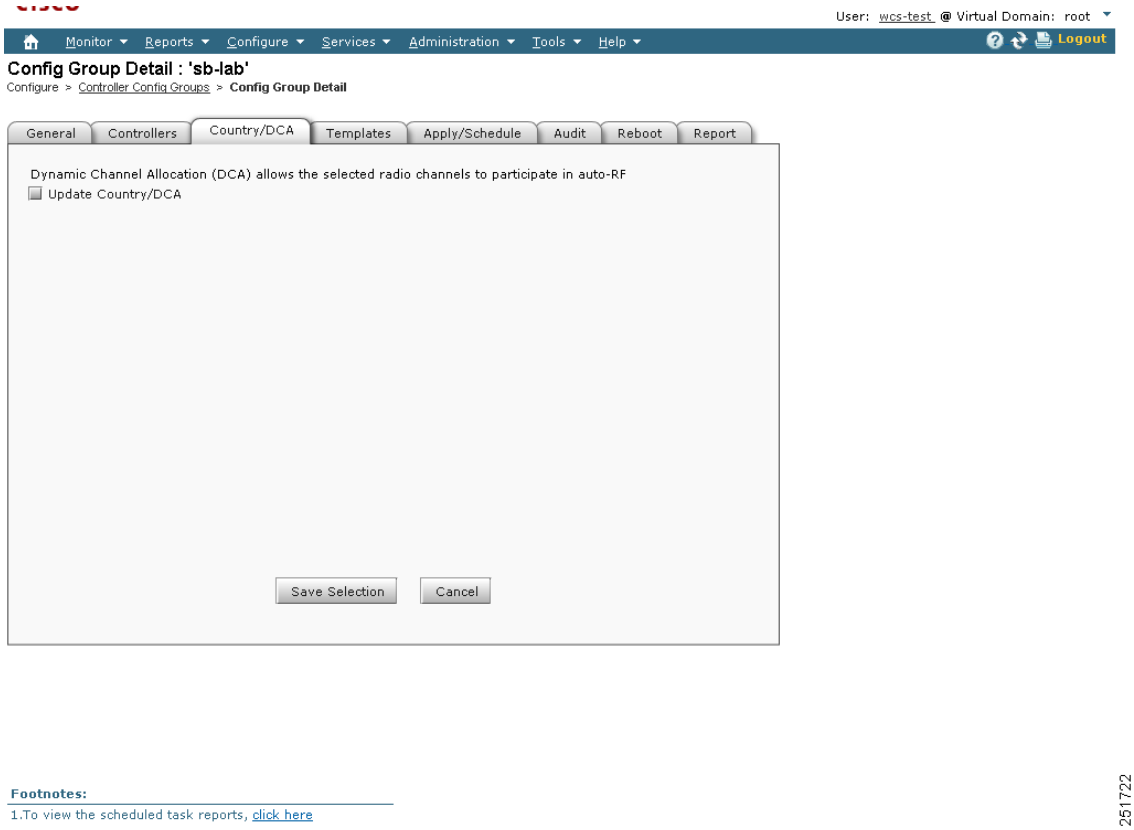
Figure 8-14 Controller Tab



Step 6 Highlight the controllers you want to add and click the **>> Add** button. The controller is added to the Group Controllers page.

Step 7 Click the **Country/DCA** tab. The Country/DCA page appears (see Figure 8-15). Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation amongst a set of managed devices connected to the controller.

Figure 8-15 Country/DCA Tab



Step 8 Select the **Update Countries/DCA** check box to display a list of countries from which to choose.

Step 9 Those DCA channels that are currently configured on the controller for the same mobility group are displayed in the Select Country Codes page. The corresponding 802.11a/n and 802.11b/n allowable channels for the chosen country is displayed as well. You can add or delete any channels in the list by selecting or deselecting the channel and clicking **Save Selection**.

Note A minimum of 1 and a maximum of 20 countries can be configured for a controller.

Creating 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, refer to Chapter 12, "Using Templates."

By choosing **Configure > Controller Config Groups**, you can view a summary of all config groups in the Cisco WCS 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

Follow these steps to add a config group.

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.

Note If the Enable Background Audit option is chosen, the network and controller audit is performed on this config group.

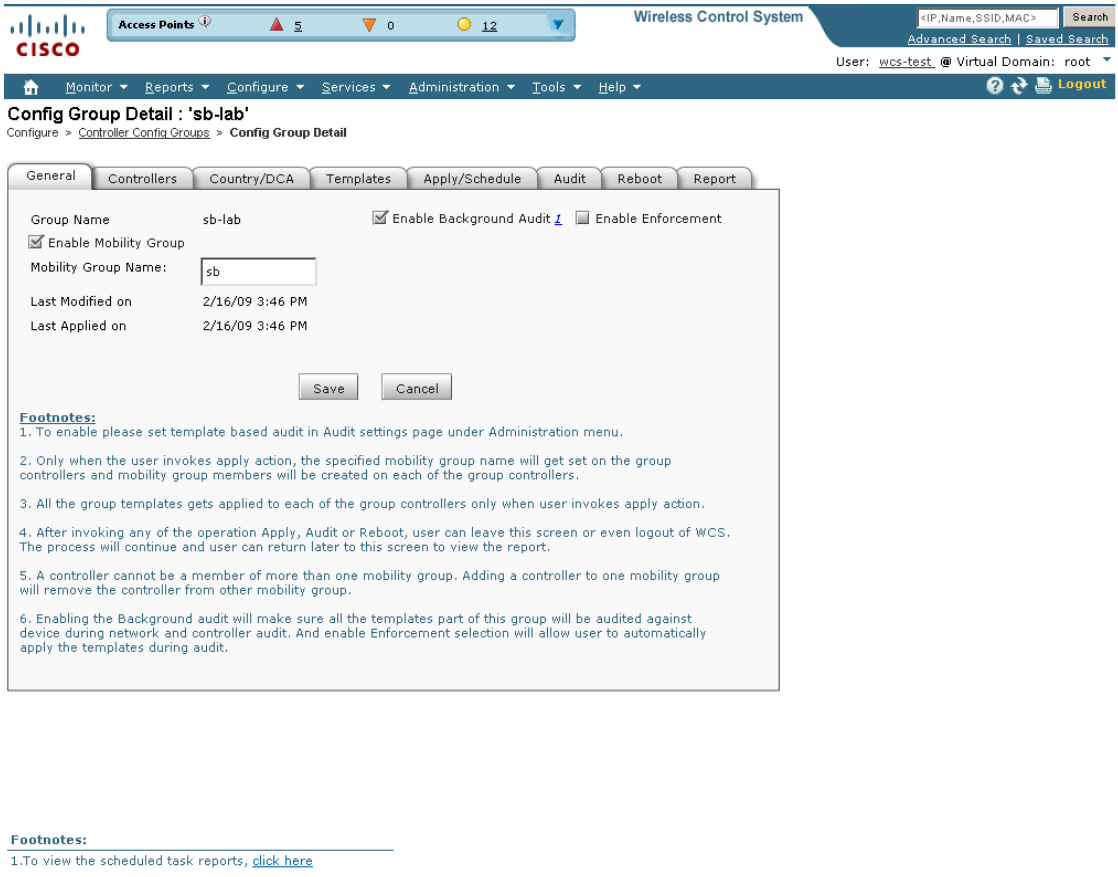
Step 4 Other templates created in WCS can be assigned to a config group. The same WLAN template can be assigned to more than one config group. Choose from the following:

- Select and add later: Click to add 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 (see Figure 8-16).

Figure 8-16 Config Groups Page



Configuring Config Groups

Follow these steps to configure a config group.

Step 1 Choose **Configure > Controller Config Groups**, and click a group name under the Group Name column. The Config Group page shown in Figure 8-16 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.
- Last Applied On: Date and time last changes were applied.

Step 3 You must choose 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 Config Group

Follow these steps to add or remove controllers from a config group.

Step 1 Choose **Configure > Controller Config Groups**, and click a group name under 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 controller's mobility group name.

Step 3 Click to highlight the row of the controller you want to add to the group.

Step 4 Click the **> 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 choose 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

Follow these steps to add or remove templates from the config group.

Step 1 Choose **Configure > Controller Config Groups**, and click a group name under 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 the **>> Add** button 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 the **<< Remove** button.

Step 5 You must choose the **Apply/Schedule** tab and click the **Apply** button to add or remove the templates to the config groups.

Step 6 Click the **Save Selection** button.

Applying or Scheduling Config Groups

Follow these steps to apply the mobility groups, mobility members, and templates to all the controllers in a config group. The scheduling function allows you to schedule a start day and time for provisioning.

Step 1 Choose **Configure > Controller Config Groups**, and click a group name under 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 Cisco WCS. 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 controller's configuration complies with the group templates and mobility group. During the audit, you can leave this screen or logout of Cisco WCS. 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.

Follow these steps to perform a config group audit.

Step 1 Choose **Configure > Controller Config Groups**, and click a group name under 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**.

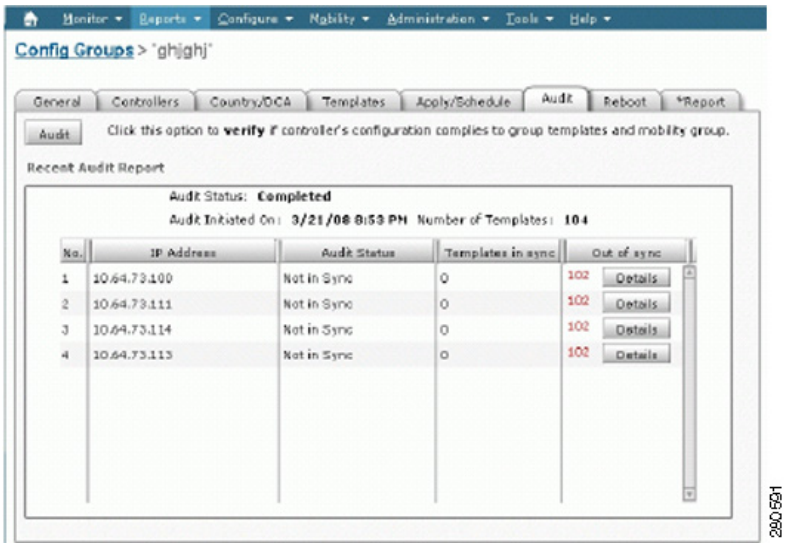
Step 4 Click to highlight a template from the Templates tab, choose **>>** (Add), and **Save Selection**.

Step 5 Click **Audit** to begin the auditing process (see Figure 8-17).

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.

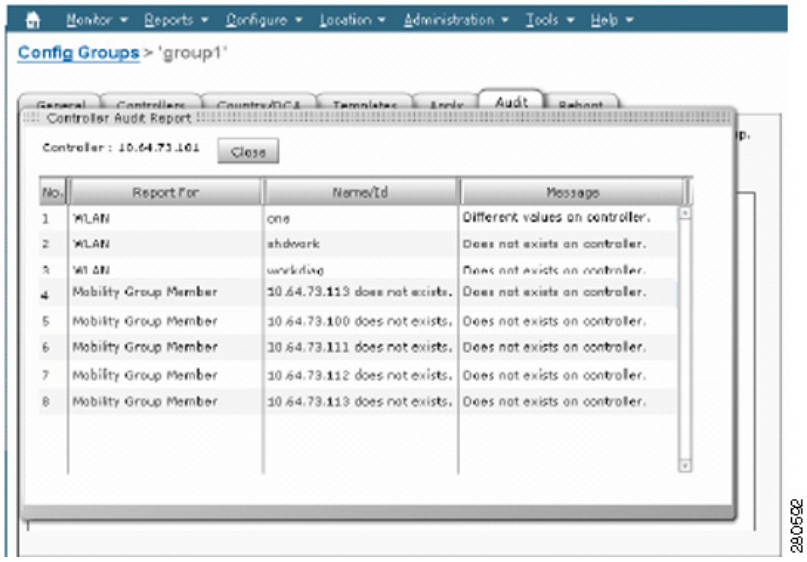
Note This audit does not enforce the WCS configuration to the device. It only identifies the discrepancies.

Figure 8-17 Config Groups Audit Tab



Step 6 Click **Details** to view the Controller Audit Report details (see Figure 8-18).

Figure 8-18 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 WCS, and its value in the controller.

Note Click **Retain WCS 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

Follow these steps to reboot a config group.

Step 1 Choose **Configure > Controller Config Groups**, and click a group name under 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 Cisco WCS. 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 WCS 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

Follow these steps to display all recently applied reports under a specified group name.

Step 1 Choose **Configure > Controller Config Groups**, and click a group name under the Group Name column.

Step 2 Click the **Report** tab. The Recent Apply Report page displays all recently applied reports including the apply status, the date and time the apply was initiated, and the number of templates. The following information is provided for each individual IP address:

- Apply Status—Indicates success, partial success, failure, or not initiated.
- Successful Templates—Indicates the number of successful templates associated with the applicable IP address.
- Failures—Indicates the number of failures with the provisioning of mobility group, mobility members, and templates to the applicable controller.
- Details—Click Details to view the individual failures and associated error messages.

Step 3 If you want to view the scheduled task reports, click the **click here** link at the bottom of the page. You are then redirected to the Configure > Scheduled Configuration Tasks > Config Group menu where you can view reports of the scheduled config groups.

Downloading Software

Follow these steps to download software to all controllers in the selected groups after you have a config group established.

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 parameter.

Step 5 Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries parameter.

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 parameter.

Step 7 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. The controller uses this local file name 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 parameter, and the Server File Name is populated for you and retried.

Step 8 Click **OK**.

Downloading IDS Signatures

Follow these steps to download Intrusion Detection System (IDS) signature files from your config group to a local TFTP server.

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 Signature**s 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 parameter.

Step 5 Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries parameter.

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 parameter.

Step 7 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. The controller uses this local file name 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 parameter, and the Server File Name is populated for you and retried.

Step 8 Click **OK**.

Downloading Customized WebAuth

Follow these steps to download customized web authentication.

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 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 parameter.

CHAPTER 9

Configuring Access Points

This chapter describes how to configure access points in the Cisco WCS database. This chapter contains the following sections:

- Setting AP Failover Priority, page 9-1
- Configuring Global Credentials for Access Points, page 9-2
- Configuring Ethernet Bridging and Ethernet VLAN Tagging, page 9-3
- Autonomous to Lightweight Migration Support, page 9-9
- Configuring Access Points, page 9-17
- Configuring Access Point Radios for Tracking Optimized Monitor Mode, page 9-33
- Searching Access Points, page 9-35
- Viewing Mesh Link Details, page 9-36
- Viewing or Editing Rogue Access Point Rules, page 9-36
- Configuring Spectrum Experts, page 9-37
- OfficeExtend Access Point, page 9-39
- Configuring Link Latency Settings for Access Points, page 9-40

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 may 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 then configure an access point's priority, refer to "Configuring Access Points" section on page 9-17.

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 access point's console port.

In WCS 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 WCS 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 Access Point Templates" section on page 12-113 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's console port. When you log in, you are in non-privileged mode, and you must enter the enable password in order 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 an access point's console port. If necessary, you can clear the access point configuration to return the access point username and password to the default setting.

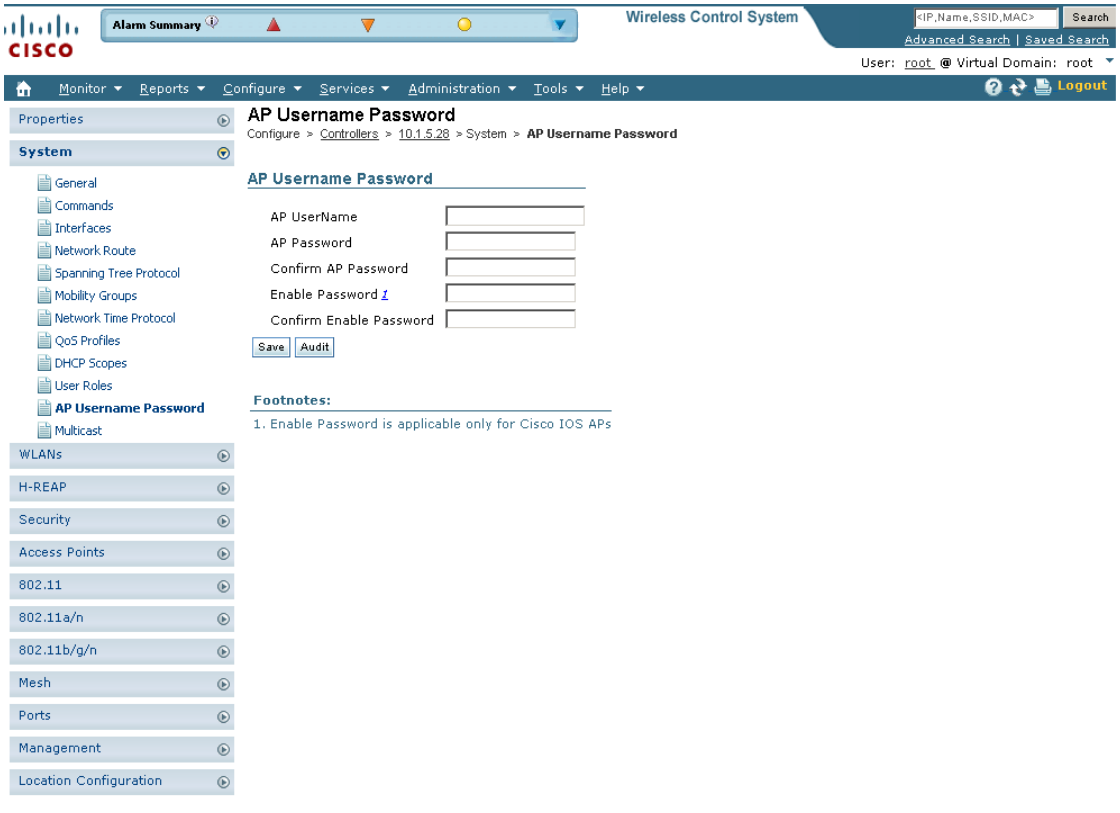
Follow these steps to establish a global username and password.

Step 1 Choose **Configure > Controllers** or **Configure > Access Points**.

Step 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.

Step 3 Choose **System > AP Username Password** from the left sidebar menu. The AP Username Password page appears (see Figure 9-1).

Figure 9-1 AP Username Password Page



Step 4 In the AP Username text box, enter the username that is to be inherited by all access points that join the controller.

Step 5 In the AP Password text box, enter the password that is to be inherited by all access points that join the controller. Re-enter in the Confirm AP Password text box.

Step 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. Re-enter in the Confirm Enable Password text box.

Step 7 Click **Save**.

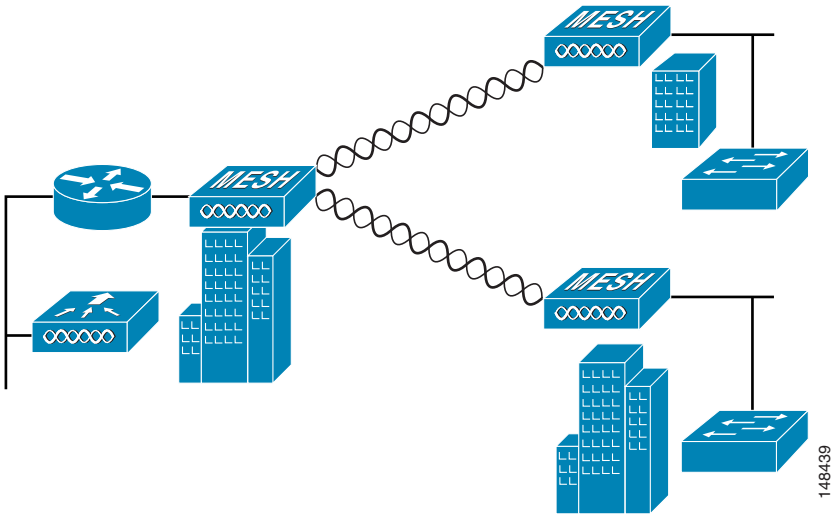
Configuring Ethernet Bridging and Ethernet VLAN Tagging

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 9-2).

Note You do not need to configure VLAN tagging to use Ethernet bridging for point-to-point and point-to-multipoint bridging deployments.

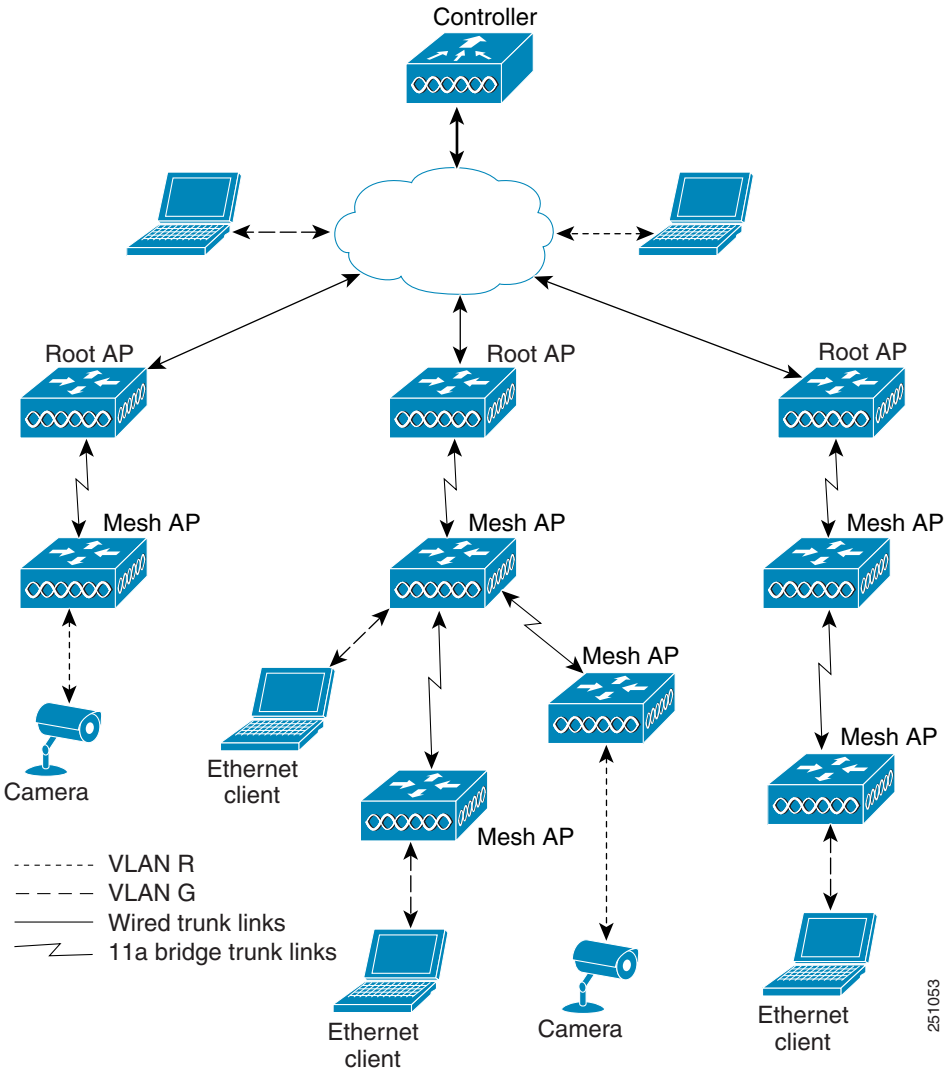
Figure 9-2 Point-to-Multipoint Bridging



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 9-3).

Figure 9-3 Ethernet VLAN Tagging



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 parameter). See "Configuring Ethernet Bridging and Ethernet VLAN Tagging" section on page 9-3.
  - 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 a RAP's children (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 RAP's primary Ethernet interface is by default the native VLAN of 1.

Enabling Ethernet Bridging and VLAN Tagging

Follow these steps to enable Ethernet Bridging and VLAN tagging on a RAP or MAP.

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

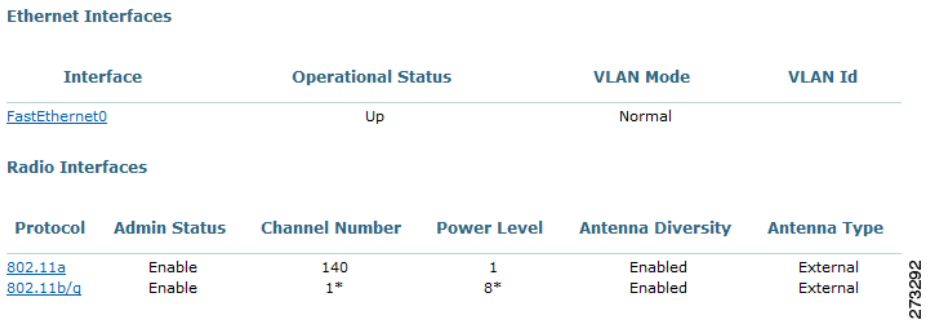
Step 2 Click the name of the mesh access point for which you want to enable Ethernet bridging. A configuration page for the access point appears.

Step 3 In the Bridging Information section, 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.

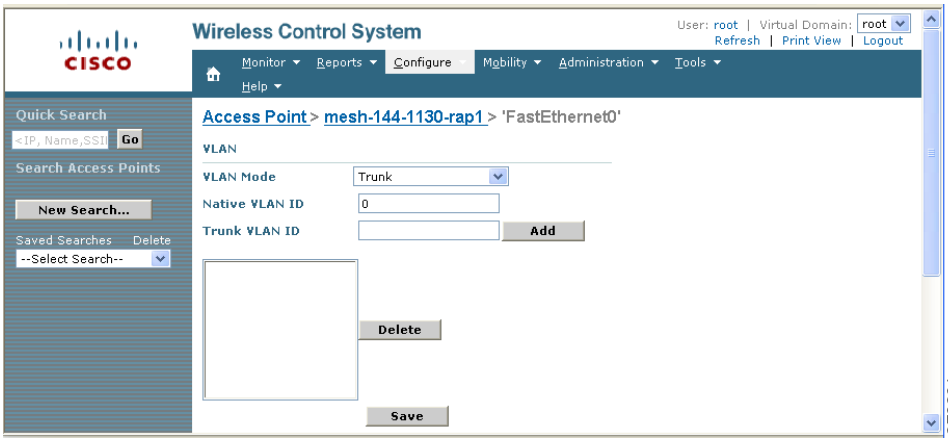
Step 5 Click the appropriate Ethernet interface link (such as FastEthernet or gigabitEthernet1). (See Figure 9-4.)

Figure 9-4 Configure > Access Points > AP Name Page



Step 6 Within the Ethernet interface page, perform one of the following (see Figure 9-5):

Figure 9-5 Access Point > Ethernet Interface Page



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.

Note A maximum of 16 VLANs in total are supported across all of a RAP's subordinate MAPs.

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 (WCS) 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 may 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 WCS, the following functions are available when managing autonomous access points:

- Adding Autonomous access points
- Configuring autonomous access points
- Viewing current autonomous access points from the Monitor > Access Points page (see Monitoring Access Points for more information)
- Adding and viewing autonomous access points from the Monitor > Maps page (see Maps for more information)
- Monitoring associated alarms
- Performing an autonomous access point background task
  - Checks the status of autonomous access points managed by WCS.
  - 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
- Migrating autonomous access points to lightweight access points

Adding Autonomous Access Points to WCS

From WCS, the following methods are available for adding autonomous access points:

- Add autonomous access points by Device information (IP addresses and credentials).
- Add autonomous access points by CSV file.

Adding Autonomous Access Points by Device Information

Autonomous access points can be added to WCS 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 Select **Device Info** from the Add Format Type drop-down list.

Step 5 Enter comma-separated IP addresses of autonomous access points.

Step 6 Select the **Verify Telnet/SSH Credentials** check box if you want this controller to verify Telnet/SSH credentials. The Telnet/SSH parameters are required by CLI templates and for conversion of autonomous access points to unified.

Step 7 Enter the SNMP parameters including version number, number of retries, and timeout in seconds.

Step 8 (Optional) Enter Telnet credentials for migration.

Note The Telnet credentials are required to convert the access points from autonomous to unified and for access point CLI templates.

Note If the autonomous access point already exists, WCS updates the credentials (SNMP and Telnet) to the existing device.

Step 9 Click **OK**.

Adding Autonomous Access Points by CSV File

Autonomous access points can be added to WCS 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 Select **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,Cisco,Cisco,2,10

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
209.165.200.224,255.255.255.224,v3,default,HMAC-MD5,default,None,,3,4
209.165.201.0,255.255.255.224,v3,default1,HMAC-MD5,default1,DES,default1,3,4,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

Step 6 Click **OK**.

To remove an autonomous access point from WCS:

Step 1 Select the check boxes of the access points you want to remove.

Step 2 Select **Remove APs** from the Select a Command drop-down list.

Viewing Autonomous Access Points in WCS

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:

- 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 selecting **Add Access Points** from the Select a Command drop-down list.

Downloading Images to Autonomous Access Points

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 WCS. Follow these steps to download images to autonomous access points.

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

Step 2 Click 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**. The image download page appears.

To ensure that no more than ten access points are selected for download, a check is made. The image must be compatible with all of the selected access points. Scheduling an immediate task initiates the image download. It is periodically refreshed.

Work Group Bridge (WGB) Mode

Wireless Group 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 client in WCS if the AP mode is set to Bridge, and the access point is bridge capable.

To view a list of all WCS clients that are WGBs, choose **Monitor > Clients**. At 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 The WCS provides WGB client information for the autonomous access point whether or not it is managed by the WCS. If the WGB access point is also managed by the WCS, WCS provides basic monitoring functions for the access point similar to other autonomous access points.

Autonomous Access Point to Lightweight Access Point Migration

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 will start at the scheduled time. When the template is in this state, you can click the Name link to edit the template.
  - Disabled—The template is disabled and will not run at the scheduled time. This is the default state for a template when it is created without selecting any autonomous access points. When the template is in this state, you can click the Name link to edit the template.
  - Expired—The template did not run at the scheduled time (this may be due to the WCS server being down). When the template is in this state, you can click the Name link to edit the template.
  - Enabled—The template is yet to start the migration and will start at the scheduled time. When the template is in this state, you can click the Name link to edit the template.
  - In progress—The template is currently converting the selected autonomous access points to CAPWAP. When the template is in this state, you cannot edit the template by clicking the Name link.
  - Success—The template has completed the migration of autonomous access point to CAPWAP successfully. When the template is in this state, you cannot edit the template by clicking the Name link.
  - 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. When the template is in this state, you cannot edit the template by clicking the Name link.
  - 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. When the template is in this state, you cannot 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 re-enter the information. WCS 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.

Viewing the Migration Analysis Summary

Follow these steps to view the Migration Analysis Summary.

Note You can also view the migration analysis summary by choosing Tools > Migration Analysis.

Step 1 Choose **Configure > Autonomous AP Migration Templates**.

Step 2 Click **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 from Cisco IOS 12.3(7)JA releases 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 in order 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.

Upgrading Autonomous Access Points

You can choose to upgrade the autonomous access points manually or automatically. From the Migration Analysis page, you can select the access point with the software version listed as failed and choose Upgrade Firmware (Manual or Automatic) from the Select a command drop-down list. This process upgrades the autonomous firmware image of the Cisco IOS access point to a supported version.

WCS uses a Telnet-based connection to upgrade the access point firmware. If you choose the automatic option, the internal TFTP server is used with the default images present in WCS. The default images as per device type are as follows:

- ap801-k9w7-tar.124-10b.JA3.tar
- c1100-k9w7-tar.123-7.JA5.tar
- c1130-k9w7-tar.123-7.JA5.tar
- c1200-k9w7-tar.123-7.JA5.tar
- c1240-k9w7-tar.12307.JA5.tar
- c1250-k9w7-tar.124-10b.JA3.tar
- c1310-k9w7-tar.123-7.JA5.tar

If you choose the manual option, an additional screen with TFTP server IP, file path, and file path name appears. The final page is the report page.

Changing Station Role to Root Mode

Because a wired connection between the access point and controller is required in order to send the association request, the autonomous access point must be assigned the appropriate role. If the role shows as ineligible, you can choose **Change Station Role to Root Mode** from the Select a command drop-down list.

Running Migration Analysis

You can choose **Run Migration Analysis** from the Select a command drop-down list of the Migration Analysis Summary page. The resulting migration analysis summary shows the current status of different criteria. Initially, migration analysis is run automatically when the access point is discovered.

Generating the Migration Analysis Report

You can choose **View Migration Analysis Report** from the Select a command drop-down list of the Migration Analysis Summary page to generate a report. The report includes the following:

- Access point address
- Status
- Timestamp
- Access point logs

Adding/Modifying a Migration Template

If you want to add a migration template, choose **Add Template** from the Select a command drop-down page of 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

When you installed and set up WCS, it provided its own TFTP and FTP server.

- TFTP Server IP—Enter the IP address of the WCS server.
- File Path—Enter the TFTP directory which was defined during WCS setup.
- File Name—Enter the CAPWAP conversion file defined in the TFTP directory during WCS setup (for example, c1240-rcvk9w8-tar.123-11JX1.tar).

Schedule Details

This area enables you to specify scheduling options for migration templates.

- Apply Template—Select an option by which you want to apply the template for migration.
  - Now—Select 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. Select the time from the hours and minutes drop-down lists. The report will begin running on this data and at this time.
- (Optional) Notification—Enter the e-mail address of recipient to send notifications via e-mail.

Note To receive email notifications, configure the WCS mail server in the Administration > Settings > Mail Server Configuration page.

- Click **Save**.

Once a template is added in WCS, the following additional buttons appear:

- **Select APs**—Selecting this option provides a list of autonomous access points in WCS 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.

Configuring Access Points

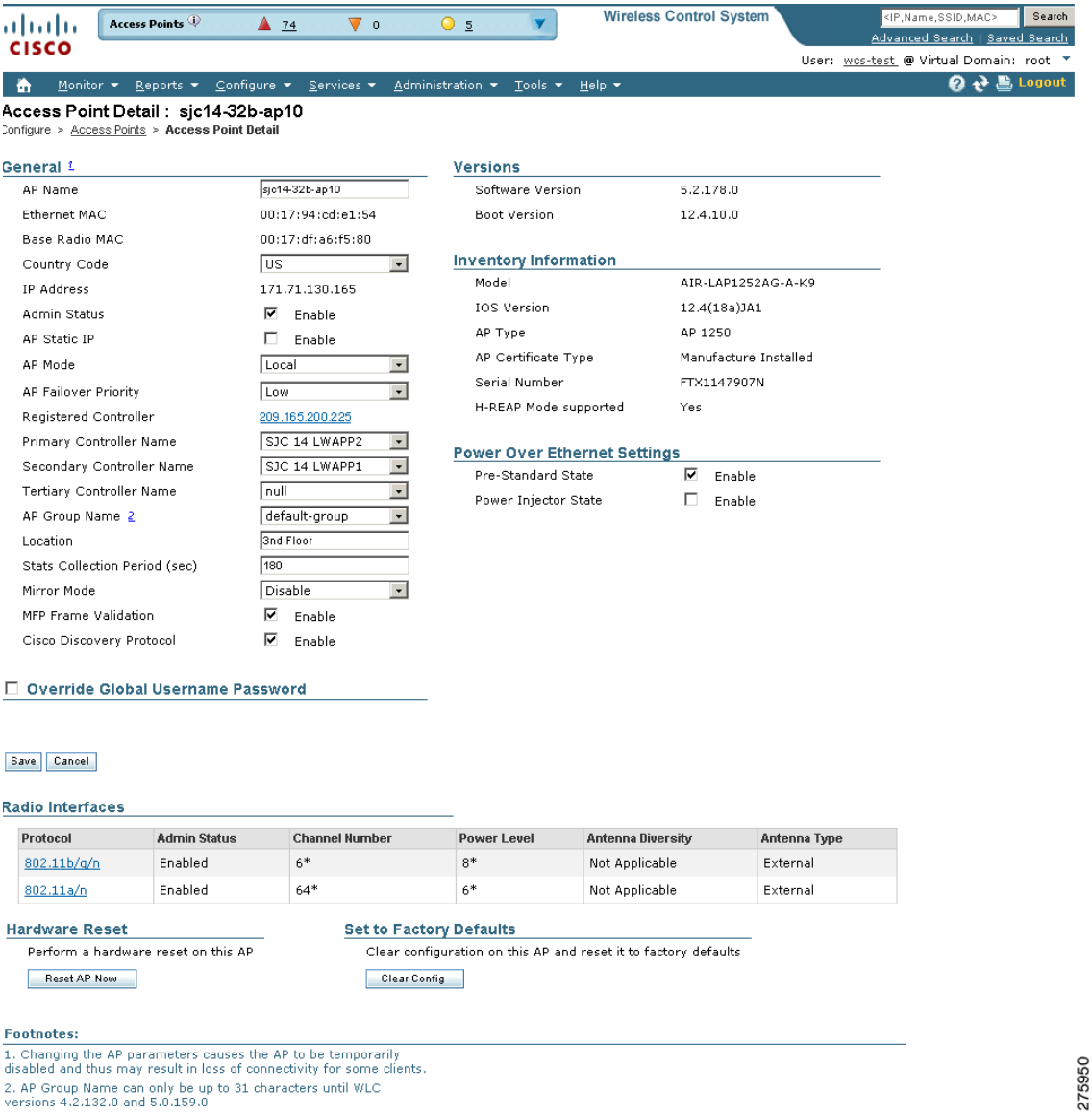
Choose **Configure > Access Points** to see a summary of all access points in the Cisco WCS database. The summary information includes the following:

- Ethernet MAC
- IP Address
- Radio
- Map Location
- AP Type
- Controller
- Operation Status
- Alarm Status
- Audit Status

Note If you hover your mouse over the Audit Status value, the time of the last audit is displayed.

Step 1 Click the link under AP Name to see detailed information about that access point name. The Access Point Detail page appears (see Figure 9-6).

Figure 9-6 Detailed Access Point Information



Note The operating system software automatically detects and adds an access point to the Cisco WCS database as it associates with existing controllers in the Cisco WCS database.

Note Access point parameters may vary depending on the access point type.

Some of the parameters on the page are automatically populated.

- The General portion displays the Ethernet MAC, the Base Radio MAC, IP Address, and status.
- The Versions portion of the page displays the software and boot version.

- The Inventory Information portion displays the model, AP type, AP certificate type, serial number, and REAP mode support.
- The Radio Interfaces portion provides the current status of the 802.11a/n and 802.11b/g/n radios such as admin status, channel number, power level, antenna mode, antenna diversity, and antenna type.

Follow the steps below to set the configurable parameters.

Note Changing access point parameters causes the access point to be temporarily disabled and this may 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 your country's regulations. 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 may be set to exceed these limitations (or you may 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 may 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 your country's regulatory domain. For a complete list of country codes supported per product, refer to this location:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html.

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.
- H-REAP—Choose **HREAP** from the AP Mode drop-down list to enable Hybrid REAP for up to six access points. The H-REAP access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost.

- 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.

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 9-33 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, choose Monitor. Choose the **Enhanced wIPS Engine Enabled** check box and select **wIPS** from the Monitor Mode Optimization drop-down list. If wIPS is disabled, you cannot use monitor mode optimization.
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 displays. After you have enabled the access point for wIPS, re-enable the radios.

- 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 www.wildpackets.com/products/airopeek/overview.
- 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 WCS 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 access point's failover priority. The default priority is low. See "Setting AP Failover Priority" section on page 9-1 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 parameter, 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. In order 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 Click 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 in order 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. See the "Rogue Access Point Location, Tagging, and Containment" section on page 16-21 for more information on 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, refer to 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. Encryption is available only if the access point is connected to a 5500 series controllers with a PLUS license.

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 may be connected directly to the WAN which could allow 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 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 On 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 9-40 for more information on link latency.

Step 23 You can now manipulate power injector settings through WCS 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 checked, 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 WCS, go to 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 H-REAP configurations:

Note H-REAP settings cannot be changed when the access point is enabled.

- OfficeExtend AP—The default is Enabled.

  Note Clearing 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 since it becomes remotely deployed. If you want to clear the access point's configuration 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 access point's personal SSID, 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 may 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.

- Enable VLAN—When selected, enter the Native VLAN identifier.

  When Enable VLAN is selected, WCS displays locally switched VLANs.

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 parameter appears whether the mesh access point is an indoor or outdoor access point, and the Backhaul Interface parameter displays the access point radio that is being used as the backhaul for the access point.

Step 27 Select 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**.

Downloading Images

From the Select a command drop-down list in the Configure > Access Points page, you can select Download Autonomous AP Image. TFTP is used for the download. WCS verifies that no more than ten access points are selected for download. An appropriate warning also appears if another download is in progress. The image must be compatible with all of the selected access points prior to image download. The image download starts immediately and cannot be scheduled for a future time. An image download status screen is displayed and refreshed periodically.

Importing Access Point Configuration

From the Select a command drop-down list in the Configure > Access Points page, you can download the startup configurations of access points that are saved in the WCS database using the Import AP Config command. Only the most recent configuration is maintained in the WCS database. You cannot download a single configuration to multiple access points with this feature. For multiple access points, you must instead use the Modify Access Point Configuration feature. You can click the Session Output icon to see the session playback of the Cisco IOS command.

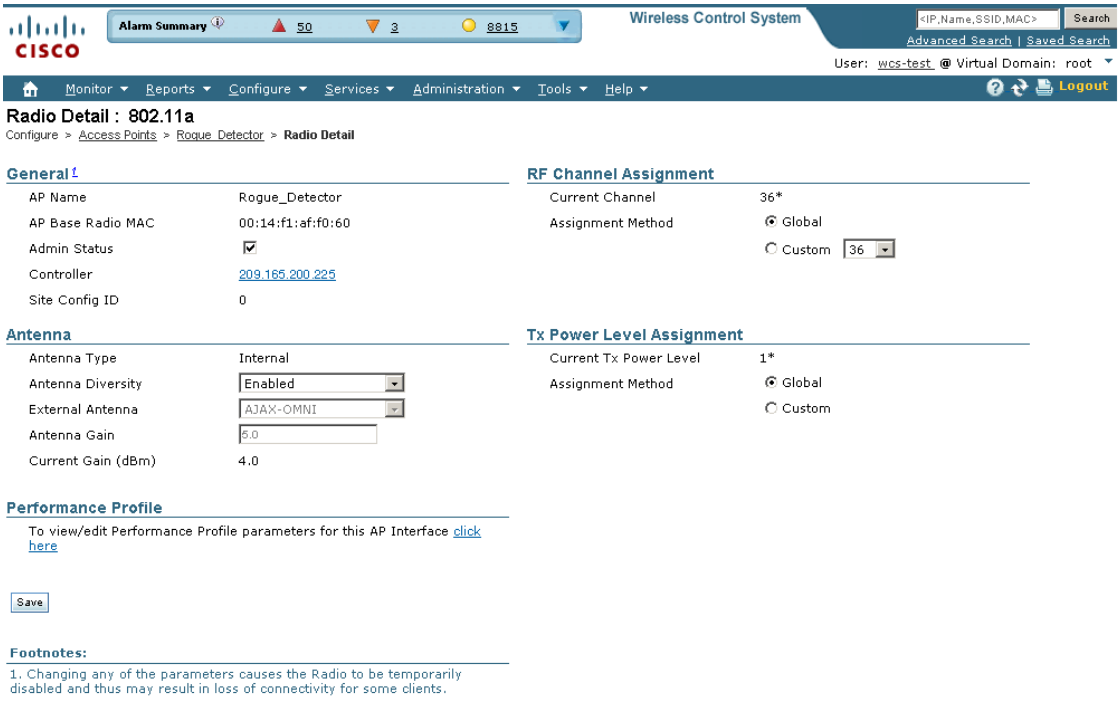
11n Antenna Selection

WCS 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 (see Figure 9-7).

Figure 9-7 Access Point > 802.11a/n



The following 11n Parameters display and can be modified:

Note Changing any of the parameters causes the radio to be temporarily disabled and thus may 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 access point's base radio.
- Admin Status—Select the box to enable the administration state of the access point.
- Controller—IP address of the controller. Click the controller's IP address for more details.
- Site Config ID—Site identification number.
- CleanAir Capable—Displays if the access point is CleanAir capable.
- CleanAir—Select the check box to enable CleanAir.

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 access point's left connector.
  - Right—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's right connector.

  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—Select the external antenna or Other from the drop-down list.
- 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 dBm. An integer value 4 means 4 x 0.5 = 2 dBm of gain.

- Current Gain (dBm)—Indicates the current gain in dBm.

Table 9-1 Antenna Names, Gain, and Descriptions

Antenna Name	Gain (dBi)	Description
AIR-ANT1000	0.00	AP 1000 Integrated antenna
CUSH-S5157WP	3.00	5.15-5.87 GHz diversity wideband panel antenna (side gain and back attenuation)
KODIAK-DIRECTIONAL	8.00	Integrated Kodiak directional antenna
KODIAK-OMNI	5.00	Kodiak omni antenna
AIR-ANT1728	5.20	Omni ceiling mount antenna
AIR-ANT1729	6.00	Patch wall mount antenna
AIR-ANT2012	6.50	Diversity patch wall mount antenna
AIR-ANT2410Y-R	10.00	Yagi master or wall mount antenna
AIR-ANT5959	2.00	Omni diversity ceiling mount antenna
AJAX-OMNI	5.00	Integrated Ajax omni antenna
AIR-ANT5135D-R	3.50	Omni dipole antenna
AIR-ANT5135DW-R	3.50	3.5-dBi white dipole antenna
AIR-ANT5135DG-R	3.50	3.5 dB5 gray non-articulating dipole antenna
AIR-ANT2422DW-R	2.20	2.2-dBi white dipole antenna
AIR-ANT2422DB-R		
AIR-ANT2422DG-R	2.20	2.2 dBi gray non-articulating dipole antenna
AIR-ANT5145V-R	4.50	Omni diversity antenna
AIR-ANT5160V-R	6.00	Omni antenna
AIR-ANT3549	9.00	Patch wall mount antenna
AIR-ANT4941	2.20	Omni dipole antenna
AIR-ANT2506	0.00	Omni mass mount antenna
AIR-ANT3213	5.20	Omni diversity pillar antenna
CUSH-S24516DBP	3.00	Integrated 2.4/5 GHz hemispheric pattern
CUSH-S5153WBPX	6.00	Ceiling mount 6-dBi omni
AIR-ANT5170V-R	7.00	Wall mount diversity patch antenna
AIR-ANT5175V	7.50	Omni antenna for Wireless Bridge
AIR-ANT5195V-R	9.50	Wall mount patch antenna
AIR-ANT58G10SSA	9.50	Sector antenna for Wireless Bridge
AIR-ANT2455V	5.50	Omni antenna for Wireless Bridge
CUSH-S54717P	17.00	Patch array antenna for Wireless Bridge
CUSH-S49014WP	14.00	Patch array antenna for Wireless Bridge
CUSH-S2406BP	8.00	Omni antenna for Wireless Bridge
AIR-ANT1100	2.20	Default antenna for AP1100
BR1310	13.00	Integrated patch directional antenna
AIR-ANT2460	6.00	Patch wall mount antenna

Table 9-1 Antenna Names, Gain, and Descriptions (continued)

Antenna Name	Gain (dBi)	Description
AIR-ANT2465	6.50	Diversity patch wall mount antenna
AIR-ANT2485	9.00	Patch wall mount antenna
AIR-ANT2480V-N	8.00	2.4 GHz omni antenna for mesh
AIR-ANT5114P-N	14.00	5 GHz patch for mesh
AIR-ANT5117S-N	17.00	5 GHz sector for mesh
AIR-ANT2450V-N	5.00	2.4 GHz omni antenna
AIR-ANT5180V-N	8.00	5 GHz omni antenna
AIR-ANT2450S-R	5.50	2.4 GHz 135-degree sector antenna
AIR-ANT2451V-R	2.4 GHz—2.0 5 GHz—3.0	2.4 GHz and 5 GHz four-element dual band antenna. **Note** Two elements for the 2.4 GHz band and two elements for the 5 GHz band.
AIR-ANT2460NP-R	6.00	2.4 GHz MIMO (3-Element) Patch Antenna
AIR-ANT5160NP-R	6.00	5 GHz MIMO (3-Element) Patch Antenna
AIR-ANT2422SDW-R	2.20	2.4 GHz “Stubby” white monopole antenna
AIR-ANT5135SDW-R	3.50	5 GHz "Stubby" white monopole antenna
AIR-ANT2451NV-R	2.4 GHz—2.5 5 GHz—3.5	2.4 GHz and 5 GHz “6-pack” ceiling mount omni antenna
AIR-ANT2452V-R	5.2	2.4 GHz Diversity Wall Mount Omni-directional Antenna **Note** This is a replacement antenna to the existing AIR-ANT3213.
AIR-ANT24020V-R	2.0	External omni diversity ceiling mount antenna **Note** This is a replacement antenna to the existing antenna AIR-ANT5959.

The following table lists the default values of some of the attributes of an access point when it is added to the WCS for the first time:

AP Type	Radio Type	Supported Antennas
AP 1200	802.11a	KODIAC-OMNI, KODIAK-DIRECTIONAL, AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R
	802.11b/g	AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1240	802.11a	AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R

AP Type	Radio Type	Supported Antennas
	802.11b/g	AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1131	802.11a	AJAX-OMNI
	802.11b/g	AJAX-OMNI
AP 1100	802.11b/g (only b/g)	AIR-ANT1100
AP 1310	802.11a	AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R
	802.11b/g	BR1310, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1250	802.11a	AIR-ANT5135D-R, AIR-ANT5135SDW-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5160NP-R, AIR-ANT5170V-R, AIR-ANT5195V-R, AIR-ANT2451NV-R-5GHz
	802.11b/g	AIR-ANT2460, AIR-ANT2460NP-R, AIR-ANT2422SDW-R, AIR-ANT2451NV-R-2.4GHz, AIR-ANT2465, AIR-ANT2485, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT3213, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1000	802.11a	AIR-ANT1000, AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R, CUSH-S5157WP, CUSH-S24516DBP
	802.11b/g	AIR-ANT1000, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT5959, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, CUSH-S24516DBP, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1030	802.11a	AIR-ANT1000, AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R, CUSH-S5157WP, CUSH-S24516DBP
	802.11b/g	AIR-ANT1000, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT5959, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, CUSH-S24516DBP, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1500	802.11a	AIR-ANT5175V, AIR-ANT58G10SSA, CUSH-S54717P, CUSH-S49014WP
	802.11b/g	AIR-ANT2455V, CUSH-S2406BP
AP 1505	802.11a	AIR-ANT5175V, AIR-ANT58G10SSA, CUSH-S54717P, CUSH-S49014WP
	802.11b/g	AIR-ANT2455V, CUSH-S2406BP

AP Type	Radio Type	Supported Antennas
AP 1260	802.11a	AIR-ANT5135DG-R, AIR-ANT5135D-R, AIR-ANT5135DB-R, AIR-ANT5135DW-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R, AIR-ANT5140V-R, AIR-ANT2451V-R, AIR-ANT2450S-R, AIR-ANT5135SDW-R, AIR-ANT2451NV-R-5GHz, AIR-ANT5160NP-R
	802.11b/g	AIR-ANT2422DG-R, AIR-ANT4941, AIR-ANT2422DB-R, AIR-ANT2422DW-R, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT3213, AIR-ANT2430V-R, AIR-ANT24120, AIR-ANT2414S-R, AIR-ANT1949, AIR-ANT2451V-R, AIR-ANT2450S-R, AIR-ANT2460NP-R, AIR-ANT2422SDW-R, AIR-ANT2451NV-R-2.4GHz, AIR-ANT24020V-R, AIR-ANT2452V-R
AP 1040	802.11a	Internal-1040-5.0 GHz
	802.11b/g	Internal-1040-2.4 GHz
AP 1140	802.11a	Internal-1140-5.0 GHz
	802.11b/g	Internal-1140-2.4 GHz
AP 3500e	802.11a	AIR-ANT5135DG-R,AIR-ANT5135D-R,AIR-ANT5135DB-R,AIR-ANT5135DW-R,AIR-ANT5145V-R,AIR-ANT5160V-R,AIR-ANT5170V-R,AIR-ANT5195V-R,AIR-ANT5140V-R,AIR-ANT2451V-R,AIR-ANT2450S-R,AIR-ANT5135SDW-R,AIR-ANT2451NV-R-5GHz,AIR-ANT5160NP-R
AP 3500e	802.11b/g	AIR-ANT2422DG-R,AIR-ANT4941,AIR-ANT2422DB-R,AIR-ANT2422DW-R,AIR-ANT2460,AIR-ANT2465,AIR-ANT2485,AIR-ANT1728,AIR-ANT2012,AIR-ANT1729,AIR-ANT2410Y-R,AIR-ANT5959,AIR-ANT3549,AIR-ANT2506,AIR-ANT3213,AIR-ANT2430V-R,AIR-ANT24120,AIR-ANT2414S-R,AIR-ANT1949,AIR-ANT2451V-R,AIR-ANT2450S-R,AIR-ANT2460NP-R,AIR-ANT2422SDW-R,AIR-ANT2451NV-R-2.4GHz,AIR-ANT24020V-R,AIR-ANT2452V-R
AP 3500i	802.11a	Internal-3500i-5 GHz
AP 3500i	802.11b/g	Internal-3500i-2.4 GHz

WLAN Override

The following 802.11a WLAN Override parameter 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 display:

- Current Channel—Channel number of the access point.
- Assignment Method—Select one of the following:
  - Global—Use this setting if your access point's channel is set globally by the controller.
  - Custom—Use this setting if your access point's channel 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.

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 your access point's power level is set globally by the controller.
  - Custom—Use this setting if your access point's power level is set locally. Choose a power level from the drop-down list.

11n Antenna Selection

WCS 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.

The following 11n Antenna Selection parameters appear:

- Transmit Antenna—Click the check box beside Antenna A or Antenna B to enable them.
- Receive Antenna—Click the check box beside Antenna A, B, or C to enable them.

11n Parameters

The following 11n parameters display:

- 11n Supported—Indicates whether or not 802.11n radios are supported.

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, refer to Step 6 in the "Configuring Access Points" section on page 9-17.

Follow the steps below to set enable TOMM and assign monitoring channels on the access point radio.

Step 1 After enabling Monitor Mode at the access point level, choose **Configure > Access Points**.

Step 2 In the Access Points page, choose the **802.11 b/g Radio** link for the appropriate access point.

Step 3 In the General portion, disable **Admin Status** by unchecking the check box. This disables the radio.

Step 4 Select the **TOMM** check box. This check box only appears for Monitor Mode APs. drop-down lists for each of the four configurable channels display.

Step 5 Select 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, select **None** from the channel drop-down list.

Step 6 Click **Save**. Channel selection is saved.

Step 7 In the Radio parameters page, re-enable the radio by checking 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 on the **Monitor > Access Points** page.

Scheduling Radio Status

To schedule a radio status change (enable or disable), follow these steps:

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

Step 2 Choose 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 Choose 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 on 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.

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.

Note If you hover 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 on 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.

Note The audit can only be run on an access point that is associated to a controller.

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 "Using the Search Feature" section on page 2-31 for further information.

After you click **Go**, the access point search results appear (see Table 9-2).

Table 9-2 Access Point Search Results

Parameter	Options
IP Address	IP address of the access point.
Ethernet MAC	MAC address of the access point.
AP Name	Name assigned to the access point. Click the access point name item to display details.
Radio	Protocol of the access point is either 802.11a/n or 802.11b/g/n.
Map Location	Campus, building, and floor location.

Table 9-2 Access Point Search Results (continued)

Controller	IP address of the controller.
AP Type	Access point radio frequency type.
Operational Status	Displays the operational status of the Cisco radios (Up or Down).
Alarm Status	Alarms are color coded as follows: • Clear = No Alarm • Red = Critical Alarm • Orange = Major Alarm • Yellow = Minor Alarm
Audit Status	The audit status of the access point.
Serial Number	The serial number of the access point.
AP Mode	Describes the role of the access point modes such as Local, H-REAP, Monitor, Rogue Detector, Sniffer, Bridge, or SE-Connect. (as described in Step 6 of Configuring Access Points).

Viewing Mesh Link Details

You can access mesh link details in several ways:

- Mesh Tab on the WCS home page
- Monitor > Access Points and clicking the **Mesh Links** tab and then 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 WCS 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. Follow these steps to access the rogue access point rules. See the "Configuring a Rogue AP Rules Template" section on page 12-77 for more information.

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address under 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 Spectrum Experts

A Spectrum Expert client acts as a remote interference sensor and sends dynamic interference data to WCS. This feature allows the WCS 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 WCS. The status appears as reachable or unreachable.

Adding a Spectrum Expert

To add a Spectrum Expert, follow these steps:

Step 1 Choose **Configure > Spectrum Experts**.

Step 2 Click **Add a Spectrum Expert** or choose **Add a Spectrum Expert** from the Select a command drop-down list.

Note This link only appears when no spectrum experts are added. You can also access the Add a Spectrum Expert page by choosing Add a Spectrum Expert from the Select a command drop-down list.

Step 3 Enter the Spectrum Expert's Hostname or IP address. If you use hostname, your spectrum expert must be registered with DNS in order to be added to WCS.

Note To be correctly added as a spectrum expert, the spectrum expert client must be running and configured to communicate to WCS.

Monitoring Spectrum Experts

You also have the option to monitor spectrum experts. Follow these steps to monitor spectrum experts:

Step 1 Choose **Monitor > Spectrum Experts**.

Step 2 From the left sidebar menu, you can access the **Spectrum Experts > Summary** page and the **Interferers > Summary** page.

Spectrum Experts > Summary

The Spectrum Experts Summary 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 WCS. 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.

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.
- 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 WCS.
- Discover Time—Indicates when the interferer was discovered.
- Affected Channels—Identifies affected channels.
- Number of APs Affected—The number of access points managed by WCS 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 WCS.
  - 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.

Spectrum Experts Details

The Spectrum Expert Details 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:

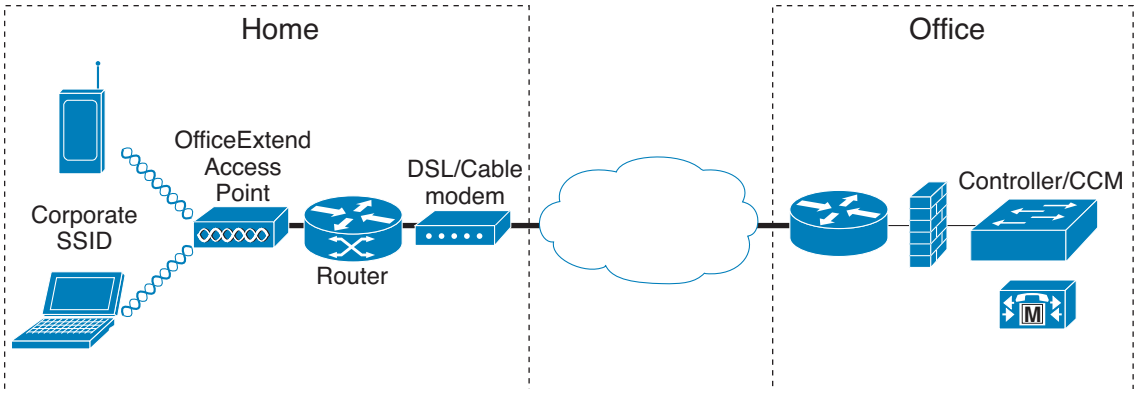
- Total Interferer Count—Given from the specific spectrum expert.
- Active Interferers Count Chart—Displays a pie chart that groups interferers by category.
- Active Interferer Count Per Channel—Displays the number of interferers grouped by category on different channels.
- AP List—Provides a list of 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 on 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 an employee's residence. The teleworker's experience at the home office is exactly the same as it would be 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 9-8 illustrates a typical OfficeExtend access point setup.

Figure 9-8 Typical OfficeExtend Access Point Setup



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 Cisco WCS database as it associates with existing controllers in the Cisco WCS 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 hybrid-REAP access points, for which the link could be a slow or unreliable WAN connection.

Note Link latency is supported for use only with hybrid-REAP access points in connected mode. Hybrid-REAP 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:

Step 1 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.

Step 2 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—Since 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—Since 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.

Step 3 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.

CHAPTER 10

Configuring Controllers and Switches

This chapter describes how to configure controllers and switches in the Cisco WCS database. This chapter contains the following sections:

- Adding Controllers, page 10-2
- Downloading Software to Controllers, page 10-4
- Discovering Templates from Controllers, page 10-9
- Displaying Templates Applied to Controller, page 10-10
- Configuring IGMP Snooping, page 10-12
- Configuring AP Timers, page 10-12
- Configuring Controller WLANs, page 10-13
- Configuring AAA General Parameters, page 10-27
- Setting Multiple Country Codes, page 10-29
- Searching Controllers, page 10-33
- Managing User Authentication Order, page 10-34
- Viewing Audit Status (for Controllers), page 10-34
- Viewing Latest Network Audit Report, page 10-37
- Configuring 802.3 Bridging, page 10-37
- Pinging a Network Device from a Controller, page 10-39
- Enabling Load-Based CAC for Controllers, page 10-39
- Sending Primary Discovery Requests, page 10-38
- Configuring an RRM Threshold Controller (for 802.11a/n or 802.11b/g/n), page 10-42
- Configuring 40-MHz Channel Bonding, page 10-42
- Configuring EDCA Parameters for Individual Controller, page 10-44
- Configuring SNMPv3, page 10-44
- Viewing All Current Templates, page 10-45
- Configuring NAC Out-of-Band Integration, page 10-45
- Configuring Wired Guest Access, page 10-51
- Using Switch Port Tracing, page 10-57
- Background Scanning on 1510s in Mesh Networks, page 10-64

- Configuring QoS Profiles, page 10-66

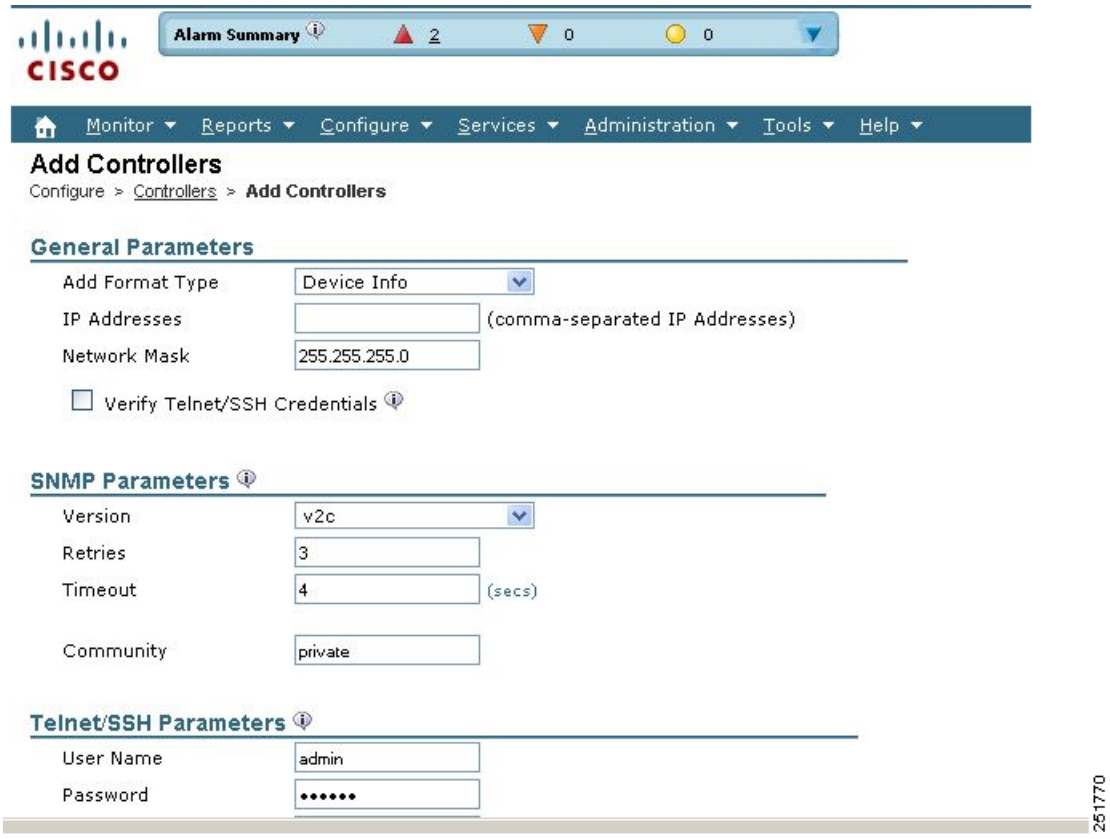
Adding Controllers

You can add controllers one at a time or in batches. Follow these steps to add controllers.

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 (see Figure 10-1).

Figure 10-1 Add Controller Page



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 WCS across a GRE link using IPsec or a lower MTU link with multiple fragments, you may need to adjust the MaxVar Binds PerPDU. If it is set too high, the controller may fail to be added into WCS. To adjust the MaxVarBindsPerPDU setting, do the following: 1) Stop WCS. 2) Go to the location of the Open SnmpParameters.properties file on the server that is running WCS. 3) Edit MaxVarBindsPerPDU to 50 or lower. 4) Restart WCS.

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 WCS. 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 sample CSV files are as follows:

Table 10-1 Sample CSV Files

ip_address	snmp_version	snmp_community	network_mask
209.165.200.224	v2	public	255.255.255.224
209.165.200.225	v2	public	255.255.255.224
209.165.200.226	v2	private	255.255.255.224
209.165.200.227	v2	private	255.255.255.224

The CSV files can contain the following fields:

- ip_address
- network_mask
- snmp_version
- snmpv2_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout
- telnet_user_name
- telnet_password
- telnet_retries
- telnet_timeout

Step 5 Select the **Verify Telnet/SSH Credentials** check box if you want this controller to verify Telnet/SSH credentials. You may want to leave this unselected (or disabled) because of the substantial time it takes for discovery of the devices.

Step 6 Use the Version drop-down list to choose v1, v2c, or v3.

Step 7 In the Retries parameter, 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 parameter, 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 will apply 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 WCS, and if the error message ‘Sparse table not supported' occurs, verify that WCS and WLC versions are compatible and retry. For information on compatible versions, see http://www.cisco.com/en/US/products/ps6366/products_tech_note09186a0080af7140.shtml.

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 WCS. In previous software releases, only TFTP was supported.

- Download Software (FTP)
- Download Software (TFTP)
- Configure IPaddr > Upload Configuration/Logs from Controller

Download 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 version 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 email notifications, configure the WCS mail server in **Administration > Settings > Mail Server Configuration** page.

Step 7 Enter the FTP credentials including username, password, and port.

Step 8 In the **File is located on** parameter, click either the **Local machine** or **FTP Server**.

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 file name 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 parameter; the server filename is populated and retried.

Download 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.

Note The pre-download option is displayed only when all selected controllers are using the version 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.
  - 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.

    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 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.

  Note 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.

  Note Schedule enough time (at least 30 minutes) 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 email notifications, configure the WCS mail server in the **Administration > Settings > Mail Server Configuration** page.

Step 7 From the File is located on parameter, choose **Local machine** or **TFTP server**.

Note If you choose TFTP server, select the Default Server or add a New server using the Server Name drop-down list.

Step 8 From the Maximum Retries parameter, enter the maximum number of tries the controller should attempt to download the software.

Step 9 In the Timeout parameter, 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 file name or click **Browse** to navigate to the appropriate file.

Note If you selected TFTP server previously, specify the Server File Name.

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 parameter; the Server File Name is populated and retried.

Configure *IPaddr* > Upload Configuration/Logs from Controller

To upload files from the controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address under 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 WCS. 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)/wcs-tftp/ or /(root)/wcs-ftp/ filename.
  - Select whether or not Cisco WCS saves before backing up the configuration.

Note The Cisco WCS uses an integral TFTP and FTP server. This means that third-party TFTP and FTP servers cannot run on the same workstation as the Cisco WCS, because the Cisco WCS and the third-party servers use the same communication port.

Step 7 Click **OK**. The selected file will be uploaded to your TFTP or FTP server and named what you entered in the File Name text box.

Discovering Templates from Controllers

When prompted, WCS can search for associated templates for a controller and show the results.

Step 1 Choose **Configure > Controller**.

Step 2 Choose a desired controller by clicking the check box in front of the IP Address column.

Step 3 From the Select a command drop-down list, choose **Discover Templates from Controller**, and click **Go**.

A warning message confirms that the template discovery refreshes the configuration from the controller first.

The results page shows the template name, number, and template type.

Note The templates that are discovered do not retrieve management/local user passwords.

Displaying Templates Applied to Controller

When prompted, WCS can display a list of templates applied to controllers and show the details for each template.

Step 1 Choose **Configure > Controller**.

Step 2 Choose a desired controller by clicking the check box in front of the IP Address column.

Step 3 From the Select a command drop-down list, choose **Templates Applied to Controller**, and click **Go**.

The template name, template type, the date last saved, and the applied time are shown.

Configuring Controllers and Switches

Configuring DHCP Scopes

Follow these steps to configure DHCP scopes on the controller through WCS. Controllers have built-in DHCP relay agents. However, when network administrators desire network segments that do not have a separate DHCP server, the controller have built-in DHCP scopes that assign IP addresses and subnet masks to wireless clients. One controller can have one or more DHCP scopes that each provide a range of IP addresses.

DHCP scopes are needed for internal DHCP to work. After DHCP is defined on the controller, we can then point the primary DHCP server IP address on the management, AP-manager, and dynamic interfaces to the controller's management interface. You can configure up to 16 DHCP scopes using the controller GUI or CLI. At least one DHCP server must be configured on either the interface associated with the WLAN or with the WLAN itself.

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the desired controller from the IP Address column.

Step 3 Choose **System > DHCP Scopes**. In the DHCP Scopes page you can add, delete, or make modifications to an existing proxy.

Step 4 In the Lease Time text box, enter the amount of time (between 0 and 65535 seconds) that an IP address is granted to a client.

Step 5 Enter the network served by this DHCP scope. This IP address is used by the management interface with the netmask (as configured in Step 6) applied.

Step 6 Enter the subnet mask assigned to all wireless clients.

Step 7 In the Pool Start and End Addresses fields, enter the IP address of the optional router(s) connecting the controllers. Each router must have a DHCP-forwarding client, which allows a single controller to serve the clients of multiple controllers.

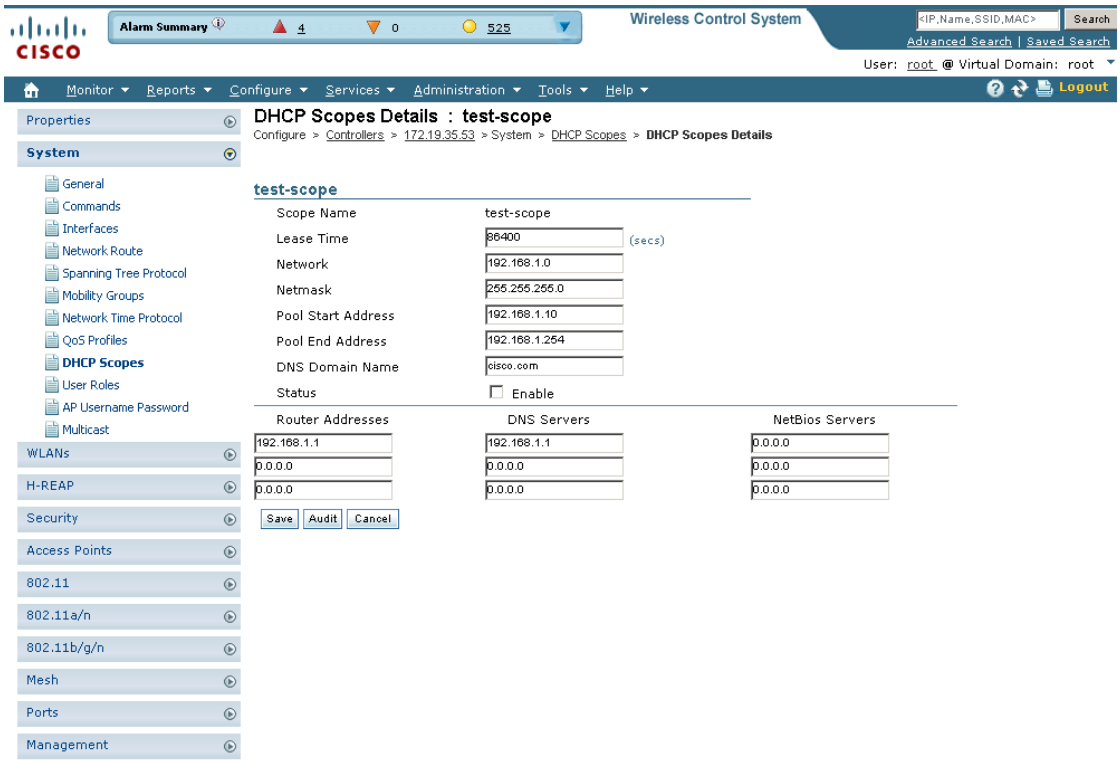
Step 8 Choose to enable or disable this DHCP scope at the Status drop-down list.

Step 9 At the Router Address parameter, enter which IP addresses are already in use and should therefore be excluded. For example, you should enter the IP address of your company's router. In doing so, this IP address will be blocked from use by another client.

Step 10 (Optional) Enter the IP address of the DNS server(s). Each DNS server must be able to update a client's DNS entry to match the IP address assigned by this DHCP scope.

Step 11 (Optional) 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.

Figure 10-2 DHCP Scope Details Page



Step 12 Click **Save**.

Configuring DHCP Proxy

To configure DHCP (Dynamic Host Configuration Protocol) information for a controller, follow these steps. Controllers have built-in DHCP relay agents. However, if network administrators desire network segments that do not have a separate DHCP server, refer to the "Configuring Controllers and Switches" section on page 10-10. If configured, a controller acts as a DHCP proxy for all DHCP requests received from device access points and clients.

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the desired controller from the IP Address column.

Step 3 Choose **System > DHCP**.

Step 4 Choose one of the following options from the DHCP Option 82 Remote ID Field Format drop-down list to specify the format of the DHCP option 82 payload:

- AP-MAC—Adds the MAC address of the access point to the DHCP option 82 payload. If chosen, the Remote ID is set as <AP-MAC>.
- AP-MAC-SSID—Adds the MAC address and SSID of the access point to the DHCP option 82 payload. If chosen, the RemoteID is set as MAP-MAC>:<SSID>.

Step 5 To enable DHCP Proxy, click the check box.

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 6 Click **Save**.

Configuring IGMP Snooping

WCS provides an option to configure IGMP snooping and timeout values on the controller. Access points subscribe to the LWAPP multicast group using IGMP. Follow these steps to configure IGMP snooping.

Step 1 Choose **Configure > Controllers**.

Step 2 Choose a desired controller.

Step 3 Choose **System > Multicast** from the left sidebar menu.

Step 4 The Ethernet Multicast Support drop-down is defaulted to disable. If you choose Unicast, the controller unicasts every multicast packet to all access point associated to the controller. This method is not the most efficient, but it may be required for networks that do not support multicasting. If you choose Multicast, the controller sends multicast packets to an LWAPP multicast group. This method reduces the overhead on the controller processor and shifts the work of packet replication to your network.

Step 5 If you choose Multicast, you must enter a group address.

Step 6 Choose **Enable** at 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.

Step 7 When the timeout expires, the controller sends a query to all WLANs. Those clients which are listening in the multicast group send a packet back to the controller.

Step 8 If you enable the Multicast Mobility Mode, you must enter a Mobility Group Multicast Address. Cisco Discovery Protocol (CDP) is a device discovery protocol that runs on all Cisco-manufactured equipment. A device enabled with CDP sends out periodic interface updates to a multicast address to make itself known to neighboring devices.

Configuring AP Timers

Some advanced timer configuration for HREAP and local mode is available for the controller on WCS. Follow these steps to configure the advanced timers and reduce failure detection time.

Step 1 Choose **Configure > Controllers**.

Step 2 Choose to which controller you want to set timer configuration.

Step 3 From the left sidebar menu, choose **System > AP Timers**. The AP Timers page appears.

Note This option is available only for controllers with version 6.0 or later.

Step 4 Click **Local Mode** or **HREAP**.

Step 5 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 1 and 10 seconds.

Note The 5500 series controller accepts an AP fast heartbeat timer value (local or HREAP mode) in the range of 10 to 15.

Step 6 Click **Save**.

Configuring Controller WLANs

Since controllers can support 512 WLAN configurations, WCS provides an effective way to enable or disable multiple WLANs at a specified time for a given controller. Follow these steps to view a summary of the wireless local access networks (WLANs) that you have configured on your network.

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 (see Figure 10-3). This WLAN Configuration page contains the values found in Table 10-2.

Figure 10-3 WLAN Configuration Summary Page

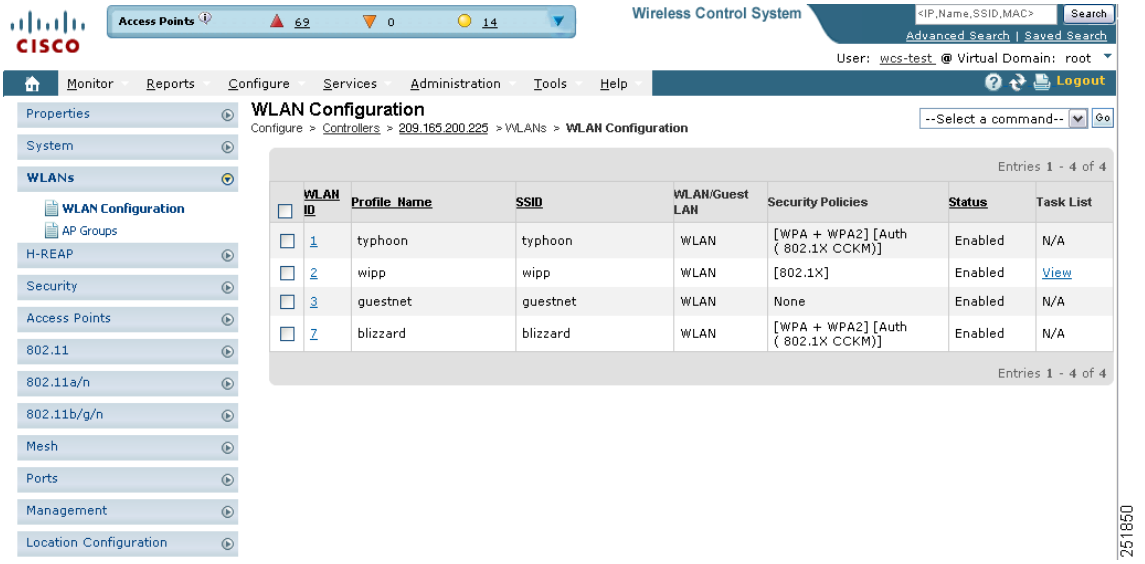


Table 10-2 WLAN Configuration Summary Page

Parameter	Description
Check box	Select the WLAN for deletion. Click **Delete WLANs** from the Select a command drop-down list.
WLAN ID	Identification number of the WLAN.
Profile Name	User-defined profile name specified when creating the WLAN template. Profile Name is the WLAN name.
SSID	Service Set Identifier being broadcast by.
WLAN/Guest LAN	Specifies if it is a WLAN or guest LAN.
Security Policies	Security policies enabled on the WLAN.
Status	Status of the WLAN is either enabled or disabled.
Task List	If a task is scheduled in Configure > Scheduled Configuration Tasks, you have a link to view the scheduled configuration task.

Viewing WLAN Details

To view WLAN details, choose **WLANs**. The WLAN Details page appears (see Figure 10-4).

Figure 10-4 WLAN Details Page

Use the tabs (General, Security, QoS, and Advanced) to view or edit parameters for the WLAN.

- General Tab
- Security Tab
- QoS Tab
- Advanced Tab

General Tab

The General tab includes the following information:

Note Depending on the WLAN template used for this controller, these parameters may or may not be available.

- 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.

  Note To configure a start time for the WLAN status to be enabled, select the **Schedule Status** check box. Select the hours and minutes from the drop-down lists. Click the calendar icon to select the applicable date.

- 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 in this section after the page is saved.
- Radio Policy—Choose from the drop-down list.

  - All, 802.11a only, 802.11g only, 802.11b/g only, 802.11a/g only.
- Interface—Select from the drop-down list.
- Broadcast SSID—Click 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—Select 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 10-3.

MAC Filtering—Select the check box if you want to filter clients by MAC address.

Table 10-3 Layer 2 Security Options

Parameter	Description
None	No Layer 2 security selected.
802.1x	802.11 Data Encryption: • Type—WEP • Key Size—40, 104, or 128 bits.
Static WEP	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. • Allowed Shared Key Authentication—Select the check box to enable.
Cranite	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.

Table 10-3 Layer 2 Security Options (continued)

Parameter	Description
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 parameters are displayed at the bottom of the page. Static WEP encryption 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. • Allowed Shared Key Authentication—Select the check box to enable.
	802.1X parameters: • 802.11 Data Encryption – Type – Key Size—40, 104, or 128 bits.

Table 10-3 Layer 2 Security Options (continued)

Parameter	Description
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's 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 Pre-Shared Key is enabled, neither CCKM or 802.1X can be enabled; although, both CCKM and 802.1X can be enabled at the same time. WPA+WPA2 parameters: • WPA1—Select the check box to enable. • WPA2—Select the check box to enable. Authentication Key Management: • 802.1X—Select the check box to enable. • CCKM—Select the check box to enable. • PSK—Select the check box to enable.
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.

Layer 3 Security

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 may or may 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, or conditional web redirect. 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 email addresses when attempting to connect to the network.

To allow guest users to view customized login pages, follow these steps:

Step 1 Unselect the **Global WebAuth Configuration** check box.

Step 2 Select the **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 "Downloading a Customized Web Authentication Page" section on page 12-67 for more information.
  - Select **Web Auth Login Page**, **Web Auth Login Failure Page**, or **Web Auth Logout Page** from the drop-down lists.
  - Select **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.

Note If External is selected, you can select up to three RADIUS and LDAP servers from the Security > AAA page. See "AAA Servers" for more information.

AAA Servers

Select RADIUS and LDAP servers to override 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, WCS 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, select 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.
- 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

- H-REAP Local Switching—Select the check box to enable Hybrid REAP local switching. When enabled, the H-REAP access point handles client authentication and switches client packets locally. See the "Configuring Hybrid REAP" section on page 15-4 for more information.

Note H-REAP 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.

- Session Timeout (secs)—Set the maximum time a client session can continue before re-authentication.
- 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 WCS polls these tables to display the results.

- Override Interface ACL—Select 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 Selecting an ACL is optional, and the default is None.

For more information, see the "Configuring Access Control List Templates" section on page 12-69.

- Peer to Peer Blocking—From the drop-down list, select 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.
- 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 in order to re-enable the client.

Note When session timeout is not set, the excluded client remains and will not time out from the excluded state. It does not imply that the exclusion feature is disabled.

- Media Session Snooping—Click 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 WCS. 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.

- NAC Support—Select the **NAC Support** check box to enable it. 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 "Configuring NAC Out-of-Band Integration" section on page 10-45 for more information.
- 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 will never know 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 will fail.

  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 5500 and 2100 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 above 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 will 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 **Optional**, **Disabled**, or **Required** for individual WLAN configurations.
- 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.

Adding a WLAN

To add a WLAN, follow these steps:

Step 1 Choose **Configure > Controllers**.

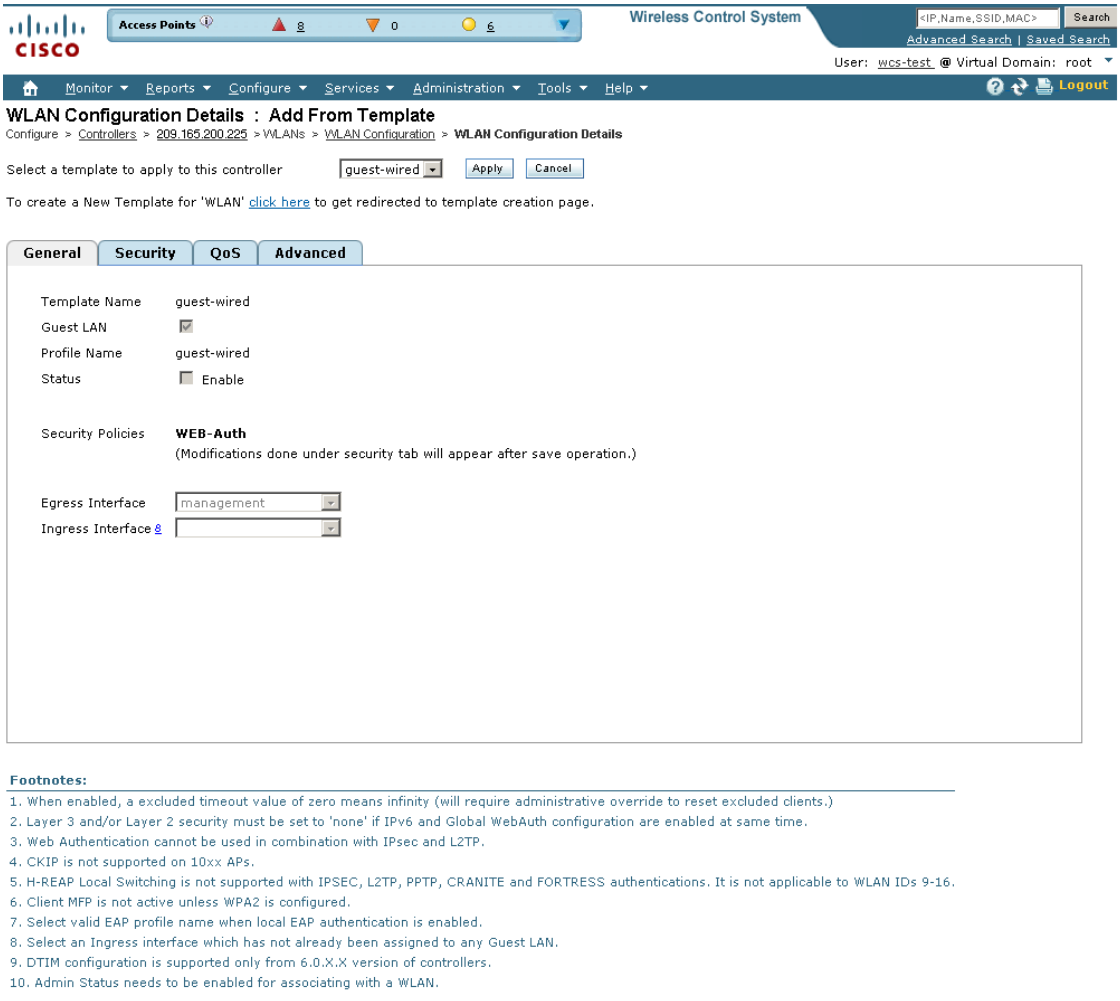
Step 2 Click the IP address of the appropriate controller.

Step 3 From the left sidebar menu, select **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 (see Figure 10-5).

Figure 10-5 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

WCS 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**.

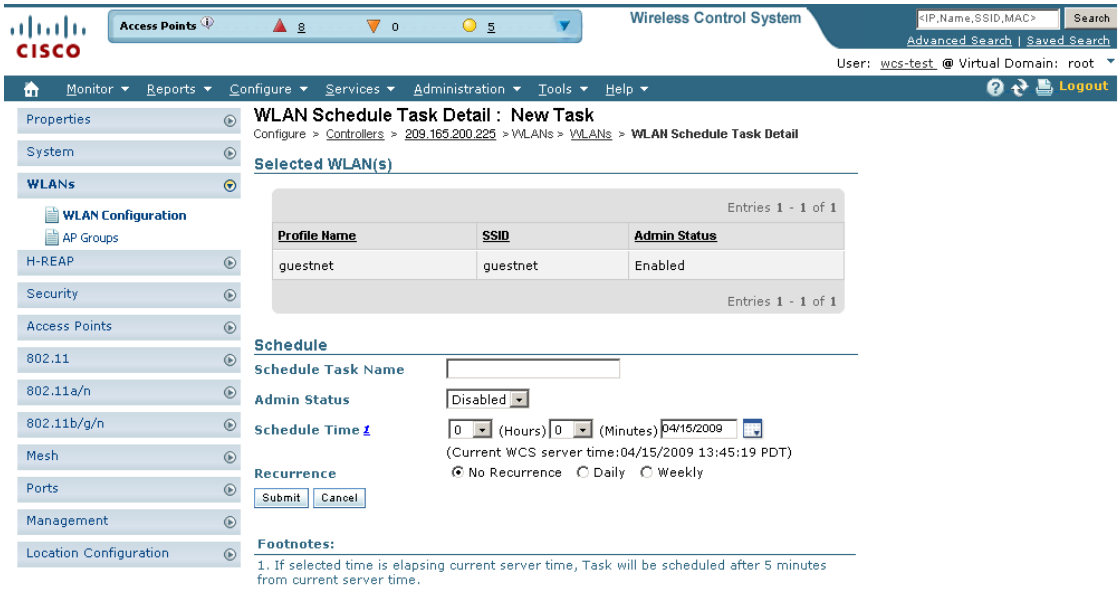
Step 2 Click the IP address of the appropriate controller.

Step 3 From the left sidebar menu, select **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 (see Figure 10-6).

Figure 10-6 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 Select the new Admin Status (Enabled or Disabled) from the drop-down list.

Step 8 Select 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.

Viewing WLAN Configuration Scheduled Task Results

To view and manage all scheduled WLAN tasks in WCS, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar, choose **WLAN Configuration** to open the WLAN Configuration Task List page.

Step 3 Select the check box of the scheduled task for which you want to view task results.

Step 4 From the Select a command drop-down list, choose **View History**. The WLAN Configuration Scheduled Task Results page opens and displays the following information:

- Status—Indicates the result status of the task.
- Templates Applied—Indicates the number of templates to which this task is applied. Click the Template Applied number to view template details.
- Template Failed—Indicates the number of templates for which this task failed. Click the Templates Failed number to view failure logs for this task.
- Task Execution Time—Indicates the date and time of the task execution.

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 client's entry point 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**.

Step 2 Click the IP address of the appropriate controller.

Step 3 From the left sidebar menu, select **WLANs > WLAN Configuration**.

Step 4 Click a WLAN ID to view the parameters for a specific WLAN.

Step 5 Click the **Advanced** tab.

Step 6 Click the **Mobility Anchors** link. Table 10-4 describes the parameters that are displayed.

Table 10-4 Mobility Anchors

Parameter	Description
Mobility Anchor	Anchor's IP address.
Status	Anchor's current status. For example, reachable or unreachable.

Configuring AAA General Parameters

The Security > AAA > General page allows you to configure the local database entries on a controller. Follow these steps to configure the local database entries:

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. The valid range is 512 to 2048. This amount becomes effective on the next reboot. The current maximum displays the effective maximum value currently set on the controller.

Configuring Local Network Users

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 may use the local user database as its backend database to retrieve user credentials. You must create a local net user and define a password when logging in as a web authentication client.

Step 1 Choose **Configure > Controllers**.

Step 2 From the left sidebar menu choose **Security > AAA > Local Net Users**.

Step 3 If you keep Import from File enabled, you need to enter a file path or click the Browse button 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 the Cisco WCS. The header can either be blank or filled. The Cisco WCS reads data from the second row onwards.

Step 4 Enter a username and password.It is mandatory to fill the Username and Password text boxes in all the rows.

Step 5 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 6 Enter a description of the profile.

Step 7 Use the drop-down list to choose the SSID which this local user is applied to or choose the *any SSID* option.

Step 8 Enter a user-defined description of this interface. Skip to Step10.

Step 9 If you want to override the existing template parameter, click to enable this parameter.

Step 10 Click Save.

Configuring New LDAP Bind Requests

WCS now supports LDAP configuration for both an anonymous or authenticated bind. A bind is a socket opening that performs a lookup. Follow these steps to configure LDAP bind requests.

Step 1 Choose **Configure > Controllers**.

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.

Step 9 Click **Save**.

Setting Multiple Country Codes

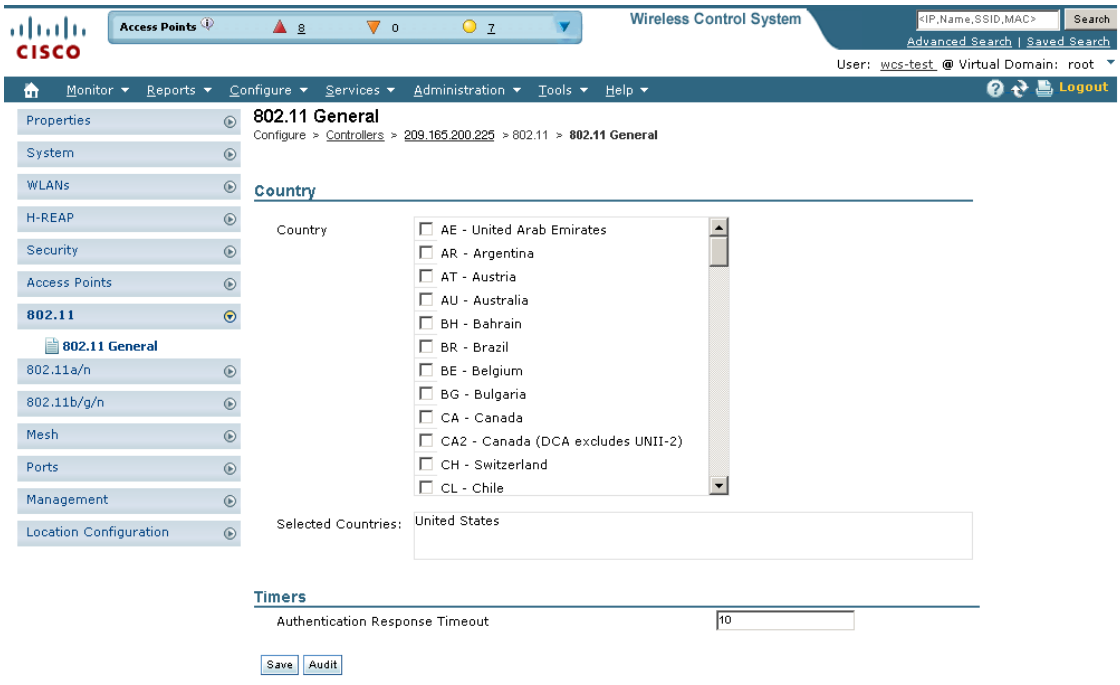
To set multiple country support for a single controllers that is not part of a mobility group, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the controller for which you are adding countries.

Step 3 Choose **802.11 > General** from the left sidebar menu. The Controller 802.11 page appears (see Figure 10-7).

Figure 10-7 Controller 802.11



Step 4 Select the check box to choose a country. 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's regulations.

Note Access points may 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's regulatory domain. For a complete list of country codes supported per product, refer to:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html.

Step 5 Enter the time in seconds after which the authentication response will timeout.

Step 6 Click **Save**.

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 page, 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 would be allowed to assciate 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).

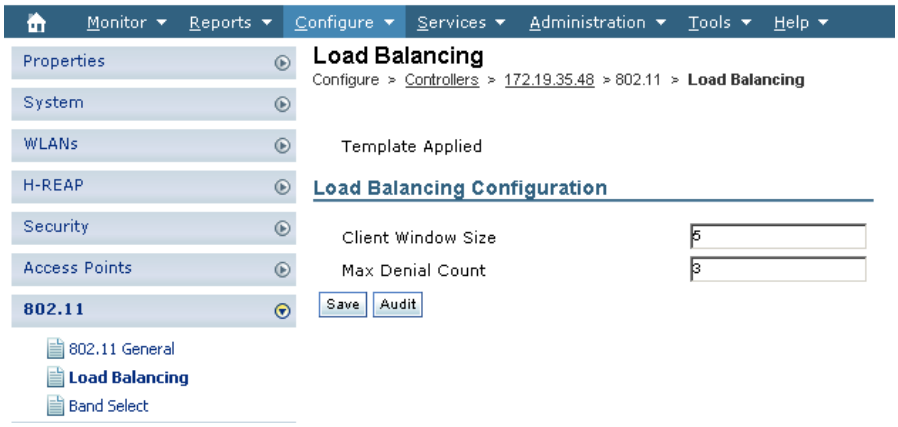
Follow these steps to configure aggressive load balancing:

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 (see Figure 10-8).

Figure 10-8 Load Balancing



Step 4 Enter a value between 1 and 20 for the client page 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 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 10-13.

Configuring Band Selection

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).

Note Band-selection-enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.

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 hybrid-REAP 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

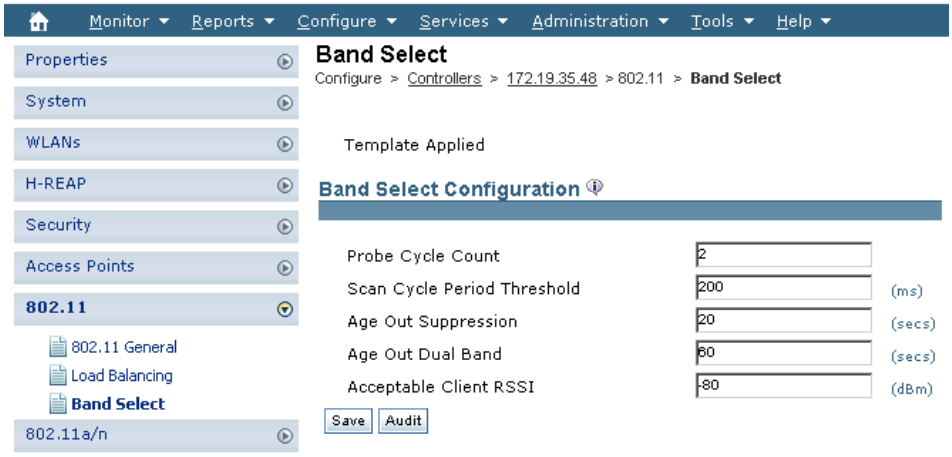
Follow these steps to configure band selection:

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 (see Figure 10-9).

Figure 10-9 Band Select



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 parameter. 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 7 Enter a value between 10 and 300 seconds for the age out dual band parameter. 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 parameter. This parameter 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 10-13.

Searching Controllers

The enhanced WCS Search feature provides easy access to advanced search options and saved searches. You can access the search options from any page within WCS making it easy to search for a device or SSID.

The Search function is located in the top right section of the WCS window. See the "Using the Search Feature" section on page 2-31 for more information on using the search feature.

- Quick Search: For a quick search, you can enter a partial or complete IP address, MAC address, name, or SSID for clients, alarms, access points, controllers, maps, tags, or rogue clients.
- Advanced Search: An advanced search allows you to search for a device based on a variety of categories and filters.
- Saved Searches: Lists the saved custom searches. To open a saved search, choose it from the Saved Searches list.

You can configure the following parameters in the Search Controllers page:

- Search for controller by— Choose all controllers, IP address, or controller name.
- Select a Network— Choose all networks or an individual network.
- Audit Status— Search by audit status of the following:
  - Not Available: Audit status is not available.
  - Identical: No configuration differences found during last audit.
  - Mismatch: Configuration differences were found between WCS and controller during last audit.
- Items per page—Choose the number of found items to display on the search results page. The range is 10 to 100 items per page. The default is 20.

When you click **New Search**, the controller search results appear:

Table 10-5 Search Results

Parameter	Options
IP Address	Local network IP address of the controller management interface. Clicking the title toggles the order from ascending to descending. Clicking an IP address in the list displays a summary of the controller details.
Controller Name	Clicking the title toggles the order from ascending to descending.
Type	Type of controller. For example, Cisco 2000 Series, Cisco 4100 Series, or Cisco 4400 Series.
Location	The geographical location (such as campus or building). Clicking the title toggles the order from ascending to descending.
Mobility Group Name	Name of the controller or WPS group.
Reachability Status	Reachable or Unreachable. Clicking the title toggles the order from ascending to descending.
AP Count	The number of access points associated with this controller.

Managing User Authentication Order

You can control the order in which authentication servers are used to authenticate a controller's management users.

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address.

Step 3 From the left sidebar menu, choose **Management > Authentication Priority**.

Step 4 The local database is searched first. Choose either **RADIUS** or **TACACS+** for the next search. If you do not want the local database searched first, choose **Second**. If authentication using the local database fails, the controller uses the next type of server.

Step 5 Click **Save**.

Viewing Audit Status (for Controllers)

You can audit a controller by choosing **Audit Now** from the Select a command drop-down list in the Configure > Controllers page or by clicking **Audit Now** directly from the Controller Audit Report.

Note A current Controller Audit Report can be viewed in the Configure > Controllers page by choosing an object from the Audit Status column.

To audit a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box for the appropriate controller. From the Select a command drop-down list, choose **Audit Now**.

Step 3 Click **Go**.

A confirmation appears after you perform the controller actions from the View Audit Status page.

The Audit Report displays the following:

- Device Name
- Time of Audit
- Audit Status
- Applied and Config Group Template Discrepancies occur because of applied templates. The config group templates are listed, and the information includes the following:
  - Template type (template name)
  - Template application method
  - Audit status (such as mismatch, identical)
  - Template attribute
  - Value in WCS
  - Value in Controller
- Config WCS Discrepancies occur because of configuration objects in the WCS database. The current WLC configuration is listed, and the information includes the following:
  - Configuration type (name)
  - Audit Status (for example, mismatch, identical)
  - Attribute
  - Value in WCS
  - 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. See the "Creating Config Groups" section on page 8-19 for more information on enabling the background audit.
- Failed Enforcements for Config Groups with background audit enabled—Check the link to view a list of failure details (including the reason for the failure) returned by the device. See the "Creating Config Groups" section on page 8-19 for more information on enabling the background audit.

Note The following sections are displayed if the audit selected is a template-based audit:

Applied and Config Group Template Discrepancies
Total enforcements for config groups with background audit enabled
Failed enforcements for config groups with background audit enabled
Config WCS discrepancies

The Config WCS discrepancies section is displayed if the audit is selected to be a basic audit.

- Restore WCS Values to Controller or Refresh Config from Controller—If the audit reveals configuration differences, you can either restore WCS values on the controller or refresh controller values. Choose **Restore WCS Values to Controller** or **Refresh Config from Controller**.
  - If you choose Restore WCS Values to Controller, all of the WCS values are enforced on the controller in an attempt to resolve the discrepancies on the device. All of the applied templates and the templates that are part of the config group are applied to this controller (for template based audit). If the audit done is a basic audit, the configuration objects in WCS database are enforced on the controller.

Note Template discrepancies can be resolved by enforcing WCS templates on the device. See the "Creating Config Groups" section on page 8-19 for more information on enforcing configurations.

  - If you choose Refresh Config from Controller, a Refresh Config page opens and shows the following message: "Configuration is present on WCS but not on device, do you wish to:" Choose one of the following options, and click **Go** to confirm your selection.

    You should choose Refresh Config from Controller after an upgrade of software to ensure that the AP timers configuration is visible.

    Retain—The WCS refreshes the configuration from the controller but will not delete any devices or configurations that no longer exist in the controller configuration. For example, if the WCS database shows an AP1, but that access point is no longer present in the controller configuration, WCS will not delete AP1 from its database.

    Delete—WCS deletes the configuration of the controller from its database and retrieves a new configuration from the controller. Delete is the recommended option so that WCS matches the most recent configuration you are refreshing from WLC.

Note In the Refresh Config page, only the configuration objects for this controller in the WCS database are updated. Upon refresh, the WCS templates are not updated.

Viewing 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. The Applied and Config Group Template Discrepancies, Total Enforcements for Config Groups with Background Audit Enabled, and Failed Enforcements for Config Groups with Background Audit Enabled sections have data only if the network audit was run as a template based audit.

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 any selected controller, and the audit status. The Audit Details page displays the configuration differences, if applicable.

You can use the General and Schedule tabs to revise the Audit Report parameters.

Note In 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 in the Reports menu, but this report is interactive and per controller.

Note To run an on-demand audit report, select 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 WCS values.

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.

You can configure 802.3 bridging using WCS release 4.1 or later. Follow these steps.

Step 1 Click **Configure > Controllers**.

Step 2 Click **System > General** to access the General page.

Step 3 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 4 Click **Save** to commit your changes.

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 may cause the controller to reach an overloaded point and reject some of the access points.

By assigned priority to an access point, you have some control over which access points are rejected. In a failover situation when the backup controller is overloaded, the higher-priority access points join the backup controller and disjoin 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 an access point's priority, follow these steps:

Step 1 Choose **Configure > Access Points > <AP Name>**.

Step 2 From the AP Priority drop-down list, choose the applicable priority (Low, Medium, High, Critical).

Note The default priority is Low.

Sending Primary Discovery Requests

The access point maintains a list of backup controllers and periodically sends primary discovery requests to each entry on the list.

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 Select the **AP Primary Discovery Timeout** check box to enable the timeout value. 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. Enter a value between 30 and 3600 seconds.

Step 5 Click **Save**.

Pinging a Network Device from a Controller

Follow these steps to ping network devices from a controller.

Step 1 Click **Configure > Controllers** to navigate to the All Controllers page.

Step 2 Click the desired IP address to display the IP Address > Controller Properties page.

Step 3 In the sidebar, choose **System > Commands** to display the IP Address > Controller Commands page.

Step 4 Choose **Ping From Controller** from the Administrative Commands drop-down list, and click **Go**.

Step 5 In the Enter an IP Address (x.x.x.x) to Ping page, enter the IP address of the network device that you want the controller to ping, and click **OK**.

WCS displays the Ping Results page, which shows the packets that have been sent and received. Click **Restart** to ping the network device again or click **Close** to stop pinging the network device and exit the Ping Results page.

Enabling Load-Based CAC for Controllers

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.

To enable load-based CAC for a controller template, refer to the "Configuring a Voice Parameter Template (for 802.11a/n or 802.11b/g/n)" section on page 12-86.

To enable load-based CAC for a controller using the WCS web interface, follow these steps.

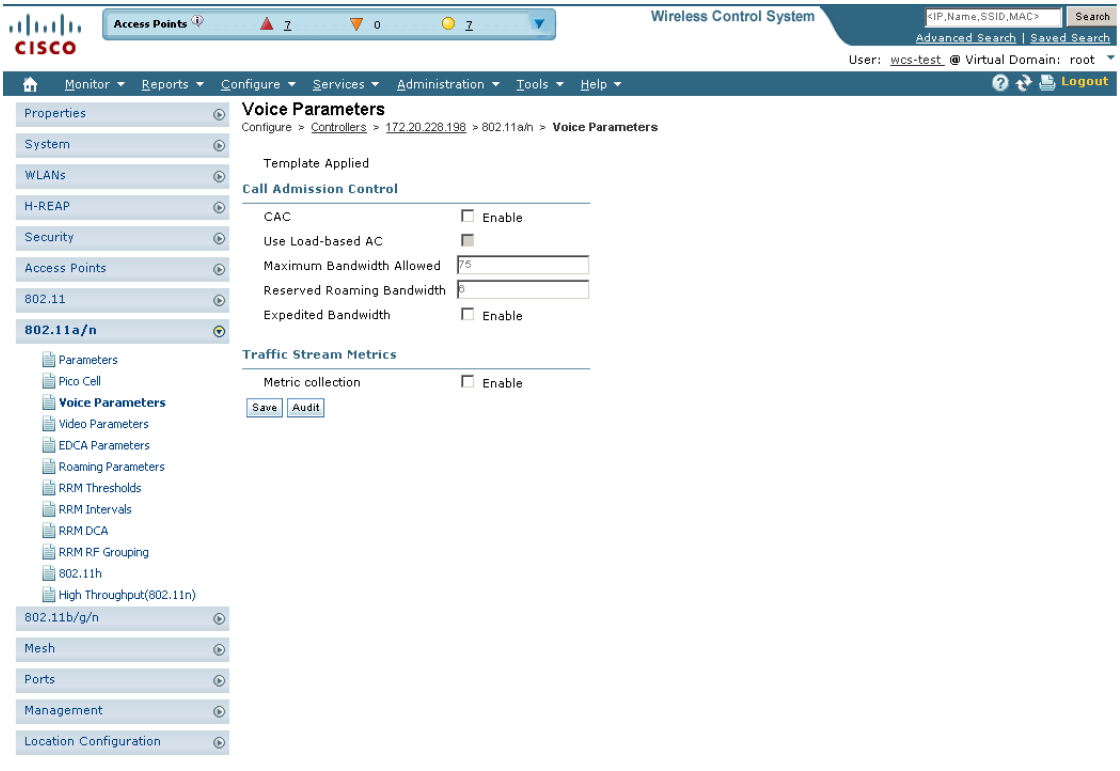
Step 1 Click **Configure > Controllers**.

Step 2 Click the IP address link of the controller.

Step 3 Click **Voice Parameters** under 802.11a/n or 802.11b/g/n.

The 802.11a/n (or 802.11b/g/n) Voice Parameters page appears (see Figure 10-10).

Figure 10-10 802.11a/n Voice Parameters Page



Step 4 Click the check box to enable bandwidth CAC. 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.

Step 5 Determine if you want to enable load-based CAC for this radio band. Doing so incorporates a measurement scheme that considers the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference.

Step 6 Enter the percentage of maximum bandwidth allowed.

Step 7 Enter the percentage of reserved roaming bandwidth.

Step 8 Click the check box if you want to enable expedited bandwidth as an extension of CAC for emergency calls. You must have an expedited bandwidth IE that is Cisco Compatible Extensions (version 5) compliant so that a TSPEC request is given higher priority.

Step 9 Click the check box if you want to enable metric collection. Traffic stream metrics are a series of statistics about VoIP over your wireless LAN, and they 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/n interfaces from all associated access points. If you are using VoIP or video, enable this feature.

Step 10 Click **Save**.

Configuring CleanAir Parameters (for 802.11a/n or 802.11b/g/n)

To configure 802.11a/n or 802.11b/g/n CleanAir parameters, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click the IP address of the appropriate controller.

Step 3 From the left sidebar menu, choose **802.11a/n > CleanAir** or **802.11b/g/n > CleanAir** to view the following information:

- CleanAir—Select the check box to enable CleanAir functionality on the 802.11a/n or 802.11b/g/n network, or unselect to disable CleanAir functionality.
- 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 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 detected.
- 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 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 35.
  - 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 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 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 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.

Command Buttons

- Save—Save the changes made.
- Audit—Compare the WCS values with those used on the controller.

Configuring an RRM Threshold Controller (for 802.11a/n or 802.11b/g/n)

Follow these steps to configure an 802.11a/n or 802.11b/g/n RRM threshold controller.

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the appropriate controller to open the Controller Properties page.

Step 3 From the left sidebar menu, choose **802.11a/n > RRM Thresholds** or **802.11b/g/n > RRM Thresholds**.

Step 4 Make any necessary changes to coverage level thresholds, load thresholds, and thresholds for traps.

Step 5 Click **Save**.

Configuring 40-MHz Channel Bonding

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 channels for an individual controller, follow these steps:

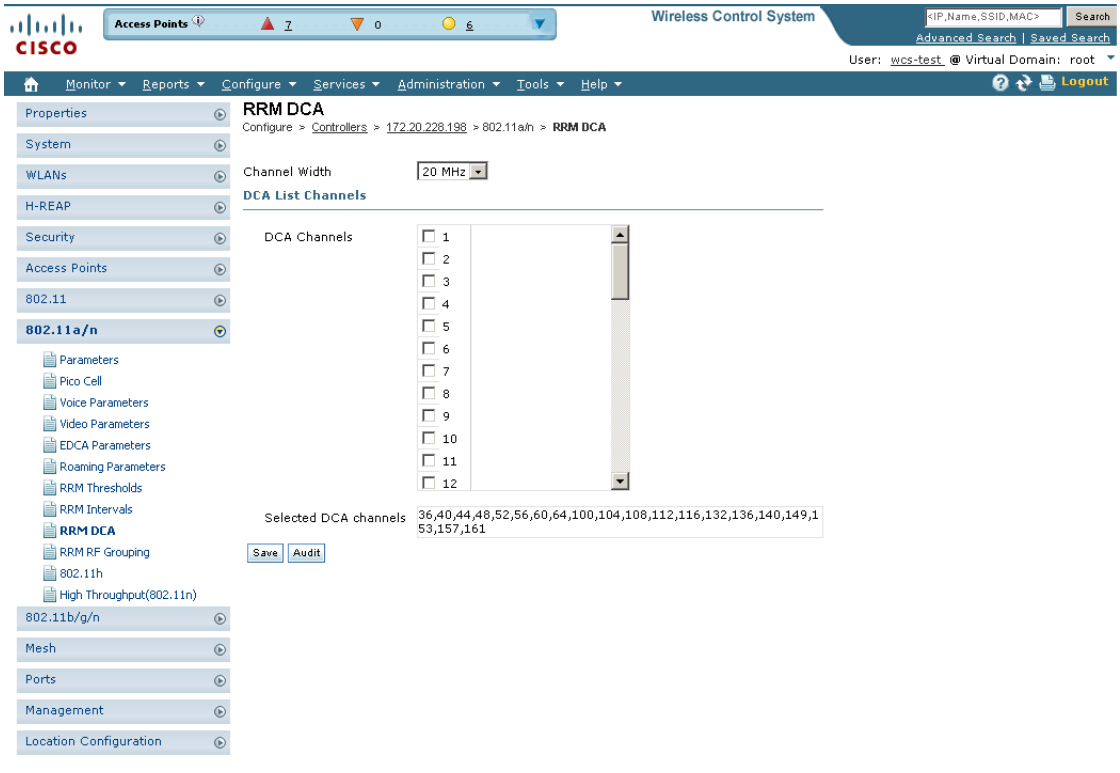
Step 1 Choose **Configure > Controllers**.

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 (see Figure 10-11).

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.

Figure 10-11 802.11a/n RRM DCA Page



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 may negatively impact the 20-MHz devices.

Note To view the channel width for an access point's radio, 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 on 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.

– 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 EDCA Parameters for Individual Controller

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. See the "Configuring EDCA Parameters through a Controller Template" section on page 12-88 for steps to configure a controller template.

To configure 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller, do the following:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP Address of the applicable controller.

Step 3 From the left sidebar menu, select **802.11a/n > EDCA Parameters** or **802.11b/g/n > EDCA Parameters**.

Step 4 Choose an EDCA profile from the drop-down list. The choices 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 **Low Latency MAC** check box to enable this feature.

Note Only enable low latency MAC if all clients on the network are WMM compliant.

Configuring SNMPv3

When you are configuring a controller, you can add SNMPv3 settings or change the setting (and any other settings) established from the previously added controller. (If SNMPv3 is enabled on the Ethernet switch, use the Ethernet switch CLI or switch UI to include all the OIDS and use the context option to create a group for each VLAN.) Follow these steps to set the SNMPv3 settings.

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP Address of the applicable controller or choose **Add Controller** from the Select a command drop-down list, and click **Go**.

Step 3 In the SNMP Parameters area of the page, choose **v3** from the Version drop-down list.

Step 4 You can change the retries and timeout values that were established for this controller if desired.

Step 5 In the Privacy Type drop-down list, choose **None, CBC-DES**, or **CFB-AES-128**. AES refers to the Advanced Encryption Standard algorithm established by the National Institute of Standards and Technology (NIST). It is more secure than older DES algorithms. CFB (Cipher Feedback) refers to the method AES uses to encrypt the packets, and 128 refers to the key length (128 bits).

Step 6 Any passwords used to derive encryption keys for algorithms using 128 but must contain a minimum of 12 characters. Enter a privacy password that fits this criteria.

Step 7 Click **OK**.

Viewing All Current Templates

Prior to software release 5.1, templates were detected when a controller was detected, and every configuration found on WCS for a controller had an associated template. Now templates are not automatically detected with controller discovery, and you can specify which WCS configurations you want to have associated templates.

The following rules apply for template discovery:

- Template discovery discovers templates that are not found in WCS.
- Existing templates are not discovered.
- Discovered templates are not associated to the configuration on the device.

Follow these steps to use the Discover Templates from Controller feature:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the check box for the applicable controller.

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 and name of each template.

Note The configuration from the controller is refreshed if you select this option.

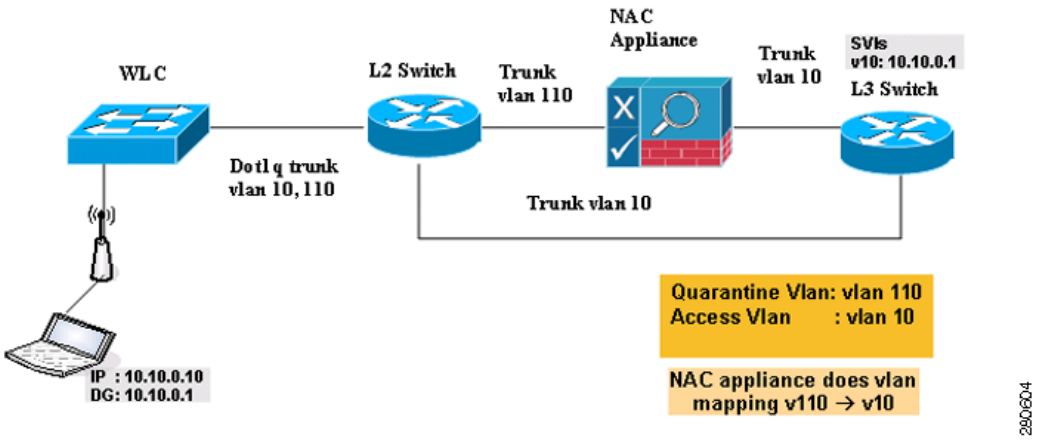
Configuring NAC Out-of-Band Integration

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).

In WCS software releases prior to 5.1, the controller integrates with the NAC appliance only in in-band mode, where the NAC appliance must remain in the data path. For in-band mode, a NAC appliance is required at each authentication location (such as at each branch or for each controller), and all traffic must traverse the NAC enforcement point. In WCS software release 5.1, 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.

To implement the NAC out-of-band feature on the controller, you need to enable NAC support on the WLAN or guest LAN and then map this WLAN or guest LAN to an interface that is configured with a quarantine VLAN (untrusted VLAN) and an access VLAN (trusted VLAN). When a client associates and completes Layer 2 authentication, the client obtains an IP address from the access VLAN subnet, but the client state is Quarantine. While deploying the NAC out-of-band feature, be sure that the quarantine VLAN is allowed only between the Layer 2 switch on which the controller is connected and the NAC appliance and that the NAC appliance is configured with a unique quarantine-to-access VLAN mapping. Client traffic passes into the quarantine VLAN, which is trunked to the NAC appliance. After posture validation is completed, the client is prompted to take action for remediation. After cleaning is completed, the NAC appliance updates the controller to change the client state from Quarantine to Access. Figure 10-12 provides an example of NAC out-of-band integration.

Figure 10-12 NAC Out-of-Band Integration



In Figure 10-12, the link between the controller and the switch is configured as a trunk, enabling the quarantine VLAN (110) and the access VLAN (10). On the Layer 2 switch, the quarantine traffic is trunked to the NAC appliance while the access VLAN traffic goes directly to the Layer 3 switch. Traffic that reaches the quarantine VLAN on the NAC appliance is mapped to the access VLAN based on a static mapping configuration.

Follow the instructions in this section to configure NAC out-of-band integration.

Note CCA software release 4.5 or later is required for NAC out-of-band integration.

Guidelines for Using NAC Out-of-Band Integration

Follow these guidelines when using 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 hybrid-REAP central switching. It is not supported for use on WLANs configured for hybrid-REAP local switching.

Note See Chapter 15 for more information on hybrid REAP.

- 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:

http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

Configuring NAC Out-of-Band Integration

Follow these steps to configure NAC out-of-band integration.

Step 1 To configure the quarantine VLAN for a dynamic interface, follow these steps:

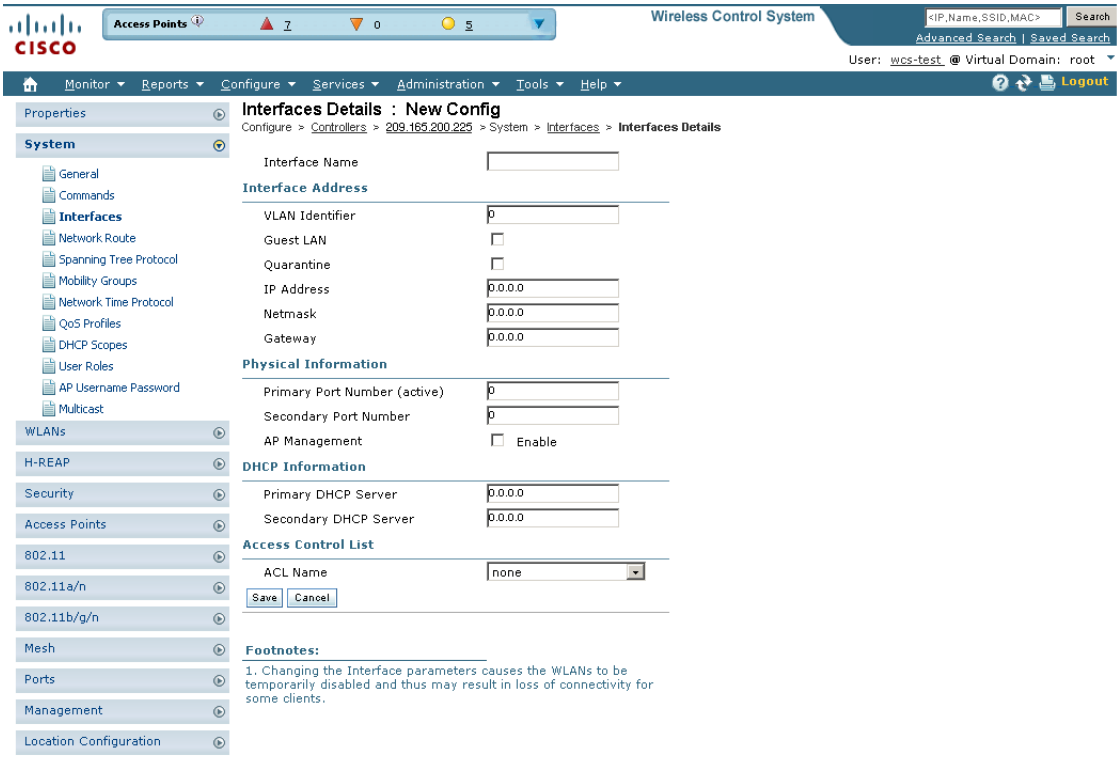
a. Choose **Configure > Controllers**.

b. Choose which controller you are configuring for out-of-band integration by clicking 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. The Interface page appears (see Figure 10-13).

Figure 10-13 Interface Page



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. Click to enable guest LAN.

h. Select the **Quarantine** check box if the interface has a quarantine VLAN ID configured on it.

Note You can have NAC support enabled on the WLAN or Guest WLAN template Advanced tab only for interfaces with quarantine enabled.

Note Cisco recommends 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.

i. Configure any remaining fields for this interface, such as the IP address, netmask, and default gateway.

j. Enter the primary port number.

k. Enter the secondary port number.

l. Select the **AP Management** check box to enable an AP-manager interface. A controller has one or more AP-manager interfaces that are used for all Layer 3 communications between the controller and lightweight access points after the access points have joined the controller.

m. Enter an IP address for the primary and secondary DHCP server.

n. Choose the user-defined name of the access control list (or none) from the drop-down list.

o. 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. Click **WLANs > WLAN Configuration** from the left sidebar menu.

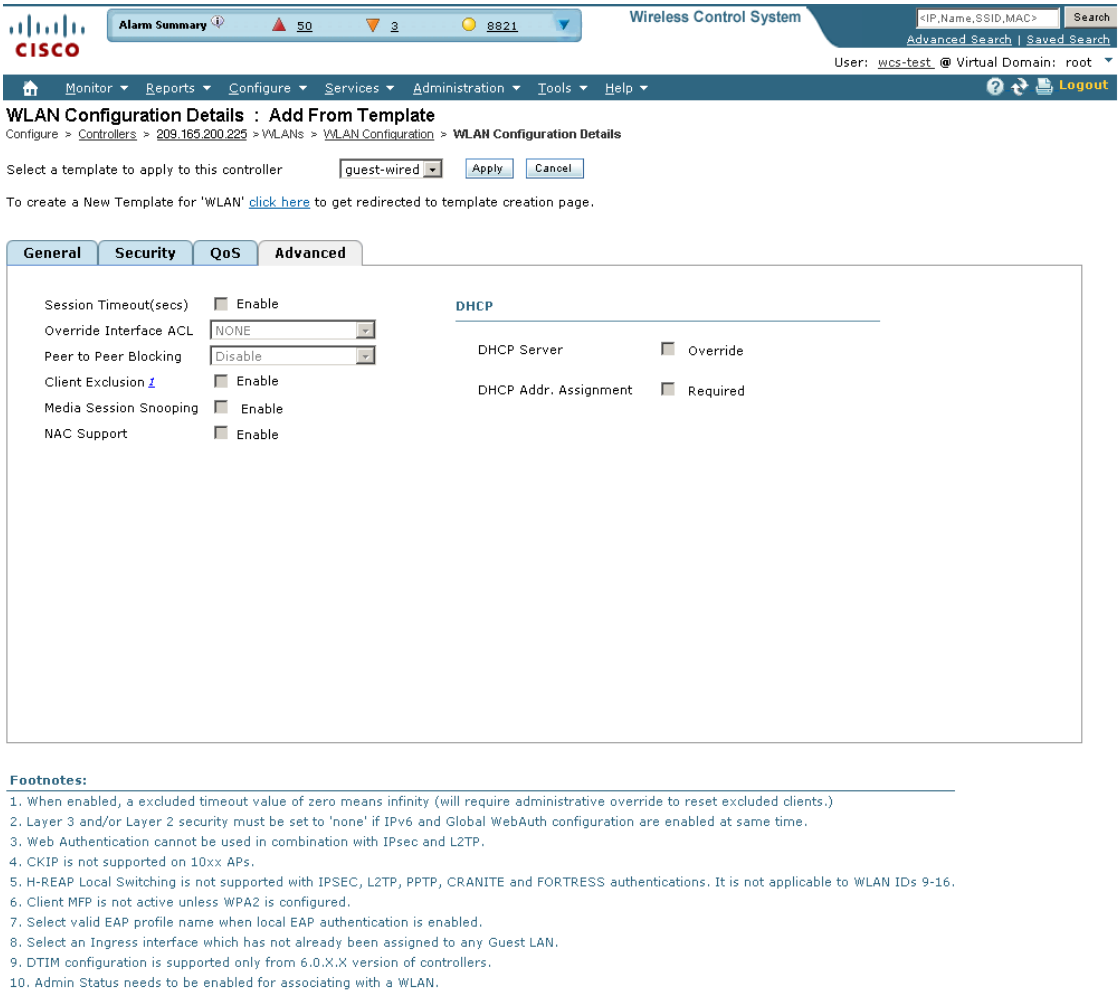
b. Choose **Add WLAN** from the Select a command drop-down list, and click **Go**.

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, refer to the "Configuring Wired Guest Access" section on page 10-51.

Note Ensure that WLAN IDs within the same network match before you forward the WLAN template.

d. Click the **Advanced** Tab (see Figure 10-14).

Figure 10-14 WLAN > Add From Template Page



e. To configure NAC out-of-band support for this WLAN or guest LAN, select the **NAC Support** check box. To disable NAC out-of-band support, leave the check box unselected, 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 VLAN, follow these steps:

a. Choose **WLANs > AP Groups** in the left sidebar menu to open the AP Groups page.

b. Click the name of the desired AP group.

c. To change the interface name to a quarantine-enabled VLAN, click the Edit icon.

d. To override NAC, click the Edit icon and click the Disabled check box.

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. Click **Monitor > Clients** to open the Clients page and perform a search for clients.

b. In the client search page, you can specify to search for quarantine or access state.

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. See the "Creating Guest User Accounts" section on page 7-10.

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.

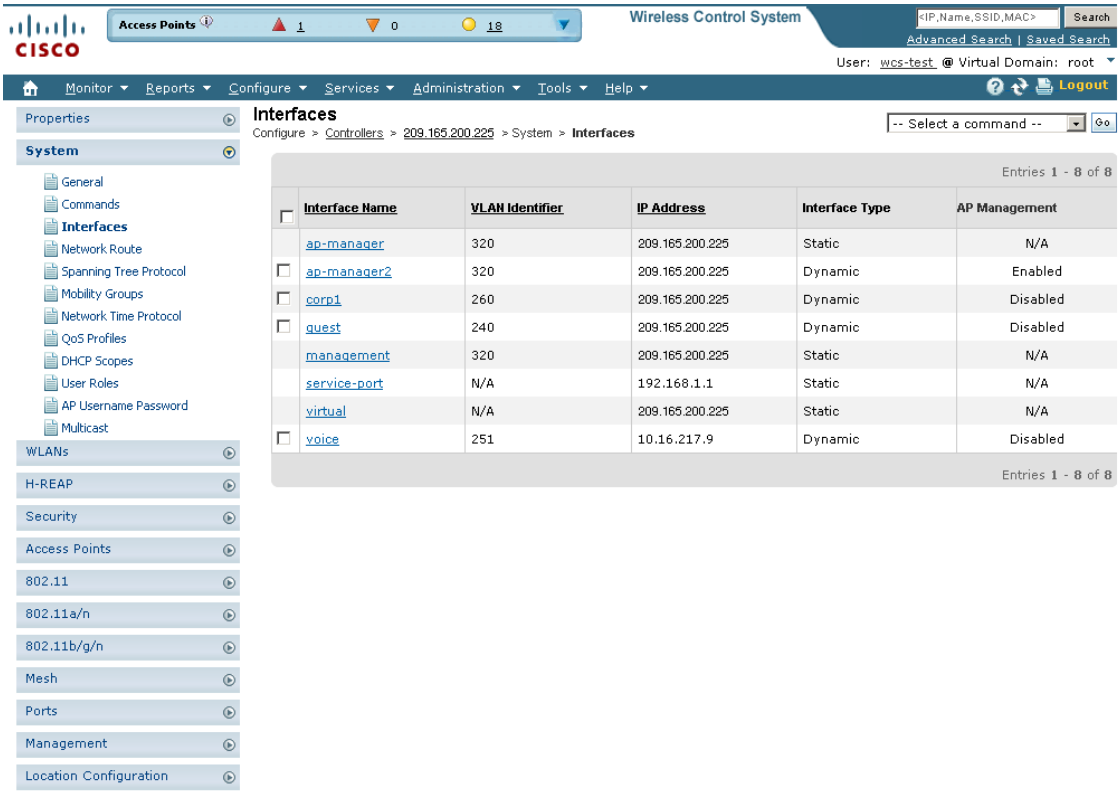
If two controllers are being used, the controller (foreign) that receives the wired guest traffic from the switch then forwards the wired guest traffic to an anchor controller that is also configured for wired guest access. After successful hand off of the wired guest traffic to the anchor controller, 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. For details on configuring these features, refer to the "Creating Guest User Accounts" section on page 7-10.

To create dynamic interfaces for wired guest user access, click **Configure > Controllers** and after choosing a particular IP address, choose **System > Interfaces**. The Interfaces page appears (see Figure 10-15). Two interfaces should be created: one for Ingress and one for Egress. The Ingress interface provides a path between the wired guest client and the controller by way of a Layer 2 access switch. The Egress interface provides a path out of the controller for the guest client traffic. You must complete the "Creating an Ingress Interface" section on page 10-52 and the "Creating an Egress Interface" section on page 10-53 before continuing to "Configuring DHCP Proxy" section on page 10-11. Both the Ingress and Egress Interfaces use the screen as shown in Figure 10-15.

Figure 10-15 Interfaces Summary Page



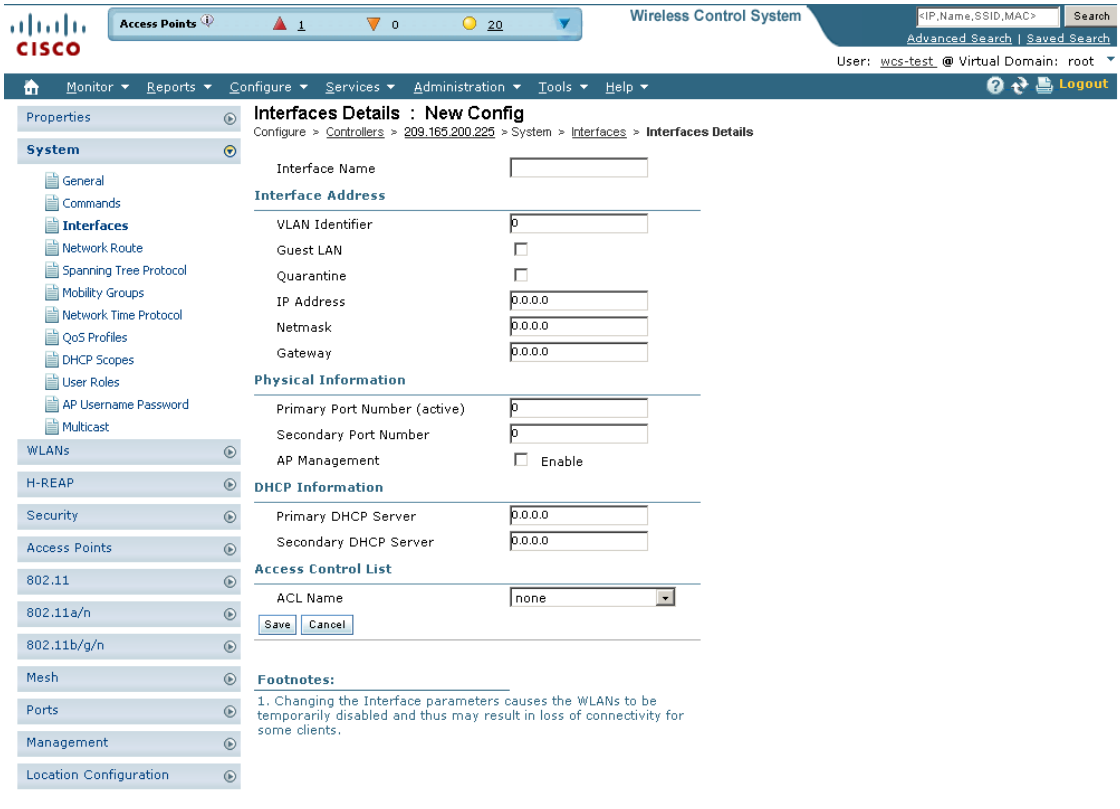
Creating an Ingress Interface

Follow these steps to create an Ingress interface.

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 (see Figure 10-16).

Figure 10-16 Interfaces Details : New Config Page



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

Follow these steps to create an Egress interface.

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 (see Figure 10-16).

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.

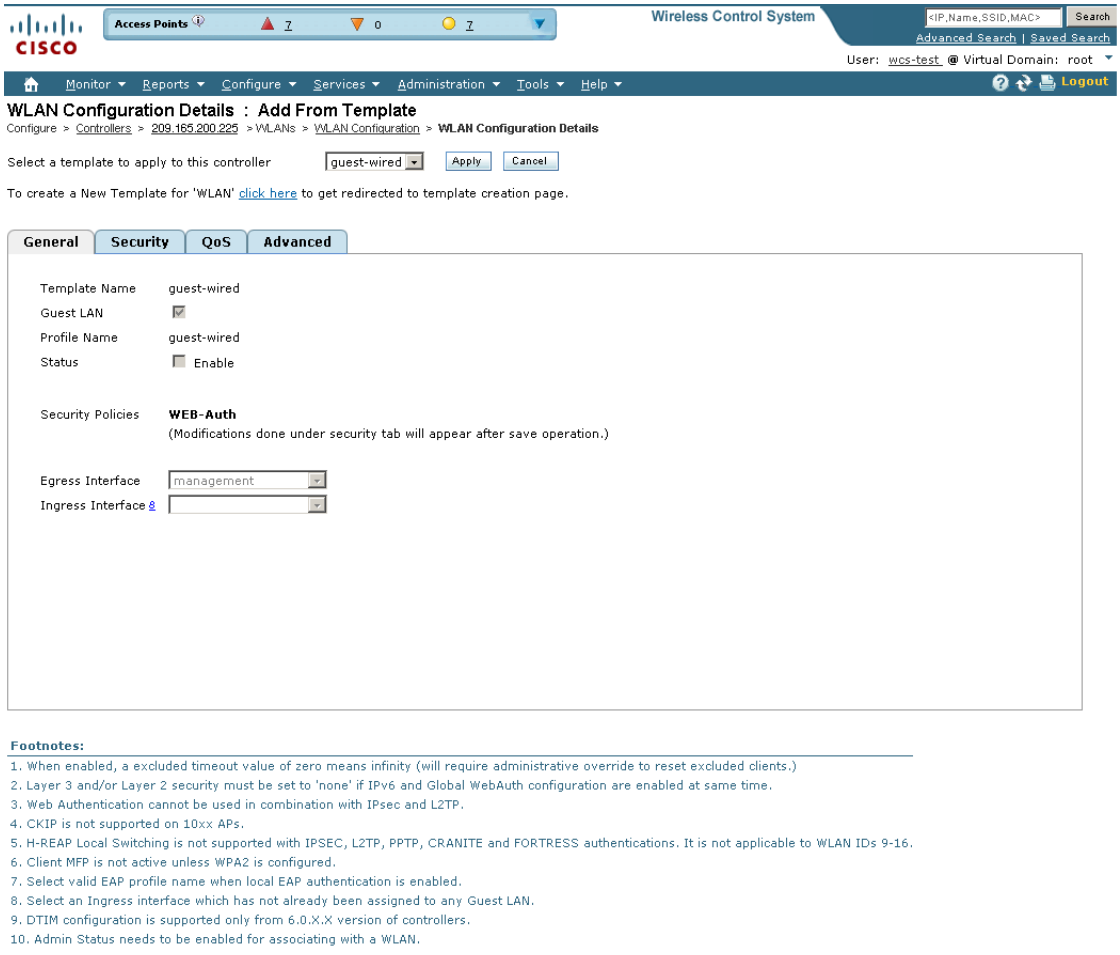
Creating a Wired LAN for Guest Access

Follow these steps to configure and enable wired guest user access on the network.

Step 1 To configure a wired LAN for guest user access, click **WLANs > WLAN Configuration** from the left sidebar menu.

Step 2 Choose **Add a WLAN** from the Select a command drop-down list, and click **Go**. The WLAN > Add From Template page appears (see Figure 10-17).

Figure 10-17 WLAN > Add From Template



Step 3 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.

Note Ensure that WLAN IDs within the same network match before you forward the WLAN template.

Step 4 On the New Template general tab, enter a name in the Template Name text box that identifies the guest LAN. Do not use any spaces in the name entered.

Step 5 Enable the **Guest LAN** check box.

Step 6 Enter the profile name.

Step 7 Select the **Enable** check box for the Status parameter.

Step 8 From the Interface Name drop-down list, choose the desired interface name.

Step 9 From the Egress Interface drop-down list, choose the Egress interface that you created in the "Creating an Egress Interface" section on page 10-53. This 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 10 From the Ingress Interface drop-down list, choose the Ingress interface that you created in the "Creating an Ingress Interface" section on page 10-52. The provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Step 11 Click **Security > Layer 3** to modify the default security policy (web authentication) or to assign 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 the **Passthrough** option. 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 **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:

Internal—Displays the default web login page for the controller. This is the default value.

Customized—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, refer to the "Downloading Customized Web Authentication" section on page 3-47.

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 page. To do so, continue with Step 12.

Note The RADIUS and LDAP external 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, TACACS+ Authentication Servers page, and LDAP Servers page.

Step 12 If you selected External as the Web Authentication Type in Step 11, click **Security > AAA Servers** and select up to three RADIUS and LDAP servers using the drop-down lists.

Step 13 Click **Save**.

Step 14 Repeat this process if a second (anchor) controller is being used in the network.

Using Switch Port Tracing

Currently, WCS 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 Lightweight Rogue AP Report message. With this method, WCS would simply gather the information received from the controllers; but with software release 5.1, you can now incorporate switch port tracing of wired rogue access point switch port. This enhancement allows you to react to found wired rogue access points and prevent future attacks. The trace information is available only in the WCS log and only for rogue access points, not rogue clients.

Note The rogue client and its rogue access point information is used to track the switch port to which the rogue access point is connected in the network.

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

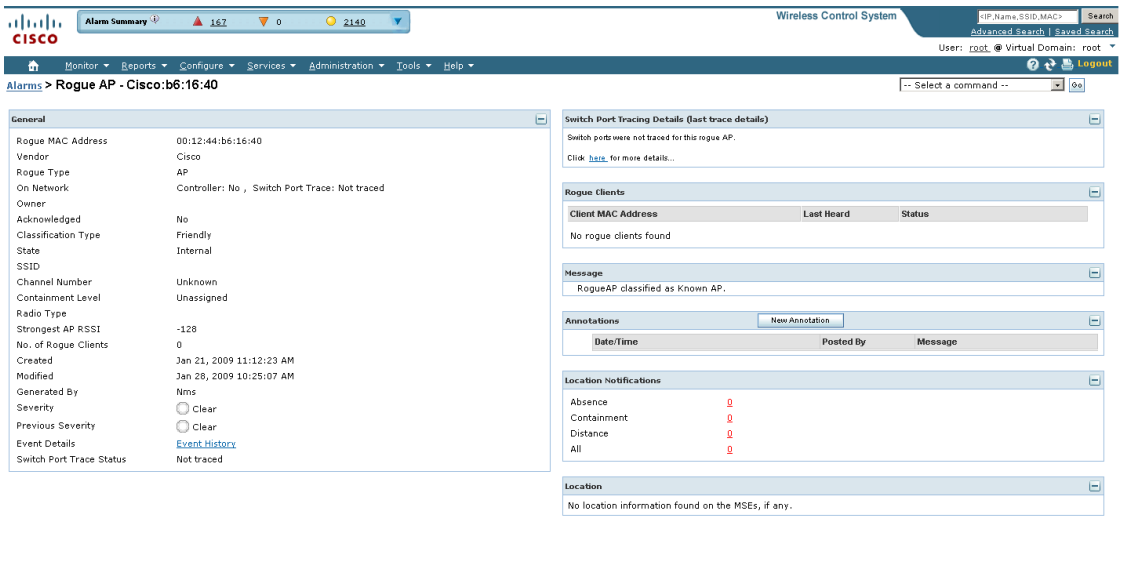
Follow these steps to establish switch port tracing. See the "Switch Port Trace" section on page 18-60 for further information.

Step 1 In the WCS home page, click the **Security** tab.

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

Step 3 Choose the rogue for which you are setting switch port tracking by clicking the URL in the Rogue MAC Address column. The Alarms > Rogue AP details page appears (see Figure 10-18).

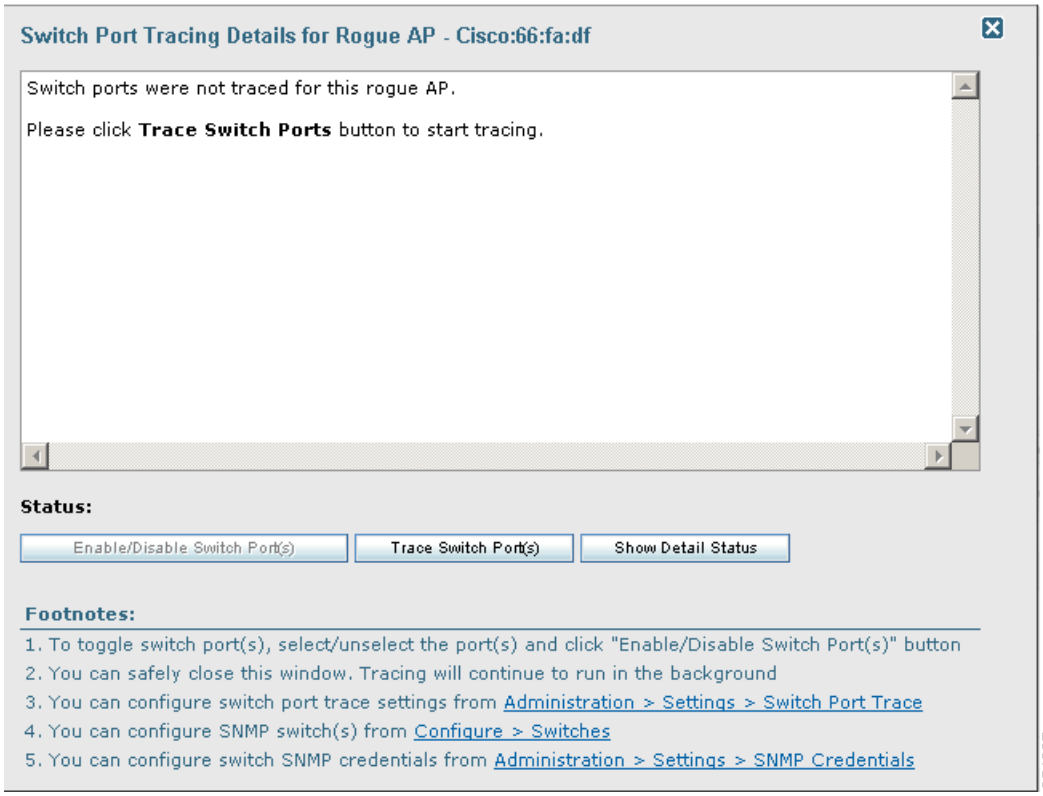
Figure 10-18 Trace Switch Port option on the Alarms > Rogue Page



251829

Step 4 In the Switch Port Tracing Details portion of the page, click the **Click here for more details** link. The Switch Port Tracing Details for Rogue AP page appears (see Figure 10-19).

Figure 10-19 Switch Port Tracing Details for Rogue AP Page



This page provides the current port status. The various status types include the following:

- Not traced—Switch port tracing was never executed.
- Failed—Switch port tracing was executed but failed for some reason. The detail status page in the SPT dialog includes more information.
- Traced and detected on network—Switch port tracing was executed, and a rogue access point was found on the wired network. A *yes* status indicates a wired network.
- Traced and wire contained—Switch port tracing was executed, but the switch port to which the rogue access point was connected is disabled. The rogue access point is now wire contained.

From this page, you can start a trace for troubleshooting purposes by clicking **Trace Switch Ports**. You can also enable and then provide the IP address and hop information or disable switch ports.

When one or more searchable MAC addresses are available, the WCS uses CDP to discover any switches connected up to two hops away from the detecting access point. SPT uses the directly connected Ethernet switches of the detecting access points as the seed switches for tracing. The MIBs of each CDP discovered switch are examined to see if they contain any of the target MAC addresses; therefore, it is important that the access point CDP information is enabled and available. If any of the MAC addresses are found, the corresponding port number is returned and reported as the rogue's switch port.

You can view the access point CDP neighbors choosing Monitor > Access Points and the CDP Neighbors tab. No entries signify that CDP is not enabled on the access point.

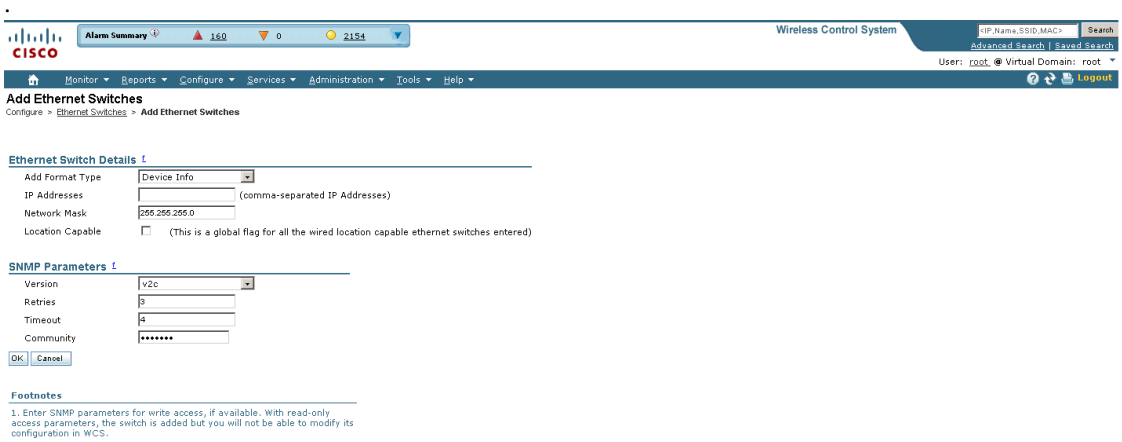
You can configure switch port trace settings by choosing Administration > Settings > Switch Port Trace. See the "Switch Port Trace" section on page 18-60 for more information.

Note If switch port tracing is taking a long time, adjust the settings in the "SNMP Settings" section on page 18-58.

Click the **Message** link in the Annotations section to re-enable the switch port.

Step 5 If you choose Configure > Ethernet Switches, the SNMP communities for the switches are visible (see Figure 10-20). The switch details configured on this page are used only for tracing the rogue access point's switch port. At this same location you can add a location-capable switch for tracking wired clients by MSE and WCS.

Figure 10-20 Configure > Ethernet Switches



251771

Step 6 Choose one of the following:

- If you want to add one switch or use commas to separate multiple switches, leave the Add Format Type drop-down list at Device Info.
- If you want to add multiple switches by importing a CSV file, choose **File** from the Add Format Type drop-down list. With the CSV file, you can generate your own import file and add the devices you want.

Step 7 If you chose Device Info, enter the IP address of the switch you want to add. If you want to add multiple switches, use a comma between the string of IP addresses.

Step 8 Enter the network mask for the IP address you specified.

Step 9 Select the Location Capable check box if the switch is capable of storing the location information.

Step 10 In the SNMP Parameters portion of the page, choose your version choice from the Version drop-down list.

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. To configure SNMPv on the switch, use the following example:

snmp-server view v3default iso included
snmp-server group v3group v3 auth write v3default snmp-server user <username> <v3group> v3 auth <md5 or sha> <authentication password>

If the switch has VLANs, the following must be configured for each VLAN. Otherwise, switch port tracing will fail:

snmp-server group v3group v3 auth context vlan-1 write v3default snmp-server group v3group v3 auth context vlan-20 write v3default

Step 11 You can change the retries and timeout values that were established for this switch if desired.

Step 12 Enter the community for this switch.

Step 13 Click **OK**.

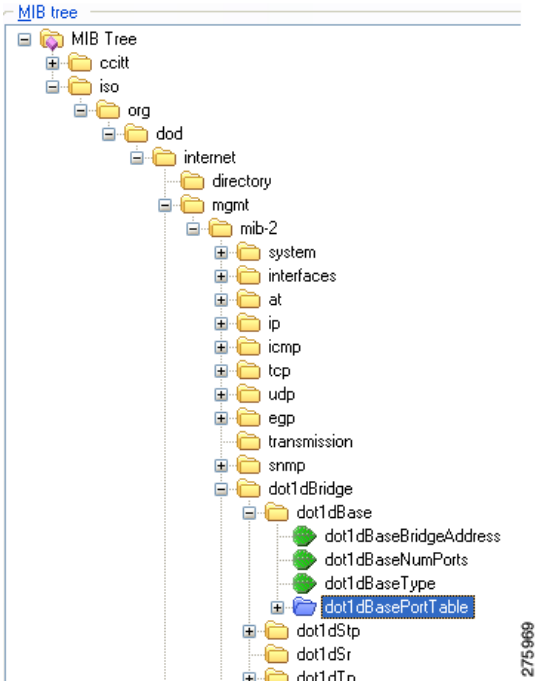
Switch VLANs

Switch Port Trace (SPT) queries the switch CAM table for each VLAN; therefore, the switch must be an unreserved and operational Ethernet VLAN for success of the query. SPT queries vtpVlanTable to determine the VLAN list.

For each VLAN, SPT searches the CAM table for the MAC address. Since CAM tables are stored per VLAN, community string indexing is used to query the switch CAM table. SPT queries dot1dTpFdbTable to get the CAM table entries. In addition to the switch CAM table, SPT also queries the following MIB tables (see Figure 10-21).

Note The switch CAM table must be accessible using community string indexing (such as public@1).

Figure 10-21 MIB Tables



The following MIBs are used by SPT:

Table 10-6 MIBs Used by SPT

MIB	Purpose
vtpVlanTable (CISCO-VTP-MIB)	For VLAN list
dot1dTpFdbTable (BRIDGE MIB)	For query of CAM table entries
dot1dBasePortTable (BRIDGE MIB)	To map base port to ifIndex
ifTable (IF-MIB)	For interface list
ifXTable (IF-MIB)	For interface description (ifAlias)
vlanTrunkPortTable	For trunk port status
cdpCacheTable	For switch CDP neighbors

Removing Switches

You can remove switches by choosing **Configure > Switches** and choosing **Remove Switches** from the Select a command drop-down list.

Shutting a Switch Port

You can suppress the switch port to which the rogue access point is connected. In the Alarms Rogue page (shown in Figure 10-18), choose **Shut Switch Port** from the Select a command drop-down list.

The Alarms page will then show the switch IP address, the switch port, the traced MAC address, the port status, and the timestamp of the suppression.

Client Access on 1524SB Dual Backhaul

The 1524 Serial Backhaul (SB) access point consists of three radio slots. Radios in slot-0 operates in 2.4 GHz frequency band and 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 Universal Client Access feature, client access is also allowed over slot-1 radio and slot-2 radio.

The two 802.11a backhaul radios use the same MAC address. So there maybe instances where same WLAN maps to the same BSSID on more than one slot.

By default Client Access is disabled over both the backhaul radios by default.

The following are the guidelines to 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 both the backhaul radio from either one of the interfaces:

- The Controller Command Line Interface (CLI)
- The Controller Graphical User Interface (GUI)
- The Wireless Control System (WCS) Graphical User Interface (GUI). For more information, see Configuring Client Access using WCS.

Note The procedure for configuring client access using Controller CLI and GUI is documented in the Controller Configuration Guide. See the *Cisco Wireless LAN Controller Configuration Guide* for more information.

Configuring Client Access using WCS

To configure client access on the two backhaul radios:

Step 1 Choose **Configure > Controllers > Controller IP > Mesh > Mesh Settings**.

The Mesh Settings dialog box appears.

Step 2 Select the **Client Access on Backhaul Link** check box to display Extended Backhaul Client Access 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**.

An alert box 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 WCS

To configure backhaul channel deselection:

Step 1 You must first configure the Mesh DCA channels flag on the controllers. See Configuring Mesh DCA Flag on Controllers Using WCS for more information.

Step 2 Then change the channel list using config groups. See Changing the Channel List Using Config Groups for more information.

Configuring Mesh DCA Flag on Controllers Using WCS

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:

Step 1 Choose **Configure > Controller Config Groups**.

Step 2 Select a config group to view its config group details.

Step 3 In the Config Group detail page, click the **Country/DCA** tab.

Step 4 Select or unselect the channels to select or deselect channels for the config group.

Note You can also configure backhaul channel deselection from controllers. For more information, see the Controller Online Help or *Cisco Wireless LAN Controller Configuration Guide*.

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 access point's associated controller.

Note Latency might increase for voice calls when they are switched to a new channel.

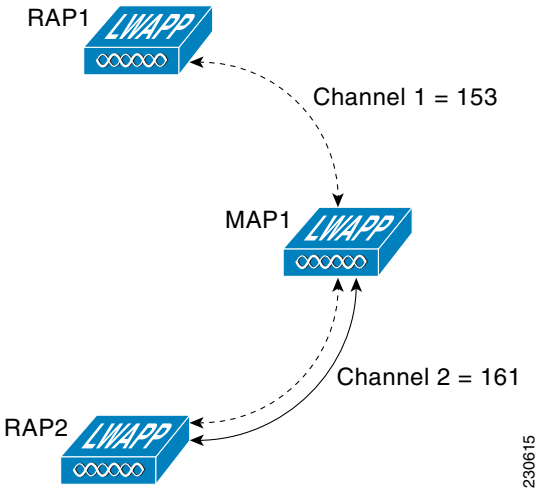
Note In the EMEA regulatory domain, locating neighbors on other channels might take longer given DFS requirements.

Background Scanning Scenarios

A few scenarios are provided below to better illustrate how background scanning operates.

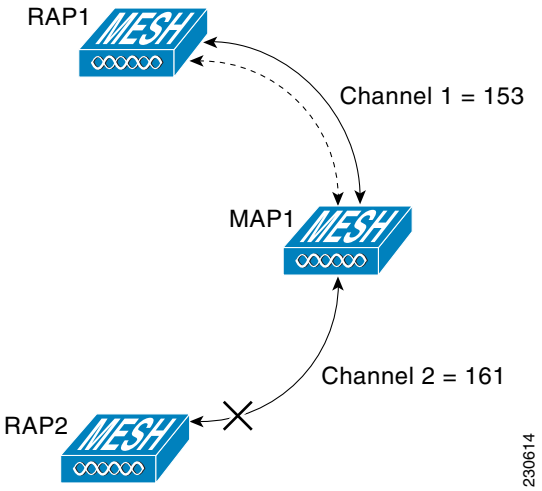
In Figure 10-22, when the mesh access point (MAP1) initially comes up, it is aware of both root access points (RAP1 and RAP2) as possible parents. It chooses RAP2 as its parent because the route through RAP2 is better in terms of hops, SNR, and so on. After the link is established, background scanning (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 10-22 Mesh Access Point (MAP1) Selects a Parent



In Figure 10-23, 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 10-23 Background Scanning Identifies a New Parent



Enabling Background Scanning

Follow these steps to enable background scanning on an AP1510 RAP or MAP:

Step 1 Click **Configure > Controllers.**

Note You can also enable this on the Controllers template. See the "Configuring a Mesh Template" section on page 12-98.

Step 2 Choose **Mesh > Mesh Settings** from the left sidebar menu. The Mesh Settings page appears (see Figure 10-24).

Figure 10-24 Mesh Settings Page

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 QoS Profiles

You can have multiple QoS Profiles on the controller. The 4 default QoS profiles are bronze, silver, gold, and platinum. Follow these steps to modify the existing QoS profiles.

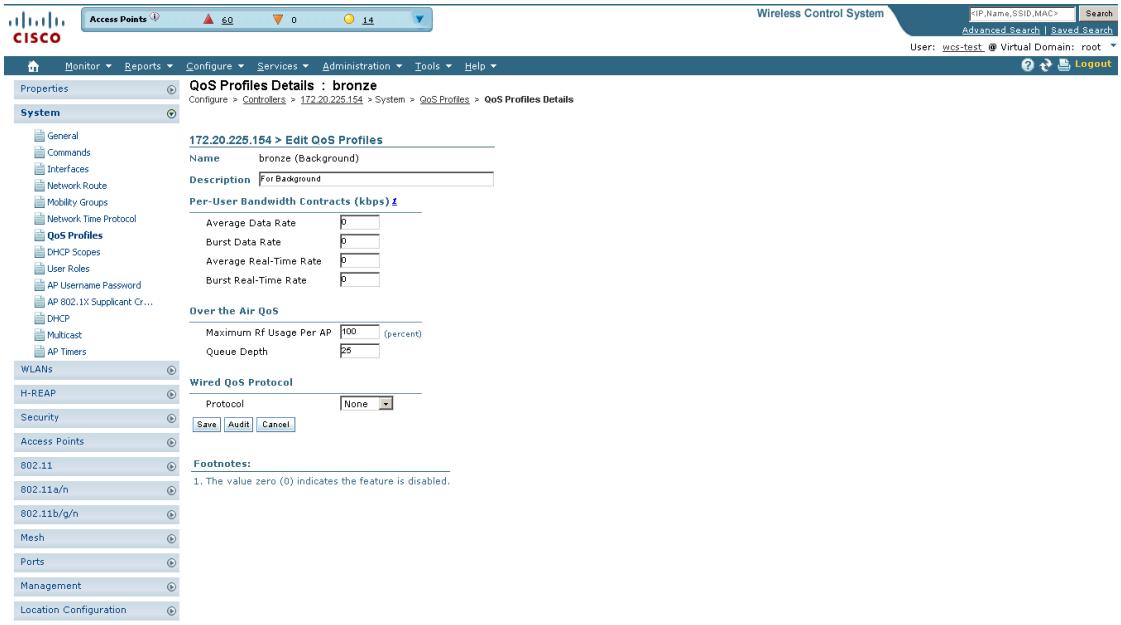
Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the desired controller.

Step 3 Choose **System > QoS Profiles** from the left sidebar menu.

Step 4 Choose the profile you want to modify. The Edit QoS Profiles page appears (see Figure 10-25).

Figure 10-25 QoS Profiles Details Page



251799

CHAPTER 11

Managing Clients

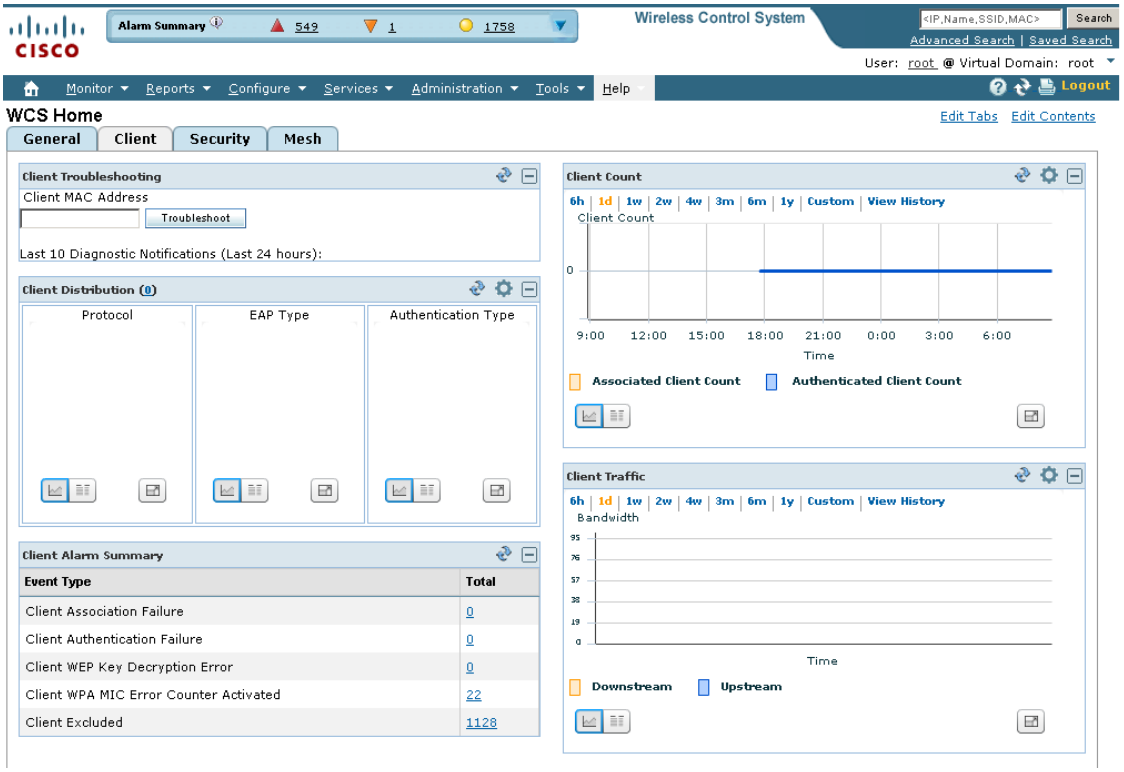
You can look at the client's association history and statistical information in several ways on the Cisco WCS GUI. With WCS 7.0 you can view client session related information and determine client presence, usage patterns, and historical session data. You can also use these tools to analyze and troubleshoot client issues. The information can be used in addition to maps to assess which areas experience inconsistent coverage and which areas have the potential to drop coverage.

Client Tab

You should use the Client tab (see Figure 11-1) on the WCS home page as the main client health monitor. Unlike the historical data retrieved from the device periodically and stored in the WCS Client Detail page, this trend data can be collected whenever you chose to refresh the dashboard with the current network status. It can be customized and acts as a main client health monitor where you can get overall client information. You can see how many client devices are connected to your network as well as where and how these devices have accessed your network. You can also see which clients are authenticated or excluded.

Note When you click the Client Tab from the WCS home page, it takes longer than average to load the data.

Figure 11-1 Client Tab



Use the **Edit Content** link to choose the components you want to have appear on the Client tab. You can choose the component from the Available Components list and then click to add it to the left or right column. For more information on using the Edit Content link, refer to the "Editing Content" section on page 2-25. For example, if you wanted to see the client count in both the General and Client dashboards, you could add the same component to both.

To return to the original client tab before customization, click **Edit Tabs** and choose the **Reset to Factory Default** button.

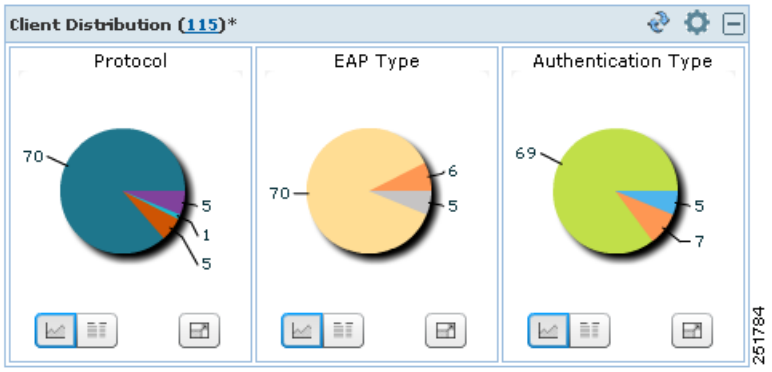
Client Distribution

This component (see Figure 11-2) shows how many clients are on your network presently. You can see how clients are distributed by protocol, EAP type, and authentication type.

- Protocol—Represents radio bands such as 802.11a/n, 802.11b/g/n, and so on
- EAP-Type—Represents 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 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 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). You can filter the data that is displayed in client distribution by clicking the Component Options icon and choosing either controller IP, SSID, or floor area.

Figure 11-2 Client Distribution

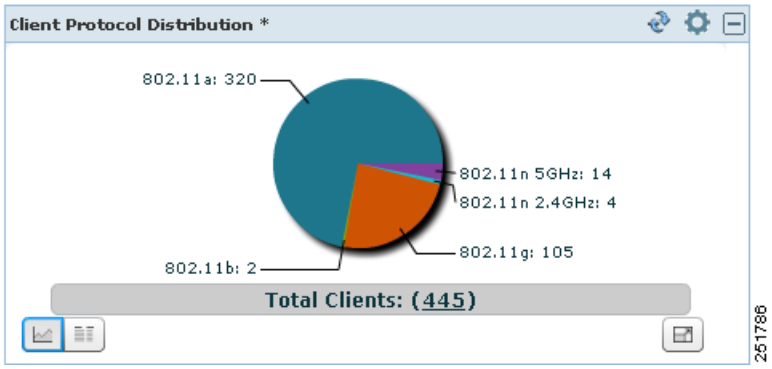


Note The asterisk next to the Client Distribution count indicates that the component has been customized. If you reset to the default page, the asterisk is cleared.

Client Protocol Distribution

This component (see Figure 11-3) shows the current client count distribution by protocols. It shows the subtotal of each radio band (802.11a/n and 802.11b/g/n) distribution and the total client count. 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). You can filter the data that is displayed in client count by clicking the Component Options icon and choosing either controller IP, SSID, or floor area.

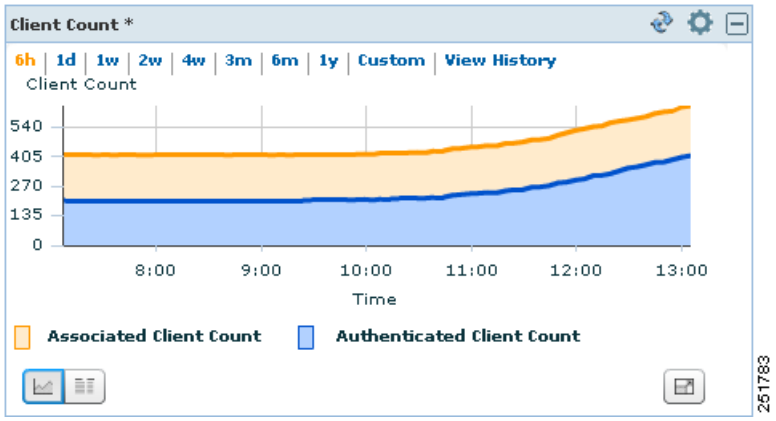
Figure 11-3 Client Protocol Distribution



Client Count

This component (see Figure 11-4) shows the trend of associated and authenticated client counts in a given period of time. You can choose to display the information in table form or in a pie chart. It shows the minimum, average, and maximum number of clients. You can filter the data that is displayed in client count by clicking the Component Options icon and choosing either controller IP, SSID, or floor area.

Figure 11-4 Client Count



If you click **View History**, Client Count Historical Charts appear for the various time frames (see Figure 11-5). The Client Count Historical Charts show the client count over the last hour, 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.

Figure 11-5 View History

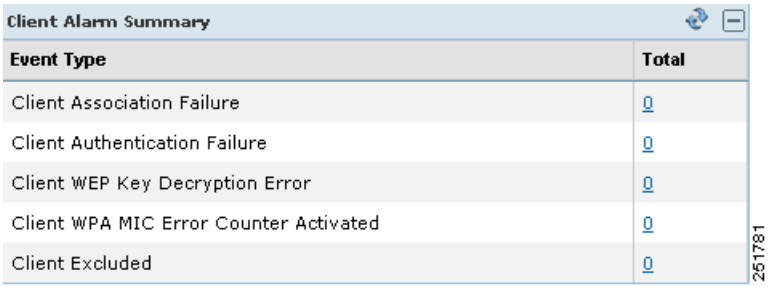
Client Alarm Summary

This component (see Figure 11-6) shows the five most recent client alarms providing the following data:

- Client Association Failure
- Client Authentication Failure
- Client WEP Key Decryption Error
- Client WPA MIC Error Counter Activated
- Client Excluded

Click the number in Total column to open the Events page (the same page that you see when you choose Monitor > Events.

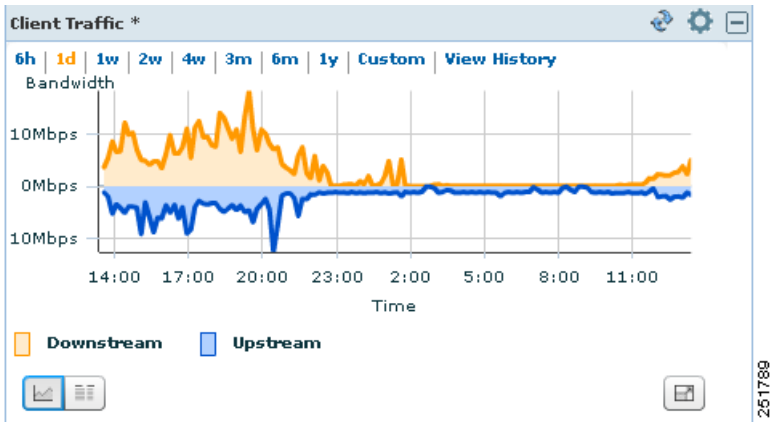
Figure 11-6 Client Alarm Summary



Client Traffic

Controllers keep counters for the number of bytes transferred and received for each client. WCS 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 (see Figure 11-7). 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 a pie chart. When generating the chart based on the floor, WCS adds up all client traffic on this floor. You can filter the data that is displayed in client traffic by clicking the Component Options icon and choosing either controller IP, SSID, or floor area.

Figure 11-7 Client Traffic



If you click **View History**, Client Traffic Historical Charts appear for the various time frames (see Figure 11-5). The Client Traffic Historical Charts show 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.

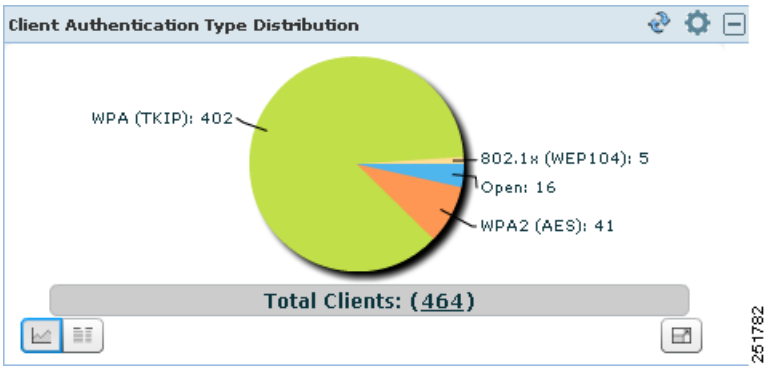
Client Authentication Type Distribution

This component (see Figure 11-8) 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). You can filter the data that is displayed in client authentication type distribution by clicking the Component Options icon and choosing either controller IP, SSID, or floor area.

Note Only the current authentication types are shown. Obsolete types are not displayed.

Figure 11-8 Client Authentication Type Distribution



AP Join Taken Time

This component (see Figure 11-9) shows how long it took each access point to join the controller. You can restrict the number of access points to display by clicking the Component Options icon and choosing the items per page.

Figure 11-9 AP Join Taken Time

AP Join Taken Time

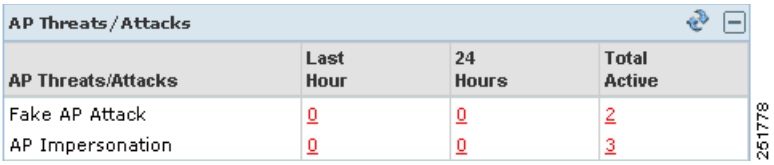
AP Name	AP Join Taken Time
AP1140-2	15 m 48 s
sjc14-12b-ap5	1 m 25 s
Rogue_Detector	1 m 21 s
AP2	1 m 12 s
AP1250	1 m 10 s

251774

AP Threats/Attacks

This component (see Figure 11-10) shows the type and number of attacks and threats that have occurred in the last hour, last 24 hours, and the total active.

Figure 11-10 AP Threats/Attacks



Client Detail Page

This section describes how to view client properties, client association history, client statistics, client session information, and so on. The Client Detail page shows the association history graph to represent the time-based data. The information will help you identify, diagnose, and resolve client issues. Follow these steps to open the Client Detail page.

Note To view complete details on the Monitor > Client details screen 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 1 Choose **Monitor > Clients**.

Step 2 Choose a hyperlink from the Client Username column to view client details. The Monitor > Client > Client Details page appears (see Figure 11-11). This data is displayed in both table and chart form.

Figure 11-11 Client Details Page

The Client Details page includes the following information:

- Client Identity and Device Information—Username, Client MAC address, Client IP address, Client host name, Vendor, CCX Version, and power save.
- Association Information—Protocol, SSID, Profile, VLAN ID, Interface, Associated AP name, Associated AP MAC address, Associated AP IP address, Associated controller name, Associated controller IP, First seen time, Last seen time, and Current associated status.
- Security Information—Security policy, 802.11 authentication, Cipher, and EAP type.
- Statistic Information—RF quality, SNR, RSSI, Throughput, Data rate, Bytes sent and received, Packets sent and received, and retries.

- Historical Charts—Client association chart and RF quality, SNR and RSSI, Bytes sent and received, Packets sent and received.
- Events—Client association failure, Client authentication failure, Client WEP key decryption error, client WPA MIC error counter activated, Client decrypt error occurred, Client excluded, AP disassociated from controller, and AP crash.
- Client Location—A small map showing the current client location.
- CCXv5—Basic CCXv5 client information if appropriate.
- Client Sessions—The details of the client session stated during the selected time range.

Running a Link Test

A link test uses a ping sent from parent to child or child to parent to test the link quality. The controller polls the RF parameters of the ping reply packets received by the access point to determine link quality. Because radio link quality can differ depending on the direction (client to access point versus access point to client), it is critical to have Cisco Compatible Extensions linktest support so that link quality is tested in both directions. The access point polls the controller on regular intervals until the row status indicates success or failure. During the link test, the table is populated. If the link test fails, the controller reverts to a ping test.

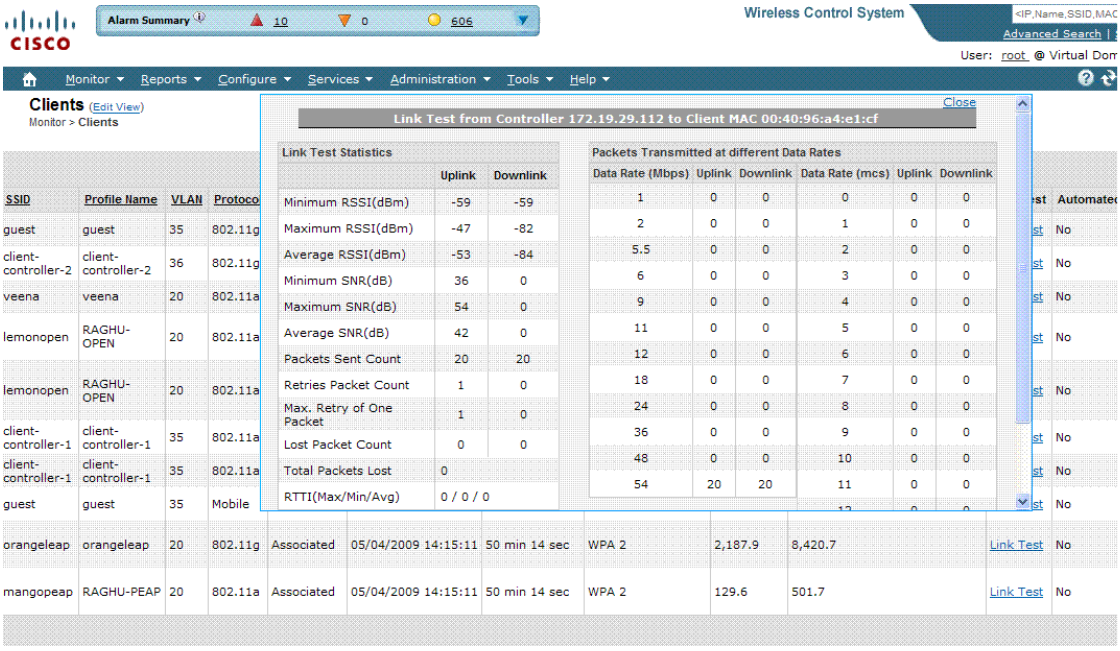
Follow these steps to run a link test:

Step 1 Choose **Monitor > Clients**.

Step 2 From the Show drop-down list, choose **All Clients**.

Step 3 Click the **Link Test** link. The link test begins. Figure 11-12 shows a sample link test result. The results show on the same page if the client is associated. Unsuccessful link tests show a failure message.

Figure 11-12 Cisco Compatible Extensions Link Test Result



Enabling Automatic Client Troubleshooting

On 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.

Follow these steps to enable automatic client troubleshooting.

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, WCS processes the diagnostic association trap. When it is not selected, WCS raises the trap, but automated troubleshooting is not initiated.

Step 4 Click **Save**.

Client Details from 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.

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 "Creating and Running a New Report" section on page 17-2

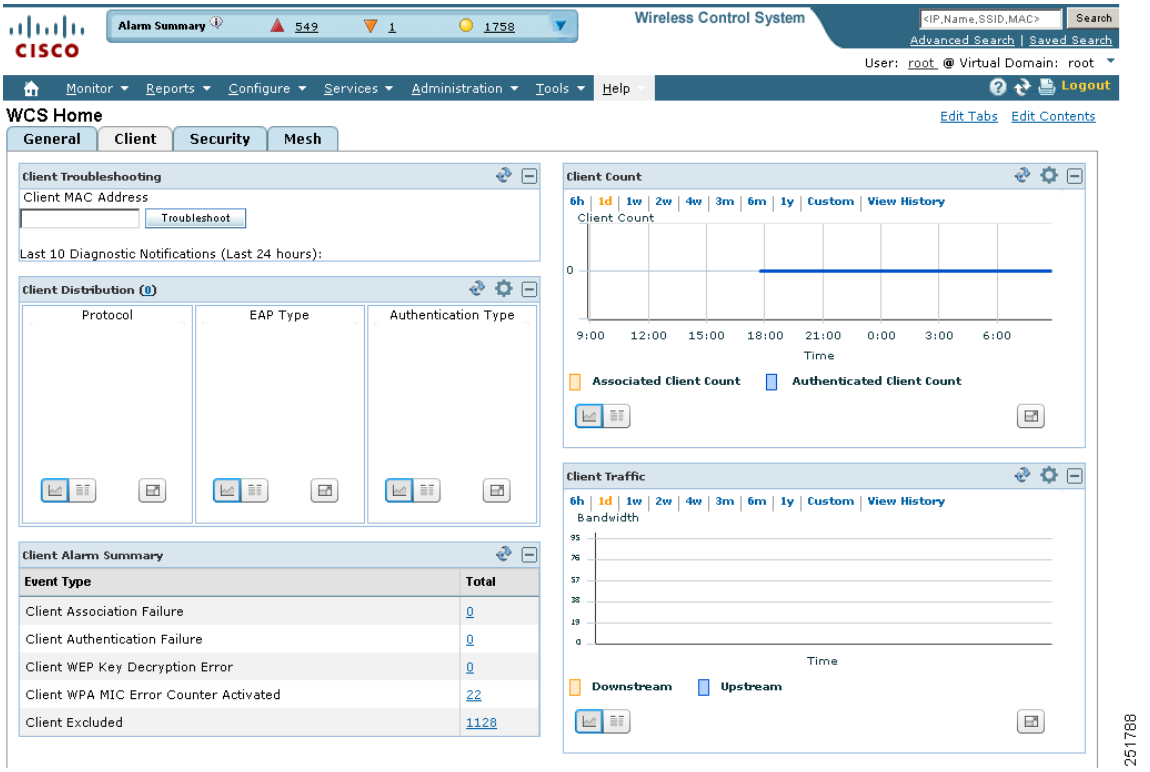
Client Troubleshooting

You can begin troubleshooting several ways: by entering a MAC address in the Client tab dashboard, by using the search function, or by clicking the Troubleshooting icon within the Client MAC Address column on the Monitor > Clients page. Any method provides all the information necessary to troubleshoot historical client issues. You can monitor the status of the connection, verify the user's current and past locations, and troubleshoot client connectivity problems. You may 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 reauthentications, and any RRM events. An administrator can correlate reassociations and reauthentications and determine if the problem was with the network or client.

Troubleshooting from the Client Tab Dashboard

If you enter a client MAC address and click the **Troubleshoot** button (see Figure 11-13), the same Client Details page as shown in Figure 11-1 appears.

Figure 11-13 Client Tab Troubleshooting



Note If the client is not currently associated, most of the information will not appear.

Troubleshooting Using the Search Feature

Client search is the primary method for you to locate clients. For a detailed description of the search feature, refer to the "Using the Search Feature" section on page 2-31. Follow these steps to troubleshoot a client using the search feature.

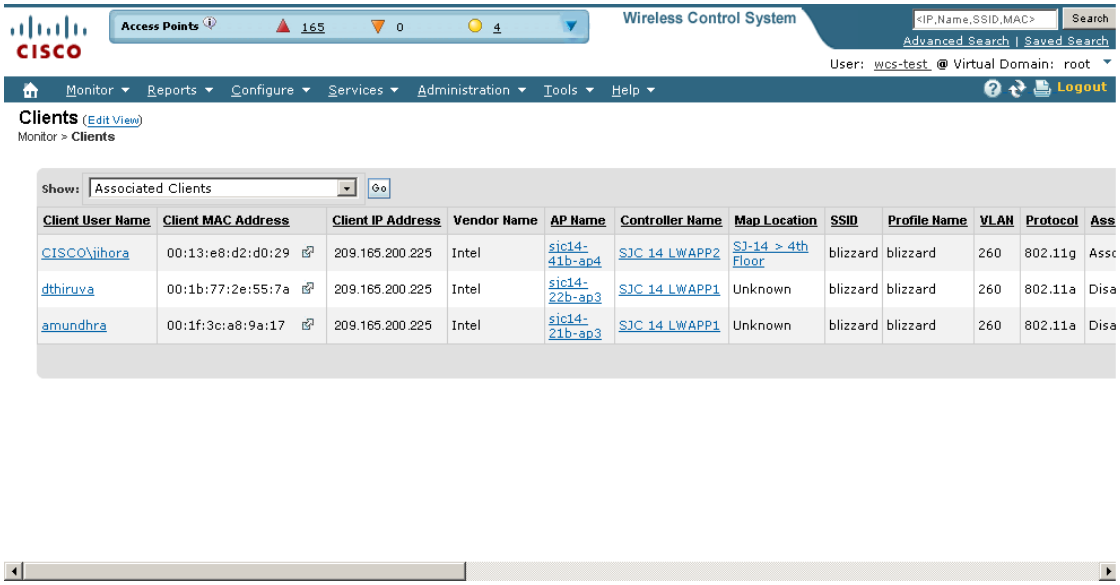
Step 1 Choose **Monitor > Clients**.

Step 2 In the Quick Search area, type the MAC address of the client and click **Search**. The Search Results page appears (see Figure 11-14).

Figure 11-14 Search Results Page

Step 3 Click **View List** to see the clients that matched the search criteria in the Clients page. The Monitor > Clients page appears (see Figure 11-15).

Figure 11-15 Clients Page



The Monitor > Clients Page displays the following information:

Table 11-1 Clients Page Information

Table Column	Description
Client Username	The username of the client used for authentication. Clicking the client username displays detailed information about the client such as client properties, association history, and client status and performance statistics.
Client IP Address	The IP address of the client.
Client MAC Address	The MAC address of the client.

Table 11-1 Clients Page Information (continued)

Table Column	Description
Vendor Name	The client's vendor information.
AP Name	The name of the access point to which the client is associated. Clicking the AP name displays information in the Monitor > Access Points page.
Controller Name	The IP address of the controller to which the client is registered. Clicking the controller name displays information in the Monitor > Controllers > System > Summary page.
Map Location	The physical location of the client (such as building, floor, and so on). Clicking the map location displays information in the Monitor > Maps page.
SSID	The SSID assigned to this WLAN. The access points broadcast the SSID on this WLAN. Different WLANs can use the same SSID as long as the Layer 2 security has a different value.
Profile Name	The profile name of the WLAN that the client is associated to or is trying to associate to.
VLAN	The client has successfully joined an access point for the given SSID. VLAN is the reverse lookup of the interface used by the WLAN on the controller side.
Protocol	Indicates whether the 802.11a/n or 802.11b/g/n protocol is being used.
Association	The state of the client. May be one of the following: • Idle—completing an AAA transaction • AAA Pending—completing an AAA transaction • Authenticated—802.11 authentication completed • Associated—802.11 association completed • Power Save—client in power save mode • Disassociated—802.11 disassociation completed • To Be Deleted—to be deleted after disassociation • Probing—client not associated or authorized yet
Association Time	The date and time that the status of the client last changed.
Session Length	The length of time the client has been in the current state.
Authentication Type	The 802.11authentication algorithm that is in use.
Traffic (MB)	The amount of client traffic (in MBs) for both inbound and outbound.
Avg Session Throughput (kbps)	The throughput averages across a session.
Link Test	Runs a link test of the client. See the "Running a Link Test" section on page 11-9 section for further information.
Automated Test Ran	Indicates whether or not an automated test has been run.
Authenticated	Indicates whether the client has been authenticated.

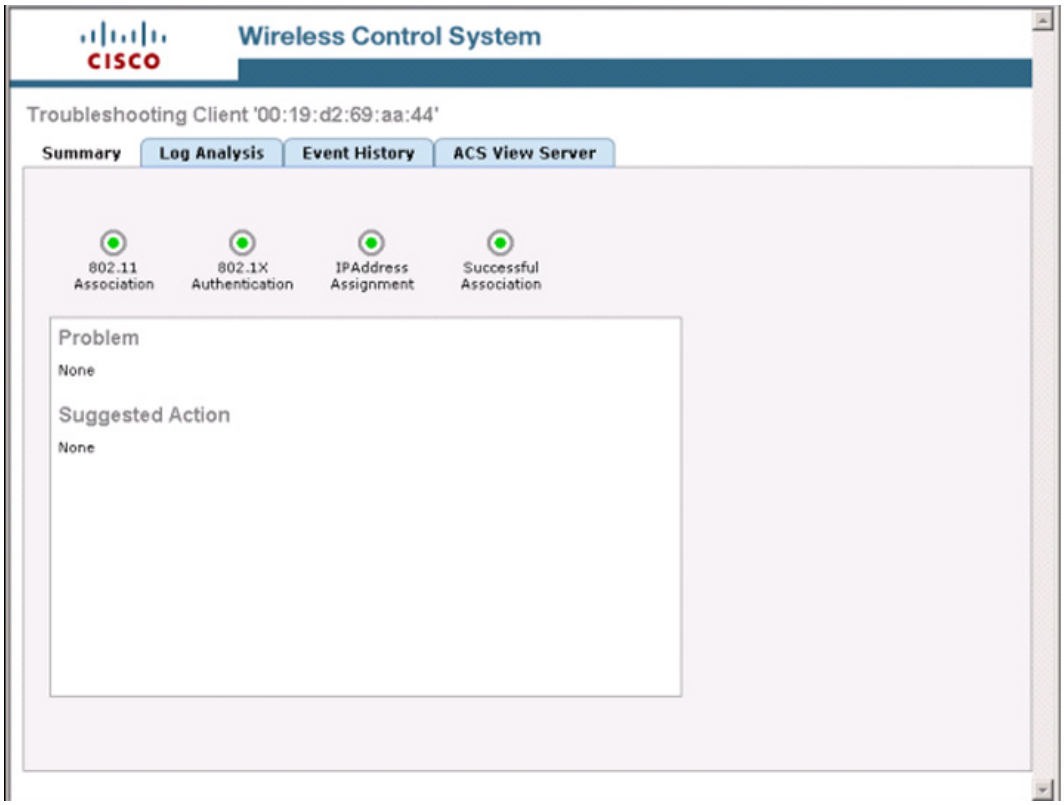
Table 11-1 Clients Page Information (continued)

Table Column	Description
CCX	Indicates the Cisco Compatible Extension version, if the client supports it.
Client Host Name	Specifies the client host name.
Controller IP Address	Clicking a controller IP address displays information from the Monitor > Controllers > System > Summary page.
Port	The port on the controller to which the client is connected.
E2E	Indicates whether E2E is supported.
Encryption Cipher	Encryption settings.
Client IP Address	The IP address of the client.

Step 4 Click the troubleshooting icon to the right of the Client MAC Address that you want to troubleshoot. The Troubleshooting Client page appears (see Figure 11-16). If you are troubleshooting a Cisco Compatible Extension v5 client, your Troubleshooting Client page has additional tabs like the page referenced in Figure 11-20.

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**.

Figure 11-16 Troubleshooting Client 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 3.0 or later or Internet Explorer 7.0 or later on a Windows workstation.

Step 5 To view log messages logged against the client, click the **Log Analysis** tab (see Figure 11-17).

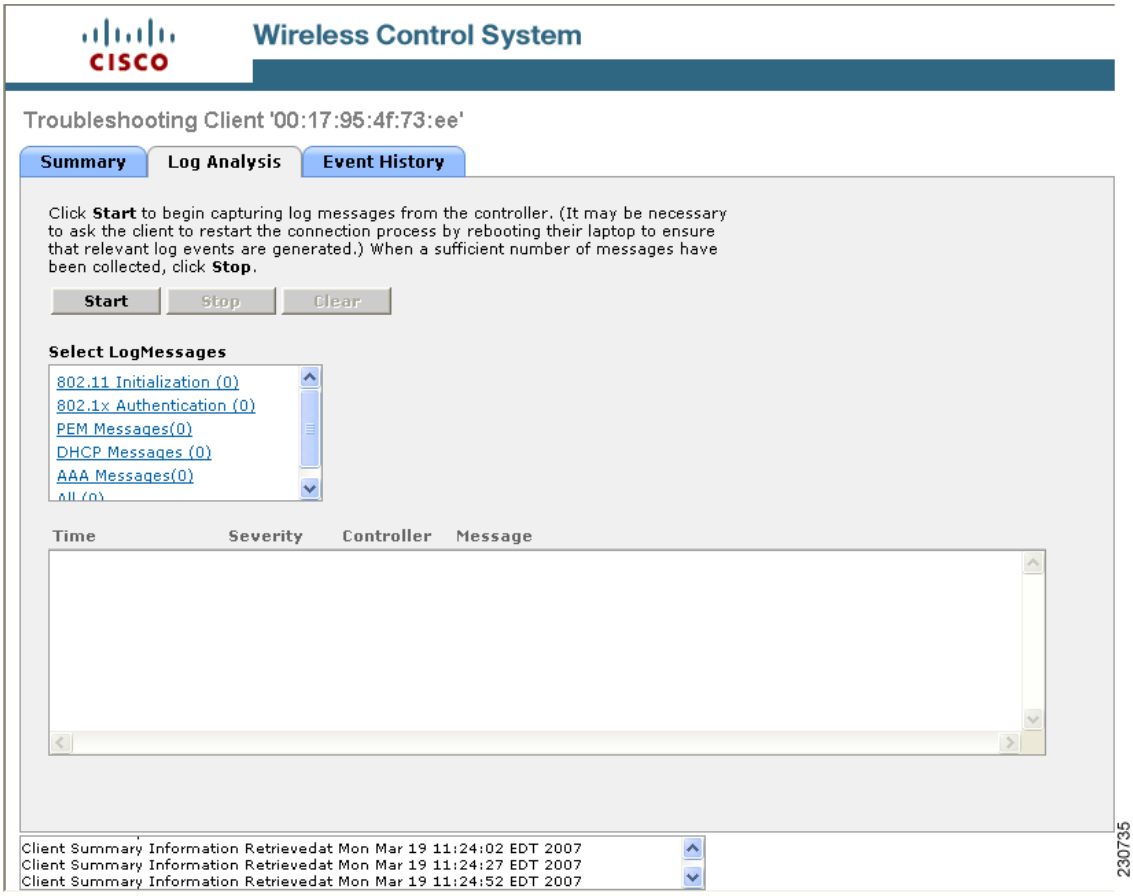
Step 6 To begin capturing log messages about the client from the controller, click **Start**. To stop log message capture, click **Stop**. To clear all log messages, click **Clear**.

Note Log messages are captured for ten minutes and then stopped automatically. A user 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 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

Figure 11-17 Log Analysis Tab

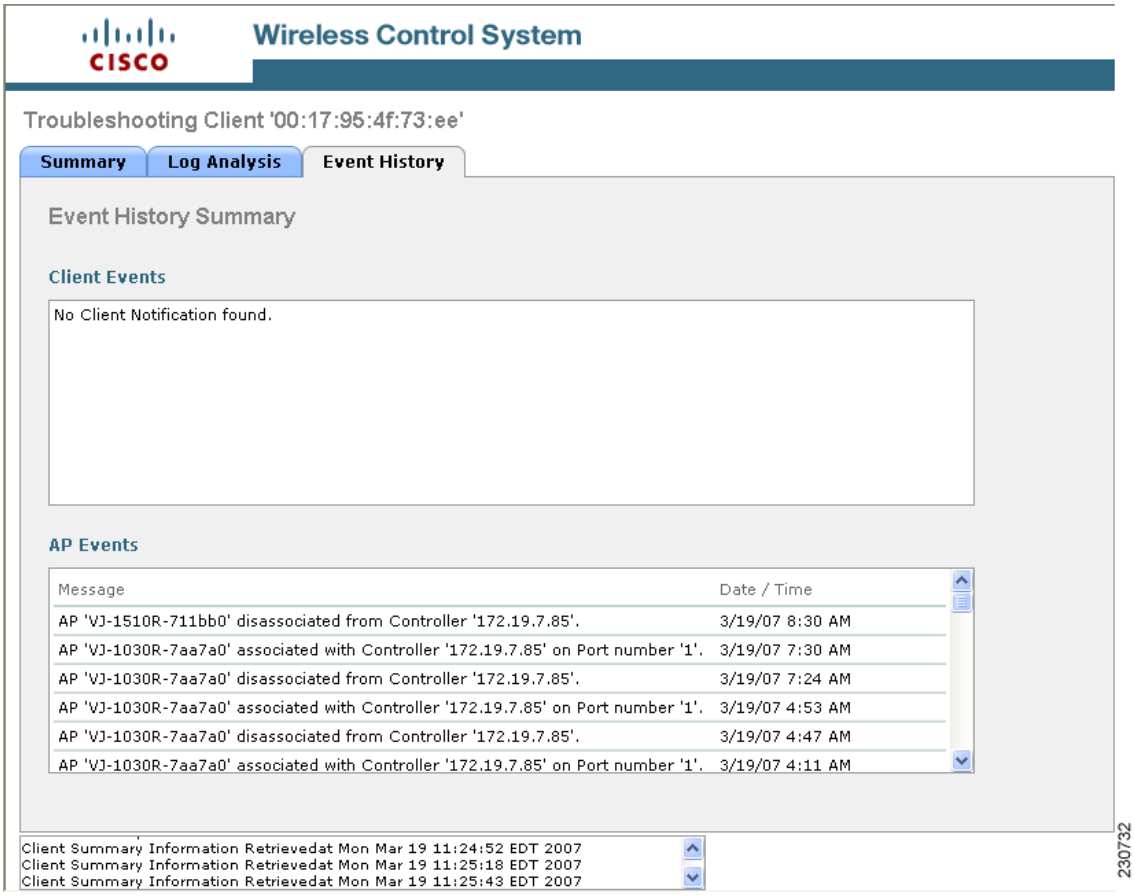


Step 8 To display a summary of the client's event history, click the **Event History** tab (see Figure 11-18).

Note If an access point that the client is associated to has Media Session Snooping enabled within the WLAN configuration, any Session Initiation Protocol (SIP) errors that are detected appear in the AP Events list.

This page displays client and access point events that occurred within the last 24 hours.

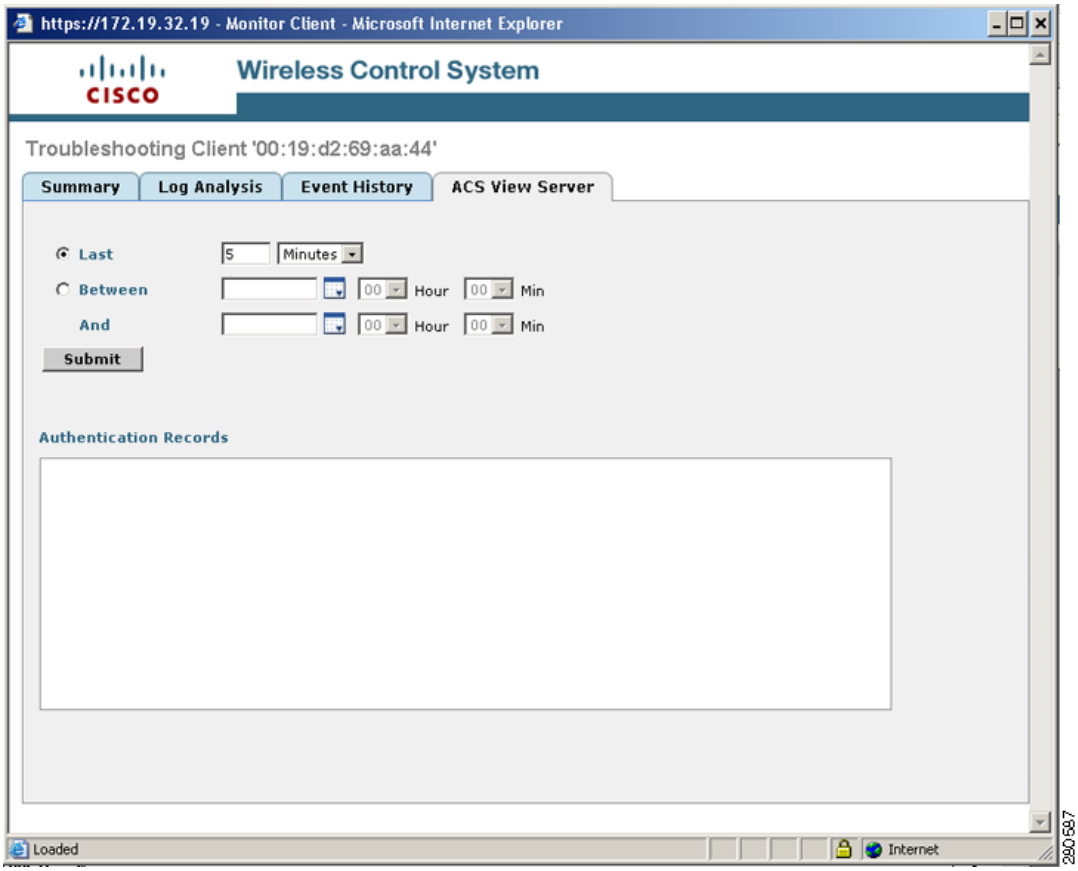
Figure 11-18 Event History Tab



Step 9 If you click the ACS View Server tab, you can interact with the Cisco Access Control (ACS) System View Server (see Figure 11-19). You must have View Server credentials established before you can access this tab. (The tab will show the server list as empty if no view servers are configured.) See the "Configuring ACS View Server Credentials" section on page 6-2 for steps on establishing credentials.

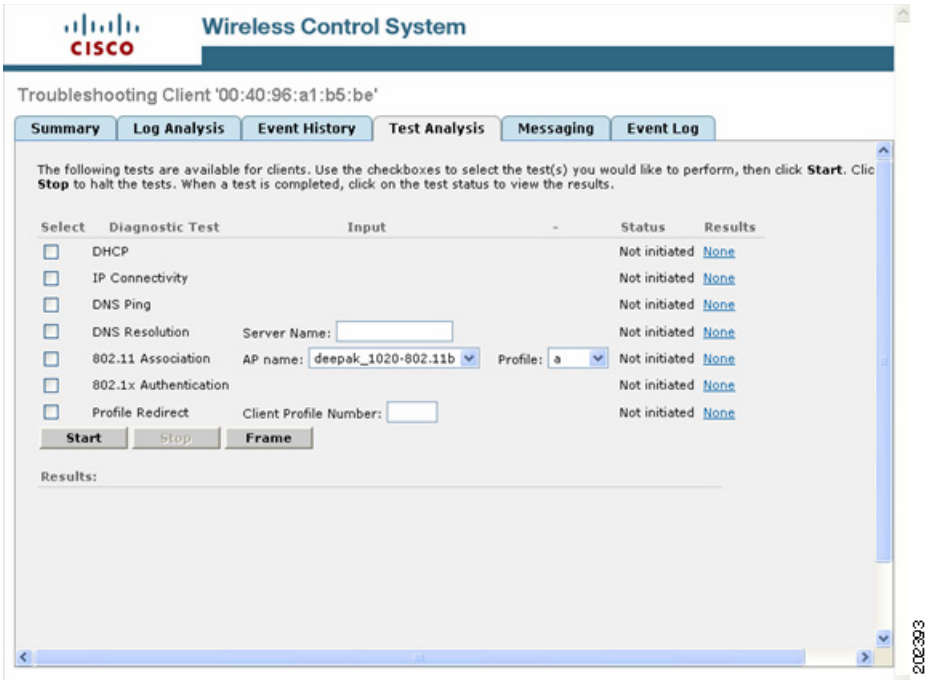
This server provides WCS with aggregated client status information from multiple ACS servers. The client status information allows you to further troubleshoot client issues and determine whether they are related to authentication or authorization. Enter the date and time ranges to retrieve the historical authentication and authorization information and click **Submit**. The results of the query are displayed in the Authentication Records portion of the page and is used as a filter for the userid logged into the client.

Figure 11-19 ACS View Server Page



Step 10 (Optional) If Cisco Compatible Extension Version 5 clients are available, you can click a Test Analysis tab as shown in Figure 11-20.

Figure 11-20 Test Analysis Tab



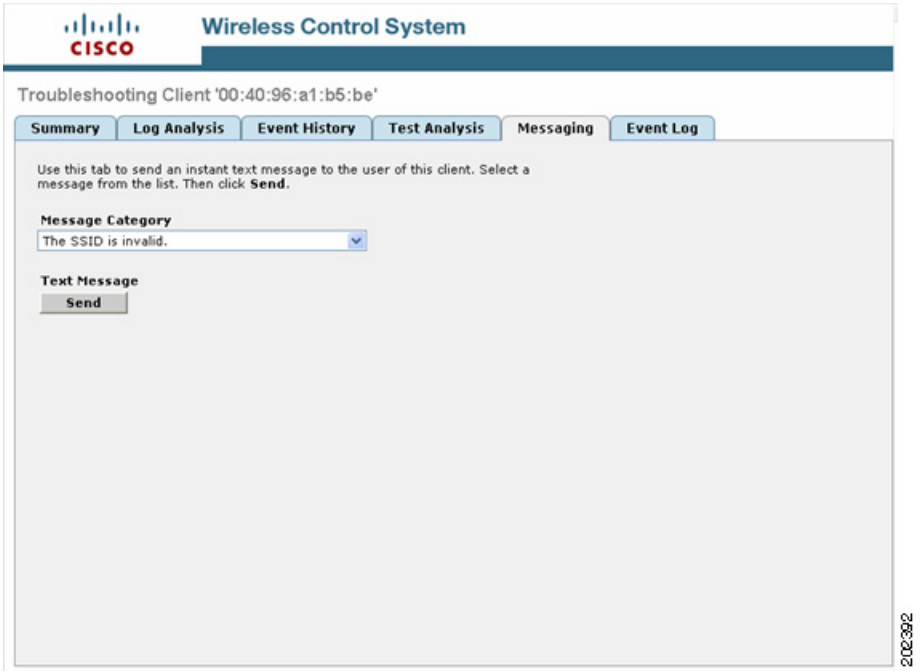
The Test Analysis tab allows you to run a variety of diagnostic tests on the client. Click the check box for the applicable diagnostic test, enter any appropriate input information and click **Start**. The following diagnostic tests are available:

- 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 in order 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 in order 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 in order to verify that name resolution is functioning correctly.
- 802.11 Association—Directs an association to be completed with a specific access point to in order 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 in order to verify that the client is able to properly complete an 802.1x authentication.
- Profile Redirect—At any time, the diagnostic system may direct the client to activate one of the client's 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 11 (Optional) If Cisco Compatible Extension Version 5 clients are available, a Messaging tab as shown in Figure 11-21 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**.

Figure 11-21 Messaging Tab



Step 12 Close the Troubleshooting Client page.

CHAPTER 12

Using Templates

This chapter describes the Controller Template Launch Pad. It is a hub for all controller templates. Templates provide a way to set parameters that you can then apply to multiple devices without having to re-enter the common information. 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.

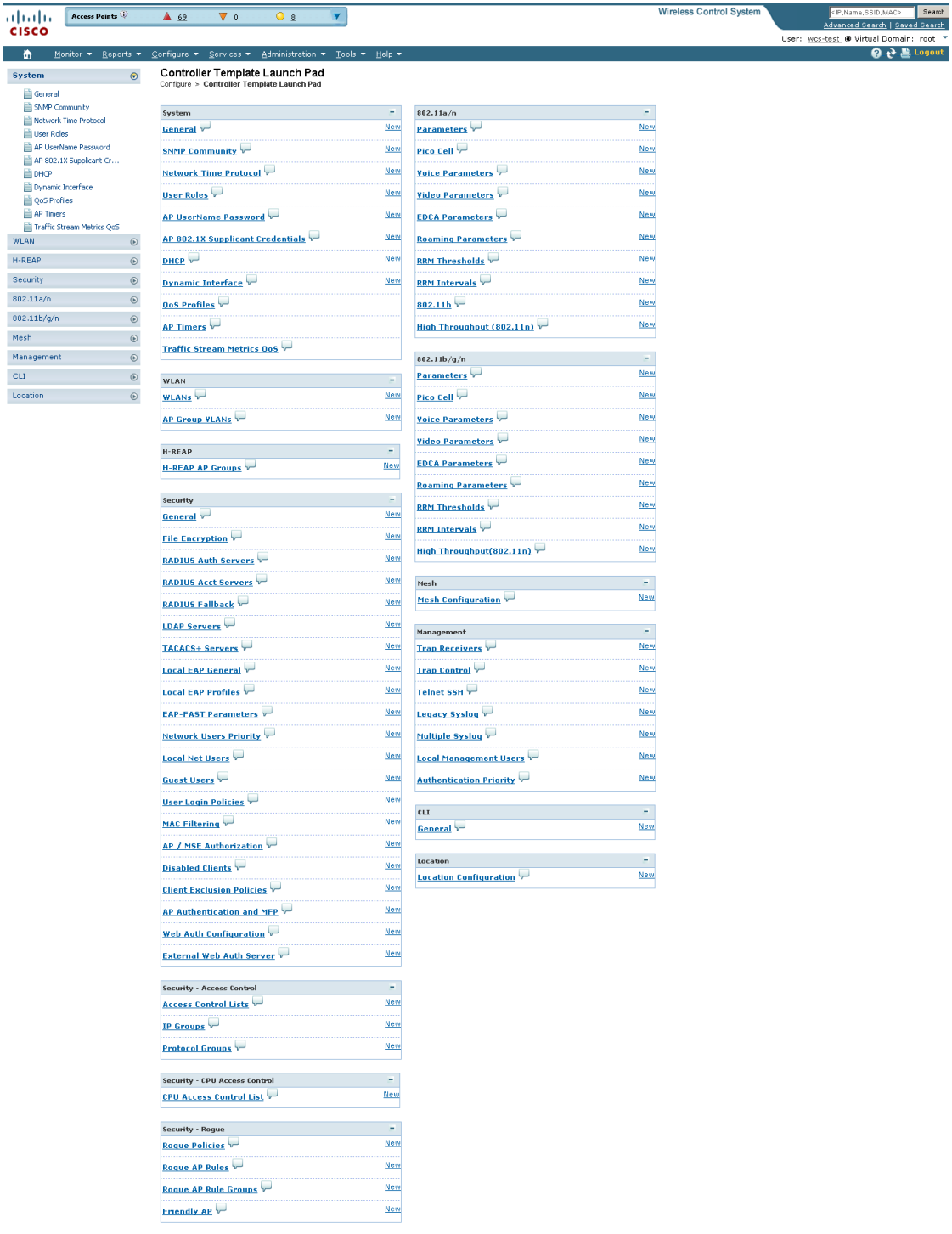
This chapter contains these sections:

- Controller Template Launch Pad, page 12-1
- Adding Controller Templates, page 12-3
- Configuring Controller Templates, page 12-3
- Applying a Set of CLI Commands, page 12-109
- Configuring Location Settings, page 12-110
- Adding Access Point Templates, page 12-113
- Configuring Access Point Templates, page 12-113

Controller Template Launch Pad

The controller template launch pad appears when you choose **Configure > Controller Template Launch Pad** (see Figure 12-1).

Figure 12-1 Controller Template Launch Pad



Tip Hold your mouse cursor over the tool tip next to the template type to view more details regarding the template.

Adding Controller Templates

Follow these steps to add a new controller template.

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.

Step 4 Describe the template.

Step 5 Click **Save**.

Note If you attempt to save a template without a name, the following popup message appears: "Template Name: This attribute is MANDATORY. Please specify it. Make the necessary corrections and try again."

Configuring Controller Templates

Within this chapter, you can find information on adding or configuring the following controller templates:

- Configuring General Templates, page 12-4
- Configuring an NTP Server Template, page 12-8
- Configuring AP 802.1X Supplicant Credentials, page 12-9
- Configuring Dynamic Interface Templates, page 12-11
- Configuring a Traffic Stream Metrics QoS Template, page 12-16
- Configuring WLAN Templates, page 12-18
- Configuring a File Encryption Template, page 12-36
- Configuring a RADIUS Authentication Template, page 12-37
- Configuring a RADIUS Accounting Template, page 12-40
- Configuring a Local EAP General Template, page 12-46
- Configuring a Local EAP Profile Template, page 12-47
- Configuring an EAP-FAST Template, page 12-49
- Configuring Network User Credential Retrieval Priority Templates, page 12-51
- Configuring a Local Network Users Template, page 12-52
- Configuring Guest User Templates, page 12-54
- Configuring a User Login Policies Template, page 12-56
- Configuring a MAC Filter Template, page 12-57
- Configuring an Access Point or MSE Authorization, page 12-59
- Configuring a Manually Disabled Client Template, page 12-60

- Configuring a CPU Access Control List (ACL) Template, page 12-74
- Configuring a Rogue AP Rules Template, page 12-77
- Configuring a Rogue AP Rule Groups Template, page 12-79
- Configuring a Friendly Access Point Template, page 12-81
- Configuring a Client Exclusion Policies Template, page 12-61
- Configuring an Access Point Authentication and MFP Template, page 12-63
- Configuring a Web Authentication Template, page 12-64
- Configuring External Web Auth Server, page 12-69
- Configuring Radio Templates (for 802.11a/n or 802.11b/g/n), page 12-83
- Configuring a Voice Parameter Template (for 802.11a/n or 802.11b/g/n), page 12-86
- Configuring EDCA Parameters through a Controller Template, page 12-88
- Configuring EDCA Parameters through a Controller Template, page 12-88
- Configuring an RRM Threshold Template (for 802.11a/n or 802.11b/g/n), page 12-91
- Configuring an RRM Interval Template (for 802.11a/n or 802.11b/g/n), page 12-93
- Configuring an 802.11h Template, page 12-94
- Configuring a High Throughput Template (for 802.11a/n or 802.11b/g/n), page 12-95
- Configuring CleanAir Controller Templates (for 802.11a/n or 802.11b/g/n), page 12-96
- Configuring a Mesh Template, page 12-98
- Configuring a Trap Receiver Template, page 12-100
- Configuring a Trap Control Template, page 12-101
- Configuring a Telnet SSH Template, page 12-104
- Configuring a Legacy Syslog Template, page 12-105
- Configuring a Multiple Syslog Template, page 12-106
- Configuring a Local Management User Template, page 12-107
- Configuring a User Authentication Priority Template, page 12-108
- Configuring Radio Templates, page 12-130

Configuring General Templates

Follow these steps to add a general template or make changes to an existing general template.

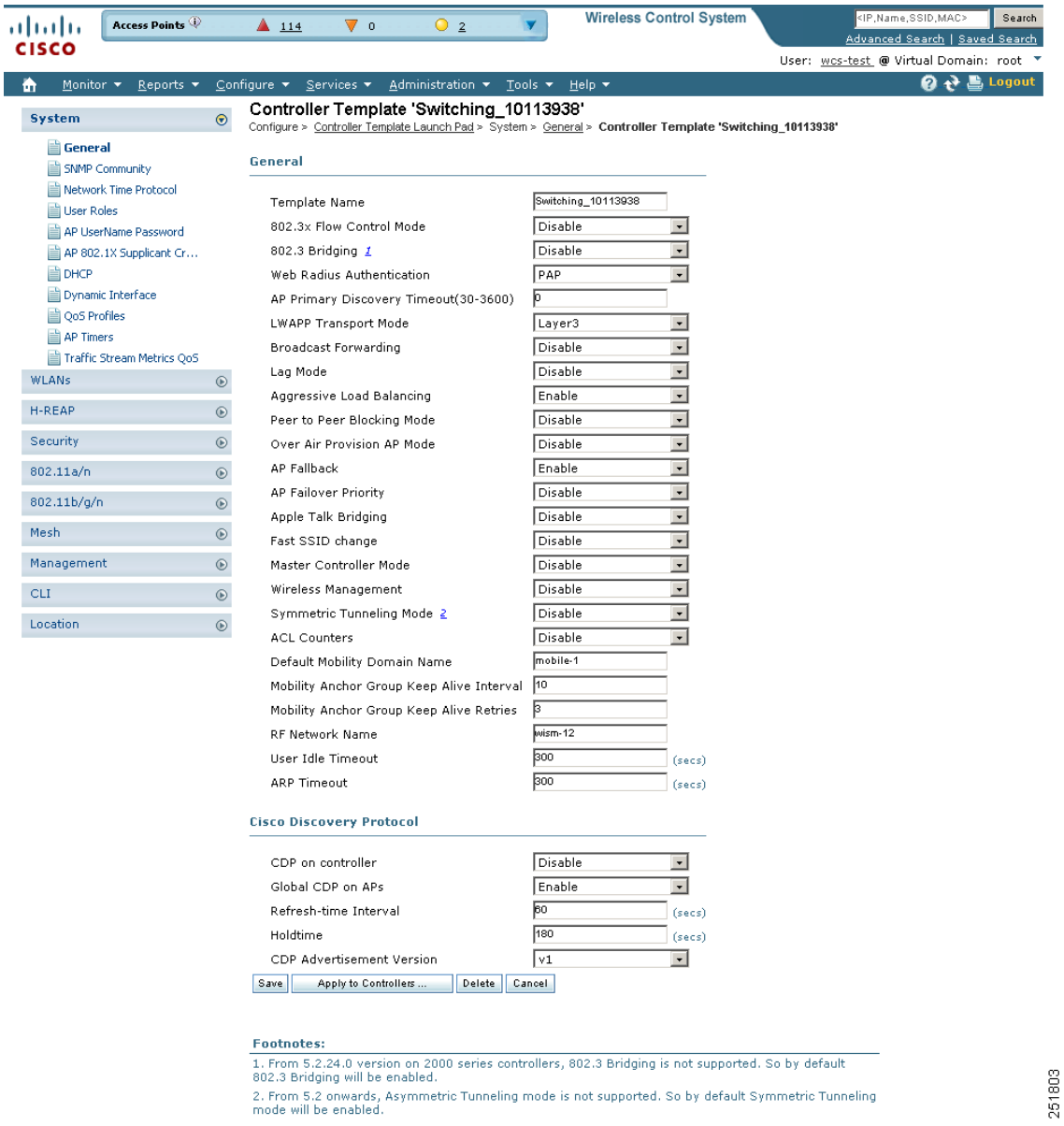
Step 1 Choose **Configure > Controller Template Launch Pad**.

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 (see Figure 12-2).

Figure 12-2 System > General Page



Step 3 Use the drop-down list to enable or disable flow control mode.

Step 4 Use the 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 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 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.

Step 8 Choose to enable or disable broadcast forwarding. The default is disabled.

Step 9 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 10 Choose to enable or disable aggressive load balancing.

Step 11 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 12 At the Over Air AP Provision Mode drop-down list, choose **enable** or **disable**.

Step 13 At 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 14 When a controller fails, the backup controller configured for the access point suddenly receives a number of discovery and join requests. This may 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 at the AP Failover Priority drop-down list if you want to allow this capability.

Step 15 Choose to enable or disable Apple Talk bridging.

Note This Apple Talk bridging option is not available on 5500 series controllers.

Step 16 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 17 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 may enable the controller as the master controller from the Master Controller Mode drop-down list.

Step 18 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 19 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 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.

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 20 Use the drop-down list to enable or disable ACL counters. The values per ACL rule can be viewed for each controller.

Step 21 Enter the operator-defined RF mobility group name in the Default Mobility Domain Name text box.

Step 22 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 over the parameter field with the mouse, the valid range for that field appears.

Step 23 At the Mobility Anchor Group Keep Alive Retries, specify the number of queries to anchor before the client declares it unreachable.

Step 24 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 25 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 26 Specify the timeout in seconds for the address resolution protocol. The factory default is 300 seconds.

Step 27 At the CDP on controller drop-down list, you can choose to enable CDP on the controller. CDP is a device discovery protocol that runs on all Cisco manufactured equipment (such as routers, bridges, communication servers, and so on).

Step 28 At the Global CDP on APs drop-down list, you can choose to enable CDP on the access point.

Step 29 At the Refresh Time Interval parameter, enter the interval at which CDP messages are generated. With the regeneration, the neighbor entries refresh.

Step 30 At the Holdtime parameter, enter the time in seconds before the CDP neighbor entry expires.

Step 31 At the CDP Advertisement Version parameter, enter the version of the CDP protocol to use.

Step 32 Choose **enable** or **disable** from the LAG Mode drop-down list. Link aggregation enables 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.

Note With the 5500 series controllers, LAG works even if packets from an IP address are not on the same physical port. LAG does the load balancing by sending packets from the source IP to a different port.

If LAG is enabled on a controller, the following configuration changes occur:

- Any dynamic interfaces that you have created are deleted 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 are as follows:

- It ensures that if one of the links goes down, the traffic is moved to the other links in the LAG. Hence, as long as one of the physical ports is working, the system remains functional.
- It eliminates the need to configure separate backup ports for each interface. The management interface is marked as an AP manager interface, and an access point can join on this interface.
- Multiple AP-manager interfaces are not required since only one logical port is visible to the application. You can, however, mark any dynamic interface as an extra AP manager interface (one AP manager interface per port).

Note When you make changes to the LAG configuration, the controller has to be rebooted for the changes to take effect.

Note When you hover over the parameter field with the mouse, the valid range for that field appears.

Step 33 Click **Save**.

Configuring an NTP Server Template

Follow these steps to add an NTP template or make modifications to an existing NTP template. NTP is used to synchronize computer clocks on the internet.

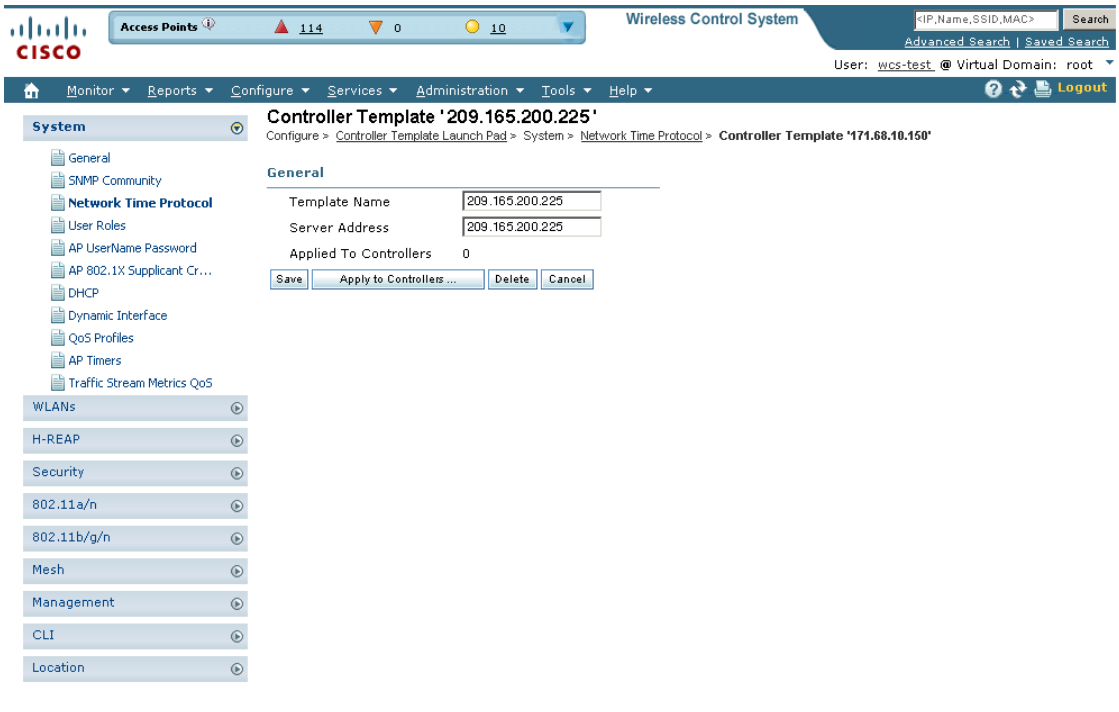
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-3).

Figure 12-3 NTP Servers Template



Step 4 Enter the NTP server IP address.

Step 5 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. All access points that are currently joined to the controller and any that join in the future are included. Follow these steps to add or modify an existing AP 802.1X Supplicant Credentials template.

Note If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point. See "Configuring Access Points" section on page 9-17 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 parameters.

Step 4 Click **Save**.

Configuring DHCP Template

Follow these steps to add a DHCP template or make modifications to an existing DHCP template.

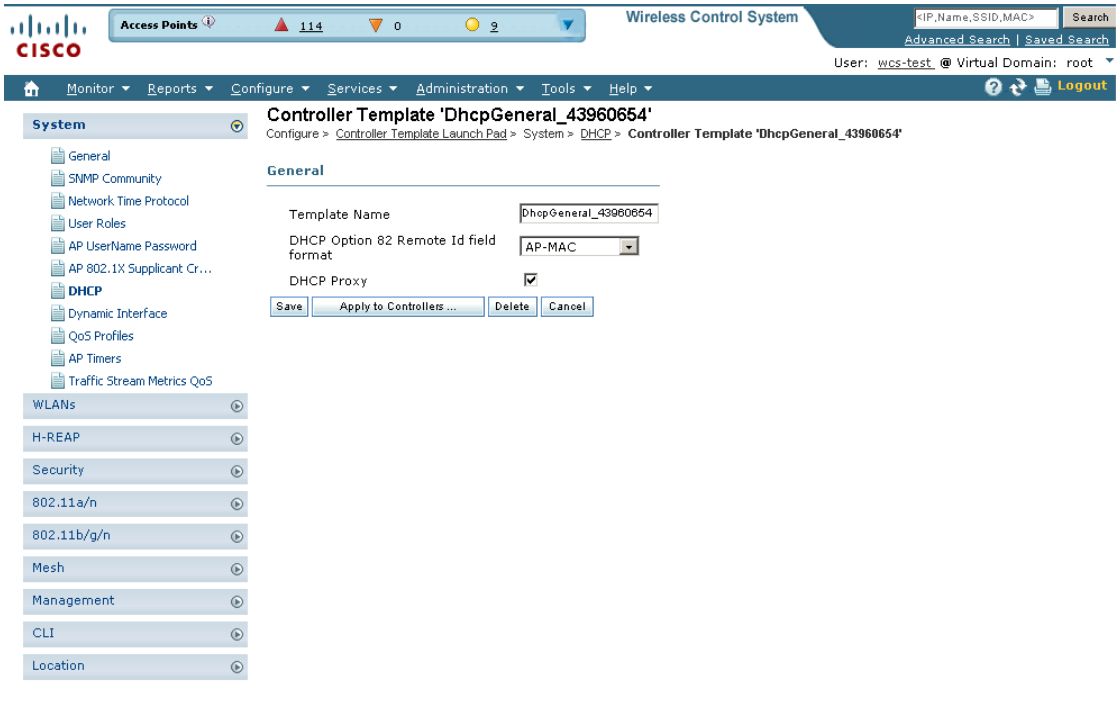
Step 1 Choose **Configure > Controller Template Launch Pad**.

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.

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, click **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 (see Figure 12-4).

Figure 12-4 DHCP Template Page



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 Click **Save**.

Configuring Dynamic Interface Templates

Follow these steps to add a dynamic interface template or make modifications to an existing interface configuration.

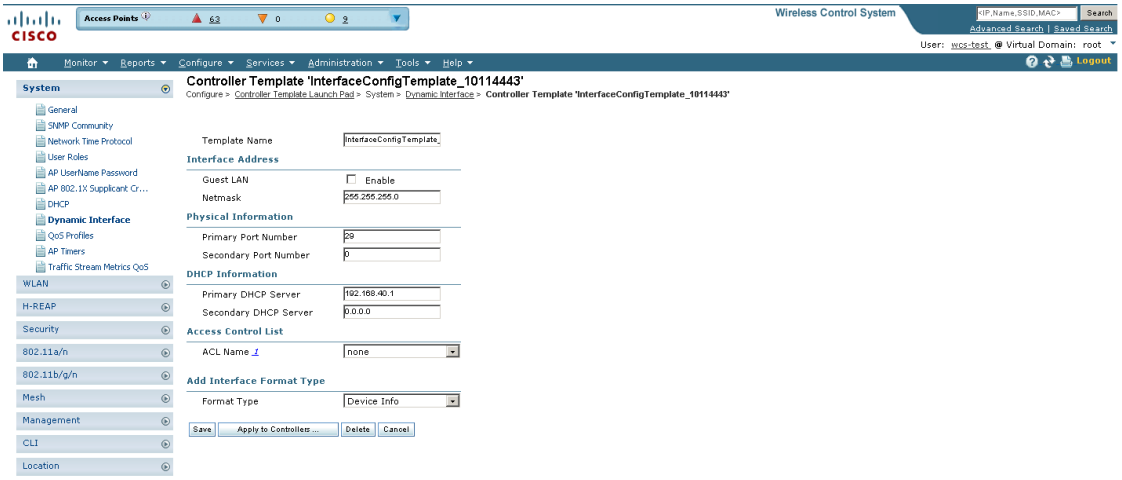
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-5).

Figure 12-5 Dynamic Interface Template



251795

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 which port is 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 Add Format Type drop-down list in the Add Interface Format Type section, choose either Device Info or File. If you choose device info, you must configure the device specific parameters for each controller. If you choose File, you must configure CSV device specific parameters (Interface Name, VLAN Identifier, Quarantine VLAN Identifier, IP Address, and Gateway) for all the managed controllers specified in the CSV file (see Table 12-1). If you choose Device Info, continue to Step 12.

The sample CSV files are as follows:

Table 12-1 Sample CSV Files

ip_address	interface_name	vlan_id	quarantine_ vlan_id	interface_ ip_address	gateway
209.165.200.224	dyn-1	1	2	209.165.200.228	209.165.200.229
209.165.200.225	interface-1	4	2	209.165.200.230	209.165.200.231

Table 12-1 Sample CSV Files

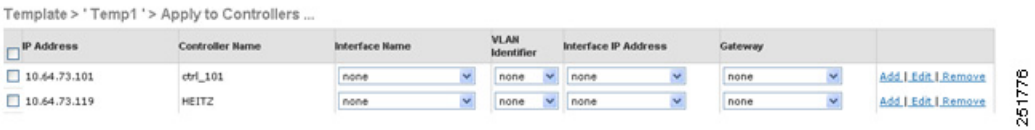
ip_address	interface_name	vlan_id	quarantine_ vlan_id	interface_ ip_address	gateway
209.165.200.226	interface-2	5	3	209.165.200.232	209.165.200.233
209.165.200.227	dyna-2	2	3	209.165.200.234	209.165.200.235

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 12 If you choose Apply to Controllers, you advance to the Apply To page where you can configure device-specific parameters for each controller (see Figure 12-6).

Figure 12-6 Apply To Page



Step 13 Use the **Add** and **Remove** options to configure device specific parameters for each controllers. If you click **Edit**, a dialog box appears with the current parameter input.

Step 14 Make the necessary changes in the dialog box, and click **OK**.

Note If you change the interface parameters, the WLANs are temporarily disabled, so, you may lose connectivity for some clients. Any changes to the interface parameters are saved only after you successfully apply them to the controller(s).

Note If you remove an interface here, it is removed only from this template and NOT from the controllers.

Configuring QoS Templates

Follow these steps to modify the quality of service (QoS) profiles.

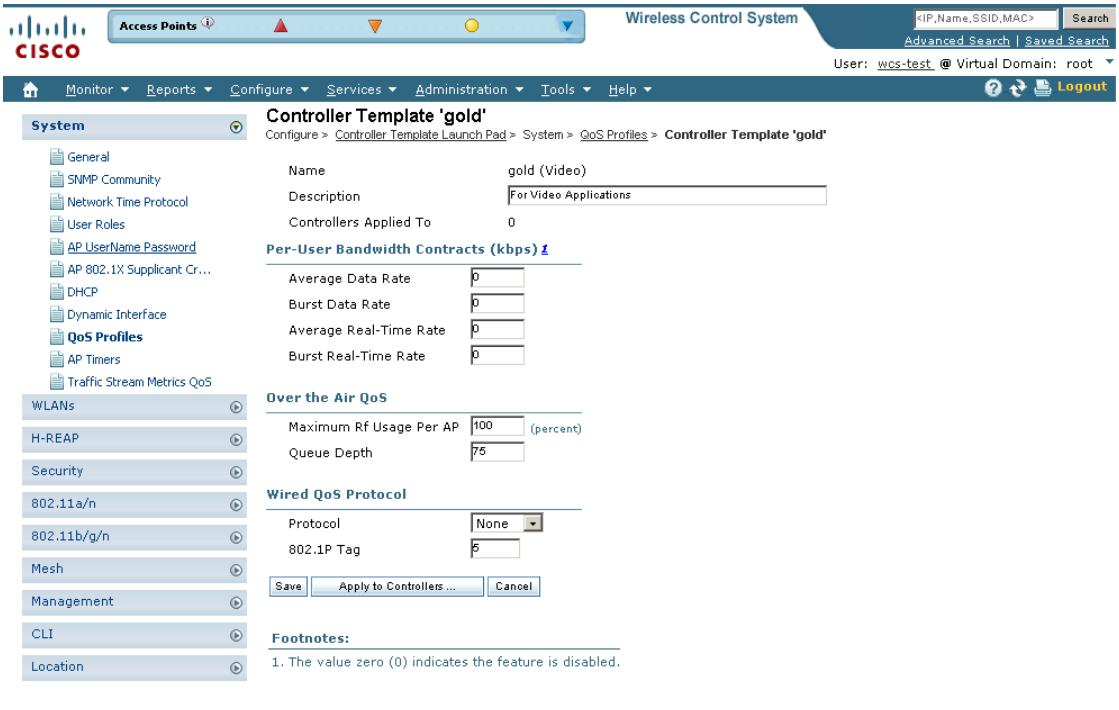
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **QoS Profiles** or choose **System > QoS Profile**s 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 (see Figure 12-7).

Figure 12-7 Edit QoS Profile Template Page



Step 4 Set the following values in the Per-User Bandwidth Contracts portion of the page. 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 for the Over-the-Air QoS portion of the page.

- 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 6 Set the following values in the Wired QoS Protocol portion of the page.

- 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

Some advanced timer configuration for HREAP and local mode is available for the controller on WCS. Follow these steps to configure a template for advanced timers.

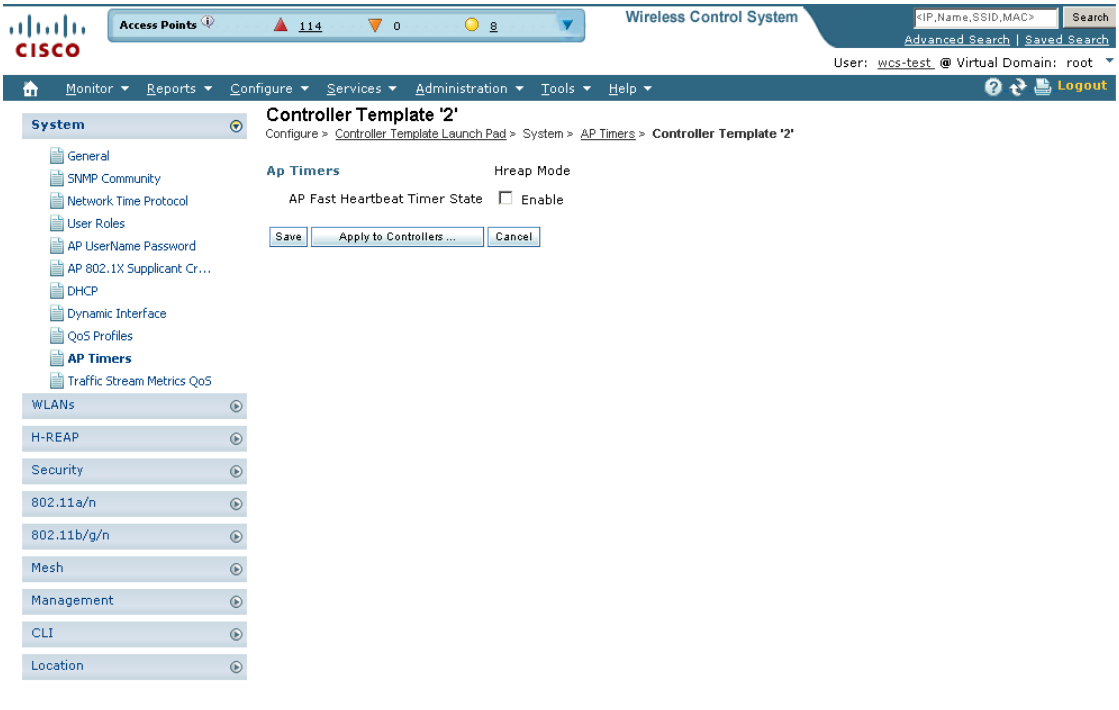
Step 1 Choose **Configure > Controller Template Launch Pad**.

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 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 To reduce the controller failure detection time, click **Local Mode** (see Figure 12-8). 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 1 and 10 seconds.

Figure 12-8 AP Timers Page



Step 4 Click **HREAP Mode**. You can then configure the HREAP timeout value. Check the AP Primary Discovery Timeout check box to enable the timeout value. Enter a value between 30 and 3600 seconds.

Step 5 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.

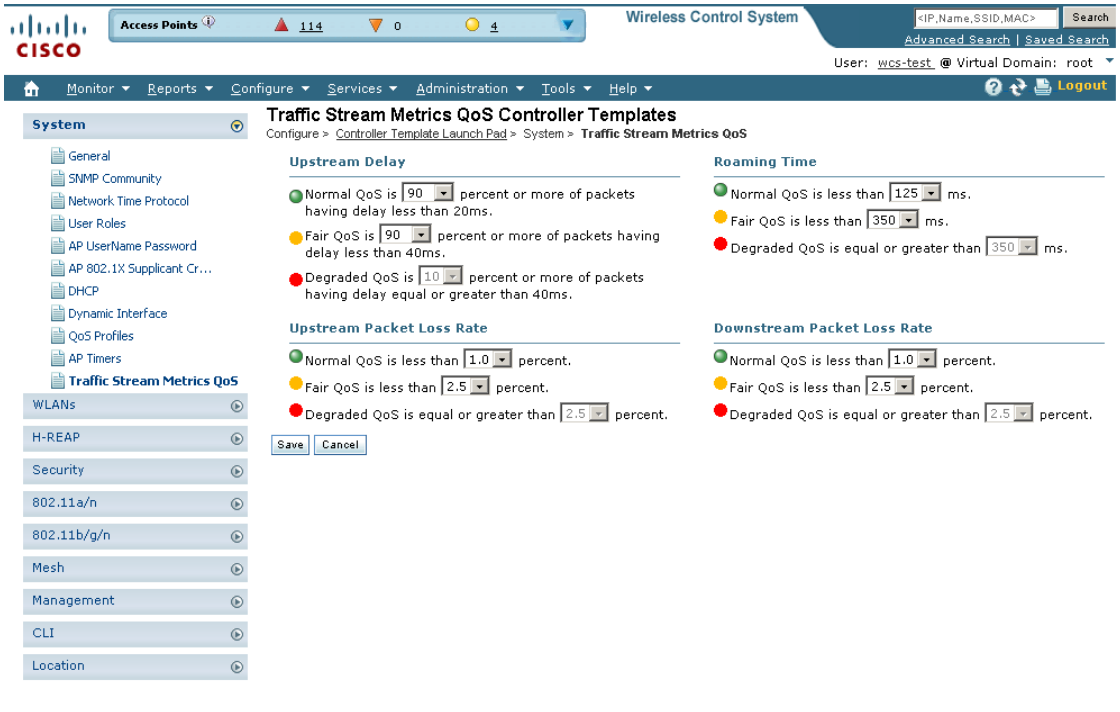
Four QoS values (packet latency, packet jitter, packet loss, and roaming time), which can affect the audio quality of voice calls, are monitored. All the wireless LAN components participate in this process. Access points and clients measure the metrics, access points collect the measurements and then 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. Cisco WCS 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.

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 System > Traffic Stream Metrics QoS Status page appears (see Figure 12-9).

Figure 12-9 Traffic Stream Metrics QoS Status Template



The Traffic Stream Metrics QoS Status 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 judgement 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 will be mobile-to-mobile; therefore, some have less stringent PLR requirements for the wireless LAN.

Configuring WLAN Templates

WLAN templates allow you to define various WLAN profiles for application to different controllers.

In WCS software release 4.0.96.0 and later releases, 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.
- Hybrid-REAP access points do not support multiple SSIDs.

Follow these steps to add a WLAN template or make modifications to an existing WLAN template.

Step 1 Choose **Configure > Controller Template Launch Pad**.

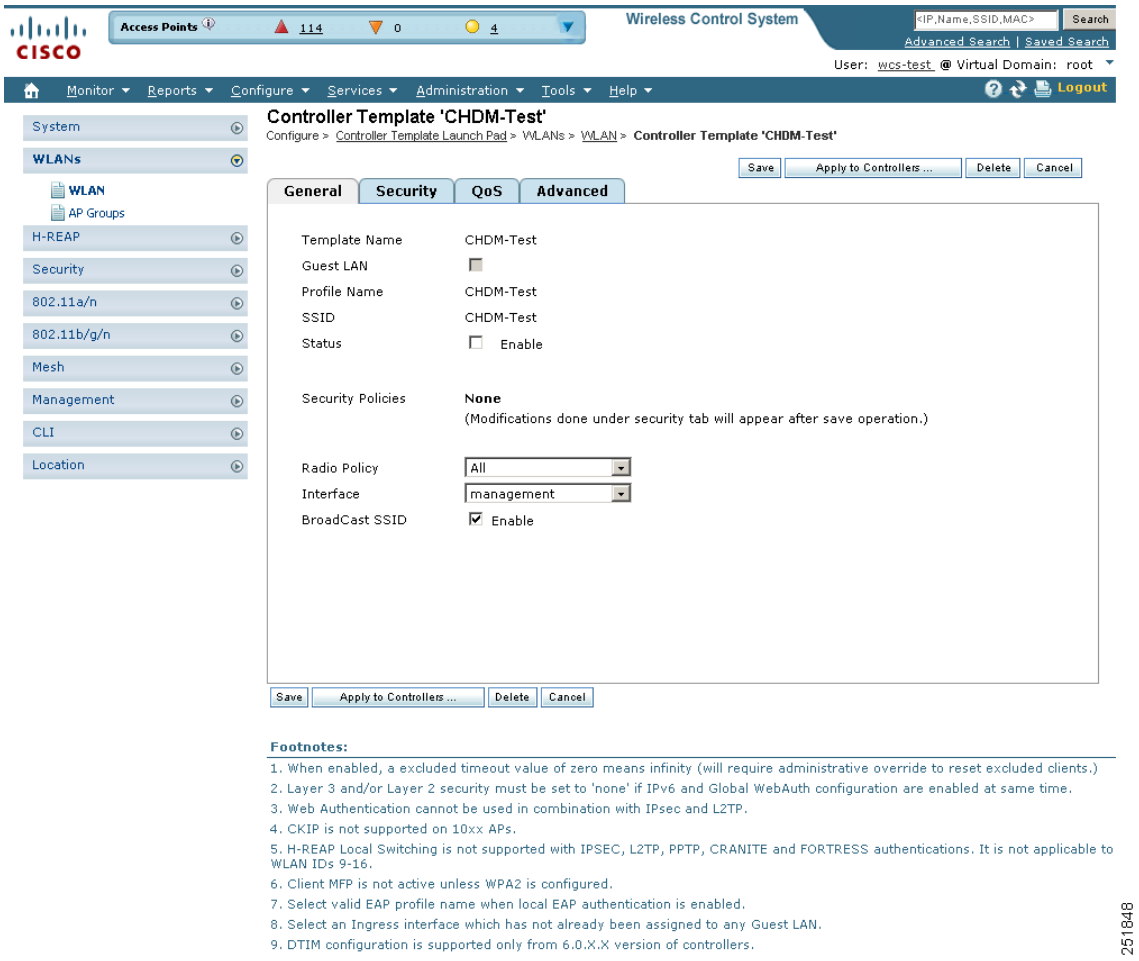
Step 2 Click **WLAN** or choose **WLANs > WLAN** from the left sidebar menu. The WLAN Template page appears with a summary of all existing defined WLANs. The following information headings are used to define the WLANs listed on the WLAN Template General page:

- Template Name—The user-defined name of the template. Clicking the name displays parameters 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, click **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 (see Figure 12-10).

Figure 12-10 WLAN Template



Step 4 Specify if you want guests 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 7-10).

Step 5 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 6 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 7 Check the **Enable** check box for the Status parameter.

Step 8 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 9 Use the Interface drop-down list to choose the available names of interfaces created by the Controller > Interfaces module.

Step 10 From the Egress Interface drop-down list, choose the Egress interface that you created in the "Creating an Egress Interface" section on page 10-53. This provides a path out of the controller for wired guest client traffic.

Step 11 From the Ingress Interface drop-down list, choose the Ingress interface that you created in the "Creating an Ingress Interface" section on page 10-52. The provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Step 12 Click **Broadcast SSID** to activate SSID broadcasts for this WLAN.

Step 13 Click **Save**.

Step 14 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" section on page 12-20.
- Click the **QoS** tab to establish which quality of service is expected for this WLAN. Continue to the "QoS" section on page 12-28.
- Click the **Advanced** tab to configure any other details about the WLAN, such as DHCP assignments and management frame protection. Continue to the "Advanced" section on page 12-29.

Security

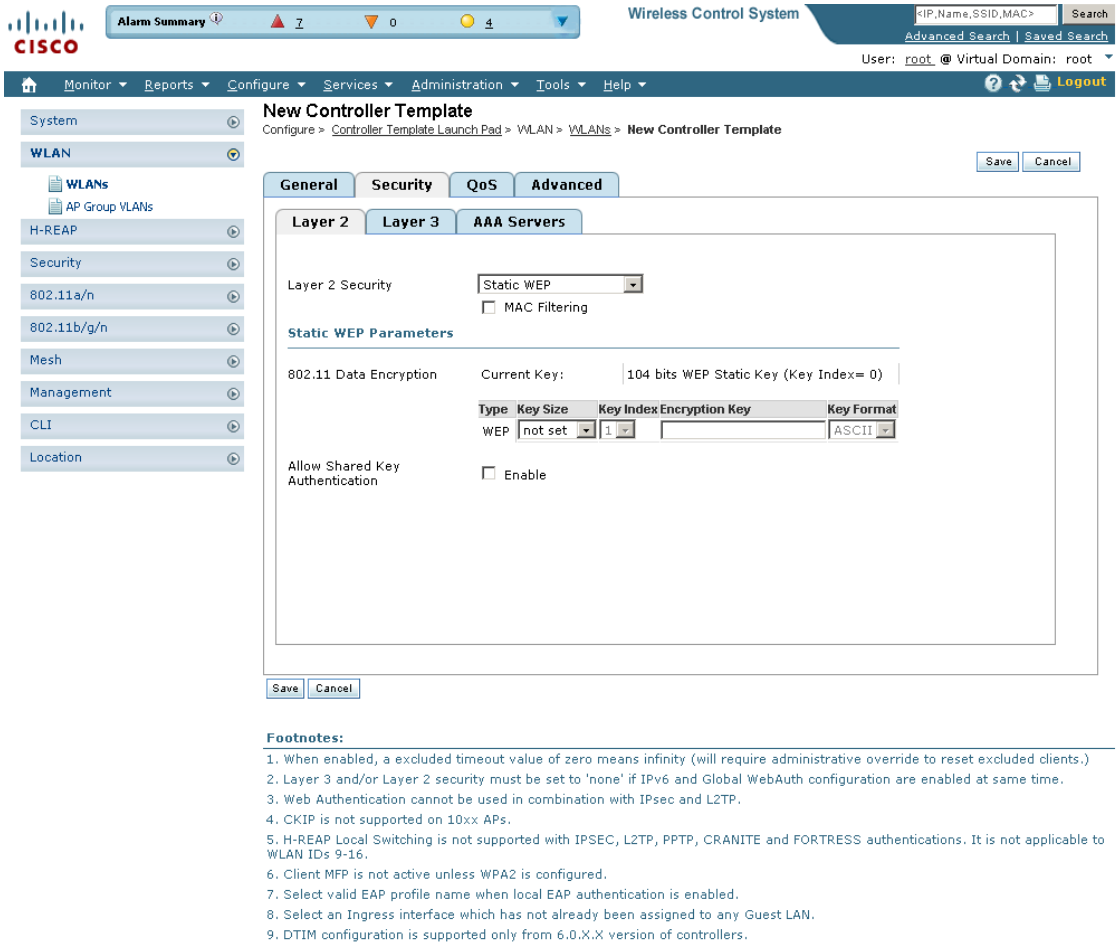
After choosing Security, you have an additional three tabs: Layer 2, Layer 3, and AAA Servers.

Layer 2

When you choose the Layer 2 tab, the page as shown in Figure 12-11 appears.

Note The screen contains different views depending on what option is chosen in the Layer 2 Security drop-down list.

Figure 12-11 Layer 2 Page



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 the table below.

Table 12-2 Layer 2 Security Options

Parameter	Description
None	No Layer 2 security selected.
802.1X	WEP 802.1X data encryption type (Note 1): 40/64 bit key. 104 bit key. 152 bit key.

Table 12-2 Layer 2 Security Options (continued)

Parameter	Description
Static WEP	Static WEP encryption parameters: 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. **Note** Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and WCS). 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 parameters are displayed at the bottom of the page. Static WEP encryption parameters: 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.

Table 12-2 Layer 2 Security Options (continued)

Parameter	Description
WPA+WPA2	Use this setting to enable WPA, WPA2, or both. See the WPA1 and WPA2 parameters displayed in the page when WPA+WPA2 is selected. 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 Pre-shared Key is enabled, then neither CCKM or 802.1X can be enabled; although, both CCKM and 802.1X can be enabled at the same time.
CKIP	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. **Note** CKIP is not supported on 10xx APs. When selected, these CKIP parameters are displayed. Key size: Not set, 40, or 104. Key Index: 1 to 4 Encryption Key: Specify encryption key. Key Format: ASCII or HEX. **Note** Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and WCS). 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. MMH Mode: Select the check box to enable. Key Permutation: Select the check box to enable.

Step 2 Check 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 may 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 WCS). 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.

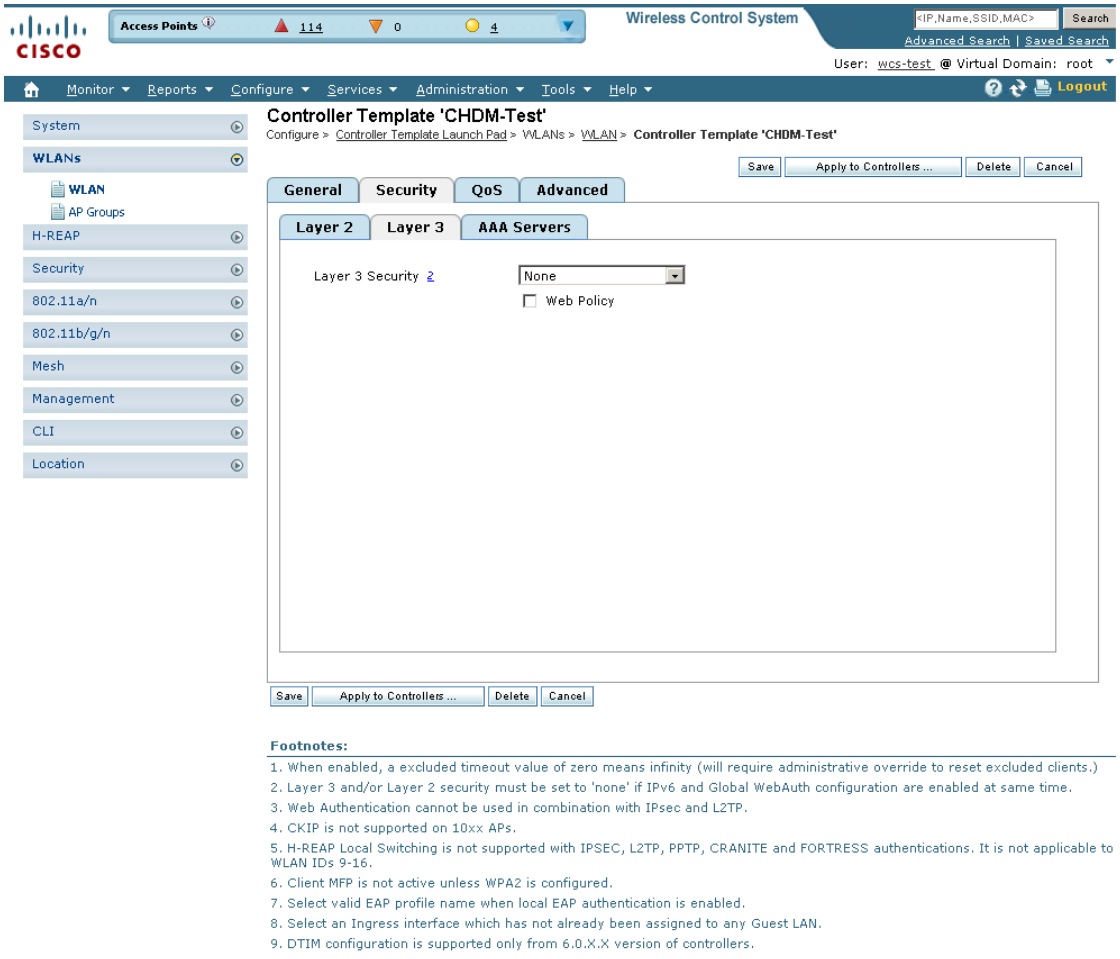
Step 4 Click **Save**.

Layer 3

When you choose the Layer 3 tab, the page shown in Figure 12-12 appears.

Note The screen contains different views depending on what option is chosen in the Layer 3 Security drop-down list.

Figure 12-12 Layer 3 Page



Follow these steps to configure the Layer 3 tab.

Step 1 Use the Layer 3 security drop-down list to choose between None and VPN Pass Through. The page parameters 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, check the **Web Policy** check box and the **Passthrough** option. This option allows users to access the network without entering a username or password.

An Email Input check box appears. Check this check box if you want users to be prompted for their email address when attempting to connect to the network.

b. 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. For specifics on downloading custom pages, refer to the "Downloading Customized Web Authentication" section on page 3-47.

   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, click **Security > AAA** and choose up to three RADIUS and LDAP servers using the drop-down lists.

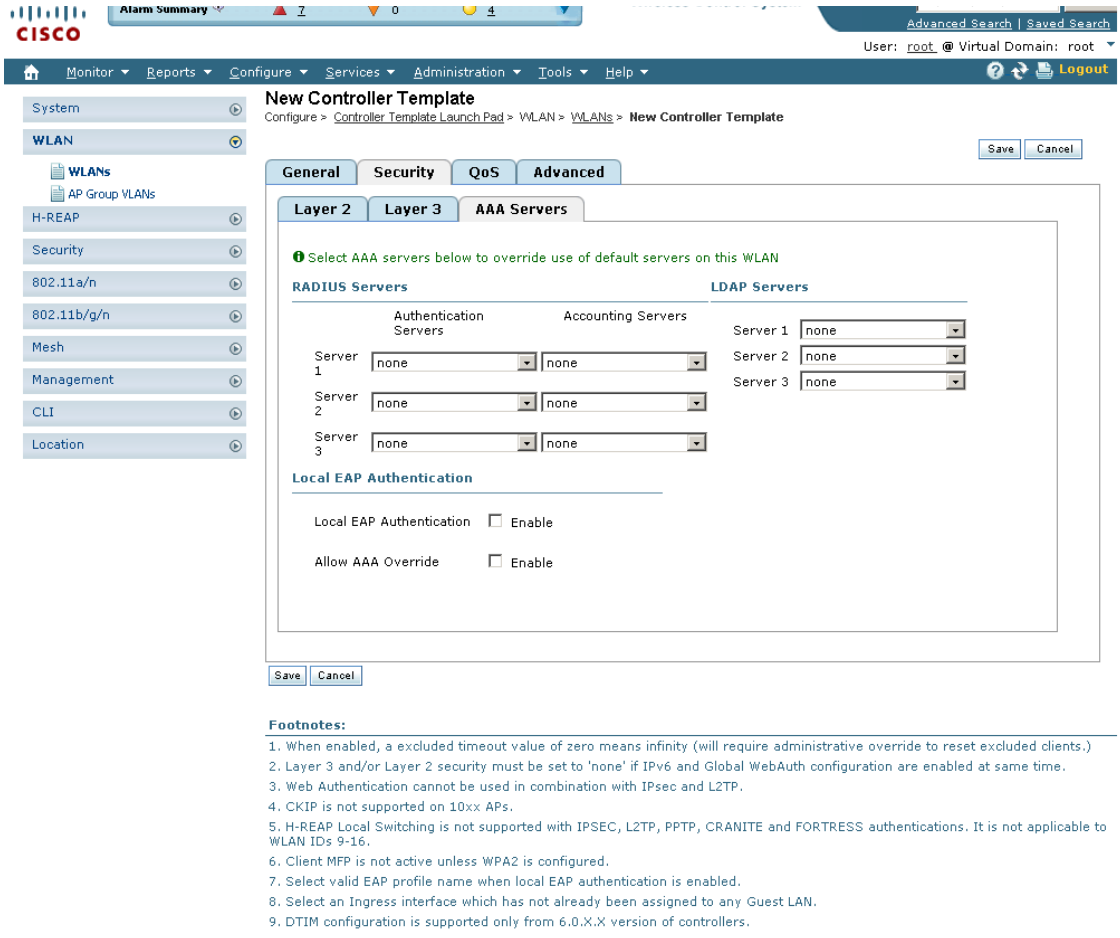
Step 4 Click **Save**.

Step 5 Repeat this process if a second (anchor) controller is being used in the network.

AAA Servers

When you choose the AAA Servers tab, the page shown in Figure 12-13 appears.

Figure 12-13 AAA Servers Page



Follow these steps to configure the AAA Servers tab.

Step 1 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, WCS uses the default LDAP server order from the database.

Step 2 Click 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 3 When AAA Override is enabled, and 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, and/or WPA operation). In all cases, the operating system also uses QoS, DSCP, 802.1p priority tag values, 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.

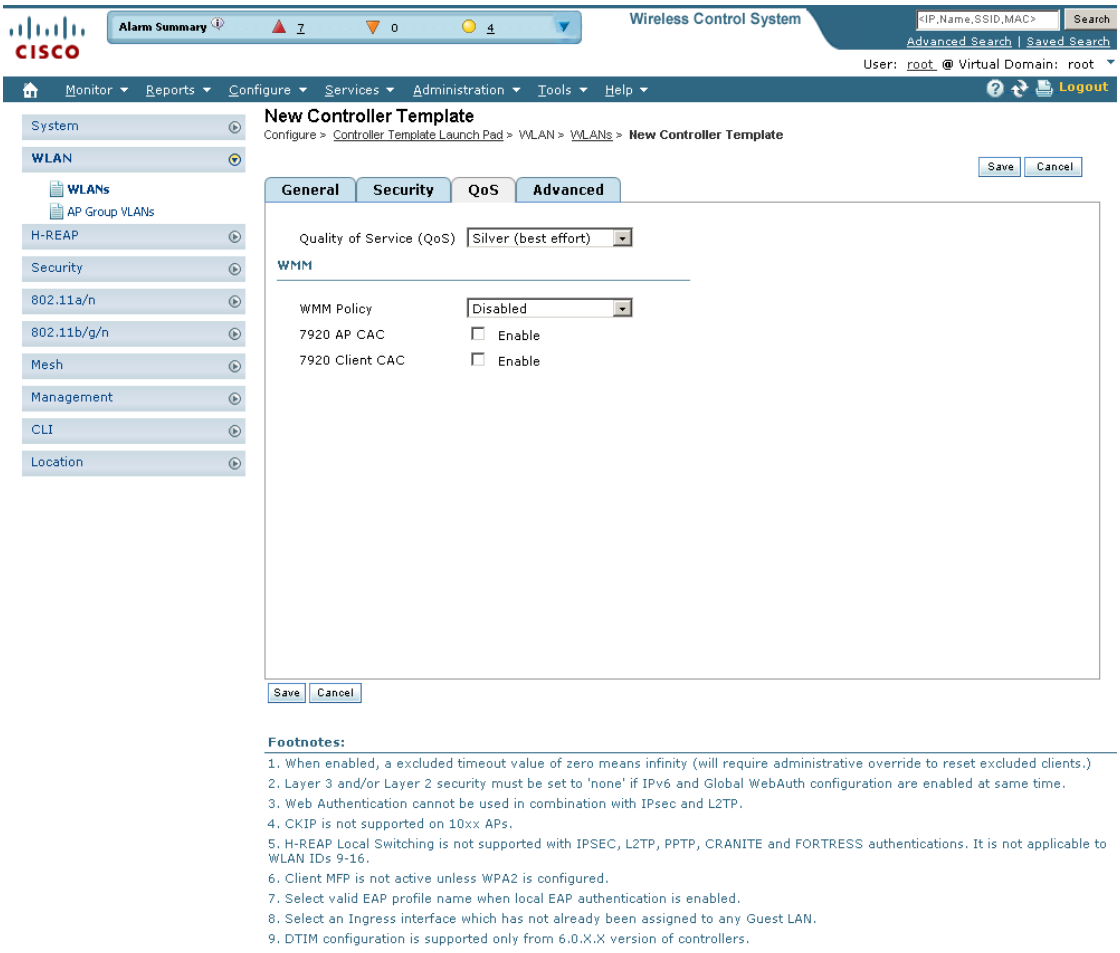
The AAA override values may come from a RADIUS server, for example.

Step 4 Click **Save**.

QoS

When you select the QoS tab from the WLAN Template page, the page as shown in Figure 12-14 appears.

Figure 12-14 QoS Page



Follow these steps to configure the QoS tab.

Step 1 Use the QoS drop-down list to 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 Use the WMM Policy drop-down list to 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 3 Click the **7920 AP CAC** check box if you want to enable support on Cisco 7920 phones.

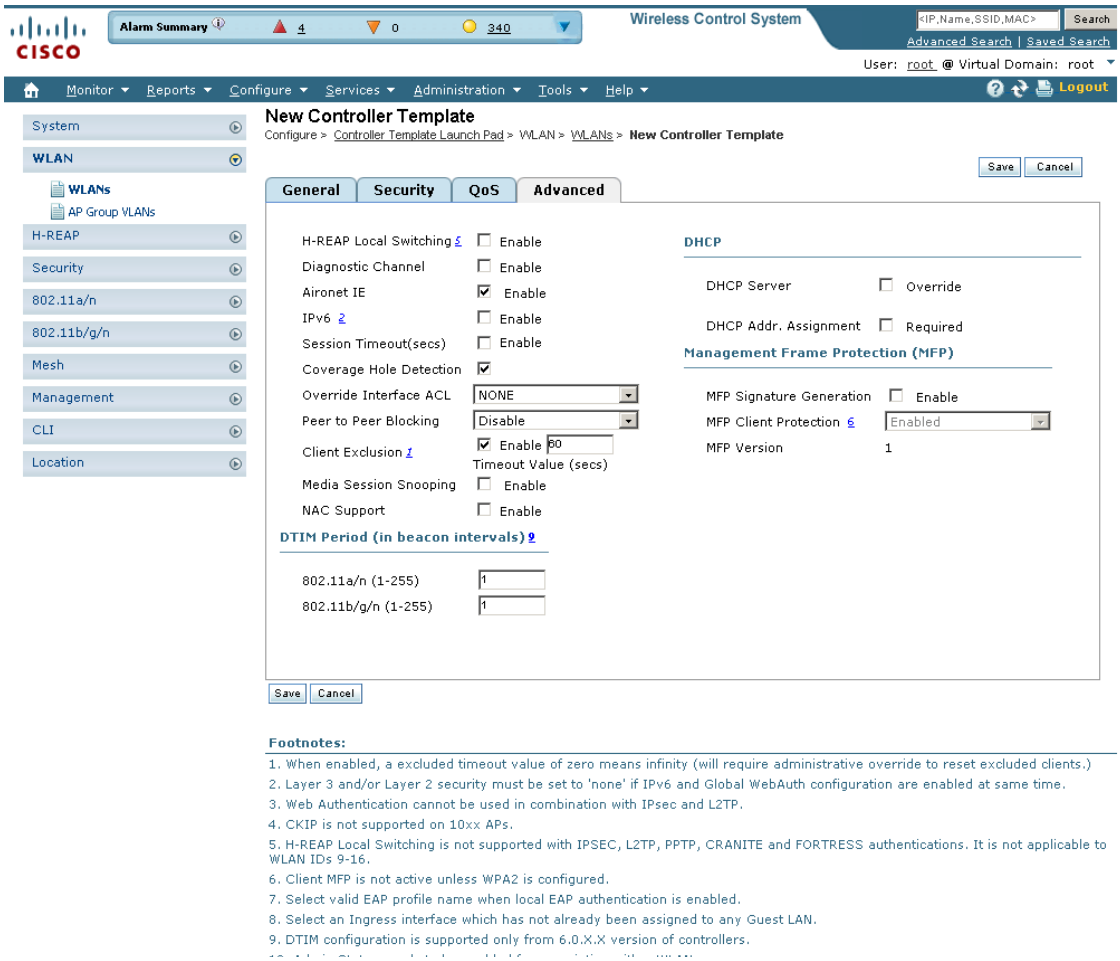
Step 4 If you want WLAN to support older versions of the software on 7920 phones, click to enable the **7920 Client CAC** check box. The CAC limit is set on the access point for newer versions of software.

Step 5 Click **Save**.

Advanced

When you click the Advanced tab in the WLAN Template page, the page shown in Figure 12-15 appears.

Figure 12-15 Advanced Page



Step 1 Click the check box if you want to enable Hybrid REAP local switching. For more information on Hybrid REAP, see the "Configuring Hybrid REAP" section on page 15-4. If you enable it, the hybrid-REAP access point handles client authentication and switches client data packets locally.

H-REAP 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 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 3 Check 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 4 Click to enable IPv6. You can configure IPv6 bridging and IPv4 web auth on the same WLAN.

Step 5 At the Session Timeout parameter, set the maximum time a client session can continue before requiring reauthorization.

Step 6 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 7 A list of defined access control lists (ACLs) is provided at the Override Interface ACL drop-down list. (See the "Configuring Access Control List Templates" section on page 12-69 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 parameter is None.

Step 8 You can configure peer-to-peer blocking per WLAN rather than applying the status to all WLANs. At 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.

If H-REAP local switching is enabled for the WLAN, which prevents traffic from passing through the controller, this drop-down list is grayed out.

Note Peer-to-peer blocking does not apply to multicast traffic.

Step 9 Click the check box if you want to enable automatic client exclusion. 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 re-enable the client.

Note When session timeout is not set, it implies that an excluded client remains and will not timeout from the excluded state. It does not imply that the exclusion feature is disabled.

Step 10 Click 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 WCS. 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 11 Check the NAC Support check box if you want to enable it. 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 "Configuring NAC Out-of-Band Integration" section on page 10-45 for more information.

Step 12 When you click the check box to override DHCP server, another parameter 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.
- 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 13 If the MFP Signature Generation check box is checked, 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 14 At the MFP Client Protection drop-down list, choose Optional, Disabled, or Required for configuration of individual WLANs of a controller. If infrastructure MFP is not enabled, this drop-down list is unavailable.

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 15 Enter a value between 1 and 255 beacon intervals in the 802.11a/n DTIM Period portion 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 16 Enter a value between 1 and 255 beacon intervals in the 802.11b/g/n DTIM Period portion 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 DTIM configuration is not appropriate for guest LANs.

Step 17 Click **Save**.

Configuring WLAN AP Groups

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.

Follow these steps to configure WLAN AP Groups.

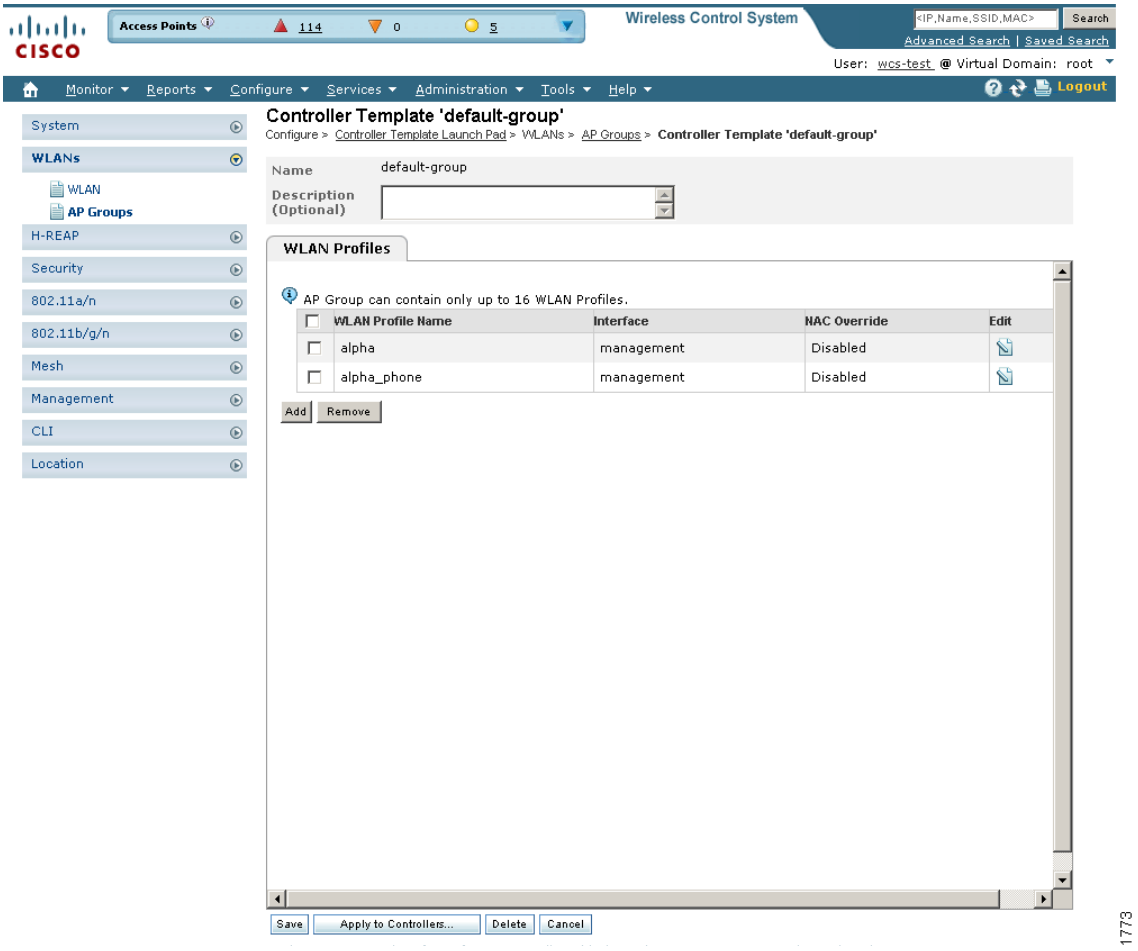
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-16).

Figure 12-16 WLAN AP Groups



This page displays a summary of the AP groups configured on your network. From here you can add, remove, edit, or view details of an AP group. Click in the Edit column to edit its access point(s). Click the check box in the WLAN Profile Name column and click Remove to delete WLAN profiles.

Adding Access Point Groups

Follow these steps to add a new access point group.

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 5.2 and above controllers) 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 Click the **WLAN Profile** check box.

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 display in the drop-down list.

Note Each access point is limited to sixteen 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).

Step 6 Type a WLAN profile name or select one from the WLAN Profile Name drop-down list.

Step 7 Enter an interface or select one from the Interface 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 display in the drop-down list.

Step 8 Click the **NAC Override** check box, if applicable. NAC override is disabled by default.

Step 9 When access points and WLAN profiles are added, click **Add**.

Note After saving, click the edit icon on the WLAN Profiles tab to edit the WLAN profile information.

Deleting Access Point Groups

Follow these steps to delete an access point group.

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 H-REAP AP Groups

Hybrid REAP 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 hybrid-REAP access points per location, but you can organize and group the access points per floor and limit them to 25 or so per building, since it is likely the branch offices share the same configuration.

Follow these steps to set up an H-REAP AP group.

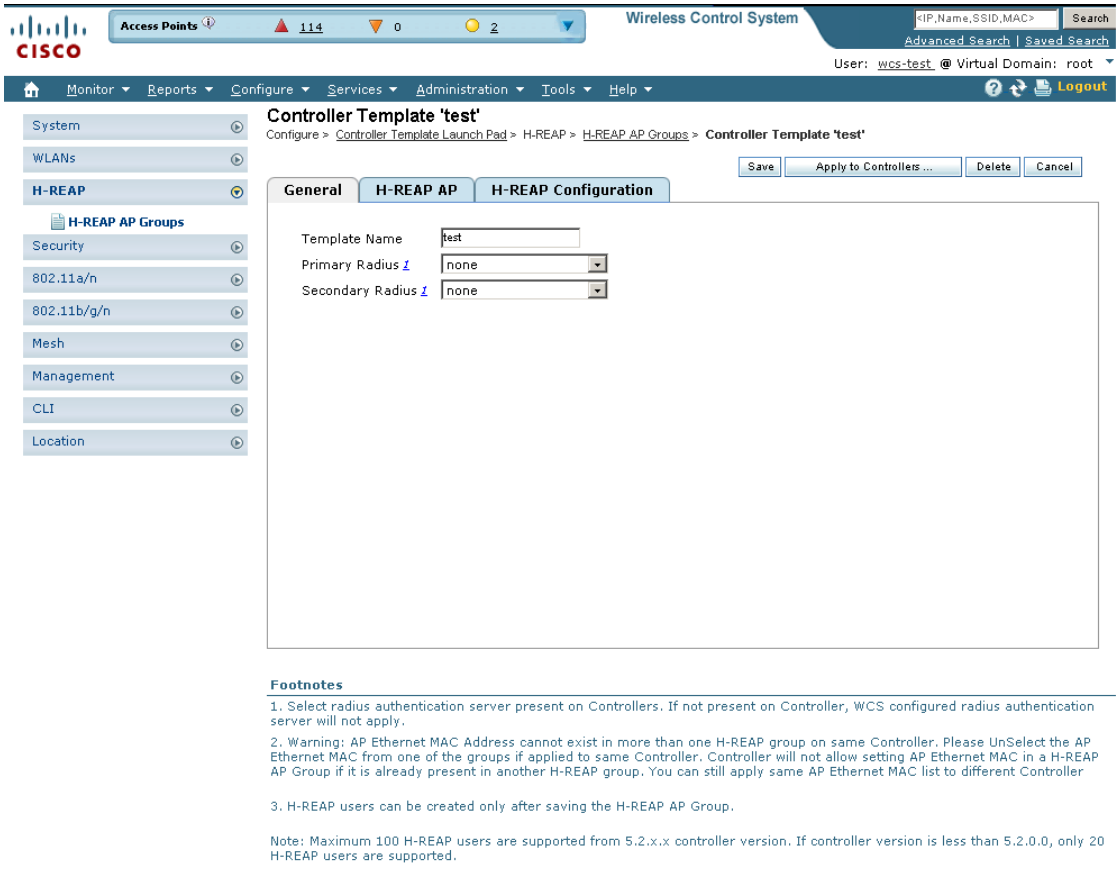
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **H-REAP AP Groups** or choose **H-REAP > H-REAP AP Groups** from the left sidebar menu. The H-REAP > H-REAP 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, click **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 H-REAP AP Groups page appears (see Figure 12-17).

Figure 12-17 AP Groups H-REAP Template



Step 4 The Template Name parameter shows the group name assigned to the HREAP 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, the WCS configured RADIUS server does not apply. A value of 10 indicates that the primary RADIUS server is not configured for this group.

Step 6 Choose the secondary RADIUS authentication servers for each group. If a RADIUS authentication server is not present on the controller, the WCS configured RADIUS server does not apply. A value of 0 indicates that the primary RADIUS server is not configured for this group.

Step 7 If you want to add an access point to the group, click the **H-REAP AP** tab.

Step 8 An access point Ethernet MAC address cannot exist in more than one H-REAP group on the same controller. If more than one group is applied to the same controller, click 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 H-REAP AP Group page appears.

Step 10 Click the **H-REAP Configuration** tab to enable local authentication for a hybrid REAP group.

Note Make sure that the Primary RADIUS Server and Secondary RADIUS Server parameters are set to **None** on the General tab.

Step 11 Select the **H-REAP Local Authentication** check box to enable local authentication for this hybrid-REAP 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 12 To allow a hybrid-REAP access point to authenticate clients using LEAP, check the **LEAP** check box. Otherwise, to allow a hybrid-REAP access point to authenticate clients using EAP-FAST, check 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 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, check 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 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.

Step 17 Click **Submit**.

Configuring a File Encryption Template

This page enables you to add a file encryption template or make modifications to an existing file encryption template.

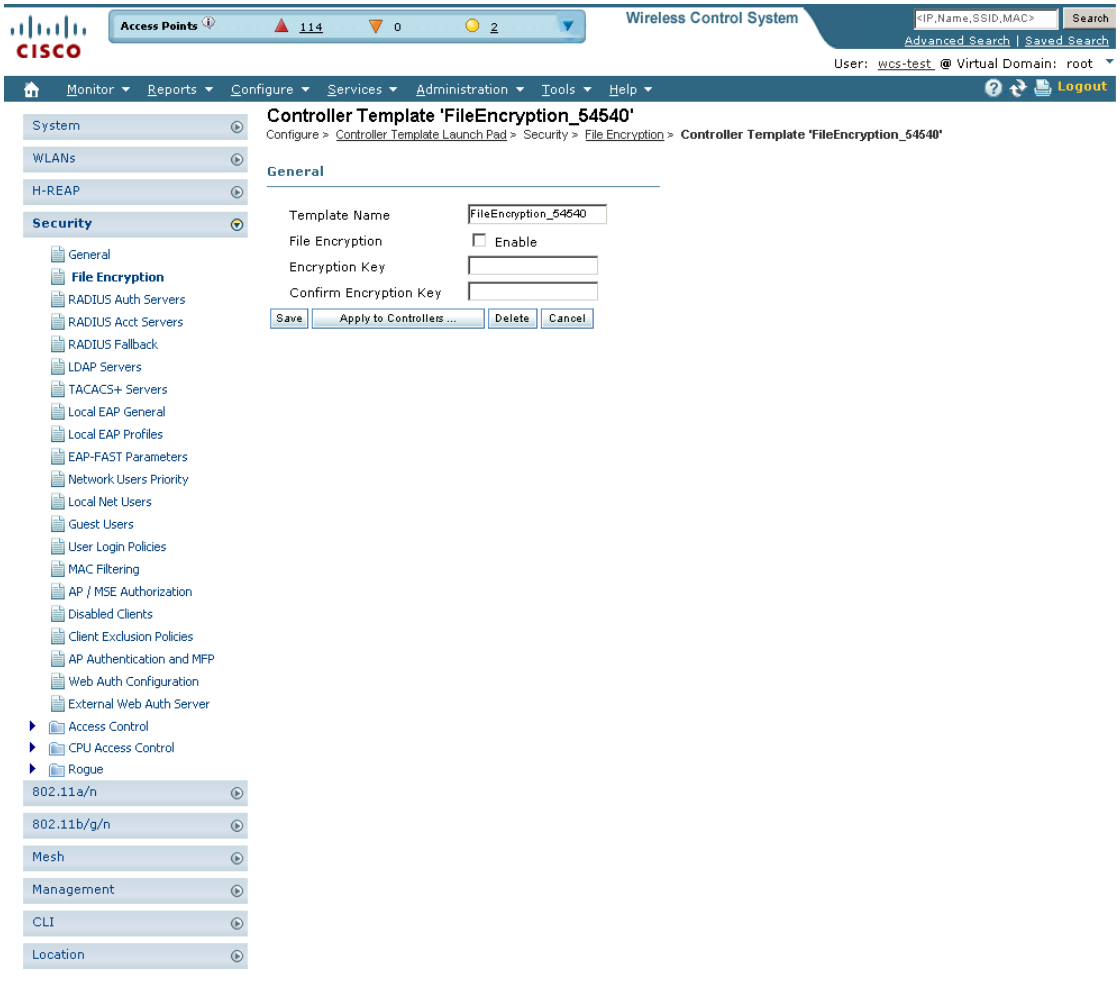
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-18).

Figure 12-18 File Encryption Template



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.

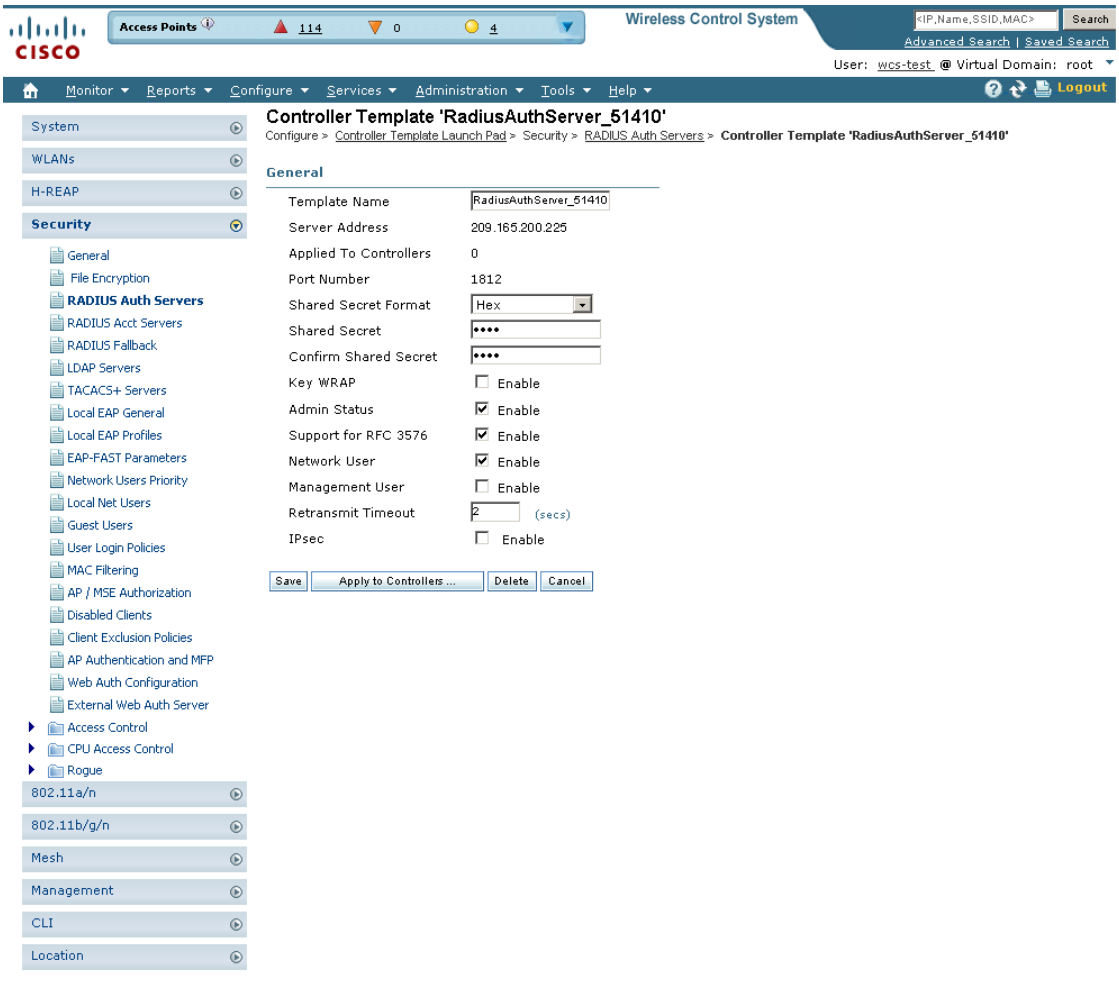
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-19).

Figure 12-19 RADIUS Authentication Server Template



Step 4 Use the Shared Secret Format drop-down list to choose either ASCII or hex shared secret format.

Note Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and WCS). 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 Click if you want to enable key wrap. If this option is enabled, the authentication request is sent to RADIUS servers that have key encryption key (KEK) and message authenticator code keys (MACK) configured. Also, when enabled, the parameters below appear:

- Shared Secret Format: Determine whether ASCII or hexadecimal.

  Note Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and WCS). 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 KEK shared secret.
- MACK Shared Secret: Enter 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 parameters 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. 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 parameter, 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.

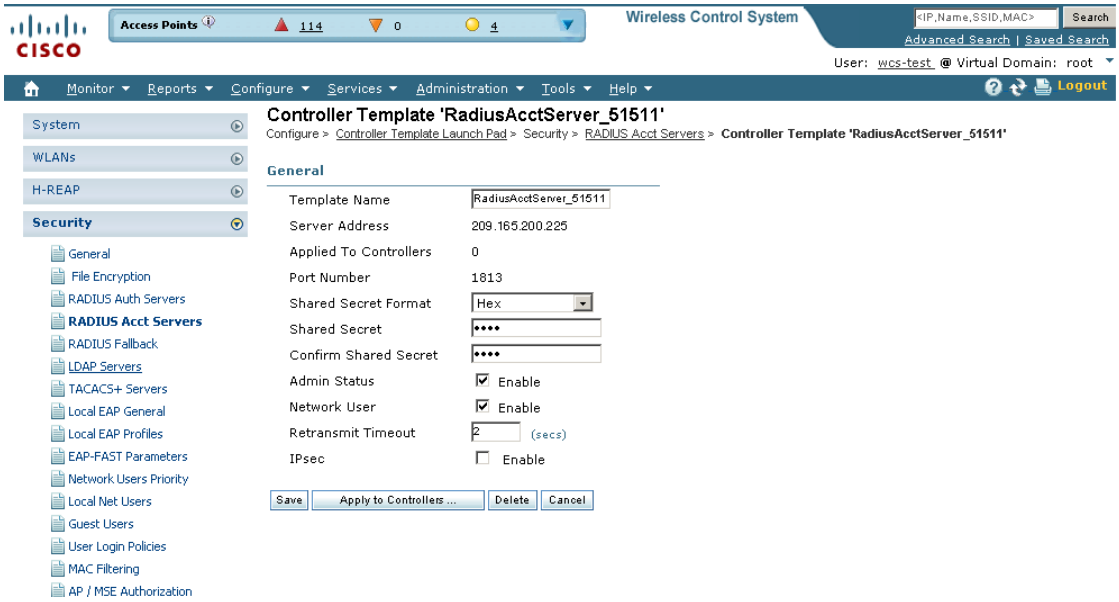
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-20).

Figure 12-20 RADIUS Accounting Server Templates



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 WCS). 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 will timeout and a retransmission by the controller will occur. 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.

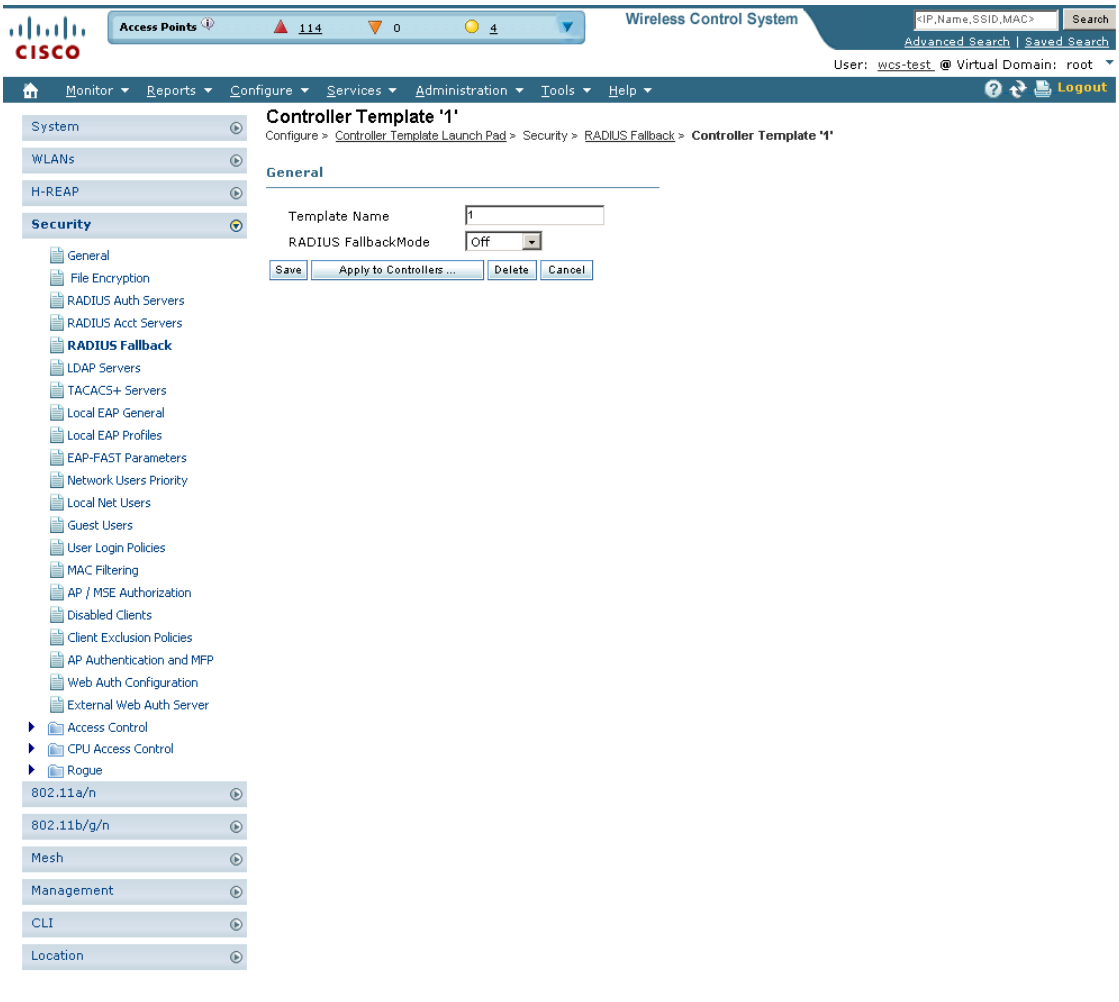
Step 1 Choose **Configure > Controller Template Launch Pad**.

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.

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, click **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 (see Figure 12-21).

Figure 12-21 RADIUS Fallback Page



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 a 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 may use an LDAP server as its backend database to retrieve user credentials. Follow these steps to add an LDAP server template or make modifications to an existing LDAP server template.

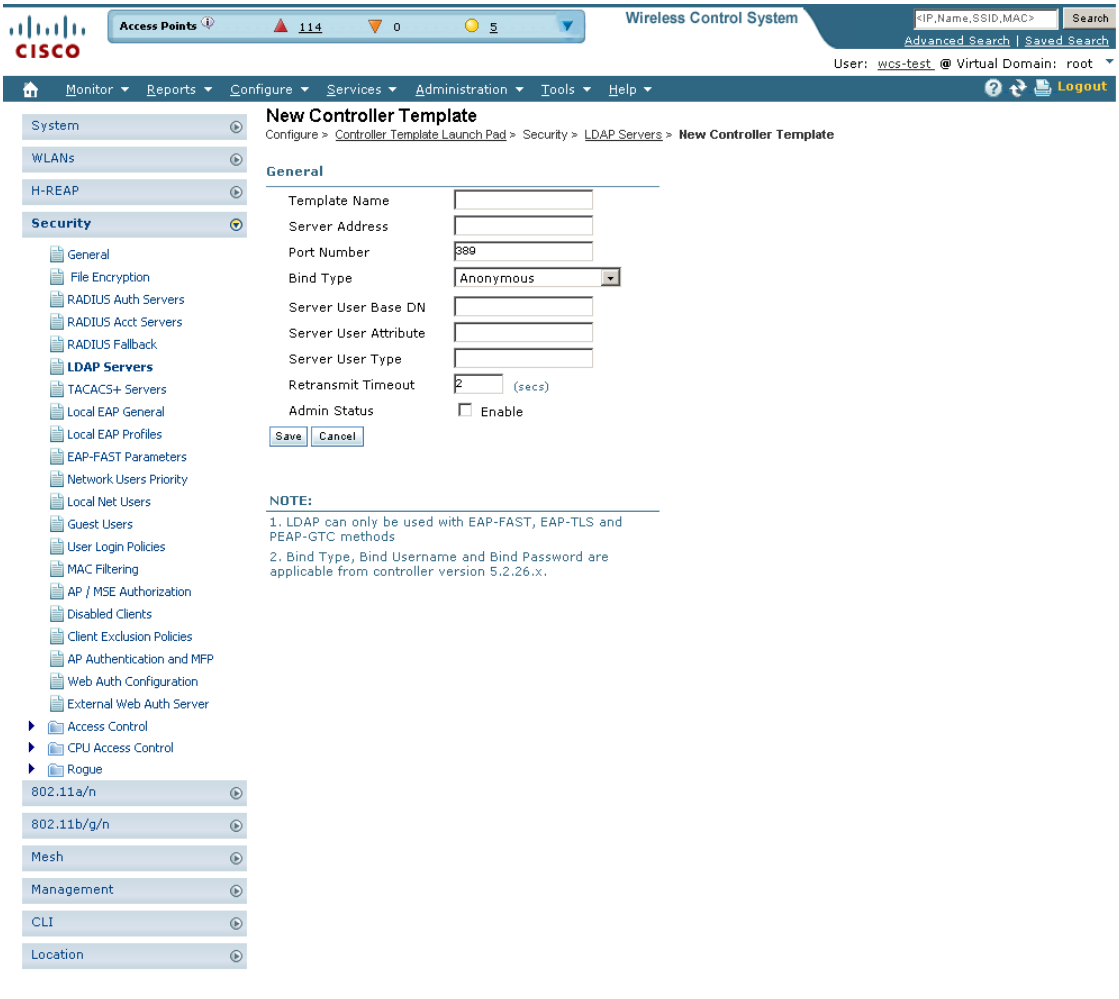
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **LDAP Servers** or choose **Security > LDAP Servers** from the left sidebar menu. The Security > LDAP Servers page appear. 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, click **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 (see Figure 12-22).

Figure 12-22 LDAP Server Template



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.

Step 9 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 10 Select the **Admin Status** check box if you want the LDAP server to have administrative privileges.

Step 11 Click **Save**.

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.

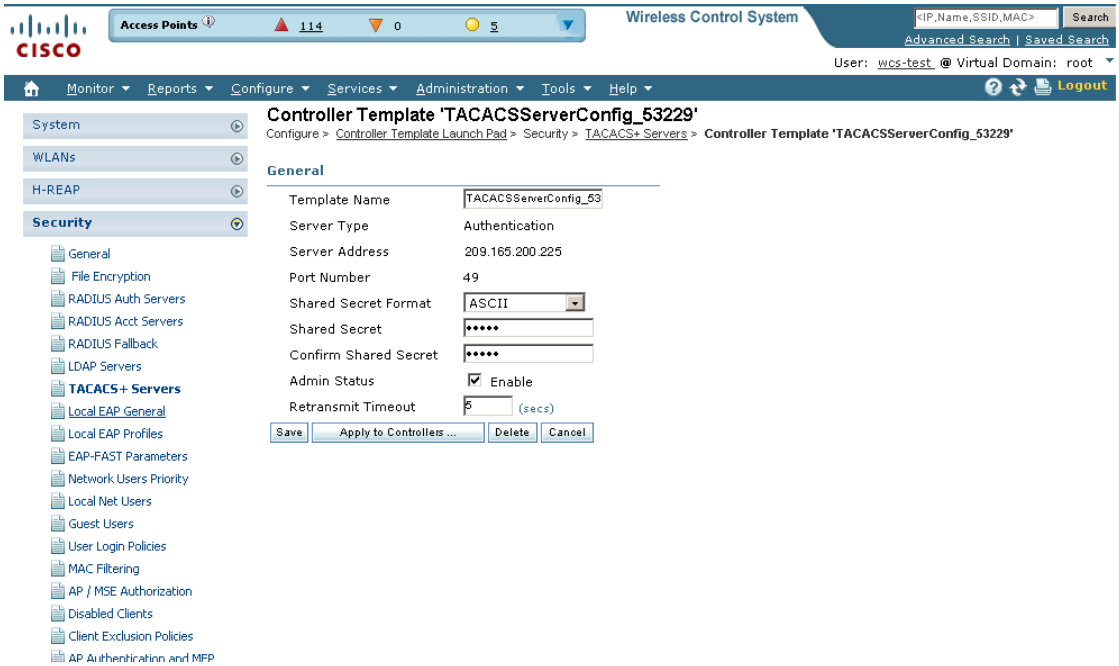
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-23).

Figure 12-23 TACACS+ Server Template



Step 4 Select the server type. The choices are authentication, authorization, or accounting.

Step 5 Use the drop-down list to choose either ASCII or hex shared secret format.

Note Regardless of which format you choose, for security reasons, only ASCII is visible on the WLC (and WCS). 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 6 Enter the TACACS+ shared secret used by your specified server.

Step 7 Re-enter the shared secret in the Confirm Shared Secret text box.

Step 8 Check the Admin Status check box if you want the TACACS+ server to have administrative privileges.

Step 9 Specify the time in seconds after which the TACACS+ authentication request times out and a retransmission is attempted by the controller.

Step 10 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.

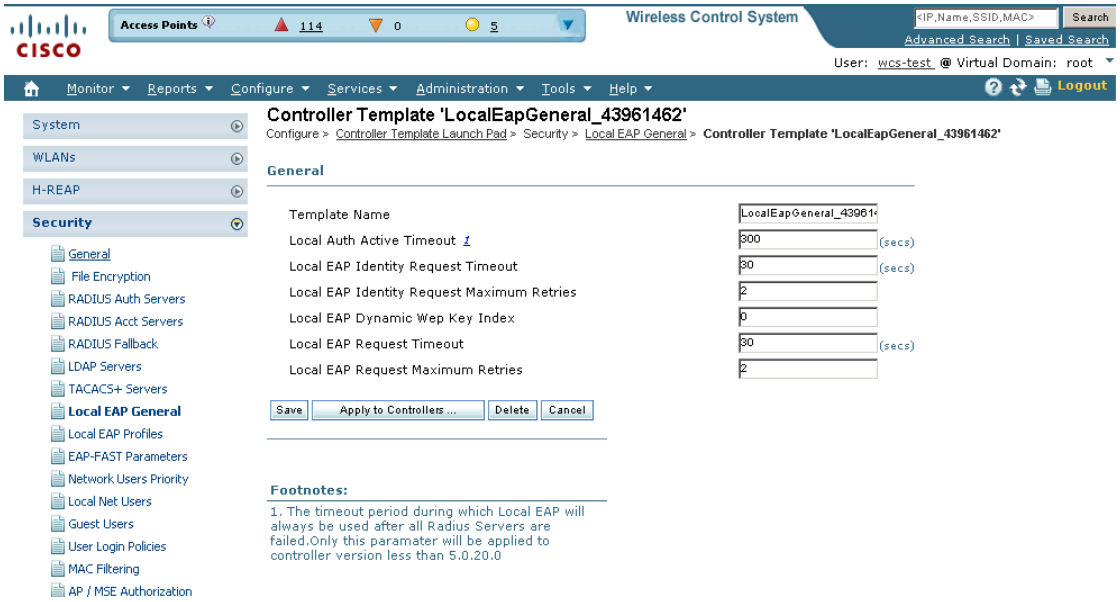
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-24).

Figure 12-24 Local EAP General Template



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.

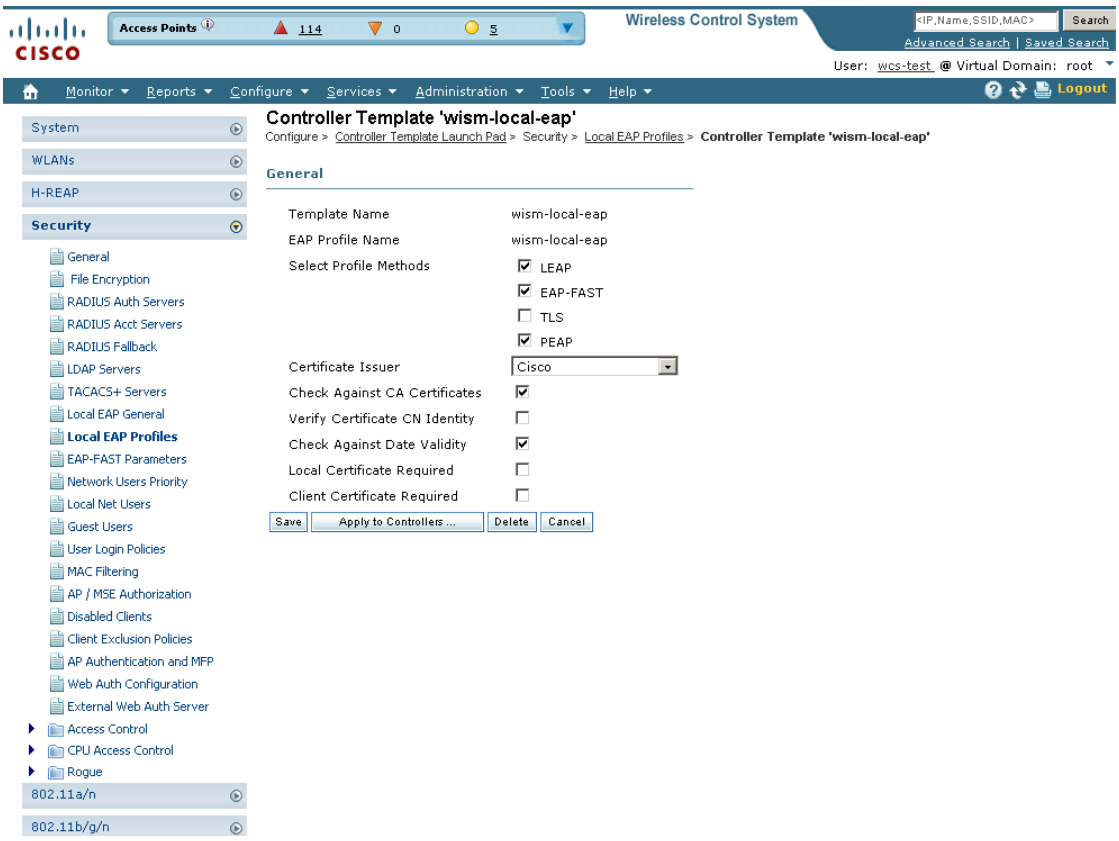
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-25).

Figure 12-25 Local EAP Profiles Template



Step 4 Each EAP profile must be associated with an authentication type(s). Choose the desired authentication type from the choices below:

- 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, check the **Check Against CA Certificates** check box.

Step 7 If you want the common name (CN) in the incoming certificate to be validated against the CA certificates' CN on the controller, check 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, check the **Check Against Date Validity** check box.

Step 9 If a local certificate is required, click the check box.

Step 10 If a client certificate is required, click the check box.

Step 11 Click **Save**.

Step 12 Follow these steps to enable local EAP:

a. Choose **WLAN > WLAN Configuration** from the left sidebar menu.

b. Click the profile name of the desired WLAN.

c. Click the **Security > AAA Servers** tab to access the AAA Servers page.

d. Check 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.

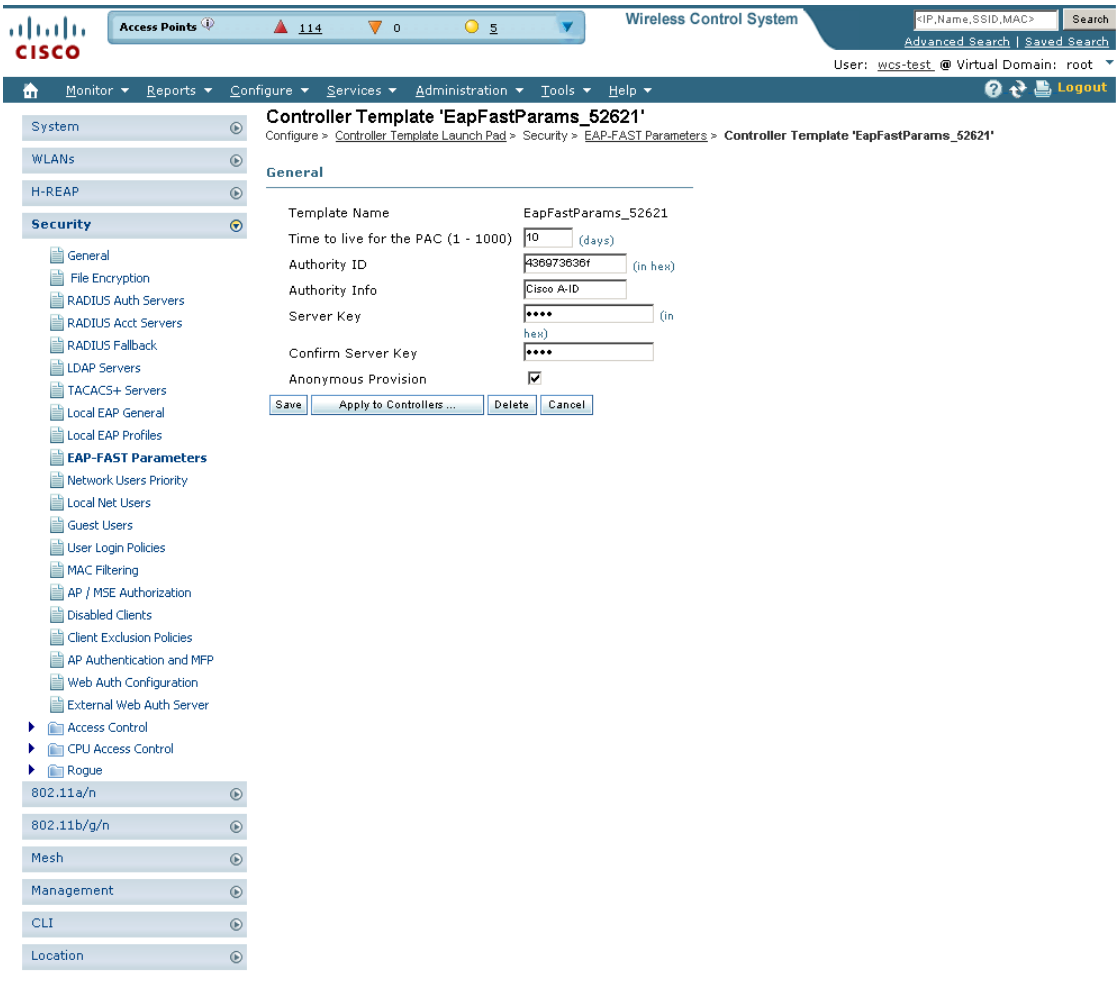
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-26).

Figure 12-26 EAP-FAST Parameters Template



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 ID text box, enter the ID for the authority identifier of the local EAP-FAST server.

Step 7 In the Authority Info text box, enter the authority identifier of the local EAP-FAST server in text format.

Step 8 In the Server Key and Confirm Server Key fields, enter the key (in hexadecimal characters) used to encrypt and decrypt PACs.

Step 9 If you want to enable anonymous provisioning, check 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 10 Click **Save**.

Configuring Network User Credential Retrieval Priority Templates

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.

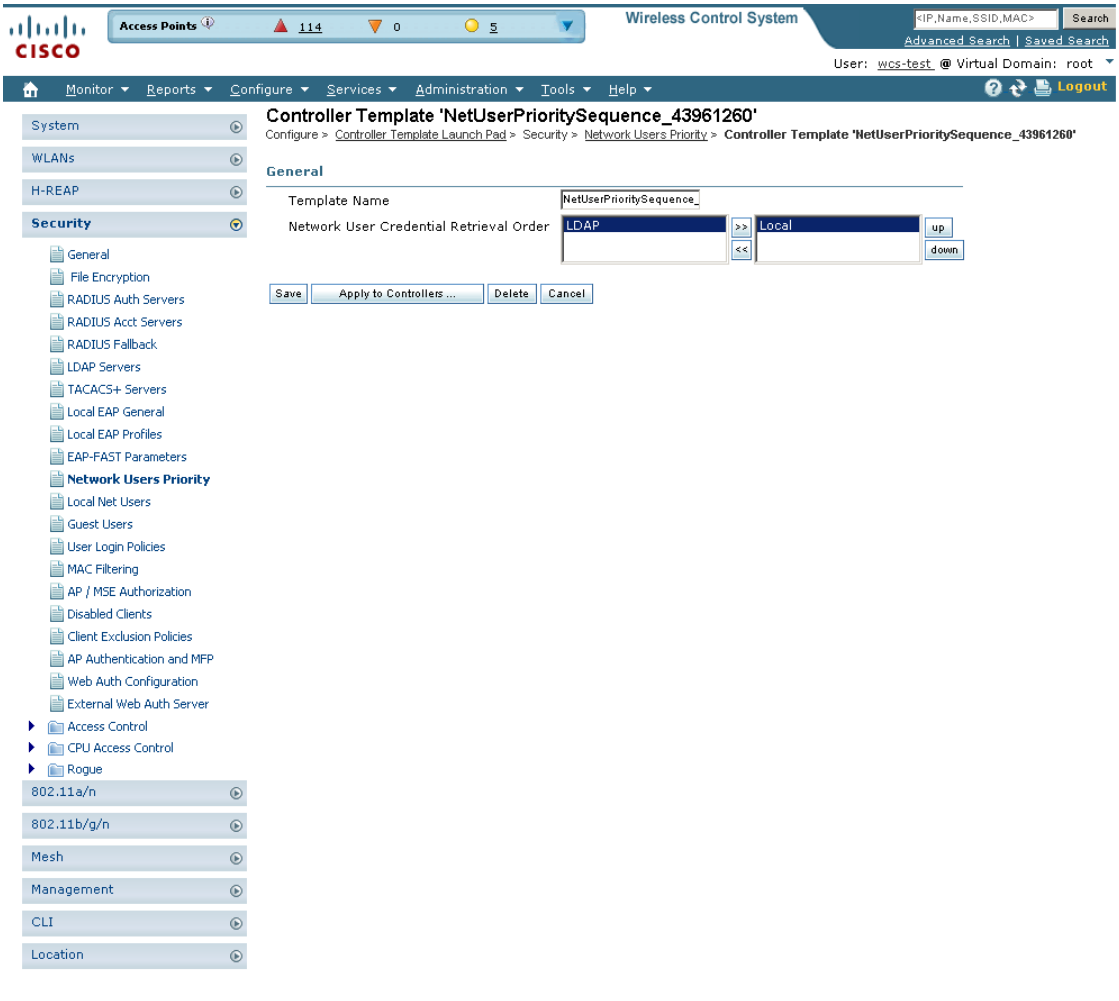
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-27).

Figure 12-27 Network User Credential Retrieval Priority Order Template



Step 4 Use the left and right pointing arrows to include or disclude 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 may 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.

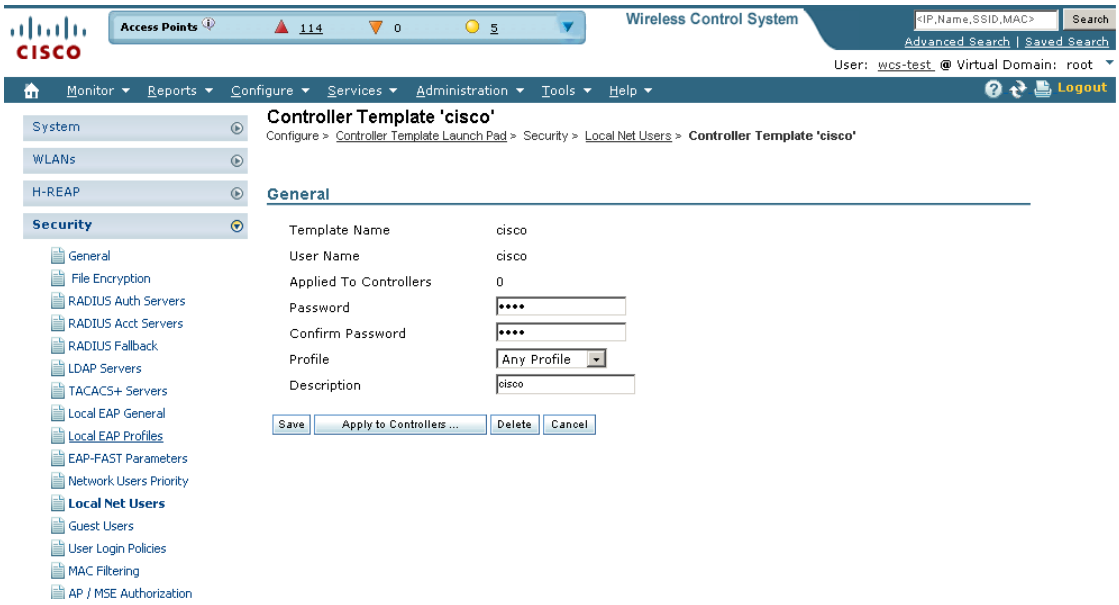
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-28).

Figure 12-28 Local Net Users Template



Step 4 If you keep Import from File enabled, you need to enter a file path or click the Browse button 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 the Cisco WCS. The header can either be blank or filled. The Cisco WCS 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 Step11.

Step 10 If you want to override the existing template parameter, click to enable this parameter.

Step 11 Click **Save**.

Configuring Guest User Templates

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 7-10 for further information on guest access.

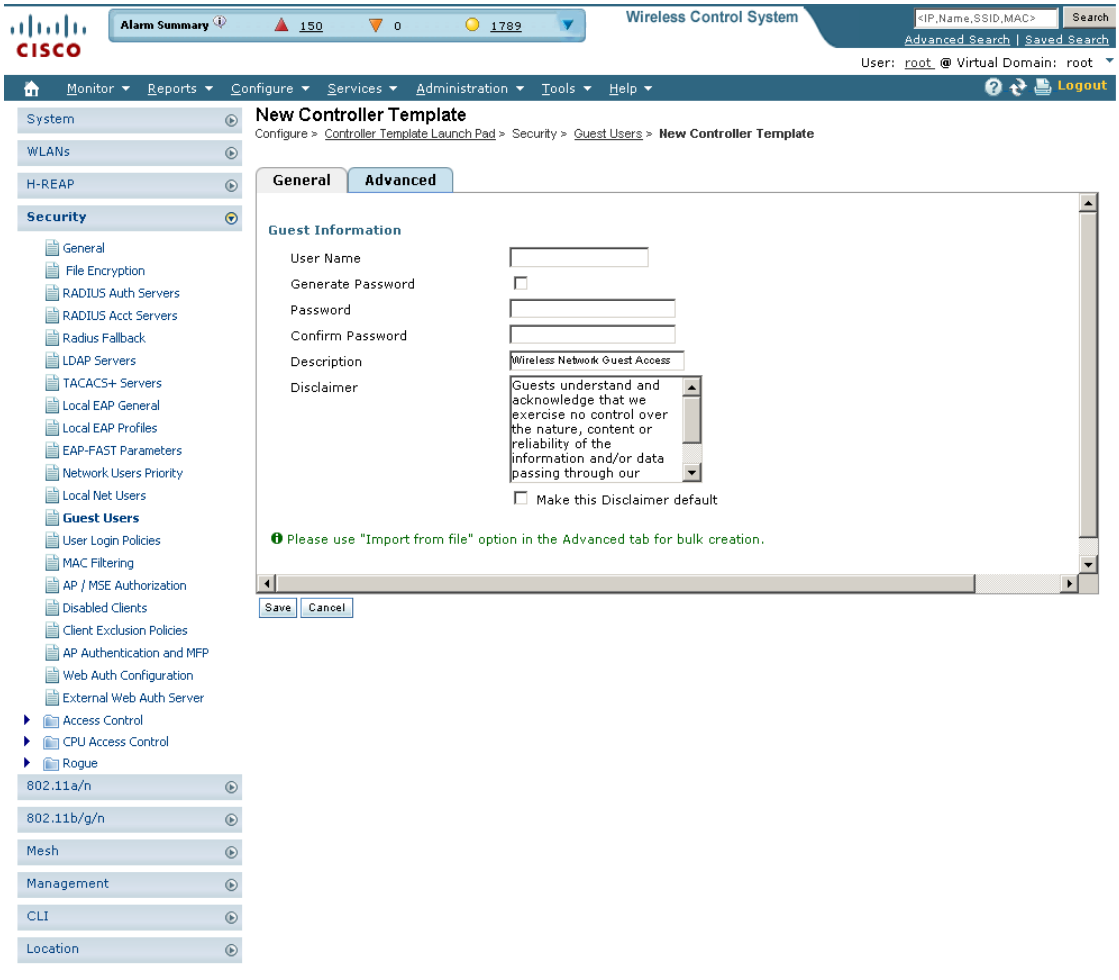
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, WCS 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, click **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 (see Figure 12-29).

Figure 12-29 Guest User Template



Step 4 Enter a guest name. Maximum size is 24 characters.

Step 5 Enter a password for this username.

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 guests' access (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 will be 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 (Optionally) Modify the default guest user description on the General tab if necessary.

Step 12 (Optionally) Modify the Disclaimer text on the General tab, if necessary. If you want the supplied text to be the default, click 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.

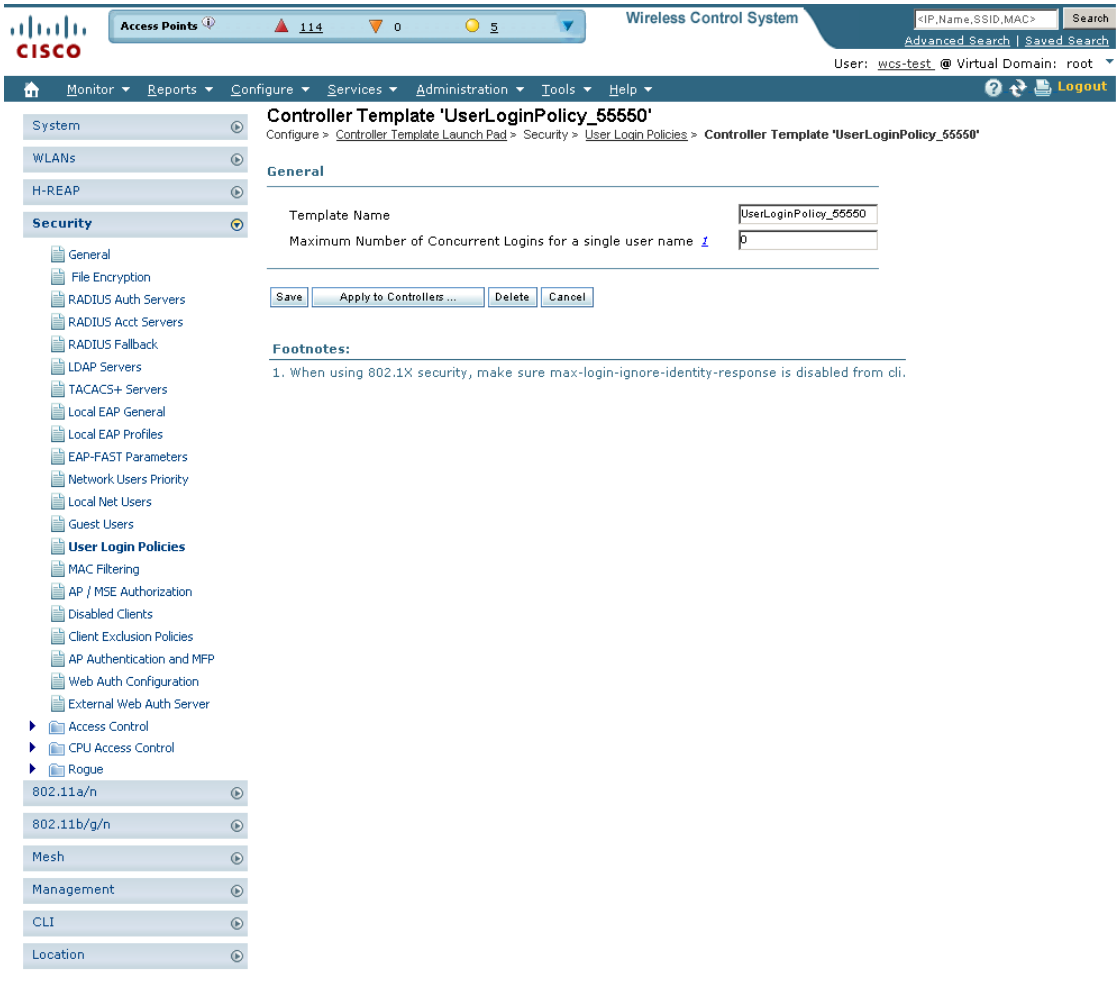
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-30).

Figure 12-30 User Login Policies Template



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

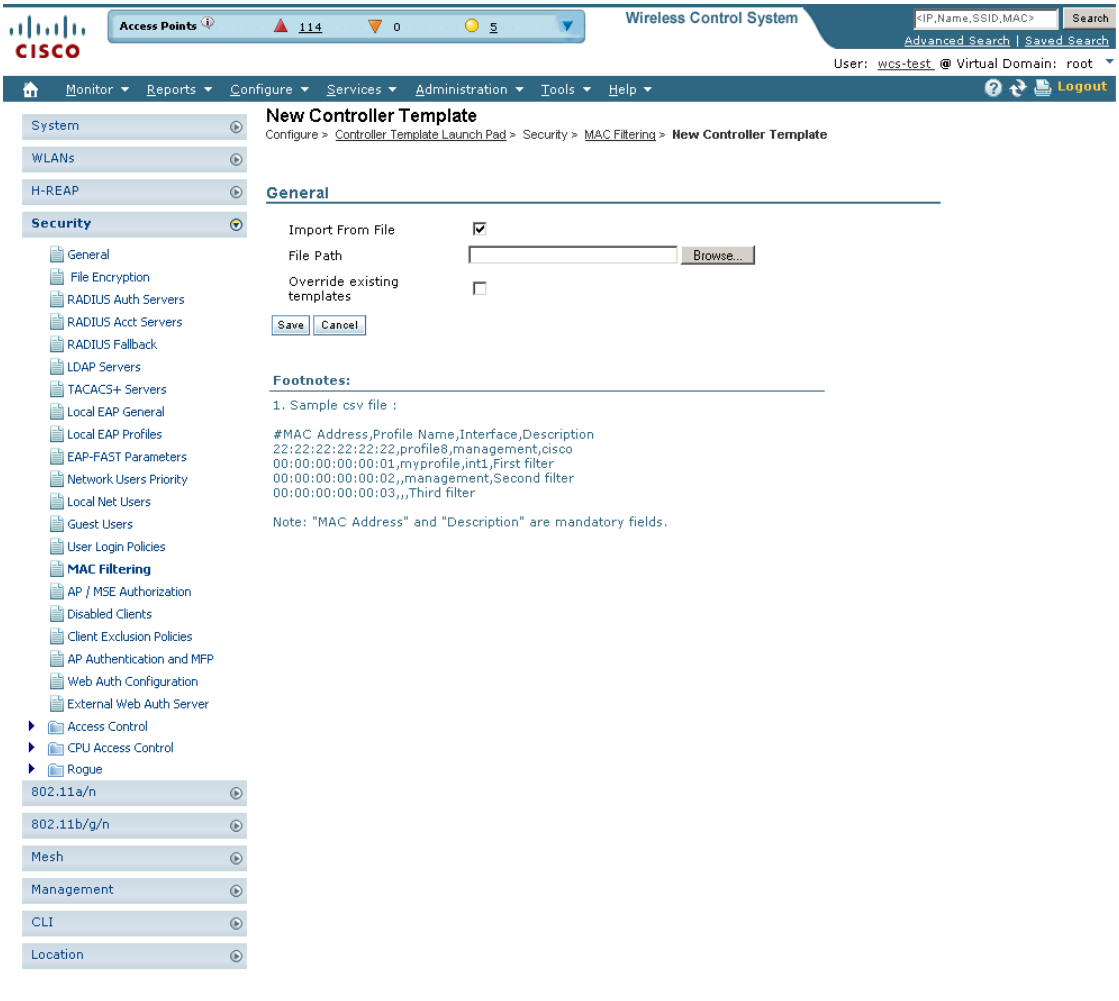
This page allows you to add a MAC filter template or make modifications to an existing MAC filter template.

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, click **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 (see Figure 12-31).

Figure 12-31 MAC Filter Templates



Step 4 If you keep Import From File enabled, you need to enter a file path or click the Browse button 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 disable Import from File, 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 parameter, click to enable this parameter.

Step 9 Click **Save**.

Configuring an Access Point or MSE Authorization

Follow these steps to add an MSE authorization or make changes to an existing access point or MSE authorization template. 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 Location Appliance Configuration Guide* for further information.

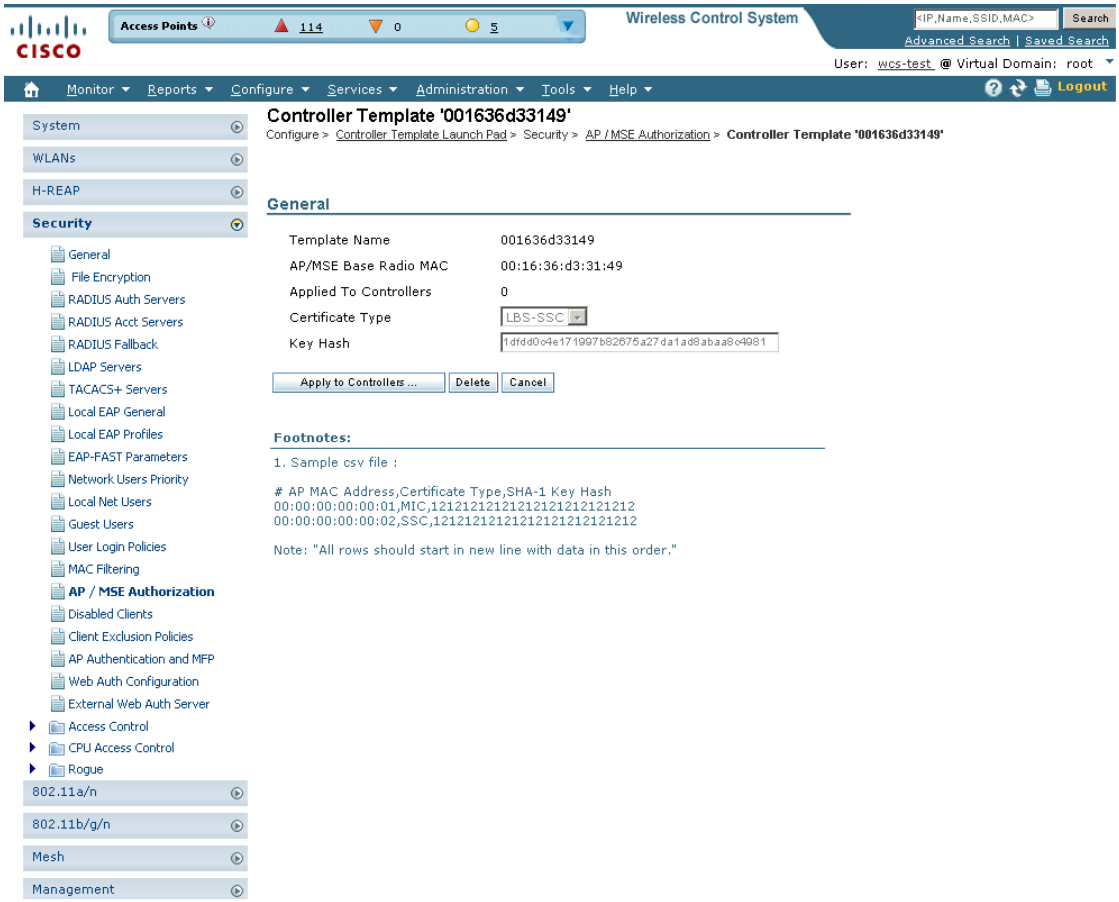
Step 1 Choose **Configure > Controller Template Launch Pad.**

Step 2 Click **AP/MSE Authorization** or choose **Security > AP/MSE Authorization** from the left sidebar menu. The Security > AP/LBS Authorization Template 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, click **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 (see Figure 12-32).

Figure 12-32 AP/MSE Authorization Templates



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 file path from where you want to import the file.

Step 6 Click **Save**.

Configuring a Manually Disabled Client Template

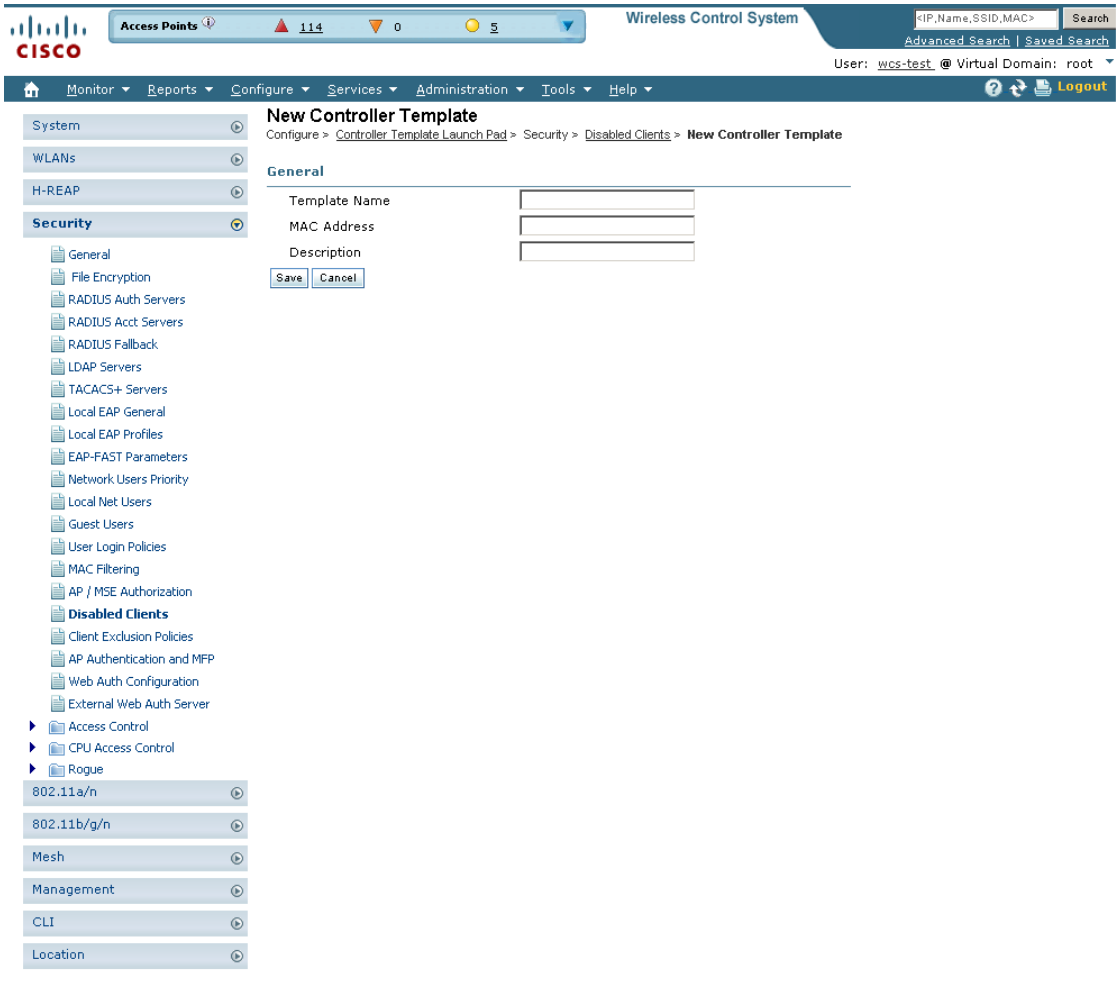
This page allows you to add a manually disable client template or make modifications to an existing disabled client template.

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, click **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 (see Figure 12-33).

Figure 12-33 Manually Disabled Clients Template



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**.

Configuring a Client Exclusion Policies Template

Follow these steps to add a client exclusion policies template or modify an existing client exclusion policies template.

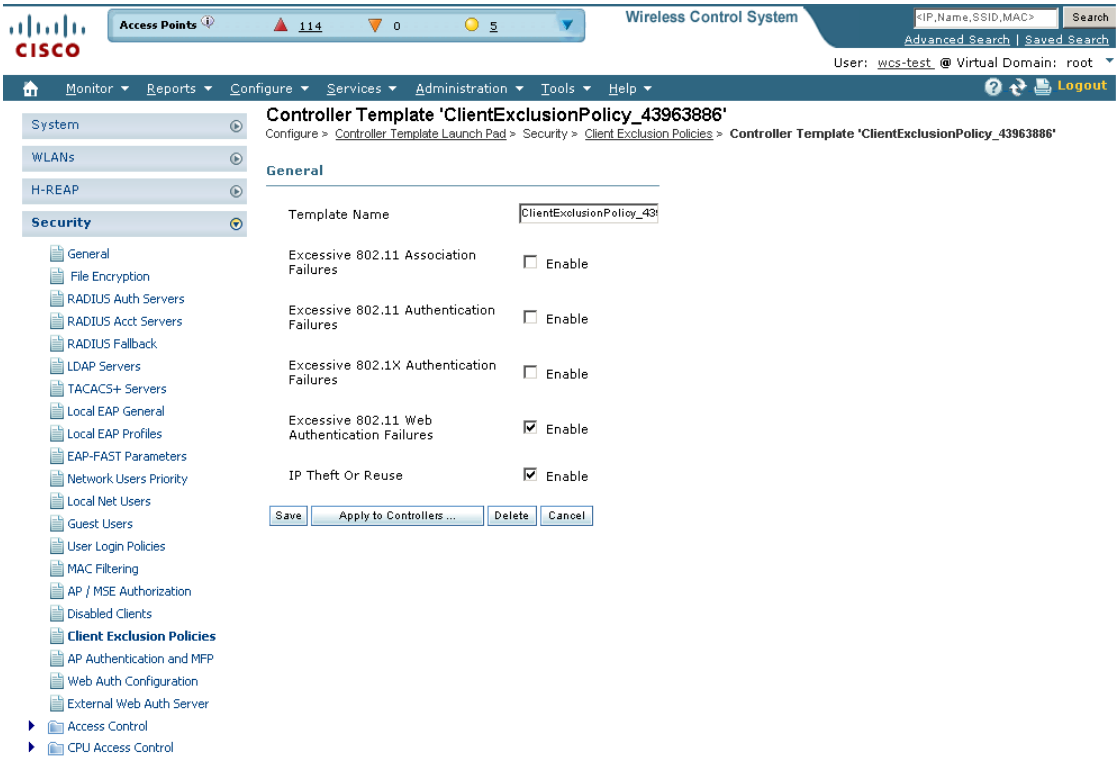
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-34).

Figure 12-34 Policies Template



Step 4 Edit a client exclusion policies template by configuring its parameters.

Table 12-3 Policies Template Parameters

Parameter	Description
Template Name	Enter a name for the client exclusion policy.
Excessive 802.11 Association Failures	Enable to exclude clients with excessive 802.11 association failures.
Excessive 802.11 Authentication Failures	Enable to exclude clients with excessive 802.11 authentication failures.
Excessive 802.1X Authentication Failures	Enable to exclude clients with excessive 802.1X authentication failures.

Table 12-3 (continued) Policies Template Parameters

Parameter	Description
Excessive 802.11 Web Authentication Failures	Enable to exclude clients with excessive 802.11 web authentication failures.
IP Theft or Reuse	Enable to exclude clients exhibiting IP theft or reuse symptoms.

Step 5 Click **Save**.

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 in order 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.

Follow these steps to add or make modifications for the access point authentication and management frame protection (MFP) template.

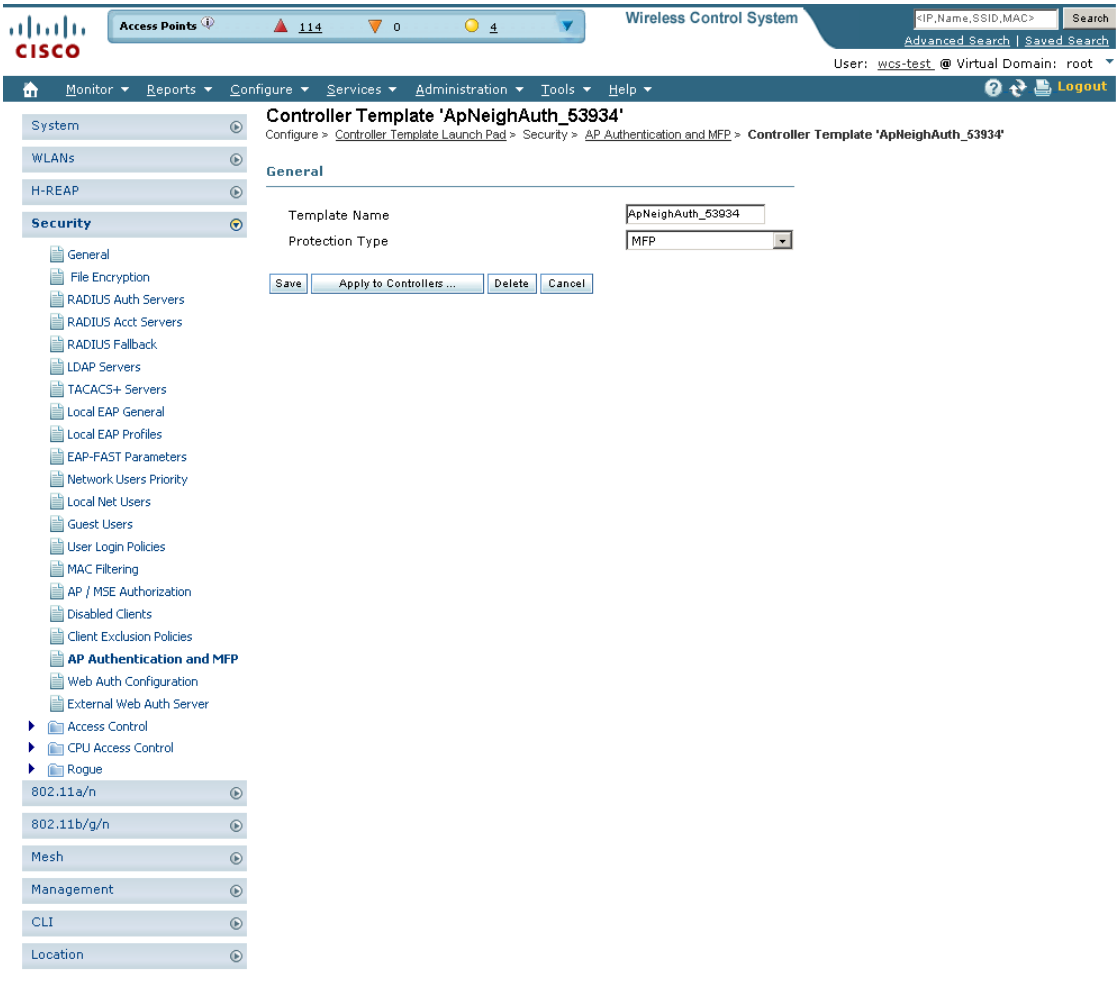
Step 1 Choose **Configure > Controller Template Launch Pad**.

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 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, click **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 (see Figure 12-35).

Figure 12-35 AP Authentication Policy Template



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 may 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.

Follow these steps to add or make modifications to an existing web authentication template.

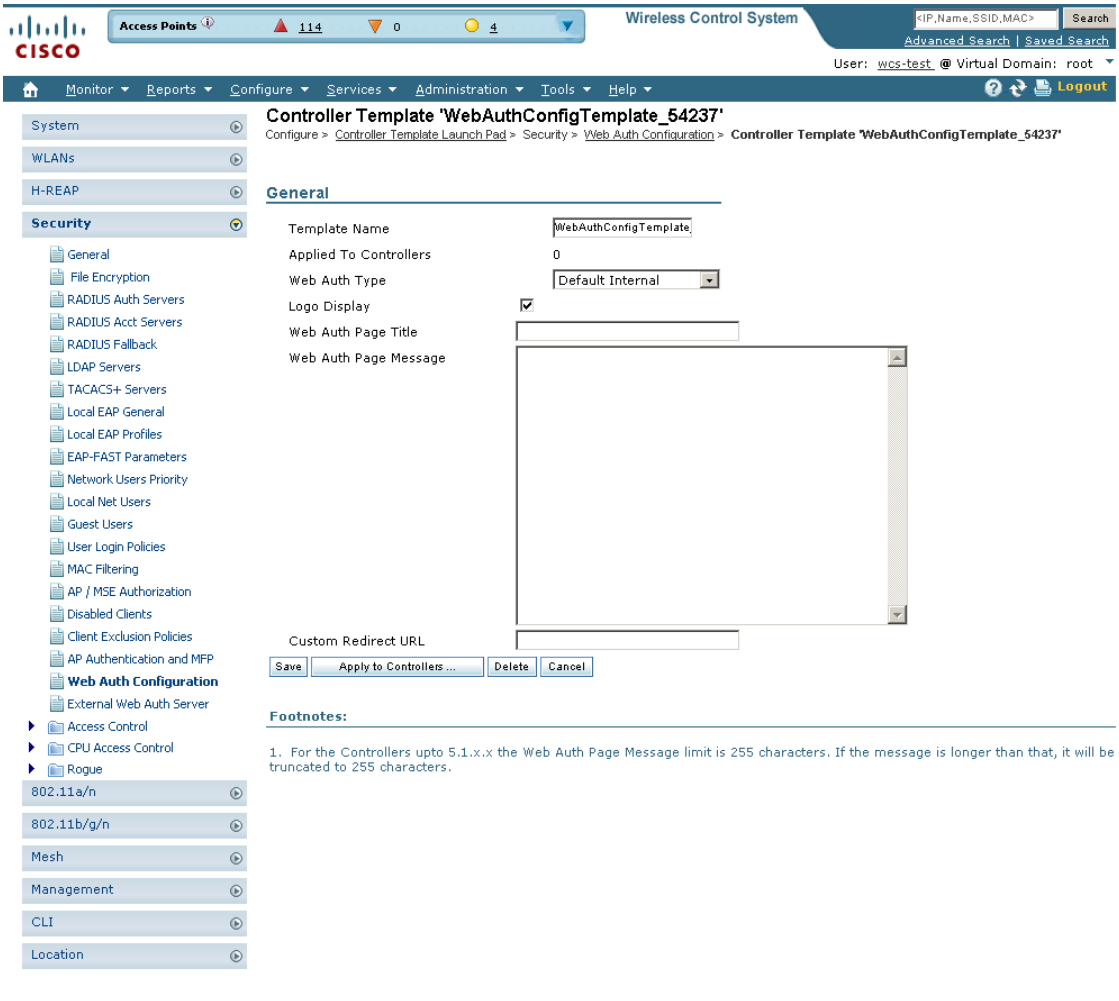
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-36).

Figure 12-36 Web Authentication Configuration Template



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 would be directed to the company home page.

Step 5 Click to enable Logo Display 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.

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.
- All paths used in the main page should be of relative type.

Perform the required following steps before downloading:

Step 1 Download the sample login.html bundle file from the server. The .html file is shown in Figure 12-37. The login page is presented to web users the first time they access the WLAN if web authentication is turned on.

Figure 12-37 Login.html

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 the Cisco WCS because WCS's built-in TFTP server 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 parameter. If you know the filename and path relative to the server's root directory, you can also select TFTP server.

Note For a local machine download, either .zip or .tar file options exists, but the WCS 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 parameter.

Step 13 Enter the maximum amount of time in seconds before the controller times out while attempting to download the file in the Timeout parameter.

Step 14 The 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.

Step 15 Click **OK**.

If the transfer times out, you can simply choose the TFTP server option in the File Is Located On parameter, and the Server File Name is populated for you. The local machine option initiates a two-step operation. First, the local file is copied from the administrator's workstation to WCS's own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in the WCS server's TFTP directory, 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 External Web Auth Server

You can create or modify an External Web Auth Server template by following 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. From here, you can edit the current template parameters.

Configuring Access Control List Templates

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. Follow these steps to add or modify an existing ACL template.

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.

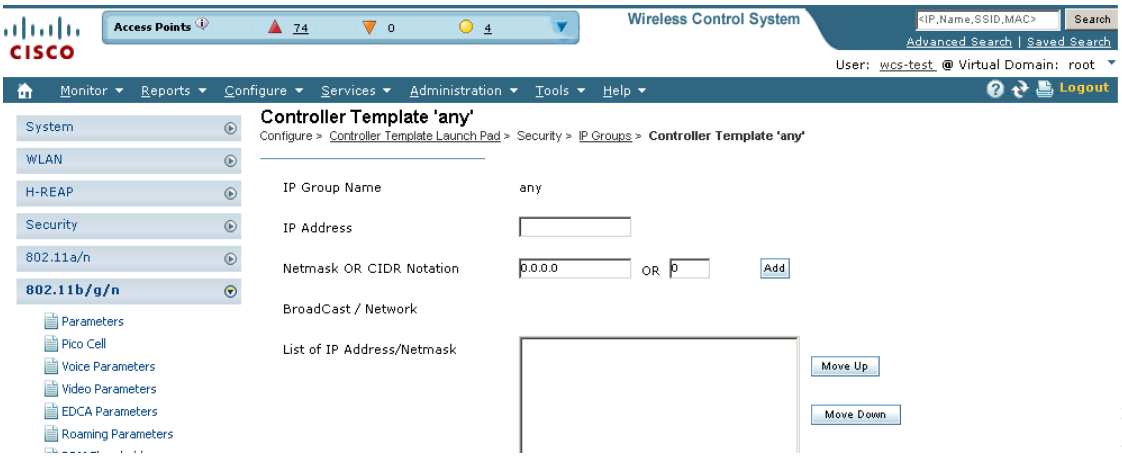
The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 To create reusable grouped IP addresses and protocols, choose **Access Control > IP Groups** from the left sidebar menu.

Step 4 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 (see Figure 12-38).

Note For the IP address of any, an *any* group is predefined.

Figure 12-38 IP Groups Controller Template



Step 5 On the ACL IP Groups details page you can edit the current IP group parameters.

- IP Group Name
- 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.

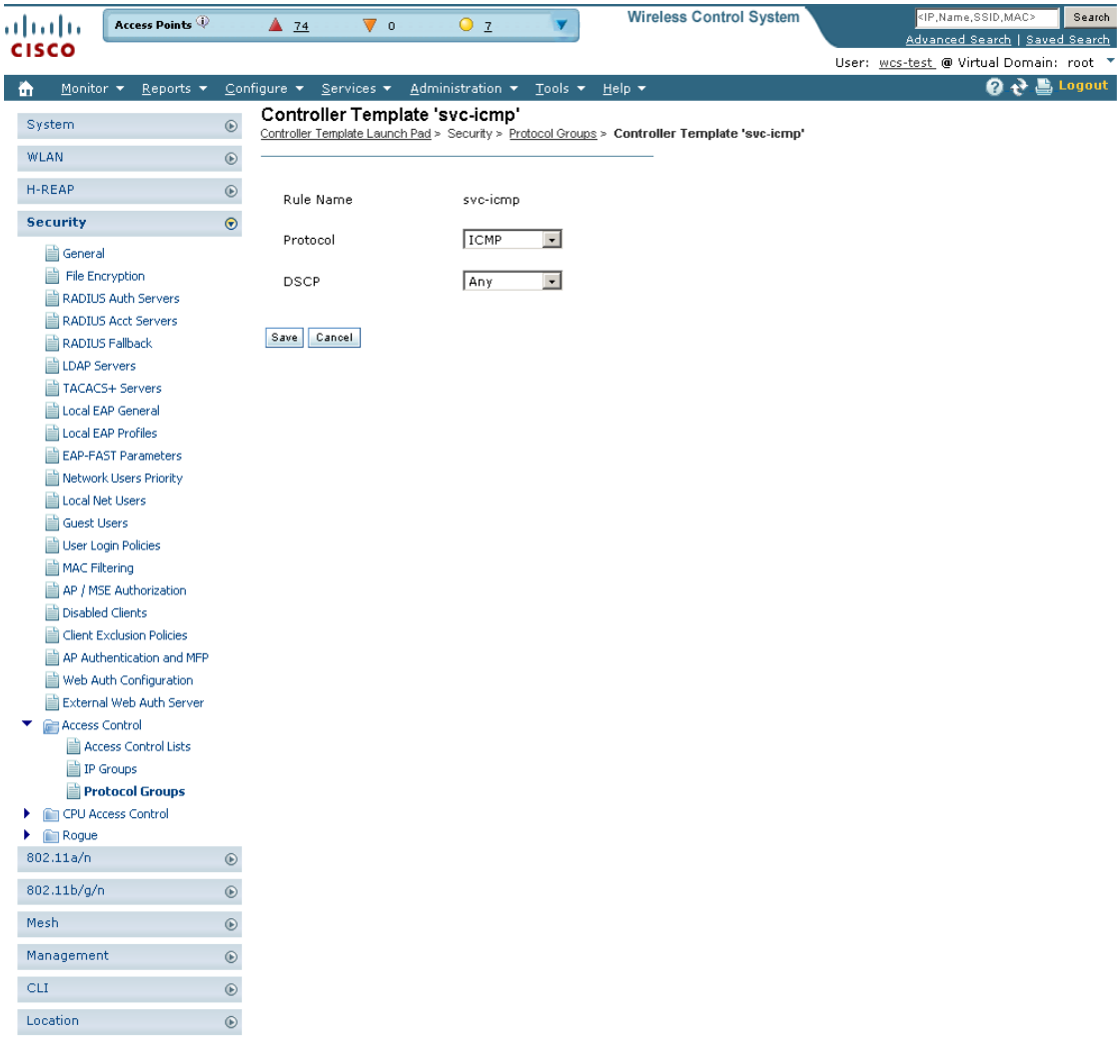
  Netmask allows you to set the subnet mask in dotted decimal notation rather than the CIDR notation for the IP address property.

  - 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 6 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 7 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 (see Figure 12-39).

Figure 12-39 Protocol Groups Controller Template



Step 8 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 9 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 10 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.

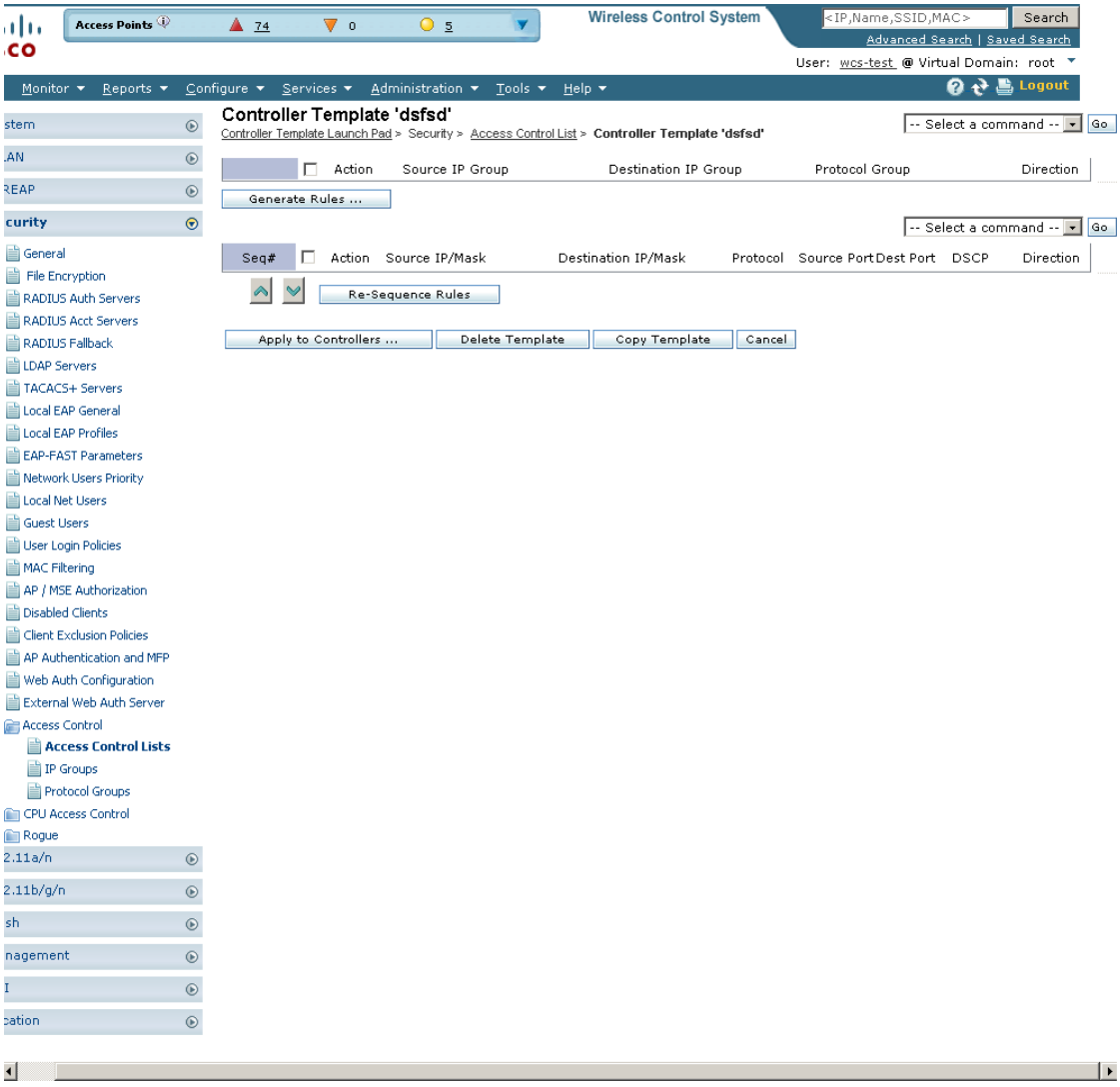
Step 11 In the DSCP (Differentiated Services Code Point) drop-down list, choose **any** or **specific**. If you choose specific, enter the DSCP (range of 0 to 255).

Note DSCP is a packet header code that can be used to define the quality of service across the Internet.

Step 12 Click **Save**.

Step 13 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 (see Figure 12-40).

Figure 12-40 Access Control List Rule Mapping



Step 14 To define a new mapping, choose **Add Rule Mappings** from the Select a command drop-down list. The Add Rule Mapping page appears.

Step 15 Choose the desired IP address groups, protocol groups, direction, and action, and click **Add**. The new mappings will populate the bottom table.

Step 16 Click **Save**.

Step 17 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 CPU Access Control List (ACL) Template

The existing ACLs established in the "Configuring Access Control List Templates" section on page 12-69 is used to set traffic controls between the central processing unit (CPU) and network processing unit (NPU). Follow these steps to add or modify an existing CPU ACL template.

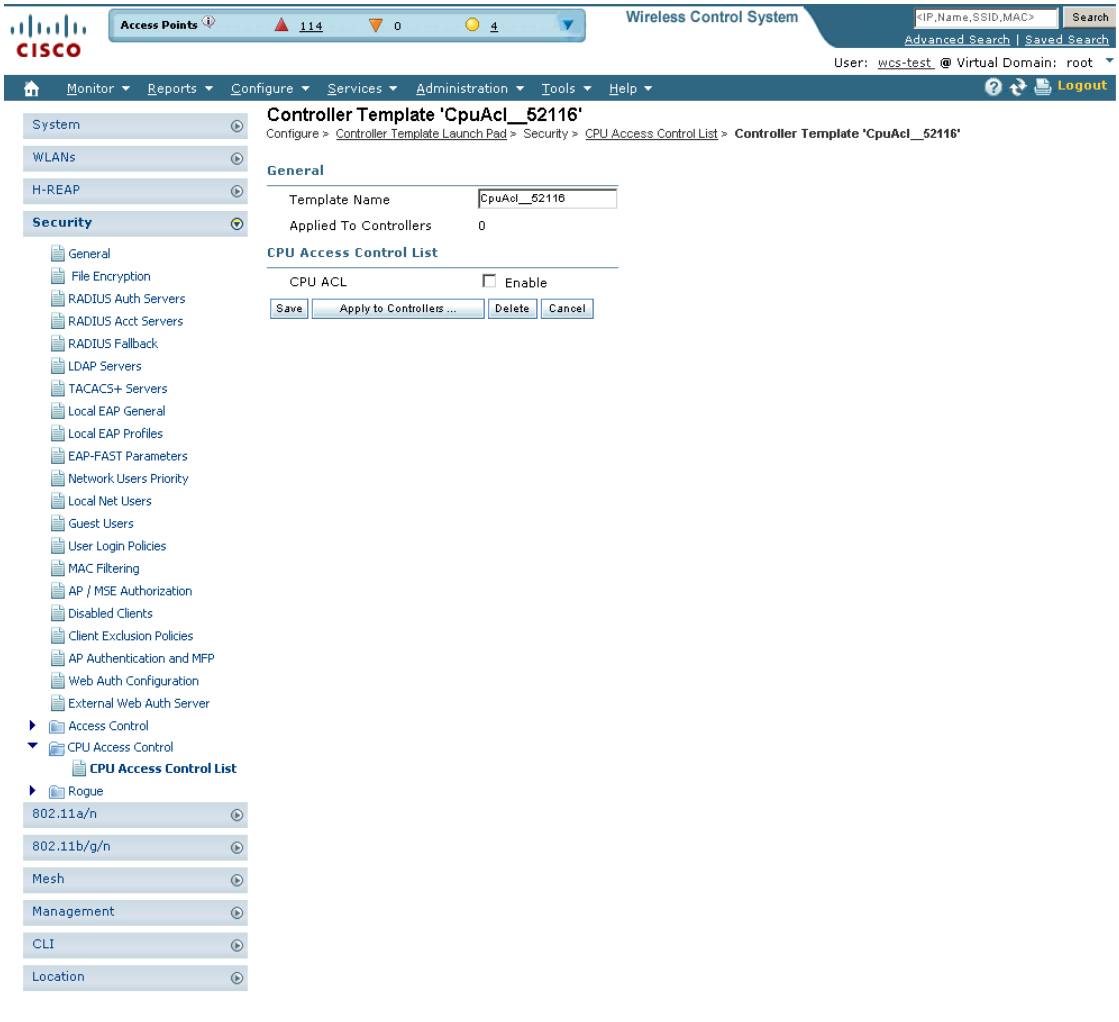
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-41).

Figure 12-41 CPU Access Control List Template



Step 4 If you click the check box to enable CPU ACL, two more parameters appear. When CPU ACL is enabled and applied on the controller, WCS 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 a Rogue Policies Template

This page enables you to configure the rogue policy (for access points and clients) applied to the controller. Follow these steps to add or modify an existing template.

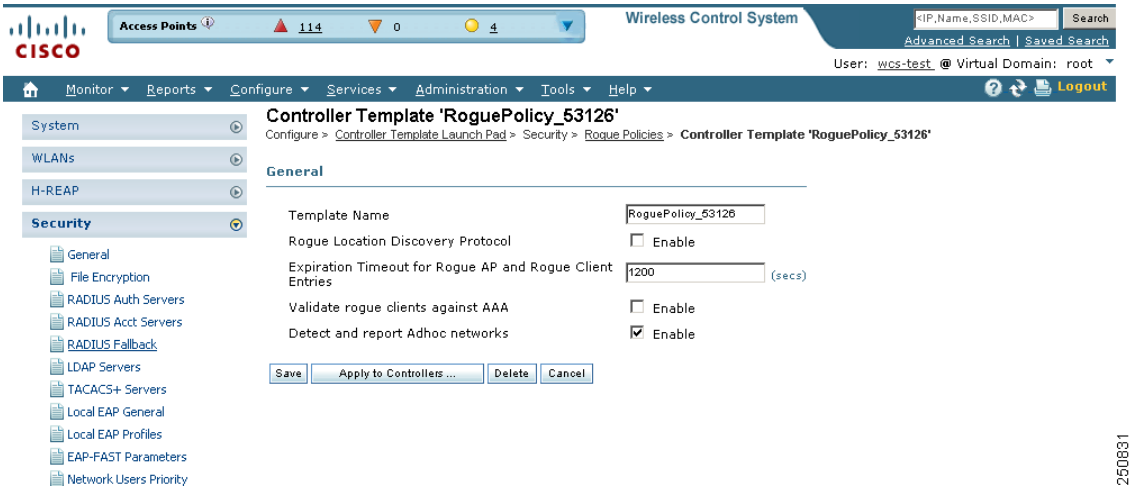
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-42).

Figure 12-42 Rogue Policy Setup Template



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:

- 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 Check the **Validate rogue clients against AAA** check box to enable the AAA validation of rogue clients.

Step 7 Check the **Detect and report Adhoc networks** check box to enable detection and reporting of rogue clients participating in ad hoc networking.

Step 8 Click **Save**.

Configuring a Rogue AP Rules Template

Rogue access point rules allow you to define rules to automatically classify rogue access points. WCS applies the rogue access point classification rules to the controllers. These rules can limit a rogue's 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).

Note Rogue access point rules also help reduce false alarms.

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, refer to the "Viewing or Editing Rogue Access Point Rules" section on page 9-36.

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.

Follow these steps to add or create a new classification rule template for rogue access points.

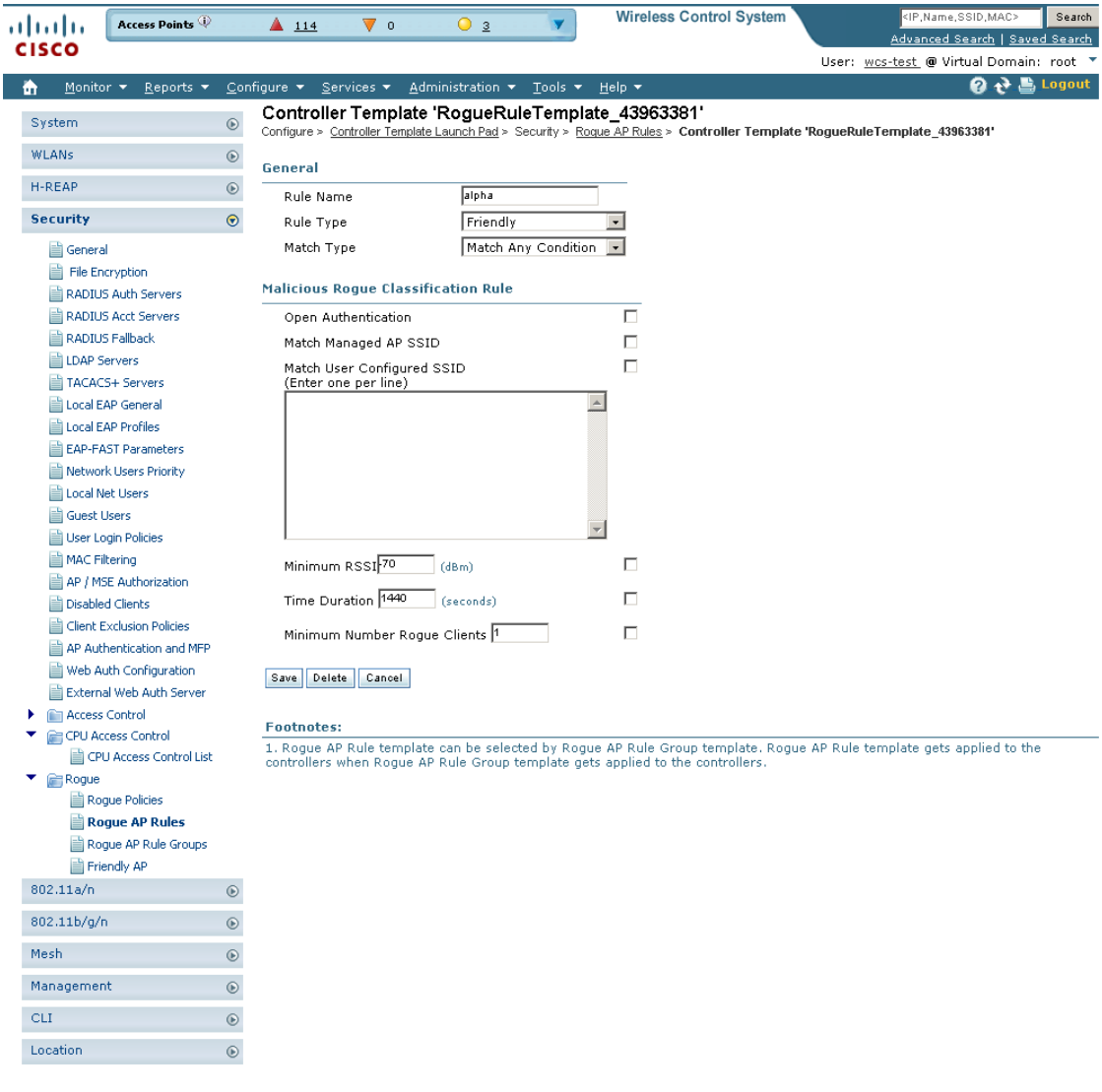
Step 1 Choose **Configure > Controller Template Launch Pad**.

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 (see Figure 12-43). 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.

Figure 12-43 Rogue AP Rules > New Template Page



Step 4 In the General portion of the page, enter the following parameters:

- Rule Name—Enter a name for the rule in the text box.
- Rule Type—Choose **Malicious** or **Friendly** 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.
- Match Type—Choose **Match All Conditions** or **Match Any Condition** from the drop-down list.

Step 5 In the Malicious Rogue Classification Rule portion of the page, enter the following parameters.

- Open Authentication—Choose the check box to enable open authentication.
- Match Managed AP SSID—Choose 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—Choose 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.

- Minimum RSSI—Choose 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—Choose 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—Choose 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. Follow these steps to view current rogue access point rule group templates or create a new rule group.

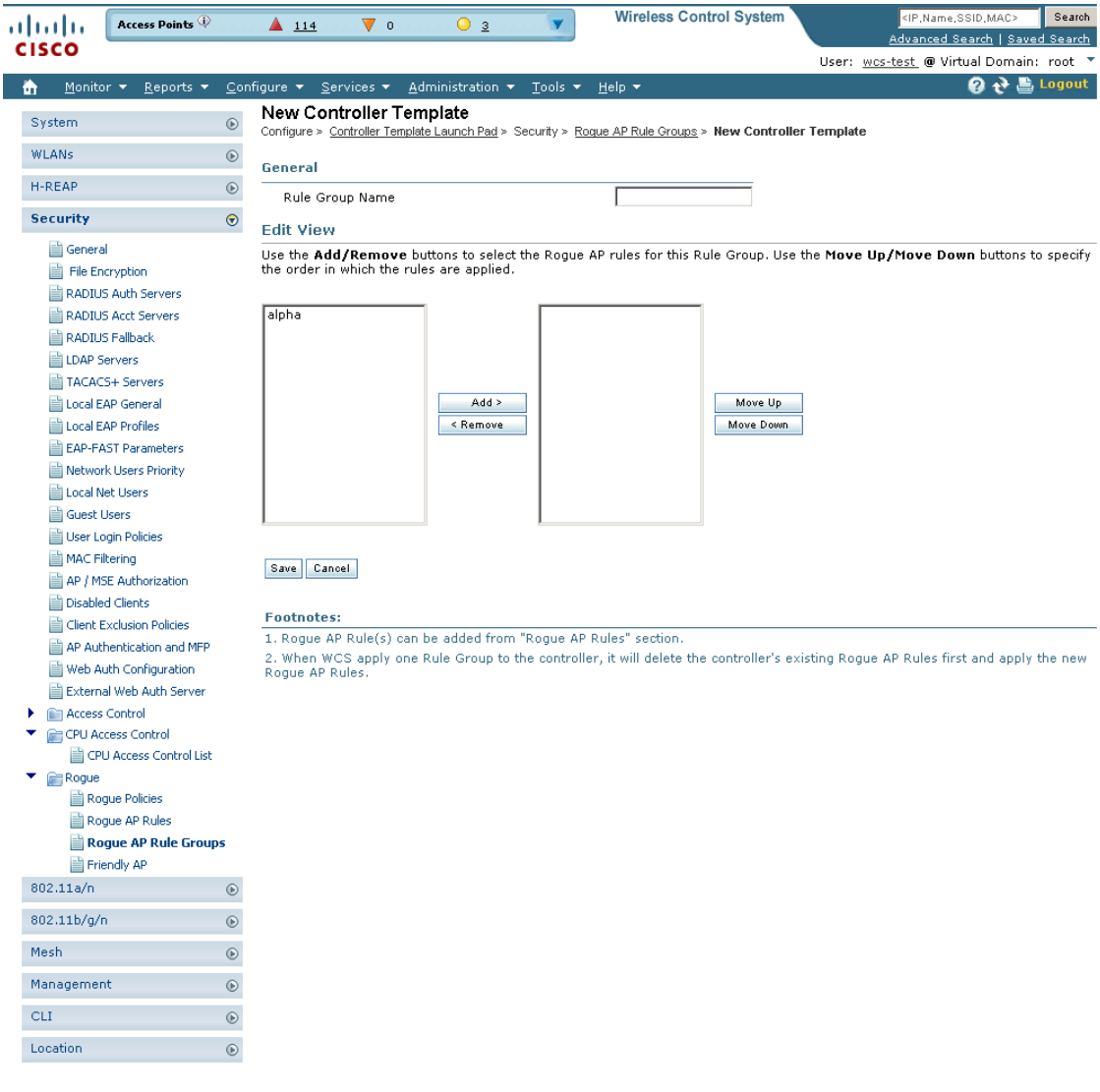
Step 1 Choose **Configure > Controller Template Launch Pad**.

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 (see Figure 12-44).

Figure 12-44 Rogue AP Rule Groups > New Template



Note 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 portion 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 12-77 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*.

Follow these steps to view or edit the current list of friendly access points. The friendly access point screen identifies the access point's MAC address, status, any comments, and whether or not the alarm is suppressed for this access point.

Step 1 Choose **Configure > Controller Template Launch Pad**.

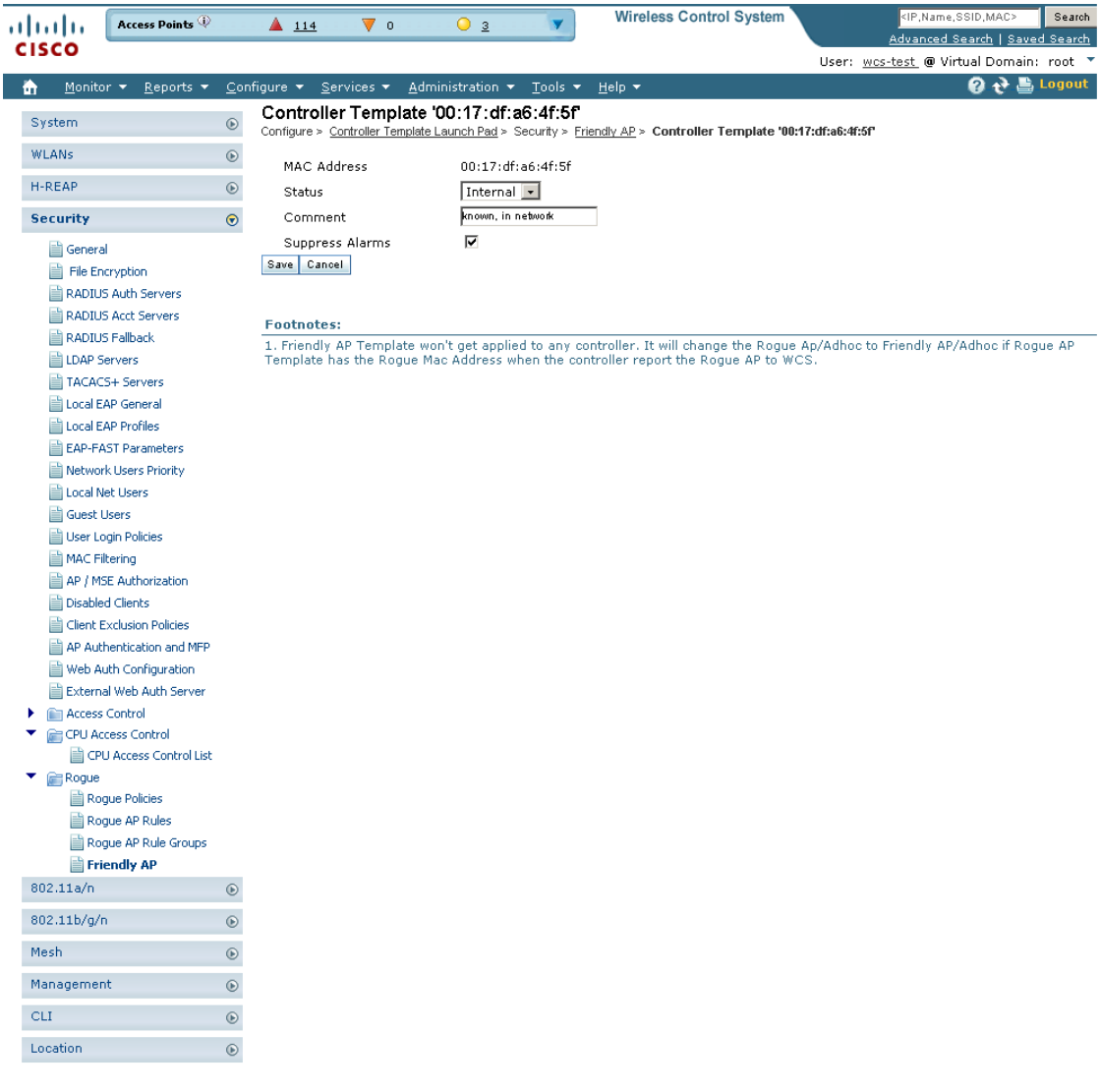
Step 2 Click **Friendly AP** or choose **Security > Rogue > Friendly AP** from the left sidebar menu.

Step 3 From the Select a command drop-down list, choose **Add Friendly**.

Step 4 Click **Go**. The Friendly AP page appears (see Figure 12-45).

Note To modify an existing friendly access point, choose **Configure > Controller Template Launch Pad > Security > Rogue > Friendly Internal** and click the access point's MAC address. Make the necessary changes to the access point and click **Save**.

Figure 12-45 Friendly AP > Add Friendly AP Page



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,
  - Choose the **Import from File** check box.
  - Enter the file path or use the **Browse** button to navigate to the correct file.
- To manually add an access point,
  - Deselect the **Import from File** check box.
  - Enter the MAC address for the access point.

Note Use a line break to separate MAC addresses. For example, you could enter the MAC addresses as follows:
00:00:11:22:33:44
00:00:11:22:33:45
00:00:11:22:33:46

- Choose **Internal** access point from the Status drop-down list.
- Enter a comment regarding this access point, if necessary.
- Check 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 Radio Templates (for 802.11a/n or 802.11b/g/n)

Follow these steps to add or modify radio templates.

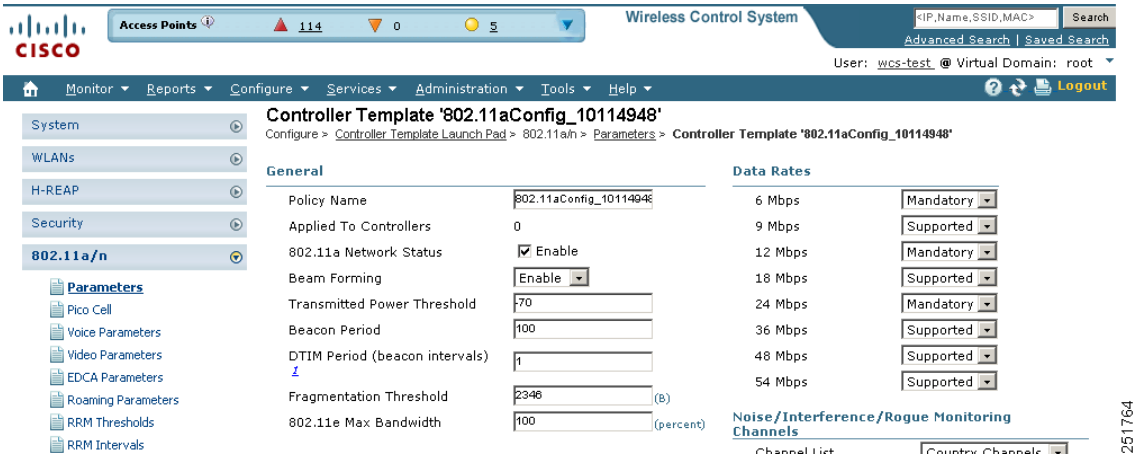
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Parameters** or choose either **802.11a/n > Parameters or 802.11b/g/n > Parameters** from the left sidebar menu. The 802.11a/n or b/g/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, click **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 Parameters template page appears (see Figure 12-46).

Figure 12-46 802.11a/n Parameters Template



Step 4 Click the check box if you want to enable 802.11a/n or b/g/n network status.

Step 5 Use the ClientLink drop-down list to enable Clientlink on all access point 802.11a/n radios which 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 may 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 At the Fragmentation Threshold parameter, 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 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.

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 At the Avoid Foreign AP Interference check box, click if you want to enable it. Enable this parameter 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) parameter monitors foreign 802.11 interference. Disable this parameter to have RRM ignore this interference.

In certain circumstances with significant interference energy (dB) and load (utilization) from foreign access points, RRM may 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 parameter to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points. Disable this parameter to have RRM ignore this value.

In certain circumstances and with denser deployments, there may not be enough channels to properly create perfect channel re-use. In these circumstances, RRM can assign better re-use 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 parameter to have access points avoid channels that have interference from non-access point sources, such as microwave ovens or Bluetooth devices. Disable this parameter to have RRM ignore this interference.

In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, RRM may 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 re-use. 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 in order to use the network. If a data rate is set as Supported by the controller, any associated client that also supports that same rate may communicate with the access point using that rate. However, it is not required that a client uses all the rates marked supported in order 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 At 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 Cisco Compatible Extension's location measurement interval 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 a Voice Parameter Template (for 802.11a/n or 802.11b/g/n)

Follow these steps to add or modify either 802.11a/n or 802.11b/g/n voice parameters, such as call admission control and traffic stream metrics.

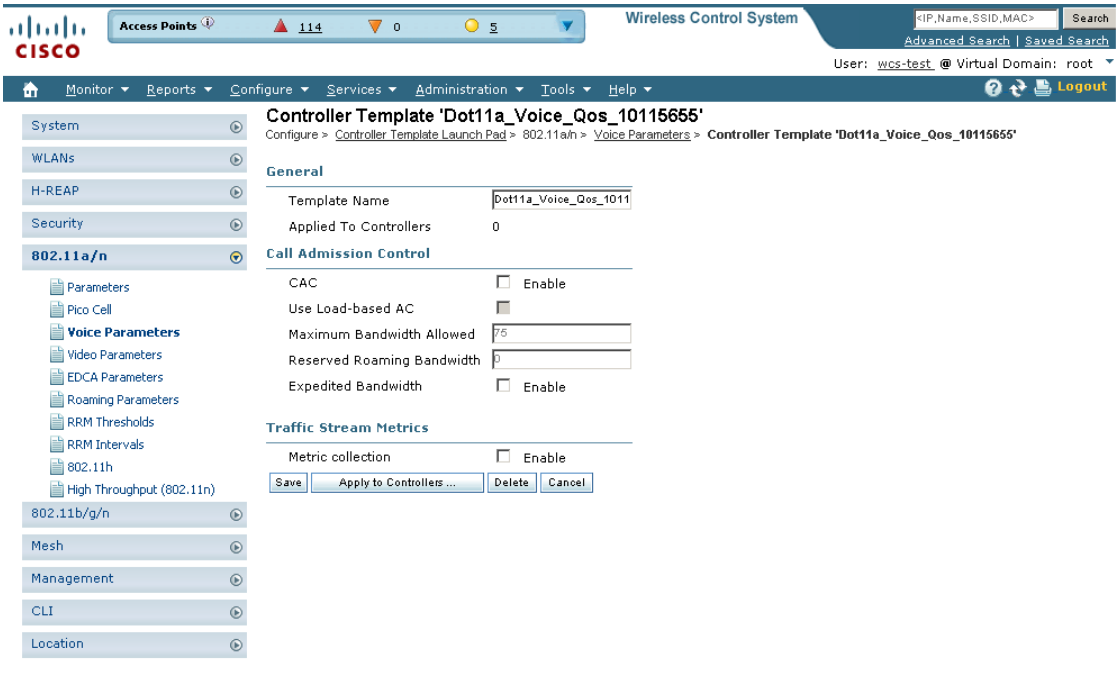
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Voice Parameters** or choose either **802.11a/n > Voice Parameters** or **802.11b/g/n > Voice Parameters**. The 802.11a/n or 802.11b/g/n Voice Parameters page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the maximum bandwidth allowed and the reserved roaming bandwidth. 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, click **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 Voice Parameters template page appears (see Figure 12-47).

Figure 12-47 802.11b/g/n Voice Parameters Template



Step 4 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. Click the check box to enable CAC.

Step 5 Load-based AC 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 AC also covers the additional bandwidth consumption resulting from PHY and channel impairment. To enable load-based AC for this radio band, check the Use Load-based AC check box.

Step 6 Enter the percentage of maximum bandwidth allowed.

Step 7 Enter the percentage of reserved roaming bandwidth.

Step 8 Click if you want to enable expedited bandwidth as an extension of CAC for emergency calls. You must have an expedited bandwidth IE that is Cisco Compatible Extensions (version 5) compliant so that a TSPEC request is given higher priority.

Step 9 Click the check box if you want to enable metric collection. Traffic stream metrics are a series of statistics about VoIP over your wireless LAN and 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 in every 90 seconds from the 802.11b/g/n interfaces of all associated access points. For VoIP and video, this feature should be enabled.

Step 10 Click **Save**.

Configuring a Video Parameter Template (for 802.11a/n or 802.11b/g/n)

Follow these steps to add or modify an 802.11a/n or 802.11b/g/n video parameter template.

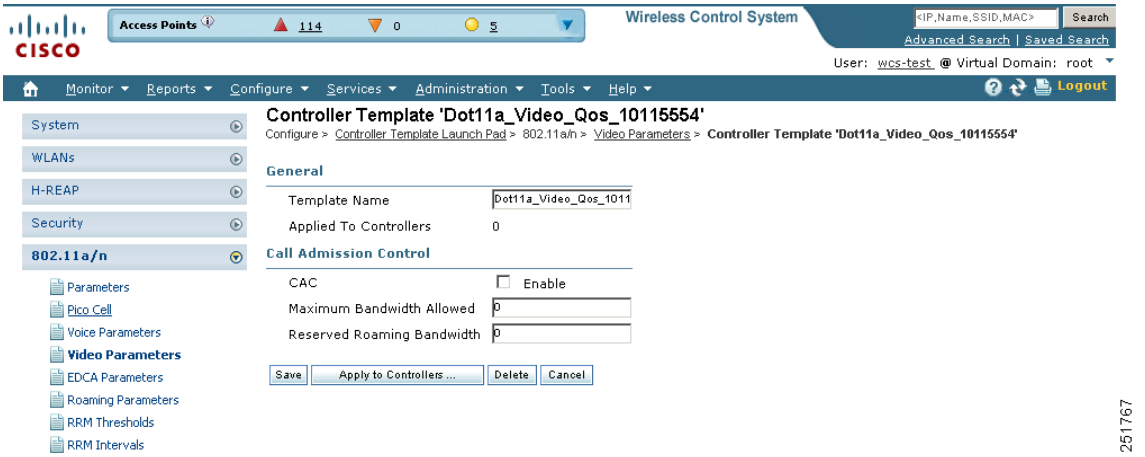
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Video Parameters** or choose either **802.11a/n > Video Parameters** or **802.11b/g/n > Video Parameters**. The 802.11a/n or 802.11b/g/n Video Parameters page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the maximum bandwidth allowed and the reserved roaming bandwidth. 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, click **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 Video Parameters template page appears (see Figure 12-48).

Figure 12-48 802.11a/n Video Parameters Template



Step 4 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 keeps the maximum allowed number of calls to an acceptable quantity. Click the check box to enable CAC.

Step 5 Enter the percentage of maximum bandwidth allowed.

Step 6 Enter the percentage of reserved roaming bandwidth.

Step 7 Click **Save**.

Configuring EDCA Parameters through a Controller Template

Enhanced distributed channel access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality-of-service (QoS) traffic. Follow these steps to add or configure 802.11a/n or 802.11b/g/n EDCA parameters through a controller template:

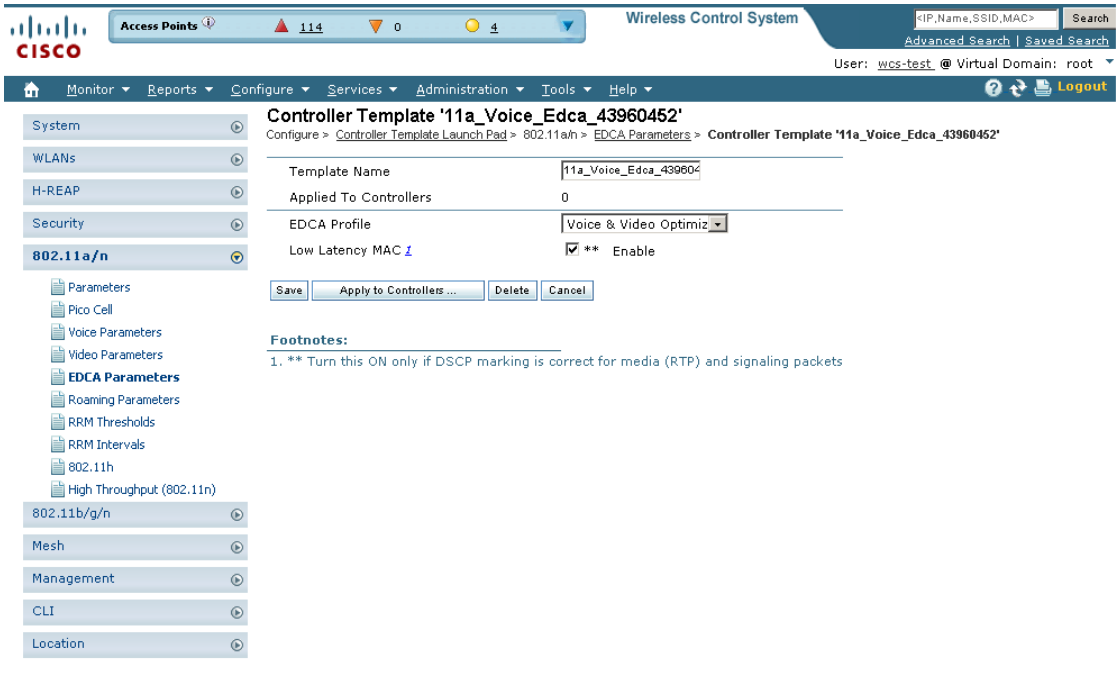
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **EDCA Parameters** or choose **802.11a/n > EDCA Parameters** or **802.11b/g/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, click **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 EDCA Parameters template page appears (see Figure 12-49).

Figure 12-49 802.11a EDCA Parameters



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 Click 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 (for 802.11a/n or 802.11b/g/n)

Follow these steps to add or modify an existing roaming parameter template.

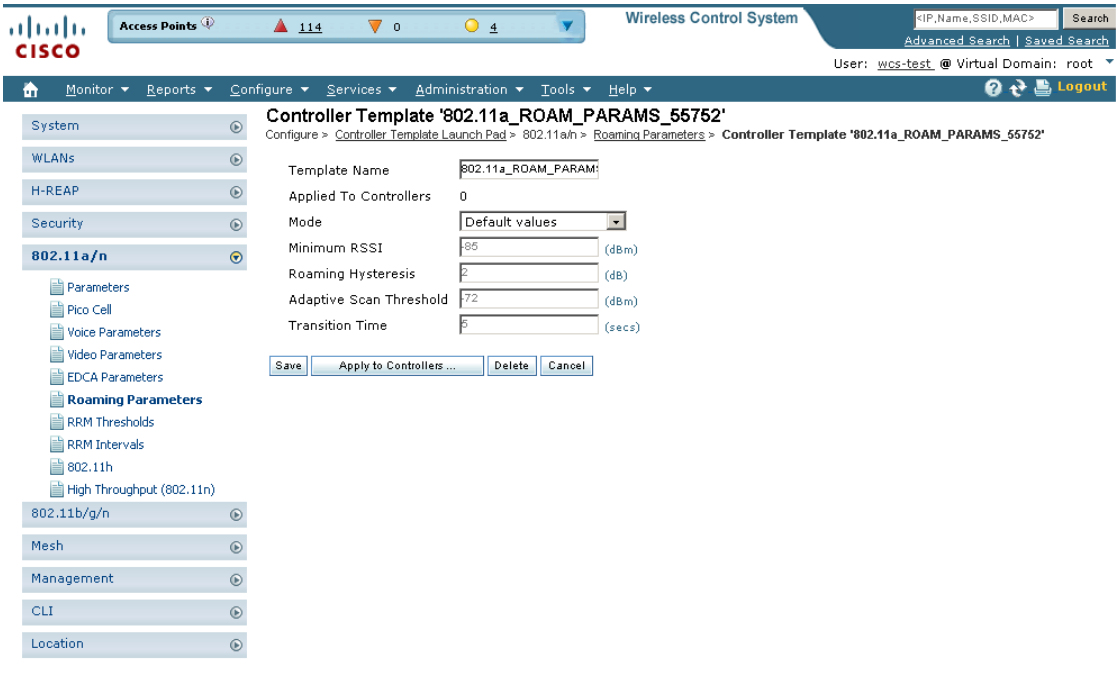
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Roaming Parameters** or choose **802.11a/n > Roaming Parameters** or **802.11b/g/n > Roaming Parameters** from the left sidebar menu. The Roaming Parameters Template 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, click **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 Roaming Parameters template page appears (see Figure 12-50).

Figure 12-50 802.11 Roaming Parameters Template



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 client's 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

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 parameter 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 field, enter the RSSI value from a client's associated access point, below which the client must be able to roam to a neighboring access point within the specified transition time. This parameter 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 client's 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 an RRM Threshold Template (for 802.11a/n or 802.11b/g/n)

Follow these steps to add or make modifications to an 802.11a/n or 802.11b/g/n RRM threshold template.

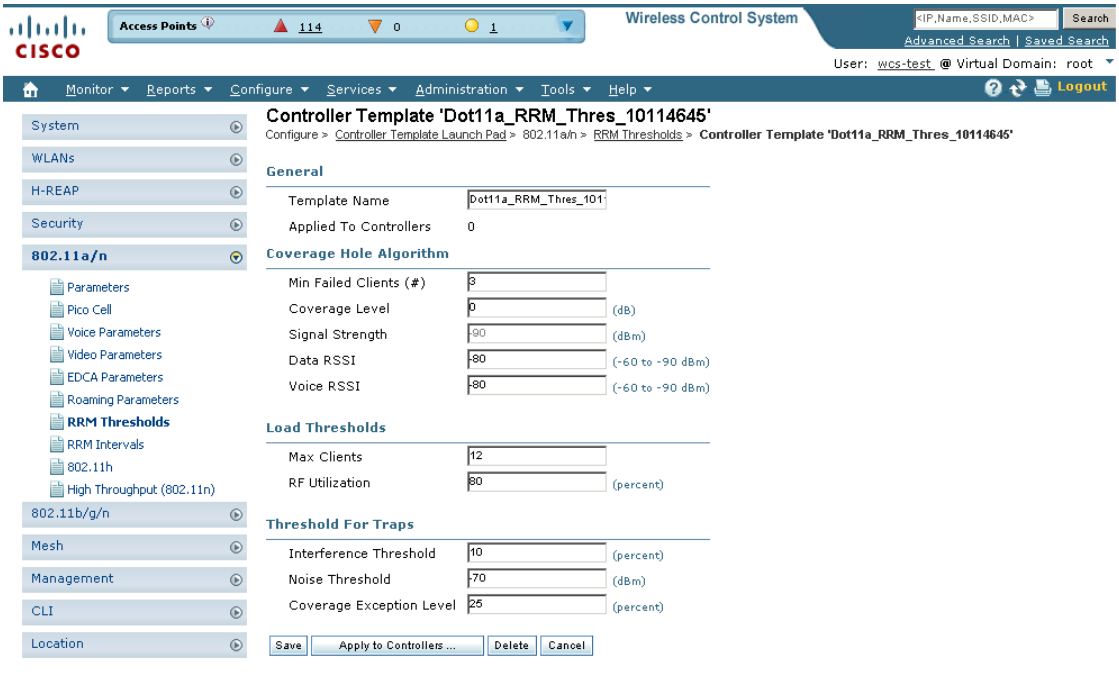
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **RRM Thresholds** or choose **802.11a/n > RRM Thresholds** or **802.11b/g/n > RRM Thresholds**. The 802.11a/n or 802.11b/g/n RRM Thresholds Template 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, click **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 Threshold template page appears (see Figure 12-51).

Figure 12-51 802.11b/g/n RRM Thresholds Template



Step 4 Enter the minimum number of failed clients currently associated with the controller.

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 or 802.11b/g/n network before applying these RRM threshold parameters.

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 At the RF Utilization parameter, enter the percentage of threshold for either 802.11a/n or 802.11b/g/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 WCS.

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 (for 802.11a/n or 802.11b/g/n)

Follow these steps to add or make modifications to an 802.11a/n or 802.11b/g/n RRM interval template.

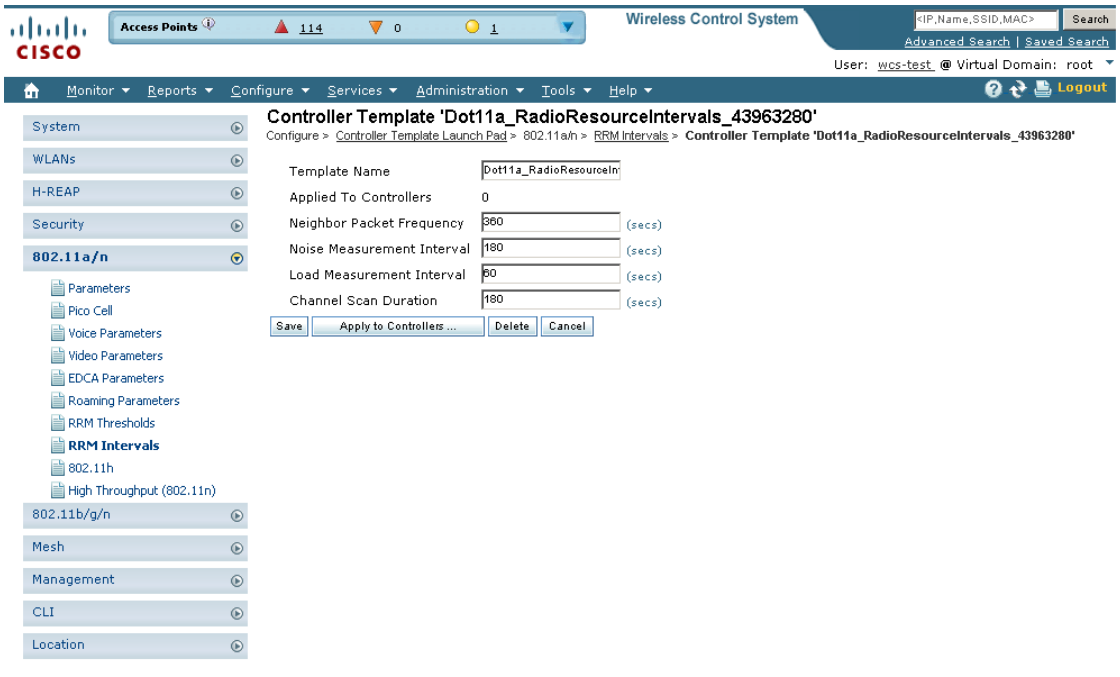
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click RRM Intervals or choose **802.11a/n > RRM Intervals** or **802.11b/g/n > RRM Intervals** from the left sidebar menu. The 802.11a/n or 802.11b/g/n RRM Threshold Template 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, click **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 (see Figure 12-52).

Figure 12-52 802.11a/n RRM Intervals Template



Step 4 At the Neighbor Packet Frequency parameter, 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 parameter, enter at which interval you want coverage measurements taken for each access point. The default is 300 seconds.

Step 8 Click **Save**.

Configuring an 802.11h Template

802.11h informs client devices about channel changes and can limit the client device's transmit power. 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. Follow these steps to add or modify an 802.11h template.

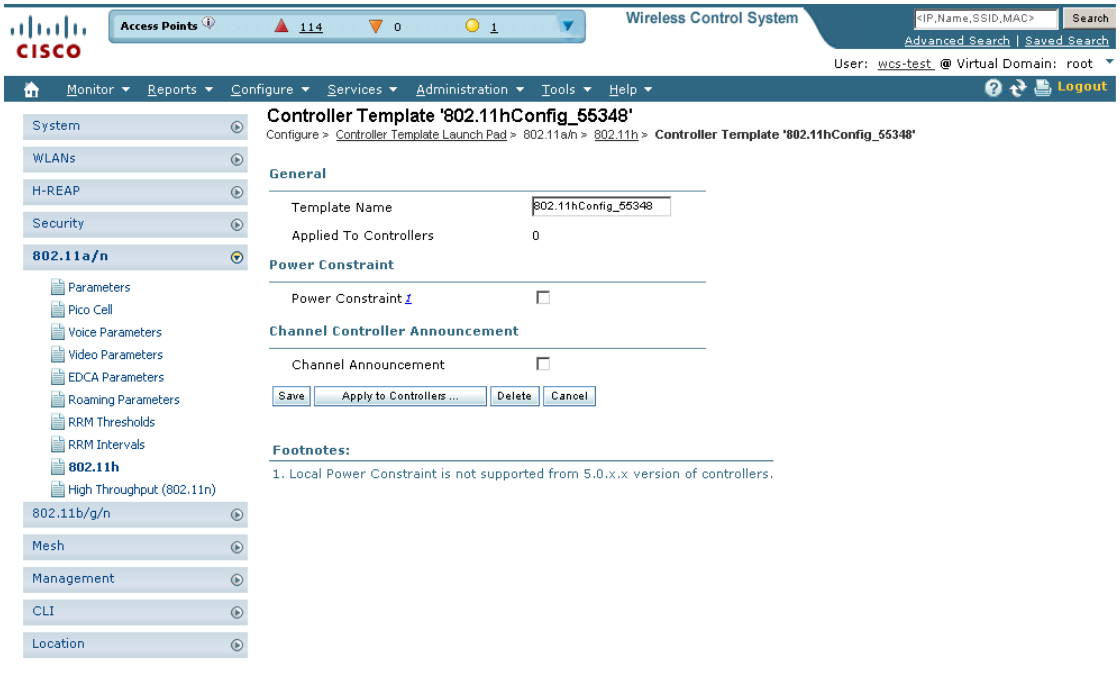
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **802.11h** or choose **802.11a/n > 802.11h** from the left sidebar menu.The 802.11h Template 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, click **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 (see Figure 12-53).

Figure 12-53 802.11h Template



Step 4 Check the **Power Constraint** check box if you want the access point to stop transmission on the current channel.

Step 5 Check 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 (for 802.11a/n or 802.11b/g/n)

Follow these steps to add or modify to an 802.11a/n or 802.11b/g/n high throughput template.

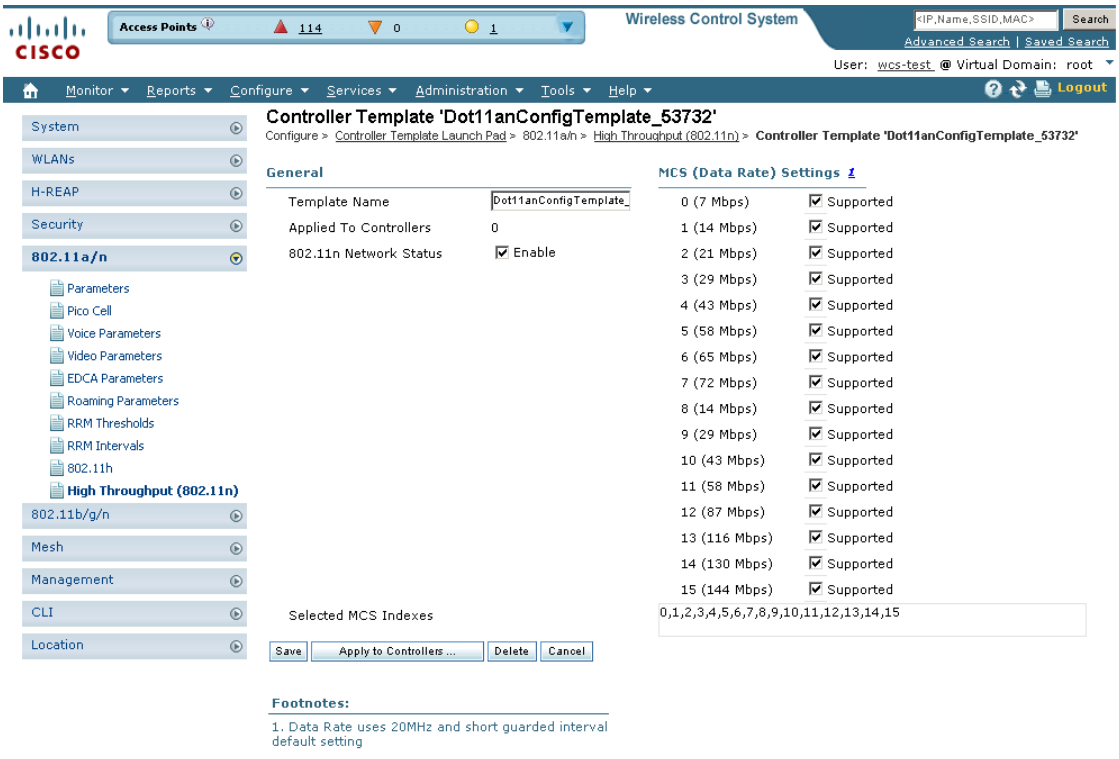
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **High Throughput (802.11n)** or choose **802.11a/n > High Throughput** or **802.11b/g/n > High Throughput** from the left sidebar menu. The 802.11n Parameters for 2.4 GHz or 802.11n Parameters for 5 GHz template 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, click **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 High Throughput template page appears (see Figure 12-54).

Figure 12-54 802.11n Parameters for 2.4GHz Template



Step 4 Click 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 (for 802.11a/n or 802.11b/g/n)

Create or modify a template for configuring CleanAir parameters for the 802.11a/n or 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.

- Editing Existing CleanAir Controller Templates (802.11a/n or 802.11 b/g/n)

- Adding a New CleanAir Controller Template (802.11a/n or 802.11 b/g/n)

Editing Existing CleanAir Controller Templates (802.11a/n or 802.11 b/g/n)

To make changes to an existing CleanAir controller, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 From the left sidebar menu, choose **802.11a/n > CleanAir** or **802.11b/g/n > CleanAir**. The 802.11a/n or 802.11b/g/n CleanAir Controller Templates page displays all currently saved 802.11a/n or 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 Click a template name to open the Controller Template list page. From here, you can edit the current template parameters.

Note See Adding a New CleanAir Controller Template (802.11a/n or 802.11 b/g/n) for information on 802.11a/n or 802.11b/g/n CleanAir template parameters.

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, select the applicable controllers, and click OK. See "Applying Controller Templates" for more information.
- 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.

Adding a New CleanAir Controller Template (802.11a/n or 802.11 b/g/n)

To add a new template with 802.11a/n or 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 **802.11a/n > CleanAir** or **802.11b/g/n > CleanAir**. The 802.11a/n or 802.11b/g/n CleanAir Controller Templates page displays all currently saved 802.11a/n or 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 Add or modify the following parameters:

- 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 sections appear.

- Reporting Configuration—Use the parameters in this section 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 checked.
  - 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 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.
  - 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 displays in the Template List page. In the Template List page, you can apply this template to controllers. See "Adding Controller Templates" for more information.

Configuring a Mesh Template

You can configure an access point to establish a connection with the controller. Follow these steps to add or modify a mesh template.

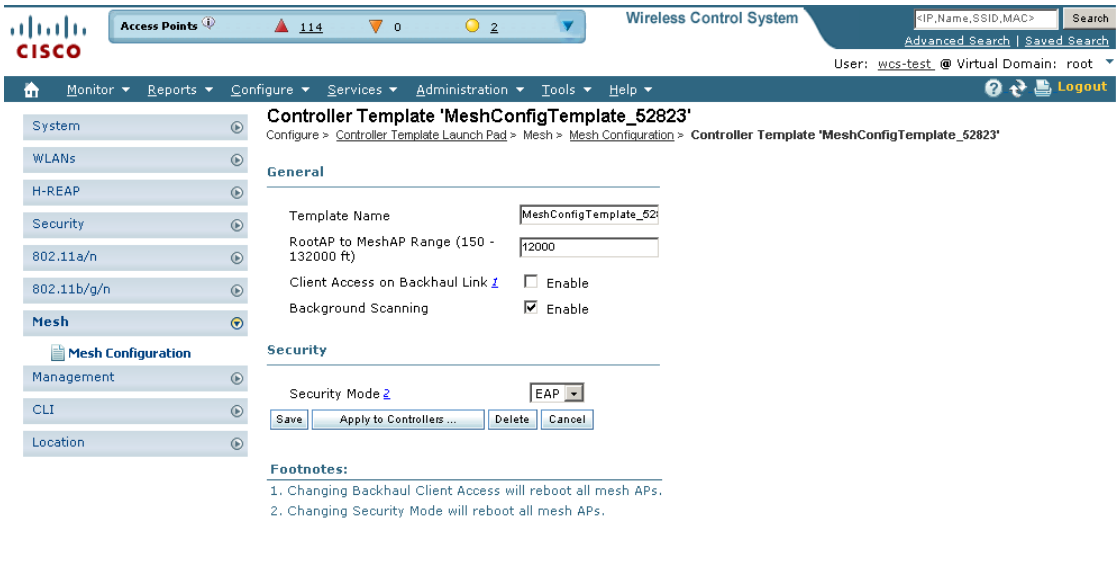
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-55).

Figure 12-55 Mesh Configuration Template



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 parameter 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 checked 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 10-64 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 a Trap Receiver Template

Follow these steps to add or modify a trap receiver template. If you have monitoring devices on your network that receive SNMP traps, you may want to add a trap receiver template.

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, click **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 (see Figure 12-56).

Figure 12-56 Trap Receiver Template

Step 5 Enter the IP address of the server.

Step 6 Click to enable the admin status if you want SNMP traps to be sent to the receiver.

Step 7 Click **Save**.

Configuring a Trap Control Template

Follow these steps to add or modify a trap control template.

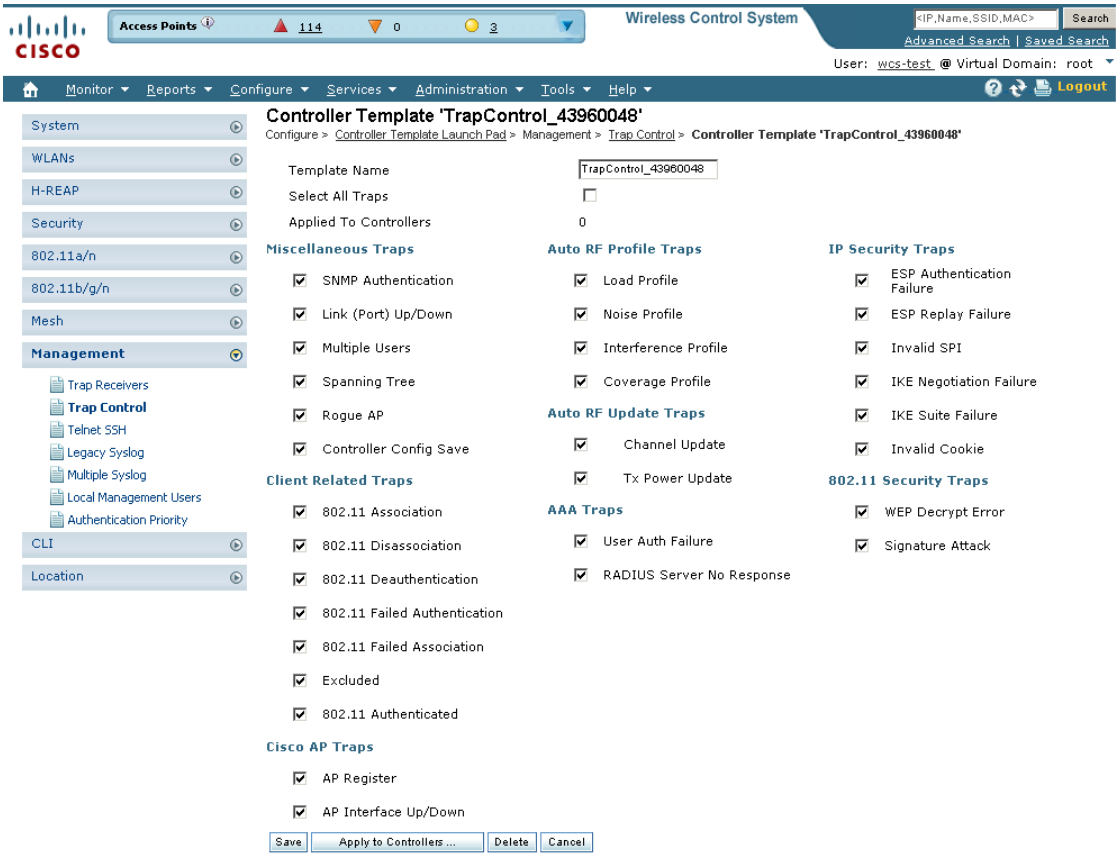
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-57).

Figure 12-57 Trap Controls Template



Step 4 Check 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 Check 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 Check 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 Check 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.
- 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 8 Check the appropriate check box to enable any of the following auto RF update traps:

- Channel Update - Notification sent when access point's dynamic channel algorithm is updated.
- Tx Power Update - Notification sent when access point's dynamic transmit power algorithm is updated.

Step 9 Check 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 Check 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 Check 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 a Telnet SSH Template

Follow these steps to add or modify a Telnet SSH configuration template.

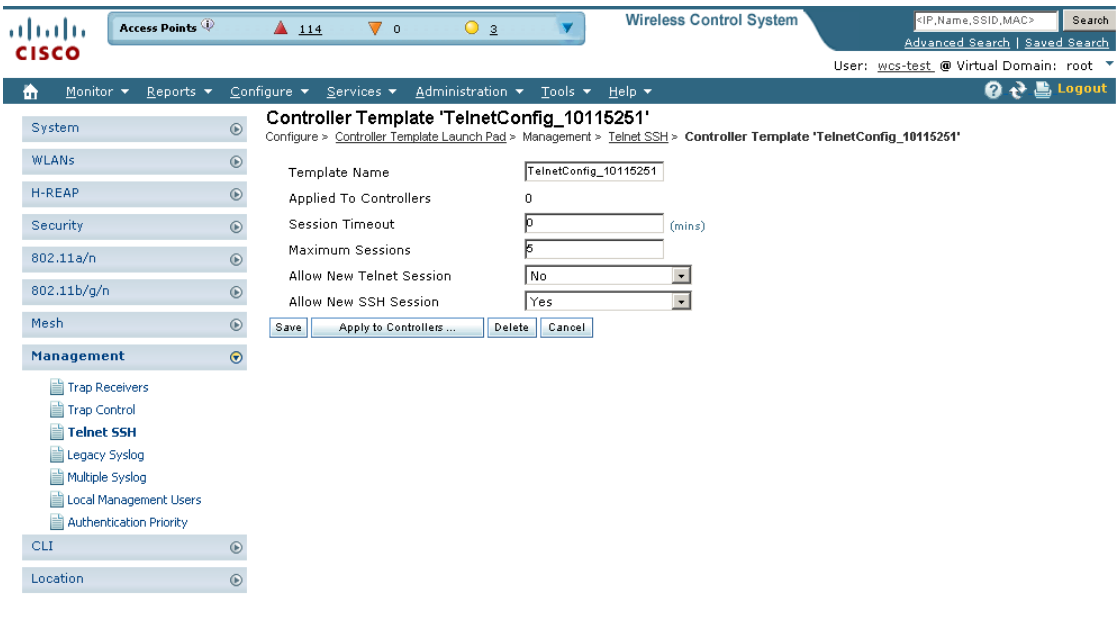
Step 1 Choose **Configure > Controller Template Launch Pad**.

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.

Step 3 If you want to add a new template, click **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 (see Figure 12-58).

Figure 12-58 Telnet SSH Configuration Template



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 parameter, 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 a Legacy Syslog Template

Follow these steps to add or modify a legacy syslog configuration template.

Note Legacy Syslog applies to controllers earlier than version 5.0.6.0

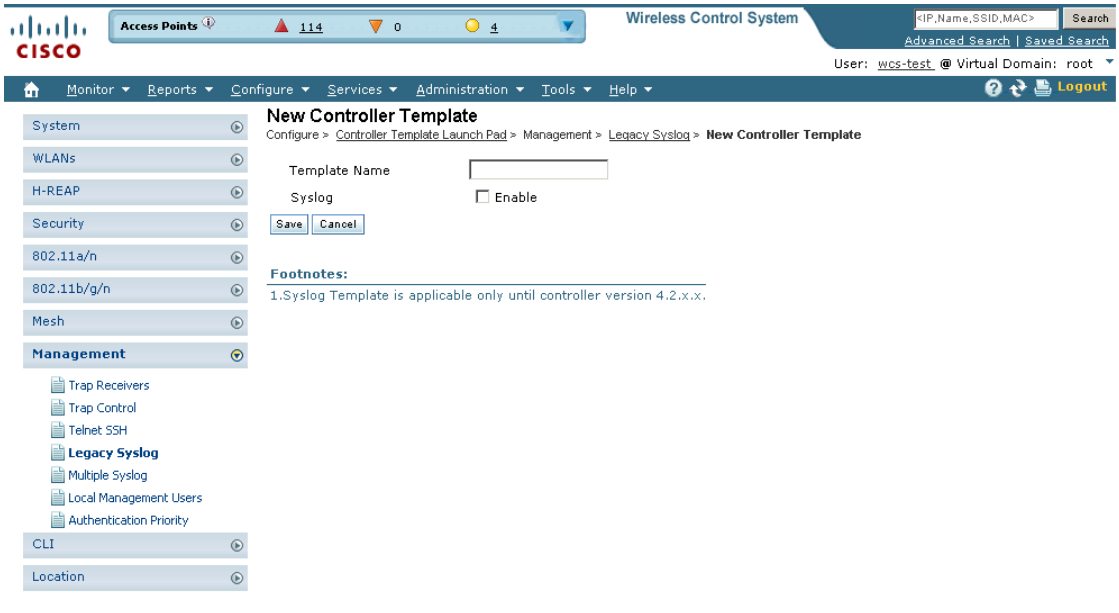
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, click **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 (see Figure 12-59).

Figure 12-59 Syslog Configuration Template



Step 4 Enter a template name. The number of controllers to which this template is applied is displayed.

Step 5 Click to enable syslog. When you do, a Syslog Host IP Address parameter appears.

Step 6 Click **Save**.

Configuring a Multiple Syslog Template

Follow these steps to add or modify a multiple syslog configuration template.

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, click **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 (see Figure 12-60).

Figure 12-60 Syslog Server Template Page

Step 4 Enter a template name and a syslog server IP address.

Step 5 Click **Save**.

Configuring a Local Management User Template

Follow these steps to add or modify a local management user template.

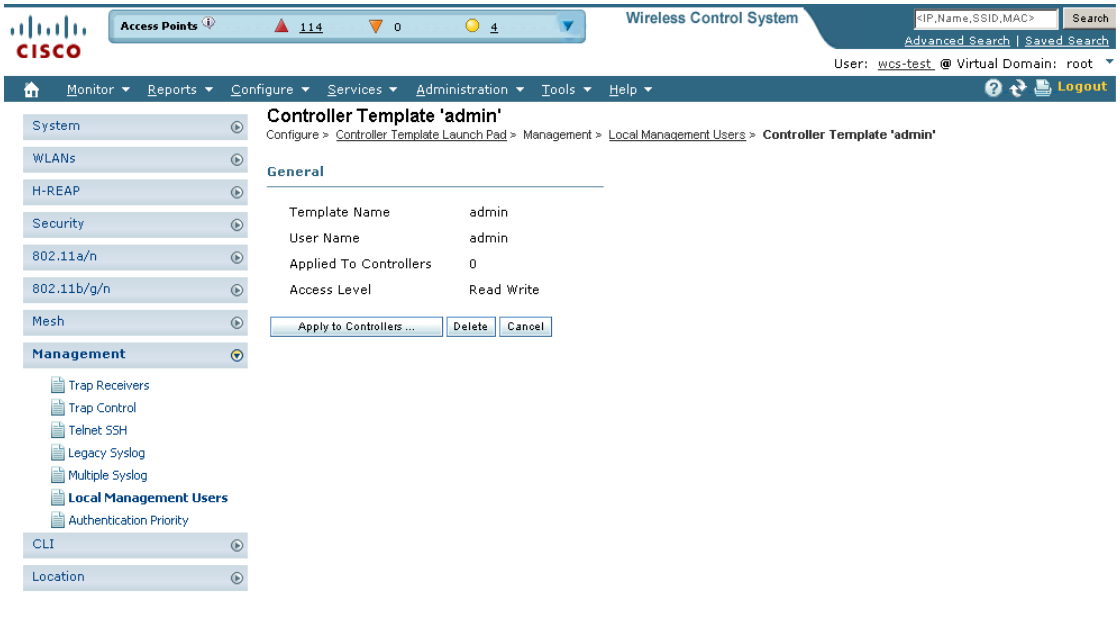
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Local Management Users** or choose **Management > Local Management Users** from the left sidebar menu. The Management > Local Management Users Template appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the user name 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, click **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 (see Figure 12-61).

Figure 12-61 Local Management Users Template



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 Re-enter the password.

Step 8 Use the Access Level drop-down list to choose either Read Only or Read Write.

Step 9 Click **Save**.

Configuring a User Authentication Priority Template

Management user authentication priority templates control the order in which authentication servers are used to authenticate a controller's management users. Follow these steps to add a user authentication priority template or make modifications to an existing template.

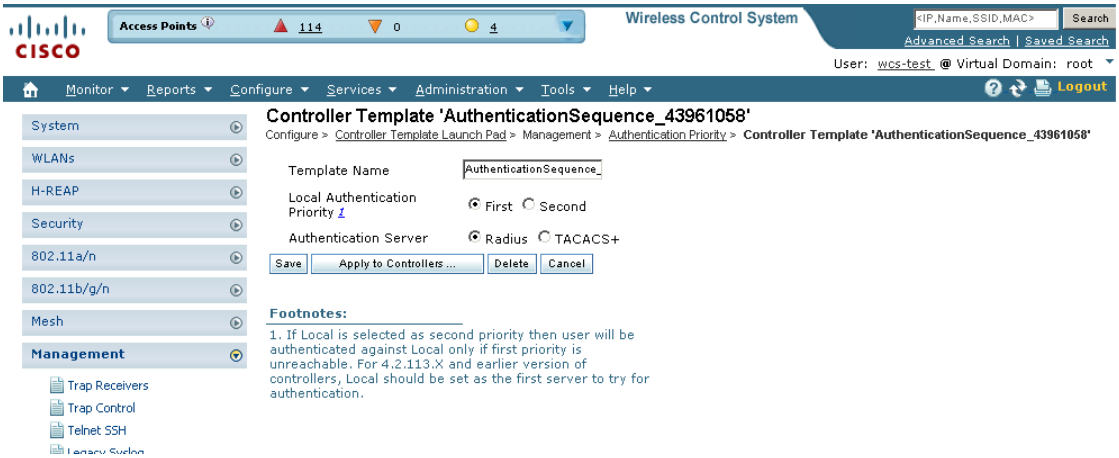
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Authentication Priority** or choose **Management > Authentication Priority** from the left sidebar menu. The Management > Local Management Users Template 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, click **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 (see Figure 12-62).

Figure 12-62 User Authentication Priority Template



Step 4 Enter a template name.

Step 5 The local server is tried first. Choose either **RADIUS** or **TACACS+** to try if local authentication fails.

Step 6 Click **Save**.

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 WCS. These templates are meant for provisioning features in multiple controllers for which there is no SNMP support or custom WCS 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. See the "CLI Session" section on page 18-41 for information on setting protocol user preferences.

Follow these steps to add or modify a CLI template.

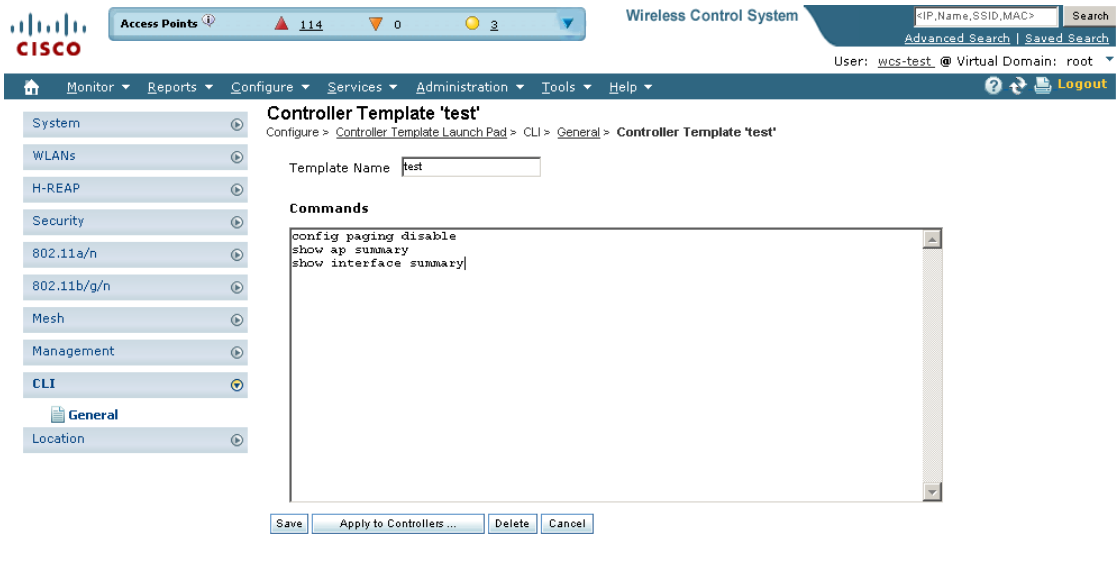
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **CLI > General** or choose **CLI > General** from the left sidebar menu. The CLI > 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.

Step 3 If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Command Line Interface General template page appears (see Figure 12-63).

Figure 12-63 Command Line Interface Template



Step 4 If you are adding a new template, provide a name that you are giving to this string of commands. If you are making modifications to an existing template, the Template Name field cannot be modified.

Step 5 In the Commands page, enter the series of CLI commands.

Step 6 Click **Save** to save the CLI commands to the WCS database without applying to the selected controllers or **Apply to Controllers** to save the commands to the WCS 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.

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 Settings

Follow these steps to add or modify a location setting template.

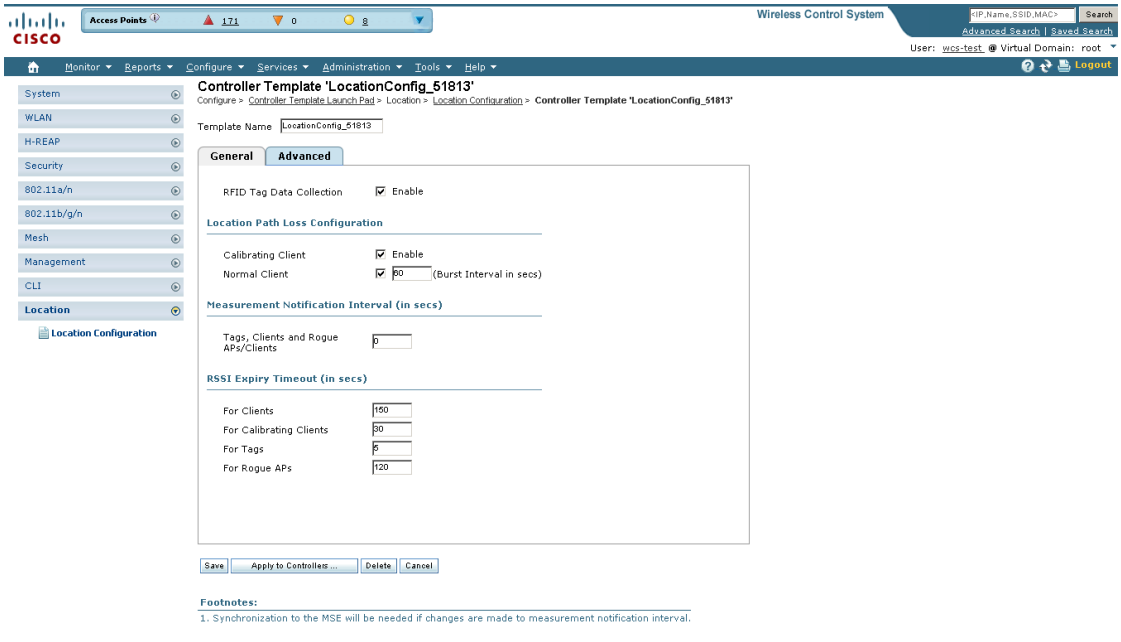
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Location > Location Configuration** or choose **Location > Location Configuration** from the left sidebar menu. The Location > Location Configuration 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.

Step 3 If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The template page appears (see Figure 12-64).

Figure 12-64 Location Configuration Template



Step 4 Check the **RFID Tag Data Collection** check box to enable tag collection. 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.

Step 5 Check 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 Check the **Normal Client** check box to have a non-calibrating client. No S36 or S60 requests are transmitted to the client.

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 Check the **Calibrating Client Multiband** check box to send S36 and S60 packets (where applicable) on all channels. Calibrating clients must be enabled on the general panel.

Step 15 Click **Save**.

Applying Controller Templates

You can apply a controller template to a controller.

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Using the left sidebar menu, choose the category of templates to apply. A list of devices is shown.

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.

Note In the Configure > Controllers page, you can see which templates are applied to controllers. See the "Displaying Templates Applied to Controller" section on page 10-10 for further information. You can also discover templates in the Configure > Controllers page. See the "Discovering Templates from Controllers" section on page 10-9 for more information.

Step 5 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(s), 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. Check 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 list the name of each configuration group along with the mobility group name and the number of controllers included.

b. Check 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 6 Click **OK**.

Deleting a Controller Template

Follow these steps to delete a controller template.

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click the template type to open its template list page.

Step 3 Click the check box(es) of the template(s) that you want to delete.

Step 4 From the Select a command drop-down list, choose **Delete Templates**, and click **Go**.

Step 5 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 6 Check the check box of each controller from which you want to remove the template.

Step 7 Click **OK** to confirm the deletion or **Cancel** to close this page without deleting the template.

Adding Access Point Templates

Follow these steps to add a new access point template.

Step 1 Choose **Configure > AP Configuration Templates > Autonomous AP** or **Lightweight AP**.

Step 2 Choose **Add Template** from the Select a command drop-down list, and click **Go**.

Step 3 Enter the template name.

Step 4 Describe the template.

Step 5 Click **Save**.

Configuring Access Point Templates

Follow these steps to configure a template of access point information that you can apply to one or more access points.

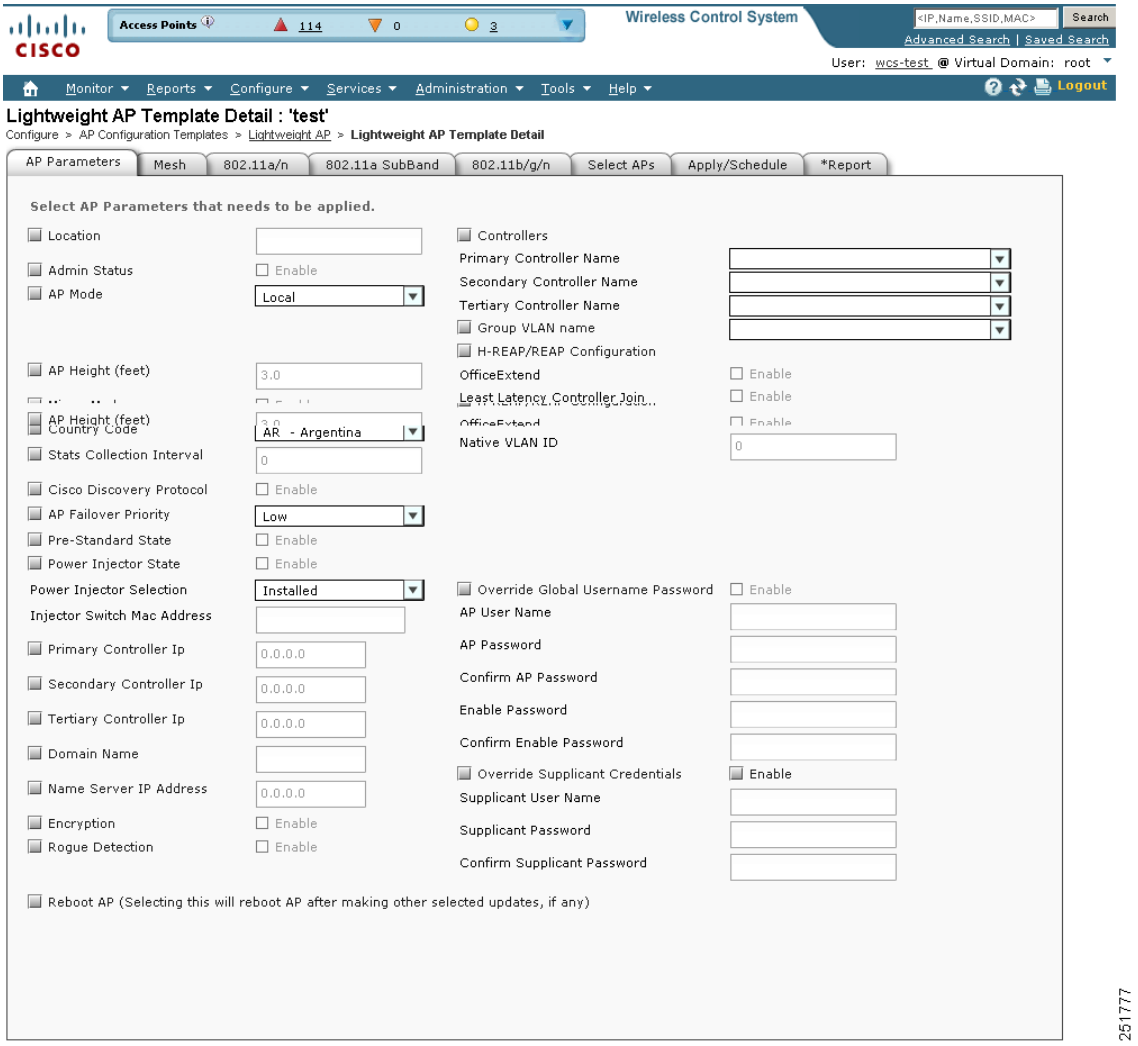
Step 1 Choose **Configure > AP Configuration Template > Autonomous AP** or **Lightweight AP**.

Step 2 In the Template Name column, click the template name you want to configure.

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.

Step 3 Click the **AP Parameters** tab. The AP/Radio Templates page appears (see Figure 12-65) if you chose Lightweight AP. If you chose Autonomous AP, the heading is Command Line Interface Templates.

Figure 12-65 AP/Radio Templates



Step 4 Select the Location check box and enter the access point location.

Step 5 Select both the **Admin Status** and **Enabled** check box to enable access point administrative status.

Note In order 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.

Step 6 Select the **AP Mode** check box and use the drop-down list to set the operational mode of the access point as follows:

- Local - Default
- Monitor - Monitor mode only.

Note Select 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. Then select the AP Monitor Mode Optimization check box and WIPS from the AP Monitor Mode Optimization drop-down list. You cannot use monitor mode optimization if wIPS is disabled. For more information on Cisco Adaptive wIPS, see the "wIPS" section on page 13-1 for more information.

- H-REAP/REAP - Cisco 1030 remote edge lightweight access point (REAP) used for Cisco 1030 IEEE 802.11a/b/g/n remote edge lightweight access points.

Note H-REAP must be selected in order to configure an OfficeExtend access point. When the AP mode is H-REAP, H-REAP configuration options display including the option to enable OfficeExtend AP and to enable Least Latency Controller Join. See the "Configuring Hybrid REAP" section on page 15-4 for further information.

- Rogue Detector - Monitors the rogue access points but does not transmit or contain rogue access points.
- Bridge

Note Changing the AP mode reboots the access point.

- Sniffer - The access point performs an inspection 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.

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 www.wildpackets.com/products/airopeek/overview.

Step 7 Select the **Enhanced wIPS engine** and the **Enabled** check box to enable.

Step 8 Select **None** or **wIPS** from the AP Monitor Mode Optimization drop-down list. You cannot choose wIPS if wIPS was not enabled in Step 7.

Step 9 Enter the access point height in feet. The height defaults to the floor height. The height must be greater than 3 feet and must not exceed the floor height. The specified height is applied to all selected access points in the template.

Note To change the height for a specific access point, go to **Monitor > Maps > Floor > Position Access Points**.

Step 10 You must click both the **Mirror Mode** and **Enabled** check box to enable access point mirroring mode.

Step 11 Click the check box to enable the country code drop-down list. For this access point, choose a country code selection to allow. 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's regulations.

Note Access points may not operate properly if they are not designed for use in your country. 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's regulatory domain. For a complete list of country codes supported per product, refer to:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html.

Note Changing the country code may cause the access point to reboot.

Step 12 Click to enable **Stats Collection Interval** and then enter the collection period (in seconds) for access point statistics.

Step 13 Click the **Cisco Discovery Protocol check box** and click **Enable** to allow CDP on a single access point or all access points. CDP is a device discovery protocol that runs on all Cisco manufactured equipment (such as routers, bridges, communication servers, and so on).

Step 14 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 overloaded, the higher-priority access points join the backup controller and disjoin the lower priority access points. Set the AP Failover Priority setting to low, medium, high, or critical.

Step 15 Choose pre-standard state if the access point is powered by a high power Cisco switch. Otherwise, it should be disabled.

Step 16 You can now manipulate power injector settings through WCS without having to go directly to the controllers. If the Power Injector State is checked, use the Power Injector Selection drop-down list to choose from the possible values of unknown, installed, override, or foreign. If you choose foreign, you must enter the Injector Switch MAC address.

Step 17 Click the **Primary**, **Secondary**, or **Tertiary Controller IP** check box, and enter the appropriate IP addresses.

Step 18 Domain Name Server IP and Domain Name can be configured only on access points which have static IP.

Step 19 Check the check box to enable rogue detection. See the "Rogue Access Point Location, Tagging, and Containment" section on page 16-21.

Step 20 Check the **Encryption** check box to enable encryption.

Note DTLS data encryption is enabled automatically for OfficeExtend access points.

Step 21 (MESH ONLY) Enter a bridge group name (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. 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. For configurations where separate sectors are required, make sure that each RAP and its associated MAPs have separate bridge group names.

Step 22 (MESH ONLY) 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.

Step 23 (MESH ONLY) Choose the **Enable** option from the Ethernet Bridging drop-down list to enable Ethernet bridging for the mesh access point.

Step 24 Check the **SSH Access** check box to enable SSH access.

Step 25 Check the **Telnet Access** check box to enable Telnet access.

Note An OfficeExtend access point may 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.

Step 26 Click the check box if you want to enable link latency. 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 the controller but is especially useful for hybrid-REAP access points, for which the link could be a slow or unreliable WAN connection. See "Configuring Link Latency Settings for Access Points" section on page 9-40 for more information.

Note Link latency is supported for use only with hybrid-REAP access points in connected mode. Hybrid-REAP access points in standalone mode are not supported.

Step 27 Check the **Reboot AP** check box to enable a reboot of the access point after making any other updates.

Step 28 Select **Low**, **Medium**, **High**, or **Critical** from the drop-down list to indicate the access point's failover priority. The default priority is low.

Step 29 Choose the **Controllers** check box to enable the drop-down lists for the primary, secondary, and tertiary controller names.

Step 30 Choose the appropriate group VLAN name from the drop-down lists.

Step 31 Check the check box to enable H-REAP configuration (including VLAN support, native VLAN ID, and profile name VLAN mappings).

- OfficeExtend—The default is Enabled.

Note Clearing the check box simply disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point. If you want to clear the access point's configuration 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 access point's personal SSID, click **Reset Personal SSID** at the bottom of the access point details page.

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).

Step 32 When Least Latency Controller Join is 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.

Step 33 The SSID-VLAN Mappings section lists all the SSIDs of the controllers which are currently enabled for HREAP local switching. You can edit the number of VLANs from which the clients will get an IP address by clicking the check box and adjusting the value.

Step 34 Enter a native VLAN ID between the range of 1 to 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.

Step 35 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 are displayed in the lower right of the AP Parameters tab page. If you want to override the global credentials for this particular access point, select the **Override Global Username Password** check box. You can then enter a unique username, password, and enable password that you want to assign to this access point.

Step 36 Select the **Override Supplicant Credentials** check box to override supplicant credentials. If selected, enter a new supplicant username and password. Confirm the supplicant password. See "Configuring AP 802.1X Supplicant Credentials" section on page 12-9 for more information on supplicant credentials.

Step 37 Click the **Mesh** tab.

Step 38 To assign this access point to a bridge group, enter a name for the group in the Bridge Group Name field. The name can be up to 10 characters.

Note Bridge groups are used to logically group the mesh access points to avoid having two networks on the same channel communicating with each other. 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. For configurations where separate sectors are required, make sure that each RAP and its associated MAPs have separate bridge group names.

Step 39 Choose a 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 The 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 40 Choose **Enabled** or **Disabled** from the Ethernet Bridging drop-down list.

Step 41 Use the Role drop-down list to choose MAP or RAP. Choose MAP (MeshAP) if the 1520 series access point has a wireless connection to the controller. Choose RAP (RootAP) if the 1520 series access point has a wired connection to the controller.

Note At least one mesh access point must be set to RootAP in the mesh network.

Step 42 Click the **Select APs** tab. Use the drop-down list to apply the parameters by controller, floor area, outdoor area, or all. Click **Apply**.

Note When you apply the template to the access point, WCS checks to see if the access point supports REAP mode and displays the application status accordingly. Clicking Apply saves and applies the template parameters to the selected access points. After applying a report, it appears in the Apply Report tab.

Applying or Scheduling Templates

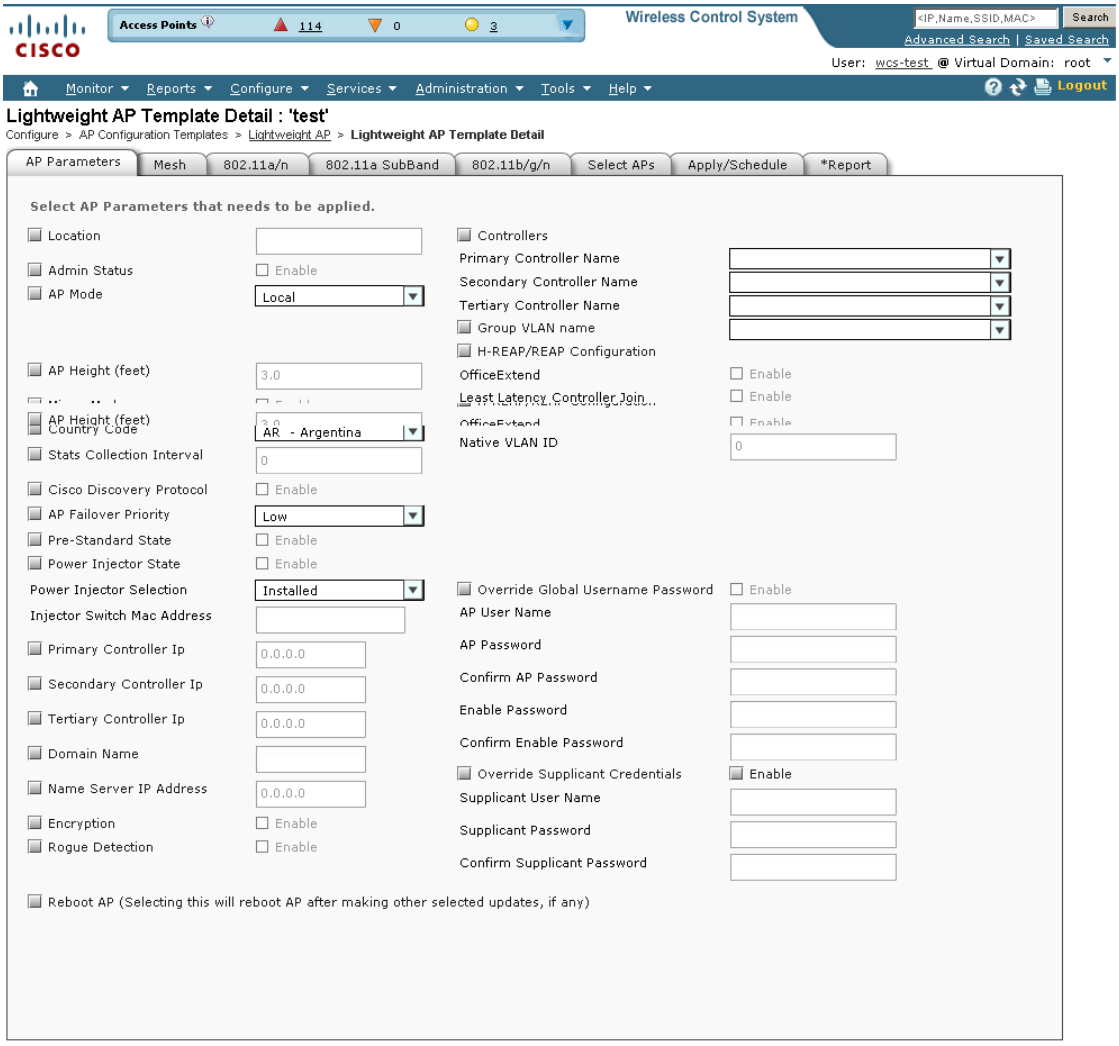
Follow these steps to apply the autonomous access point and lightweight radio templates to all the controllers in a config group.

Step 1 Choose **Configure > AP Configuration Templates > Lightweight AP** or **Autonomous AP**.

Step 2 Under Template Name, choose the access point template to which you want to add a schedule.

Step 3 Click the **Apply/Schedule** tab to access this page (see Figure 12-66).

Figure 12-66 Apply/Schedule Tab



Step 4 Click **Apply** to start the provisioning of access point and radio templates to all the controllers. After you apply, you can leave this page or log out of Cisco WCS. The process continues, and you can return later to this page and view a report.

A report is generated and appears in the Recent Apply Report page. It shows which templates 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 5 The scheduling function allows you to schedule a start day and time for provisioning. Check the **enable schedule** check box to enable the scheduling feature.

Step 6 Enter a starting date in the text box or use the calendar icon to choose a start date.

Step 7 Choose the starting time using the hours and minutes drop-down lists.

Step 8 Determine how often you want the provisioning of the template to occur. The choices are no recurrence, hourly, daily, or weekly. You can also specify a certain number of days in the Every ___ Days field.

Step 9 Click **Schedule** to start the provisioning at the scheduled time.

Configuring Scheduled Configuration Tasks

The Scheduled Configuration Tasks feature allows you to view, modify, and delete scheduled access point template and configuration group tasks. To access the Scheduled Configuration Tasks page, choose **Configure > Scheduled Configuration Tasks**.

- AP Template Tasks
- Config Group Tasks
- WLAN Configuration
- Download Software

AP Template Tasks

The AP Template Tasks page allows you to view, modify, delete, enable, or disable current access point template tasks. To access the AP Template Tasks page and view current access point template tasks, choose **Configure > Scheduled Configuration Tasks**.

- Modifying a Current AP Template Task, page 12-121
- Viewing AP Status Report for the Scheduled Task, page 12-121
- Enabling or Disabling a Current AP Template Task, page 12-122
- Viewing an AP Template Task History, page 12-122
- Deleting a Current AP Template Task, page 12-122

Modifying a Current AP Template Task

To modify a current access point template task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Choose the template name of the applicable task.

Step 3 In the AP Radio/Template page, click the **Apply/Schedule** tab.

Step 4 Make any necessary changes to the current schedule or AP template parameters and click **Schedule**.

Viewing AP Status Report for the Scheduled Task

The AP Status Report for the scheduled task includes the following information:

- AP Name—Lists all of the access points included in the scheduled access point template task.
- Ethernet MAC—Indicates the ethernet MAC addresses for the applicable access points.
- Controller—Indicates the associated controller for each of the applicable access points.
- Map—Displays the map location for the applicable access points.

- Status—Indicates whether the access point template has been successfully applied or not. The possible states are not initiated, success, failure, partial failure, and not reachable.
- Task Execution Time—Indicates the execution time of the scheduled task for the applicable access point.

To view the status report for the access points included in the scheduled task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Choose the AP Status Report for the applicable task.

Enabling or Disabling a Current AP Template Task

To enable or disable a current access point template task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Choose the check box of the scheduled task to be enabled or disabled.

Step 3 From the Select a command drop-down list, choose **Enable Schedule** or **Disable Schedule**, as applicable.

Step 4 Click **Go**.

Viewing an AP Template Task History

To view previously scheduled task reports, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Choose the check box of the applicable scheduled task.

Step 3 From the Select a command drop-down list, choose **View History**.

Step 4 Click **Go**.

Deleting a Current AP Template Task

To delete a scheduled access point template task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Choose the check box of the applicable scheduled task.

Step 3 From the Select a command drop-down list, choose **Delete Task(s)**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Config Group Tasks

The Config Group Tasks page allows you to view, modify, delete, enable, or disable current configuration group tasks.

A config group allows controllers to spawn across multiple config groups. A controller cannot be a member of more than one mobility group. Adding a controller to one mobility group removes the controller from the other mobility group if the controller is already a mobility group member.

To access the Config Group Tasks page and view current config group tasks, choose **Configure > Scheduled Configuration Tasks > ConfigGroup**.

- Modifying a Current AP Template Task, page 12-121
- Viewing Controller Status Report for the Scheduled Task, page 12-123
- Enabling or Disabling a Current Config Group Task, page 12-123
- Viewing a Config Group Task History, page 12-124
- Deleting a Current Config Group Task, page 12-124

Modifying a Current Config Group Task

To modify a current configuration group task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **ConfigGroup**.

Step 3 Choose the group name of the applicable task.

Step 4 In the Config Groups page, click the **Apply/Schedule** tab.

Step 5 Make any necessary changes to the current schedule and click **Schedule**.

Viewing Controller Status Report for the Scheduled Task

The Controller Status Report for the scheduled task includes the task execution results of templates applied to the controller.

To view the controller status report, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **ConfigGroup**.

Step 3 Choose the Controller Status Report for the applicable task.

Enabling or Disabling a Current Config Group Task

To enable or disable a current configuration group task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **ConfigGroup**.

Step 3 Choose the check box of the scheduled task to be enabled or disabled.

Step 4 From the Select a command drop-down list, choose **Enable Schedule** or **Disable Schedule**, as applicable.

Step 5 Click **Go**.

Viewing a Config Group Task History

To view previous scheduled task reports, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **ConfigGroup**.

Step 3 Choose the check box of the applicable scheduled task.

Step 4 From the Select a command drop-down list, choose **View History**.

Step 5 Click **Go**.

Deleting a Current Config Group Task

To delete a scheduled configuration group task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **ConfigGroup**.

Step 3 Choose the check box of the applicable scheduled tasks.

Step 4 From the Select a command drop-down list, choose **Delete Task(s)**.

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the deletion.

WLAN Configuration

To view and manage all scheduled WLAN tasks in WCS, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **WLAN Configuration** to open the WLAN Configuration Task List page.

Note Select the Task Name link to open the WLAN Schedule Detail page. In this page, you can modify the date and time of the scheduled task.

Step 3 Use the Select a command drop-down list located in the WLAN Configuration Task List page to enable, disable, or delete selected tasks.

- Enable Schedule—Enable the task if its schedule is disabled on the server.

- Disable Schedule—Disable the running scheduled task on the server. Once disabled, the task will not run at the scheduled time. You can re-enable the task at a later time.
- View History—View the execution results for individual WLAN tasks including reasons for any failures.
- Delete Task(s)—Delete the selected task from the WCS server.

Download Software

By using this feature you can schedule tasks for downloading software to controllers. The Download Software Tasks page allows you to add, delete, view, enable, or disable scheduled download software tasks. To access the Download Software Tasks page and view current download software tasks, choose **Configure > Scheduled Configuration Tasks > Download Software**.

The Download Software Tasks list page displays the following information:

- Task Name—Specifies the template name.
- Image Name—Specifies the image file name.
- Download Type—Specifies the download type.
- Selected Controllers—Specifies the number of controllers that you have selected.
- Schedule Run—Specifies the time at which the task is scheduled to run.
- Reboot Type—Specifies the reboot type.
- Status—Indicates one of the following task statuses:
  - Not initiated—The task is yet to start the download software and will start at the scheduled time. When the task is in this state, you can click the Task Name or Selected Controllers link to edit the task.
  - Disabled—The task is disabled and will not run at the scheduled time. This is the default state for a task when it is created without selecting any controllers. When the task is in this state, you can click the Task Name or Selected Controllers link to edit the task.
  - Expired—The task did not run at the scheduled time (may be due to the WCS server was down). When the task is in this state, you can click the Task Name or Selected Controllers link to edit the task.
  - Enabled—The task is yet to start the download software and will start at the scheduled time. When the task is in this state, you can click the Task Name or Selected Controllers link to edit the task.
  - In progress—The task is currently downloading the software to the selected controllers. When the task is in this state, you cannot edit it.
  - Success—The task has completed the download software to the selected controllers successfully. When the task is in this state, you cannot edit it.
  - Failure—The task failed to download software to all the controllers. You can check the detailed status about the failures by using the View Scheduled Run Results command. When the task is in this state, you cannot edit it.
  - Partial Success—The task failed to download software to a subset of selected controllers. You can check the detailed status about the failures by using the View Scheduled Run Results command. When the task is in this state, you cannot edit it.

From the Select a command drop-down list, the following functions can be performed:

- Add a Download Software Task
- Modify a Download Software Task
- Select Controllers for Download Software Task
- View Download Software Results
- Delete a Download Software Task
- Enable or Disable a Download Software Task

Add a Download Software Task

To add a download software task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software** to open the Download Software Task List page.

Step 3 From the Select a command drop-down list, choose **Add Download Software Task**.

Step 4 Click **Go**. The New Download Software Task page appears.

Step 5 Configure the following information:

- General
  - Task Name—Enter a Scheduled Task Name to identify this scheduled software download task.
- Schedule Details
  - Download Type—Select the download type. Select the **Download software to controller** check box to schedule download software to controller or select the **Pre-download software to APs** check box to schedule the pre-download software to APs. If you select Download software to controller, specify the image details.

Note The pre-download option is displayed only when all selected controllers are using the version 7.0.x.x or later.

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.

  - Reboot Type—Indicates whether the reboot type is manual, automatic, or scheduled.

Note 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. Select 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. Select 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 email notifications, configure the WCS mail server in the Administration > Settings > Mail Server Configuration page.

- Image Details—Specify the TFTP or FTP Server Information:

Note Complete these details if you selected the Download software to controller option under Schedule Details.

TFTP—Specify the TFTP Server Information:

– From the **File is Located on** drop-down list, choose **Local machine** or **TFTP server**.

Note If you choose TFTP server, select the Default Server or add a New server using the Server Name drop-down list.

– Specify the IP address of the TFTP server. This is automatically populated if the default server is selected.

– Specify the local file name or click **Browse** to navigate to the appropriate file.

– If you selected TFTP server previously, specify the File Name.

FTP—Specify the FTP Server Information:

– FTP Credentials Information—Enter the FTP username, password, and port if you selected the FTP radio button.

– From the File is Located on parameter, choose **Local machine** or **FTP server**.

Note If you choose FTP server, select the Default Server or add a New server using the **Server Name** drop-down list.

– Specify the IP address of the FTP server. This is automatically populated if the default server is selected.

– Specify the local file name or click **Browse** to navigate to the appropriate file.

– If you selected FTP server previously, specify the File Name.

Step 6 Click **Save**.

Modify a Download Software Task

To modify a download software task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software**.

Step 3 Select the Task Name link to open the **Download Software Task** page.

Step 4 Make any necessary changes.

Note Any changes in Download Type (Download/Pre-download) or Server Type (FTP/TFTP) for the task in 'Enabled' state will set the task to 'Disabled' state and all the existing controllers will be disassociated from the task.

Step 5 Click **Save**.

Select Controllers for Download Software Task

This page lists all the supported controllers that can be selected for the scheduled image download/pre-download task.

To select a controller for scheduled image download, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software**.

Step 3 Click the Controller to open the **Download Software Task** details page.

Step 4 In the Download Software Task details page, Click **Select Controller** to view the controller list.

Note The Select Controllers page can also be accessed from Configure > Scheduled Configuration Tasks > Download Software. Click the hyperlink under the Select Controller column for any download task which is in Enabled, Disabled or in the Expired state.

Note If the pre-download option is chosen for the task, then the controllers with software version 7.0.x.x or later only will be listed.

Note Controllers with Reachability Status '**Unreachable**' cannot be selected for Download Software Task.

Step 5 Select the controllers for the scheduled image download task.

Step 6 Make any necessary changes.

Step 7 Click **Save**.

View Download Software Results

To view the Schedule Run Results report, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, select **Download Software**.

Step 3 Select the **Task Name** check box.

Step 4 From the Select a command drop-down list, choose **Schedule Run Results**.

Step 5 Select the controller for which you want to view the report.

Step 6 Click **Go**. The Schedule Run Results page provides the information:

- IP Address—The IP address of the controller to which the software to be downloaded.
- Controller Name—Name of the controller.
- Scheduled Run Time—Scheduled time of the download process.
- Last Updated Time—Last update time of the schedule download status (or result).
- Transfer Status—Current download status of the image in controller. For example, Not Initiated, Wrong file Type, Writing the code into flash, Transfer Successful.
- Reboot Status—Reboot status of the controller. For example, NA (if the reboot type is “Manual”), Reboot failed, Reboot Successful.
- Details—Detailed status about the download and reboot process.

Delete a Download Software Task

To delete a scheduled download software task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software**.

Step 3 Select the check box of the applicable scheduled task.

Step 4 From the Select a command drop-down list, choose **Delete Download Software Task**.

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the deletion.

Enable or Disable a Download Software Task

To enable or disable a download software task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software**.

Step 3 Select the check box of the scheduled task to be enabled or disabled.

Step 4 From the Select a command drop-down list, choose **Enable Schedule** or **Disable Schedule**, as applicable.

Step 5 Click **Go**.

Configuring Radio Templates

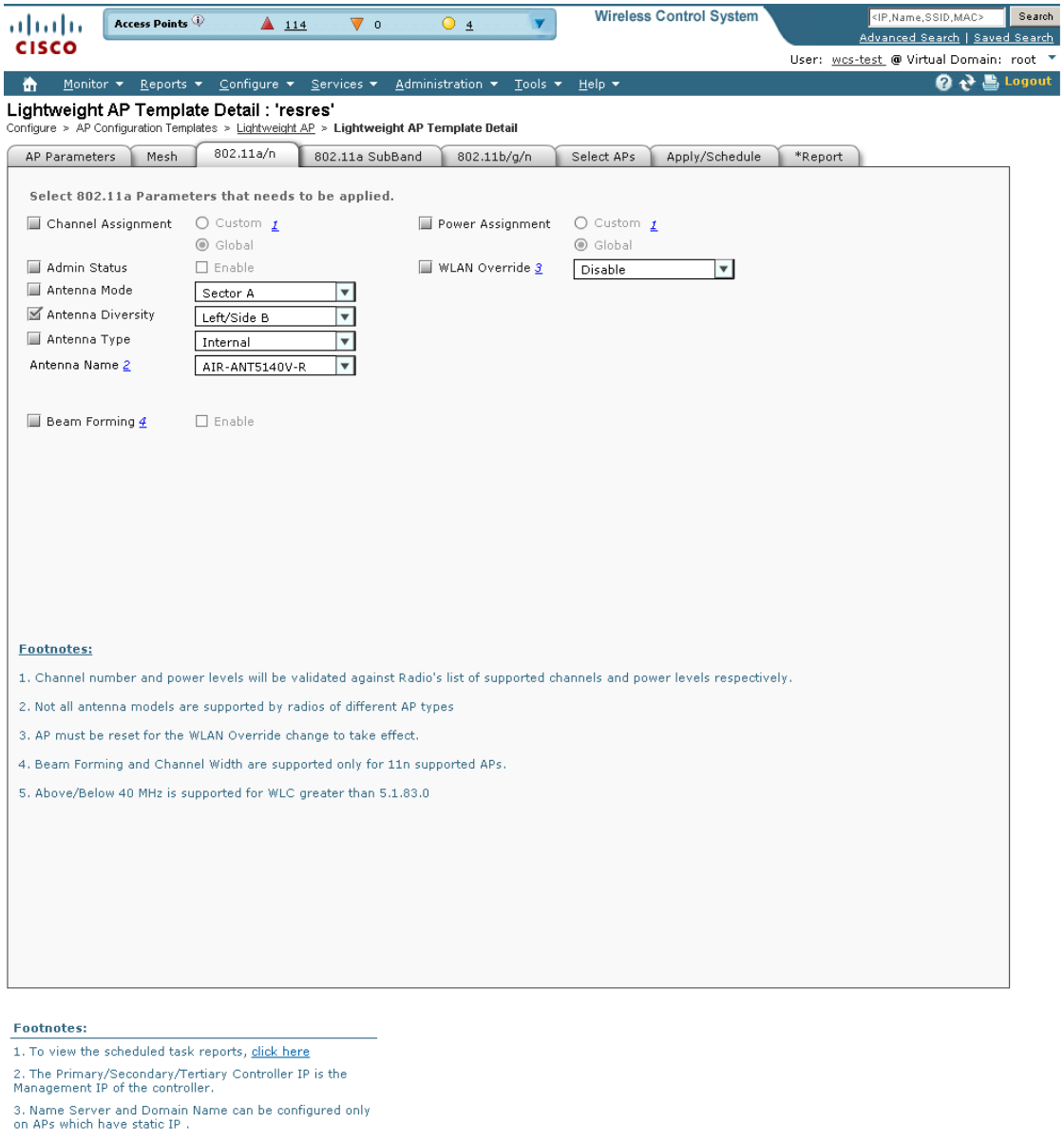
This page allows you to configure a template of radio information that you can apply to one or more access points.

Step 1 Choose **Configure > AP Configuration Templates > Lightweight AP**.

Step 2 From the Template Name column, click the template name you want to configure.

Step 3 Click the **802.11a/n or 802.11b/g/n** tab. The AP/Radio Templates page appears (see Figure 12-67).

Figure 12-67 802.11a/n Parameters



Step 4 Click the Channel Assignment check box to enable it. To choose a specific channel, click **Custom** and use the drop-down to designate the channel number. Otherwise, click **Global**.

Note The channel assignment is validated the radio's list of supported channels.

Step 5 Click both the **Admin Status** and **Enabled** check box to enable access point administrative status.

Step 6 Use the Antenna Mode drop-down list to choose the antenna model. The choices are omni, sector A, and sector B.

Note Not all antenna models are supported by radios of different access point types.

Step 7 For external antennas, choose one of the following:

- Enabled—Use this setting to enable diversity on both the left and right connectors of the access point.
- Left/Side B—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's left connector.
- Right/Side A—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's right connector.

For internal antennas, choose one of the following:

- Enabled—Use this setting to enable diversity on both Side A and Side B.
- Left/Side B—Use this setting to enable diversity on Side B (rear antenna) only.
- Right/Side A—Use this setting to enable diversity on Side A (front antenna) only.

Step 8 Click to enable Antenna Type and use the drop-down list to specify if the antenna is external or internal.

Step 9 Use the Antenna Name drop-down list to determine whether the antenna is a Kodiak directional, AIR-ANT1000, CUSH-S5157WP, etc.

Step 10 Select the Power Assignment check box and choose the power level currently being used to transmit data. (Some PHYs also use this value to determine the receiver sensitivity requirements.) If you choose Global, the power level is assigned by dynamic algorithm. If you choose Custom, you can select a value using the drop-down list. Power level 1is the maximum.

Step 11 Enable or disable WLAN override for this access point. When you enable WLAN override, the operating system displays a table showing all current Cisco WLAN Solution WLANs. In the table, choose WLANs to enable WLAN operation and deselect WLANs to disallow WLAN operation for this access point 802.11b/g Cisco Radio.

Note The access point must be reset for the WLAN override change to take effect.

Step 12 Enable or disable ClientLink for the access point radios per interface. This feature is only supported for legacy 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.

Step 13 Select the **CleanAir** check box for controllers whose version is 7.0 (for CleanAir supported APs).

Step 14 Select the **Enable** check box to enable CleanAir.

Selecting Access Points

After you have completed the radio template configuration, you must pick the access point to which these attributes are applied. Follow these steps to select access points.

Step 1 Click the **Select APs** tab.

Step 2 Use one of the search criterias to choose the access points and click **Search**. For example, you can search for access points that this template was last saved or search by controller name, by floor area, etc. The search criterias change based on the selection you choose.

The AP name, ethernet MAC, controller and map information appears.

Step 3 Click the check box in the AP Name column and select to which access points you want the access point and radio parameters applied. You can also click the **Select All** or **Unselect All** options.

Step 4 Click **Save** to save the parameter selection or click **Apply** to save and apply the access point and radio parameters to the selected access points.

Applying the Report

After access points are selected and applied, click the **Apply Report** tab.

CHAPTER 13

Mobility Services

This chapter briefly describes the CAS or wIPS services that Cisco WCS supports and gives steps for mobility procedures that are common across all services. You can refer to the Cisco Context-Aware Services documentation with the provided links for additional CAS and wIPS configuration and management details.

CAS

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

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. For details on tag and client licenses, refer to the *Cisco 3350 Mobility Services Engine Release Note* at:

http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html.

wIPS

The Cisco Adaptive Wireless IPS (wIPS) is an advanced approach to wireless threat detection and performance management. Cisco Adaptive wIPS combines network traffic analysis, network device and topology information, signature-based techniques and anomaly detection to deliver highly accurate and complete wireless threat prevention.

Note wIPS functionality is not supported for non-root partition users.

MSE Services Co-Existence

Starting from MSE Release 6.0, you can enable multiple services (Context Aware and wIPS) to run concurrently. Prior to version 6.0, mobility services engines could only support one active service at a time.

The following must be considered with co-existence of multiple services:

- Co-existence of services may be impacted by license enforcement. As long as the license is not expired, you can enable multiple services.

  Note Limits for individual services differ. For example, a low-end mobility services engine (MSE-3310) tracks a total of 2,000 CAS elements; a high-end mobility services engine (MSE-3350) tracks a total of 18,000 CAS elements.
  A low-end mobility services engine has a maximum limit of 2,000 wIPS elements; a high-end mobility services engine has a maximum limit of 3,000 wIPS elements. See the license order guide for the valid combination matrix.

- Expired evaluation licenses prevent the services from coming up.
- If a CAS license is added or removed, this process restarts all services on the mobility services engine including wIPS. If a wIPS license is added or removed, the process does not impact CAS; only wIPS restarts.
- Other services can be enabled in evaluation mode even if a permanent license for the maximum number of elements has been applied.

  Whenever one of the services has been enabled to run with its maximum license, another service can not be enabled to run concurrently because the capacity of the MSE would not be sufficient to support both services concurrently. For example, on MSE-3310, if you install a wIPS license of 2000, then you can not enable CAS to run concurrently. However, evaluation licenses are not subject to this limitation.

Note See the "MSE License Information" section on page 18-70 for more information on mobility services engine licensing.

Adding a Mobility Services Engine to Cisco WCS

To add a Cisco 3300 Series Mobility Services Engine to WCS, log into WCS and follow these steps:

Step 1 Verify that you can ping the mobility service engine that you want to add from Cisco WCS.

Step 2 Choose **Services > Mobility Services** to display the Mobility Services page.

Step 3 From the Select a command drop-down list, select **Add Mobility Services Engine** and click **Go**.

Step 4 In the Device Name text box, enter a name for the mobility services engine.

Note An MSE is added only if a valid IP address is entered. The Device Name helps you distinguish between devices if you have multiple WCSs with multiple MSEs, but it is not considered when validating an MSE.

Step 5 In the IP Address text box, enter the mobility services engine's IP address.

Step 6 (Optional) In the Contact Name text box, enter the name of the mobility services engine administrator.

Step 7 In the User Name and Password text boxes, enter the username and password for the mobility services engine.

The default username and password are both *admin*.

Note If you changed the username and password during the automatic installation script, enter those values here. If you did not change the default passwords, Cisco strongly recommends that you rerun the automatic installation script and change the username and password.

Step 8 Click **Next**. The Select Mobility Service page appears.

Note If you click **Cancel**, the MSE is not added. Any services that are already running on MSE are maintained, but if you want a change to a service to be accepted, you must complete Step 10.

Step 9 Click the circle next to the service(s) that you want to enable.

Step 10 Click **Save**.

Note After adding a new mobility services engine, you can synchronize network designs (floor, campus, building, and outdoor maps) and event groups on the local mobility services engine with Cisco WCS. You can also choose to synchronize the mobility services engine with a specific controller or with a wired switch. You can do this synchronization immediately after adding a new mobility services engine or at a later time. To synchronize the local and Cisco WCS databases, continue to the "Synchronizing Cisco WCS and a Mobility Services Engine" section on page 13-4.

Deleting a Mobility Services Engine from the Cisco WCS

To delete a mobility services engine from the Cisco WCS database, follow these steps:

Step 1 Click **Services > Mobility Services** to display the Mobility Services page.

Step 2 Select the mobility services engine(s) to be deleted by checking the corresponding check box(es).

Step 3 From the Select a command drop-down list, select **Delete Service(s)**, and click **Go**.

Step 4 Click **OK** to confirm that you want to delete the selected mobility services engine from the WCS database.

Step 5 Click **Cancel** to stop deletion.

Keeping the Mobility Services Engines Synchronized

This section describes how to synchronize Cisco WCS and mobility service engines manually and automatically.

After adding a mobility services engine to Cisco WCS, you can synchronize network designs (floor, campus, building, and outdoor maps), event groups, or controller information (name and IP address) with the mobility services engine.

Note Be sure to verify software compatibility between the controller, Cisco WCS, and the mobility services engine before synchronizing. See the latest mobility services engine release note at the following link: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html.

Note Communication between the mobility services engine and Cisco WCS and the controller is in universal time code (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 Cisco WCS server. An NTP server is required to automatically synchronize time between the controller, Cisco WCS, and the mobility services engine.

Synchronizing Cisco WCS and a Mobility Services Engine

This section describes how to synchronize Cisco WCS and mobility services engines manually and smartly.

After adding a mobility services engine to Cisco WCS, you can synchronize network designs (campus, building, floor, and outdoor maps), controllers (name and IP address), specific Catalyst Series 3000 and 4000 switches, and event groups with the mobility services engine.

- Network Design—Is 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.
- Controller—A selected controller that is associated and regularly exchanges location information with a mobility services engine. Regular synchronization ensures location accuracy.

- Switches (wired)—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 4000 series: 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
- Event Groups—A group of predefined events that define triggers that generate an event. Regular synchronization ensures that the latest defined events are tracked.

Note Be sure to verify software compatibility between the controller, Cisco WCS, and the mobility services engine before synchronizing. See the latest mobility services engine release note 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 and Cisco WCS 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 Cisco WCS server. An NTP server is required to automatically synchronize time between the controller, Cisco WCS, and the mobility services engine.

To synchronize network designs, a controller, a Catalyst switch, or event group with the mobility services engine, follow these steps:

Step 1 Choose **Services > Synchronize Services**.

Four menu items appears with the following headings: Network Designs, Controllers, Switches, and Event Groups.

Step 2 Choose the appropriate menu option (network designs, controllers, wired switches, or event groups).

To assign a network design to a mobility services engine:

a. On the synchronization page, choose Network Designs from the menu on the left side.

b. Choose all the maps to be synchronized with the mobility services engine.

Note Through Release 6.0, you can assign only a campus level to a mobility services engine. Starting with Release 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.

c. Click **Change MSE Assignment**.

d. Select the mobility services engine to which the maps are to be synchronized.

e. Click either of the following in the MSE Assignment dialog box:
   - OK—Saves the mobility services engine assignment. The following message appears in the Messages column of the Network Designs page.

– Cancel—Discards the changes to mobility services engine assignment and returns to the Network Designs page.

You can also select one or more maps and click **Reset** to undo the yellow button assignments for those maps.

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.

Step 3 Click **Synchronize** to update the mobility services engine(s) database(s).

When items are synchronized, a green, two-arrow icon appears in the Sync. Status column for each synchronized entry.

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 Cisco WCS and a Mobility Services Engine, page 13-4 for more information.

Configuring Automatic Database Synchronization and Out of Sync Alerts

Manual synchronization of Cisco WCS and mobility services engine databases is immediate. However, future deployment changes (such as changes to maps and access point positions) can yield incorrect location calculations and asset tracking until resynchronization reoccurs.

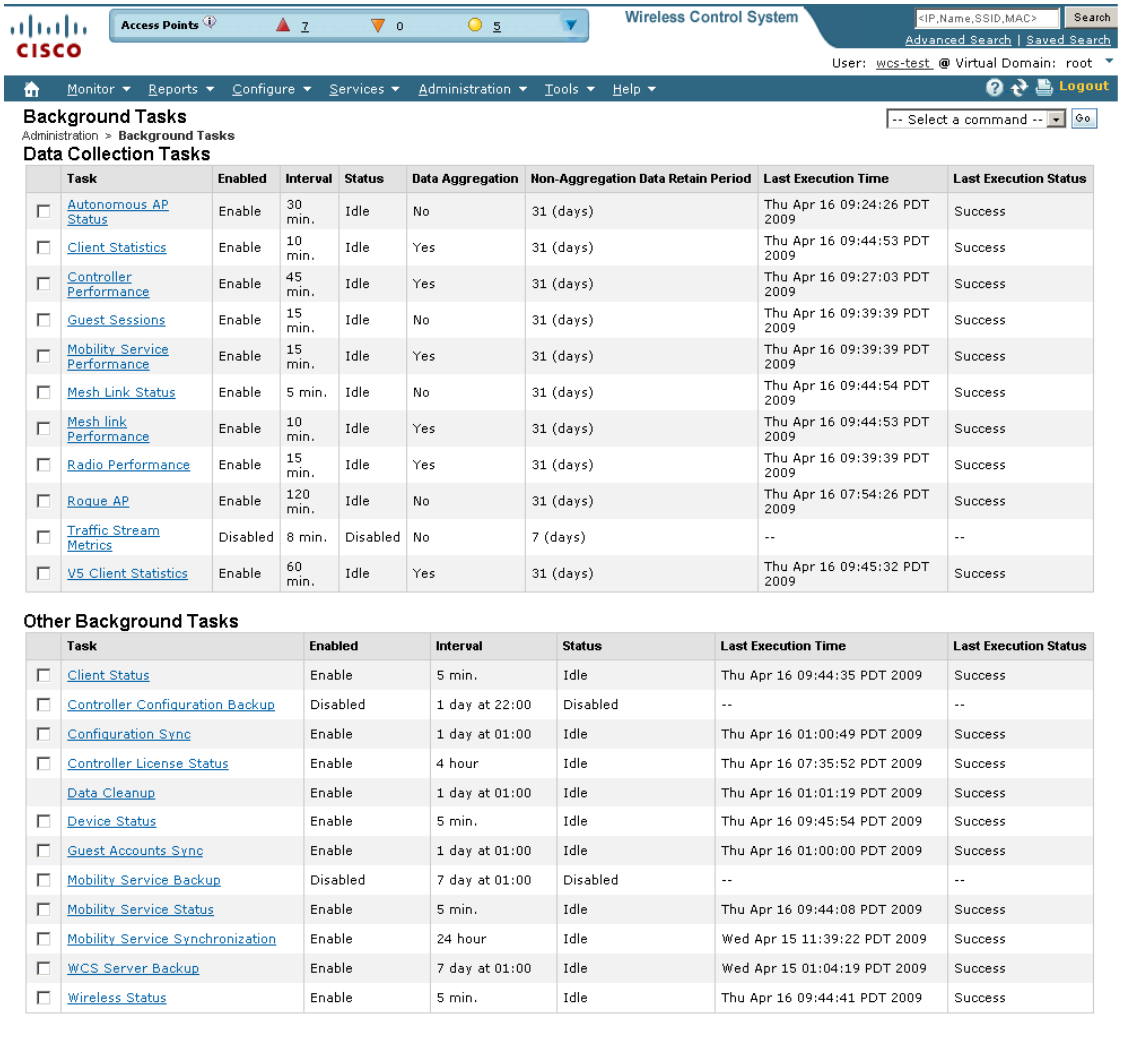
To prevent out-of-sync conditions, use Cisco WCS to enable smart synchronization. This policy ensures that synchronization between Cisco WCS and mobility services engine databases is triggered periodically and any related alarms are cleared.

To configure smart synchronization, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

The Background Tasks summary page appears (see Figure 13-1).

Figure 13-1 Administration > Background Tasks



Task	Enabled	Interval	Status	Data Aggregation	Non-Aggregation Data Retain Period	Last Execution Time	Last Execution Status
Autonomous AP Status	Enable	30 min.	Idle	No	31 (days)	Thu Apr 16 09:24:26 PDT 2009	Success
Client Statistics	Enable	10 min.	Idle	Yes	31 (days)	Thu Apr 16 09:44:53 PDT 2009	Success
Controller Performance	Enable	45 min.	Idle	Yes	31 (days)	Thu Apr 16 09:27:03 PDT 2009	Success
Guest Sessions	Enable	15 min.	Idle	No	31 (days)	Thu Apr 16 09:39:39 PDT 2009	Success
Mobility Service Performance	Enable	15 min.	Idle	Yes	31 (days)	Thu Apr 16 09:39:39 PDT 2009	Success
Mesh Link Status	Enable	5 min.	Idle	No	31 (days)	Thu Apr 16 09:44:54 PDT 2009	Success
Mesh link Performance	Enable	10 min.	Idle	Yes	31 (days)	Thu Apr 16 09:44:53 PDT 2009	Success
Radio Performance	Enable	15 min.	Idle	Yes	31 (days)	Thu Apr 16 09:39:39 PDT 2009	Success
Rogue AP	Enable	120 min.	Idle	No	31 (days)	Thu Apr 16 07:54:26 PDT 2009	Success
Traffic Stream Metrics	Disabled	8 min.	Disabled	No	7 (days)	--	--
V5 Client Statistics	Enable	60 min.	Idle	Yes	31 (days)	Thu Apr 16 09:45:32 PDT 2009	Success

Task	Enabled	Interval	Status	Last Execution Time	Last Execution Status
Client Status	Enable	5 min.	Idle	Thu Apr 16 09:44:35 PDT 2009	Success
Controller Configuration Backup	Disabled	1 day at 22:00	Disabled	--	--
Configuration Sync	Enable	1 day at 01:00	Idle	Thu Apr 16 01:00:49 PDT 2009	Success
Controller License Status	Enable	4 hour	Idle	Thu Apr 16 07:35:52 PDT 2009	Success
Data Cleanup	Enable	1 day at 01:00	Idle	Thu Apr 16 01:01:19 PDT 2009	Success
Device Status	Enable	5 min.	Idle	Thu Apr 16 09:45:54 PDT 2009	Success
Guest Accounts Sync	Enable	1 day at 01:00	Idle	Thu Apr 16 01:00:00 PDT 2009	Success
Mobility Service Backup	Disabled	7 day at 01:00	Disabled	--	--
Mobility Service Status	Enable	5 min.	Idle	Thu Apr 16 09:44:08 PDT 2009	Success
Mobility Service Synchronization	Enable	24 hour	Idle	Wed Apr 15 11:39:22 PDT 2009	Success
WCS Server Backup	Enable	7 day at 01:00	Idle	Wed Apr 15 01:04:19 PDT 2009	Success
Wireless Status	Enable	5 min.	Idle	Thu Apr 16 09:44:41 PDT 2009	Success

Step 2 Select the **Mobility Service Synchronization** check box. Select **Enable Task** from the Select a command drop-down list if not already enabled. Click **Go**.

Step 3 Click **Mobility Service Synchronization**. The Mobility Service Synchronization page appears.

Step 4 To set the mobility services engine to send out-of-sync alerts, select the **Out of Sync Alerts** check box in the Edit Task pane. By default, out-of-sync alarms are enabled.

Note Unselect the **Out of Sync Alerts** check box to disable forwarding of out-of-sync alarms.

Note For a summary of out of sync alerts that are sent, refer to the "Out-of-Sync Alarms" section on page 13-8.

Step 5 To enable smart synchronization, select the **Smart Synchronization** 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 will still be generated for these unassigned elements. For smart synchronization to apply to these elements, you need to manually assign them to a mobility services engine.
- When a mobility services engine is added to a WCS, the data in the WCS 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 WCS are removed automatically from mobility services engine.

Step 6 Enter the time interval in days and the time of day (xx:yy AM or PM) that the smart synchronization is to be performed.

By default, smart-sync is enabled.

Step 7 Click **Submit**.

For Smart controller assignment and selection scenarios, see Smart Controller Assigment and Selection Scenarios, page 13-8.

Smart Controller Assigment 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 MSE. If that access point changes its controller from controller A to controller B, then controller B is automatically synchronized to the mobility services engine.

Scenario 4

Delete all access points of controller A from a floor that is assigned to a mobility services engine. The controller A will be auto unassigned for that mobility services engine.

Out-of-Sync Alarms

Out-of-sync alarms are of minor severity (yellow), and are raised in response to the following conditions:

- Elements are modified in Cisco WCS (the auto-sync policy pushes these elements)
- Elements are modified in the mobility services engine (the auto-sync policy pulls these elements)
- Elements other than controllers exist in the mobility services engine database but not in Cisco WCS (the auto-sync policy pulls these elements)
- Elements are not assigned to any mobility services engine (the auto-sync policy does not apply)

Out-of-sync alarms are cleared when the following occurs:

- Mobility services engine is deleted

Note When you delete a mobility services engine, the out-of-sync alarms for that system are also deleted. In addition, if you delete the last available mobility services engine, the alarms for the following event: *elements not assigned to any server* will also be deleted.

- Elements are synchronized manually or automatically
- User manually clears the alarms (although the alarms may reappear in the future when the scheduled task is next executed)

Viewing Synchronization Information

This section describes how to view synchronization status and history.

Viewing Mobility Services Engine Synchronization Status

You can use the Synchronize Services feature in Cisco WCS to view the status of network design, controller, switch, and event group synchronization with a mobility services engine.

To view synchronization status, follow these steps:

Step 1 In Cisco WCS, choose **Services > Synchronize Services**.

Step 2 Select the applicable menu option (Network Designs, Controllers, Wired Switches, or Event Groups).

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 given server.

The Message column displays the reason for failure if the elements are out of sync.

You can also see the synchronization status of the floor to the mobility services engine on the Floor View page.

To access this page, go to **Monitor > Maps > System Campus >** *Building* **>** *Floor*

where *Building* is the building within the Campus and *Floor* is a specific floor in that campus building.

On the left side there is a menu option called MSE Assignment. This 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.

To view synchronization history, follow these steps:

Step 1 In Cisco WCS, choose **Services > Synchronization History**. The Synchronization History page appears.

Step 2 Table 13-1 lists and describes the text boxes that appear in the Synchronization History page.

Table 13-1 Synchronization History

Text Box	Description
Timestamp	The date and time at which the synchronization has happened.
Server	The mobility services engine server.
Element Name	The name of the element that was synchronized.
Type	The type of the element that was synchronized.
Sync Operation	The sync operation that was performed. It could either be an Update or an Add or Delete.
Generated By	The method of synchronization. It could either be Manual or Automatic.
Status	The status of the synchronization. It could be either Success or Failed.
Message	Any additional message about the synchronization.

Click the column headers to sort the entries.

Adding and Deleting Event Groups

You can add and delete event groups. Event groups help you organize your event definitions.

Adding Event Groups

To add an event group, follow these steps:

Step 1 Click **Services > Context Aware Notifications**.

Step 2 Click **Notification Settings** from the left sidebar menu.

Step 3 From the Select a command drop-down list, click **Add Event Group**, and click **Go**.

Step 4 Enter the name of the group in the Group Name text box.

Step 5 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 Click **Services > Context Aware Notifications**.

Step 2 Click **Notification Settings** from the left sidebar menu.

Step 3 Select the event group to delete by checking its corresponding check box.

Step 4 From the Select a command drop-down list, select **Delete Event Group(s)**, and click **Go**.

Step 5 In the panel that appears, click **OK** to confirm deletion.

Step 6 Click **Save**.

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.

Cisco WCS 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 information on deleting or testing event definitions.

To add an event definition, follow these steps:

Step 1 Choose **Services > Context Aware Notifications**.

Step 2 Click **Notification Settings** 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 At 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 could 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, select **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 could 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 area 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 will trigger 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, select 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 text box to 60 feet, an event notification will be generated if the monitored asset moves more than 60 feet away from the marker. 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, check the box next to the battery level (low, medium, normal) that will trigger 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 will trigger 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 will be generated if the trigger condition is met.

Note If you select 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.

Note Emergency and chokepoint events apply only to Cisco compatible extension tags version 1 (or later).

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, 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.

Note If you are defining a chokepoint, you must select the chokepoint after you add the condition.

To select a chokepoint, do the following:

1. Click **Select Chokepoint**. An entry page appears.
2. Select **Campus**, **Building**, and **Floor** from the appropriate drop-down lists.
3. Select 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 field next to the Select Checkpoint button.

Step 6 At 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 will receive 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, Cisco WCS 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. Select **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 checking 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 via e-mail.

  If you choose Mail, you need to choose the protocol for sending the 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.

Port Number auto-populates.

h. Click **Save**.

Step 7 At 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).

Planning for and Configuring Context-Aware Software

Context-Aware Software (CAS) resides on the mobility services engine. For more information on the CAS service, refer to the *Cisco Context-Aware Software Configuration Guide.*

Note If you have a location server, you can track or map non-Cisco CX tags.

Note Context-Aware Software was previously referred to as *Cisco location-based services*.

Chapter 4 of the *Cisco Conxtext-Aware Software Configuration Guide* contains the following information on configuring and viewing system properties on the mobility services engine:

- Configuring general properties
- Modifying NMSP parameters
- Viewing active sessions on a system
- Adding and deleting trap destinations
- Viewing and configuring advanced parameters

Chapter 5 of the *Cisco Context-Aware Software Configuration Guide* contains information on configuring and managing users and groups on the mobility services engine.

Chapter 6 of the *Cisco Context-Aware Software Configuration Guide* contains the following information on event notifications:

- Adding and deleting event groups
- Adding, deleting, and testing event definitions
- Viewing event notification summary
- Notifications cleared
- Notification message formats

Chapter 7 of the *Cisco Context-Aware Software Configuration Guide* contains the following information on the tools and configurations that can be used to enhance the location accuracy of elements (clients, tags, rogue clients, interferers and rogue access points):

- Planning for data, voice, and location deployment
- Creating and applying calibration models
- Inspecting location readiness and quality
- Inspecting location quality using calibration data
- Verifying location accuracy
- Using chokepoints to enhance tag location reporting
- Using Wi-Fi TDOA receiver to enhance tag location reporting
- Using tracking optimized monitor mode to enhance tag location reporting
- Defining inclusion and exclusion regions on a floor
- Defining a rail line on a floor
- Modifying context aware software parameters
- Enabling Location Services on Wired Switches and Wired Clients.
- Assigning a Catalyst Switch to Mobility Services Engine and Synchronizing

Chapter 8 of the *Cisco Context-Aware Software Configuration Guide* contains the following information on how to monitor the mobility services engine by configuring and viewing alarms, events, and logs and how to generate reports on system utilization and element counts:

- Working with alarms
- Working with events
- Working with logs
- Generating reports
- Monitoring wireless clients
- Monitoring tagged assets
- Monitoring chokepoints
- Monitoring Wi-Fi TDOA receivers
- Monitoring Wired Switches
- Monitoring Wired Clients
- Monitoring Interferers

Chapter 9 of the *Cisco Context-Aware Software Configuration Guide* contains the following information on backing up and restoring mobility services engine data and updating the mobility services engine software:

- Recovering a lost password
- Recovering a lost root password
- Backing up and restoring mobility services engine data
- Downloading software to mobility services engines
- Configuring the NTP server
- Defragmenting the mobility services engine database
- Rebooting the mobility services engine hardware
- Shutting down the mobility services engine hardware
- Clearing mobility services engine configurations

wIPS Planning and Configuring

With a fully integrated solution, Cisco can continually monitor wireless traffic on both the wired and wireless networks and can use that network intelligence to analyze attacks from many different sources of information to more accurately pinpoint and proactively prevent attacks versus waiting until damage or exposure has occurred. See *Cisco Adaptive Wireless IPS* documentation for the following information:

- WCS and wIPS integration overview
- Mobility services engines
- wIPS profiles
- Configuring SSID group list
- Viewing wIPS alarms
- Viewing wIPS events
- Configuring access points and access point templates
- policy alarm encyclopedia
- WCS security vulnerability assessment
- Rogue management
- Radio resource management

CHAPTER 14

Performing Maintenance Operations

This chapter provides routine procedures for maintaining Cisco WCS. It contains these sections:

- Verifying the Status of WCS, page 14-1
- Stopping WCS, page 14-2
- Backing Up the WCS Database, page 14-3
- Restoring the WCS Database, page 14-5
- Upgrading WCS, page 14-9
- Upgrading WCS in a High Availability Environment, page 14-15
- Upgrading the Network, page 14-15
- Reinitializing the Database, page 14-15
- Recovering the WCS Password, page 14-16

Verifying the Status of WCS

This section provides instructions for checking the status of WCS on either a Windows or Linux server.

Checking the Status of WCS on Windows

Follow these steps to check the status of WCS when it is installed as a Windows application or Windows service. You can check the status at any time.

Step 1 Log into the system as administrator.

Step 2 Perform one of the following:

- From the Windows Start menu, click **Programs > Wireless Control System> WCSStatus**.
- From the command prompt, navigate to the WCS installation directory (such as C:\Program Files\WCS7.0.X.X) and enter **WCSAdmin status**.

The WCSAdmin window appears and displays messages indicating the status of WCS.

Step 3 Close the WCSAdmin window when the Close button becomes active.

Checking the Status of WCS on Linux

Follow these steps to check the status of WCS when it is installed as a Linux application or Linux service. You can check the status at any time.

Step 1 Log into the system as **root**.

Step 2 Using the Linux CLI, perform one of the following:

- Navigate to the installation directory (such as /opt/WCS7.0.X.X) and enter **./WCSStatus**.
- Navigate to the installation directory (such as /opt/WCS7.0.X.X) and enter **WCSAdmin status**.

The CLI displays messages indicating the status of WCS.

Stopping WCS

This section provides instructions for stopping WCS on either a Windows or Linux server.

Stopping WCS on Windows

Follow these steps to stop WCS when it is installed as a Windows application or Windows service. You can stop WCS at any time.

Note If any users are logged in when you stop WCS, their WCS sessions stop functioning.

Step 1 Log into the system as administrator.

Step 2 Perform one of the following:

- From the shortcut location (defaulted to Windows Start menu > Programs > Cisco Wireless Control System A.B.C.D), select **StopWCS**.
- From the command prompt, navigate to the WCS installation directory (defaulted to C:\Program Files\WCSA.B.C.D\bin) and enter **StopWCS**.

  Note You can use **StopWCS** for a graceful shut down. A graceful shut down does not trigger the automatic failover. Use the CLI command **<WCSROOT>\nmsadmin.bat -switchover stop** to trigger automatic failover when shutting down WCS.

The WCSAdmin window appears and displays messages indicating that WCS is stopping.

Note If WCS is installed as a service, messages also appear to indicate that the Nms_Server service is stopping.

Step 3 Close the WCSAdmin window when the Close button becomes active.

Stopping WCS on Linux

Follow these steps to stop WCS when it is installed as a Linux application or Linux service. You can stop WCS at any time.

Note If any users are logged in when you stop WCS, their WCS sessions stop functioning.

Step 1 Log into the system as root.

Note To see which version of WCS you currently have installed, enter **nmsadmin.sh version**.

Step 2 Using the Linux CLI, perform one of the following:

- Navigate to the shortcut location (defaulted to /opt/WCSA.B.C.D) and enter **./StopWCS**.
- Navigate to the installation bin directory (defaulted to /opt/WCSA.B.C.D/bin) and enter **StopWCS**.

The CLI displays messages indicating that WCS is stopping.

Backing Up the WCS Database

This section provides instructions for backing up the WCS database. You can schedule regular backups through the WCS user interface or manually initiate a backup on either a Windows or Linux server.

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 backup and restore function if the backup is restored to a different device.

Scheduling Automatic Backups

Follow these steps to schedule automatic backups of the WCS database.

Step 1 Log into the WCS user interface.

Step 2 Click **Administration > Background Tasks** to display the Scheduled Tasks page.

Step 3 Click **WCS Server Backup** to display the Task > WCS Server Backup page.

Step 4 Select the **Enabled** check box.

Step 5 At the Report History Backup parameter, select the **Enabled** check box to run history backup.

Step 6 In the Max Backups to Keep text box, enter the maximum number of backup files to save on the server.

Range: 7 to 50

Default: 7

Note To prevent the WCS platform from running out of disk space, the server automatically deletes old backup files when the number of files exceeds the value entered for this text box.

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 WCS server. Therefore, Cisco recommends that you schedule backups to run when the WCS 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/root/WCSBackup directory using this format: *dd-mmm-yy_ hh-mm-ss*.zip (for example, 11-Nov-05_10-30-00.zip).

Performing a Manual Backup

This section provides instructions for backing up the WCS database on either a Windows or Linux server.

Backing Up the WCS Database (for Windows)

Follow these steps to back up the WCS database on a Windows server.

Step 1 Log into the system as administrator.

Step 2 Create a backup directory for the WCS database with no spaces in the name, such as C:\WCS7.0.X.X_Backup.

Note Make sure that the directory name does not contain spaces. Spaces can generate errors.

Step 3 Perform one of the following:

- Follow these steps from the Windows Start menu:

a. Click **Programs > Wireless Control System> Backup**. The Enter Information window appears.

b. Browse to the backup directory that you created and choose the filename or enter the full path of the backup directory that you created and a name for the backup file (such as C:\WCS7.0.X.X_Backup\Nov11) and click **OK**.

- Follow these steps from the command prompt:

a. Navigate to the WCS installation directory (C:\Program Files\WCS7.0.X.X\bin).

b. Enter **DBAdmin backup *backup-filename***, where *backup-filename* is the full path of the backup directory that you created plus a name for the backup file (such as C:\WCS7.0.X.X_Backup\Nov11).

The DBAdmin window appears and displays messages indicating the status of the backup.

Step 4 Close the DBAdmin window when the Close button becomes active.

Note In the example above, the backup file would appear in the C:\WCS7.0.X.X_Backup directory as Nov11.nmsbackup.

Backing Up the WCS Database (for Linux)

Follow these steps to back up the WCS database on a Linux server.

Step 1 Log into the system as root.

Step 2 Using the Linux CLI, navigate to the /opt/WCS7.0 directory (or any other directory).

Step 3 Create a backup directory for the WCS database with no spaces in the name (for example, **mkdir WCS7.0.X.X_Backup**).

Note Make sure that the directory name does not contain spaces. Spaces can generate errors.

Step 4 Perform one of the following:

- Navigate to the /opt/WCS7.0.X.0 directory (or the directory chosen during installation) and enter **./Backup**. Enter a name for the backup file when prompted (such as WCS7.0.X.X_Backup/Nov11).
- Navigate to the /opt/WCS7.0.X.X/bin directory (or the directory chosen during installation) and enter **DBAdmin backup *backup-filename***, where *backup-filename* is the full path of the backup directory that you created plus a name for the backup file (such as WCS7.0.X.X_Backup/Nov11).
- Using KDE or X-Windows, enter **DBAdmin - gui backup**, browse to the backup directory, and choose the file.

The CLI displays messages indicating the status of the backup.

Note In the example above, the backup file would appear in the WCS7.0.X.X_Backup directory as Nov11.nmsbackup.

Restoring the WCS Database

This section provides instructions for restoring the WCS database on either a Windows or Linux server.

Restoring the WCS Database (for Windows)

Follow these steps to restore the WCS database from a backup file on a Windows server. If you are restoring the WCS database in a high availability environment, refer to the "Restoring the WCS Database in a High Availability Environment" section on page 14-8.

Note The server may incorrectly perceive the amount of free space available during a restore if a FAT32 file system is used. Microsoft's recommended file system for Windows servers is NTFS.

Step 1 Log into the system as administrator.

Step 2 Perform one of the following:

- Follow these steps from the Windows Start menu:

a. Click **Start > Programs > Wireless Control System> Restore**. The DBAdmin and Enter Information window appears.

b. Browse to the backup directory that you created and choose the filename or enter the full path and filename of the backup file (such as C:\WCS7.0.X.X_Backup\Nov11.nmsbackup) and click **OK**.

< OR >

- Follow these steps from the command prompt:

a. Navigate to the WCS installation directory (C:\Program Files\WCS7.0.X.X\bin).

b. Enter **DBAdmin restore *backup-filename***, where *backup-filename* is the full path and filename of the backup file (for example, C:\WCS7.0.X.X_Backup\Nov11.nmsbackup).

Note When you perform a restore of a large database, you must instead enter **dbadmin.bat -gui -largedb restore**.

Note If you are restoring from WCS version 4.0.96.0, some previous client data may not be collected.

Step 3 If you have a large event table to migrate, you must limit the size of the event table. You cannot decline this process, but it generally only affects pre-5.1 to 5.2 or later migration. The following warning message appears:

WARNING: You are migrating from a pre-5.1 database to a post-5.1 database. This may take a very long time -- possibly several hours. You can considerably speed this migration by retaining only the most recent events from the restored database. Even if you do this, the event table will be repopulated within seven days. This does not affect current alarms. This does not affect the backed-up database.

Would you like to retain only recent events?

If you type **Y** or **Yes** (or click **Yes** from the GUI prompt), the restore retains only the most recent 40,000 events.

Note When you perform a restore of a UBC database, it is strongly recommended that you choose to retain only recent events.

Note You can also type **-dropoldevents** at the CLI prompt as an equivalent to answering yes here.

Step 4 Click **Yes** if a message appears indicating that WCS is running and needs to be shut down.

Step 5 The DBAdmin window appears and displays messages indicating that WCS is shutting down (if applicable) and the WCS database is being restored. Close the DBAdmin window when the Close button becomes active.

Note If the restore process shuts down WCS, a restart is attempted after a successful restore.

Restoring the WCS Database (for Linux)

Follow these steps to restore the WCS database from a backup file on a Linux server. If you are restoring the WCS database in a high availability environment, refer to the "Restoring the WCS Database in a High Availability Environment" section on page 14-8.

Step 1 If possible, stop all WCS user interfaces to stabilize the database.

Step 2 Log into the system as root.

Step 3 Using the Linux CLI, perform one of the following:

- Navigate to the /opt/WCS7.0.X.X directory (or the directory chosen during installation) and enter **./Restore** to start the restoration process. Enter the backup filename when prompted (such as WCS7.0.X.X_Backup/Nov11.nmsbackup).
- Navigate to the /opt/WCS7.0.X.X/bin directory (or the directory chosen during installation) and enter **DBAdmin restore *backup-filename***,
where *backup-filename* is the full path and filename of the backup file (such as WCS7.0.X.X_Backup/Nov11.nmsbackup).

  Note If you are restoring from a WCS version prior to 3.2, you must enter a directory rather than a backup file because tar/gzip did not exist prior to 3.2. Enter **DBAdmin restore *directory***, where *directory* is the backup directory that you created.

Step 4 Click **Yes** if a message appears indicating that WCS is running and needs to be shut down.

Step 5 The DBAdmin window appears and displays messages indicating that WCS is shutting down (if applicable) and the WCS database is being restored. Close the DBAdmin window when the Close button becomes active.

Note If the restore process shuts down WCS, a restart is attempted after a successful restore.

The CLI displays messages indicating that the WCS database is being restored.

Restoring the WCS Database in a High Availability Environment

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

Note If you attempt to restore the database while the status is set to HA enabled, unexpected results may occur.

Follow one of these procedures to change the status from HA enabled to HA not configured:

- Click the **Remove** button on the HA Configuration window (Administration > High Availability).
- Restart the primary server. Go to the secondary HealthMonitor GUI (https://<SecondaryWCS>:8082) and click **Failback**.
  - Use this method when one of the following instances has occurred:

    The primary server is down and failover has not been executed, so the secondary server is in SecondaryLostPrimary state.

    or

    The primary server is down and failover is already executed, so the secondary server is in the SecondaryActive state.

The primary server will now be in HA Not Configured mode, and you can safely restore the database.

Uninstalling WCS

This section provides instructions for uninstalling WCS on either a Windows or Linux server. You can uninstall WCS at any time, even while WCS is running.

Uninstalling WCS on Windows

Follow these steps to uninstall WCS on a Windows server.

Step 1 Log into the system as administrator.

Step 2 From the Windows Start menu, click **Programs > Wireless Control System> Uninstall WCS**.

Step 3 When the Uninstall Wireless Control System window appears, click **Uninstall**.

Step 4 Follow the instructions on the window to continue the uninstall process.

Step 5 When the WCS Uninstaller window indicates that the program is uninstalled, click **Finish** to close the window.

Note If any part of the C:\Program Files\WCS7.0.X.X folder remains on the hard drive, manually delete the folder and all of its contents. If you fail to delete the previous WCS installation, this error message appears when you attempt to reinstall WCS: "Cisco WCS already installed. Please uninstall the older version before installing this version."

Uninstalling WCS on Linux

Follow these steps to uninstall WCS on a Linux server.

Step 1 Stop WCS.

Step 2 Log into the system as root through an X terminal session.

Step 3 Using the Linux CLI, navigate to the /opt/WCS7.0.X.X directory (or the directory chosen during installation).

Step 4 Enter **./UninstallWCS**.

Step 5 Click **Yes** to continue the uninstall process.

Step 6 Click **Finish** when the uninstall process is complete.

Note If any part of the /opt/WCS7.0.X.X directory remains on the hard drive, manually delete the directory and all of its contents. If you fail to delete the previous WCS installation, this error message appears when you attempt to reinstall WCS: "Cisco WCS already installed. Please uninstall the older version before installing this version."

Upgrading WCS

This section provides instructions for upgrading WCS on either a Windows or Linux server. An automated upgrade is available in software release 4.2 and later. It handles the steps you would normally follow to accomplish an upgrade (shut down WCS, perform a backup, install new version, restore the backup, remove the old WCS version, and start WCS). If you choose to use the installer, it searches for any previous WCS versions.

If you are upgrading WCS in a high availability environment, refer to the "Upgrading WCS in a High Availability Environment" section on page 14-15.

Note You must have software release 4.1.91.0 before you can automatically upgrade to 4.2.

Note You should perform a Refresh Config from Controller after an upgrade of software to ensure that FTP details for the controller are retained. This Refresh Config from Controller drop-down option is available from the Configuration Commands section after choosing Configure > Controller > System > Commands.

If you choose to use the easy upgrade process, it provides error checking at each step and gives an informative message if an error causing an exit occurs. An upgrade-*version*.log is also produced and provides corrective measures. As part of the automatic upgrade process, machine specific settings are migrated.

If WCS is configured to use TACACS+ or RADIUS for external authentication, the custom vendor attribute list should be updated in the TACACS+ or RADIUS server with any new permissions. The attribute list for the appropriate UserGroup is found in Administration > AAA > UserGroups. Click the **Export** link for the appropriate user group.

Note Scheduled task settings are not preserved when you upgrade from WCS 4.0 or earlier releases. Be sure to record your settings manually if you wish to retain them or go to Administration > Background Tasks after starting WCS to check or change the settings as necessary.

Note If you upgrade to a WCS software release later than 4.0.87.0 from a release prior to 4.0.87.0, the users, user groups, tasks, and user passwords do not migrate. Upgrading to 4.0.87.0 before upgrading to a later release migrates the users, user groups, tasks, and user passwords.

Using the Installer to Upgrade WCS for Windows

Follow these steps to upgrade WCS (on a Windows platform) using the automated upgrade:

Step 1 Insert the Windows Cisco WCS CD into the CD-ROM drive and double-click the WCS-STANDARD-K9-7.0.X.Y.exe file where 7.0.X.Y is the software build. If you downloaded the installer from Cisco.com, double-click the WCS-STANDARD-WB-K9-7-0-X-Y.exe file that you downloaded to your local drive.

Step 2 The Install Anywhere window appears and prepares the system for installation. After a few seconds, the Introduction window appears, followed by the license agreement window. You must click the “I accept the terms of the License Agreement” option to continue.

Step 3 At this point, the install wizard detects whether a previous version of WCS is installed and specifies whether the current version is eligible for an automated upgrade. If your most recent WCS version cannot participate in the automated upgrade, you receive a notification as shown in Figure 14-1. If your WCS version is eligible for an automated upgrade, you receive a notification as shown in Figure 14-2.

Figure 14-1 Ineligible for Automated Upgrade

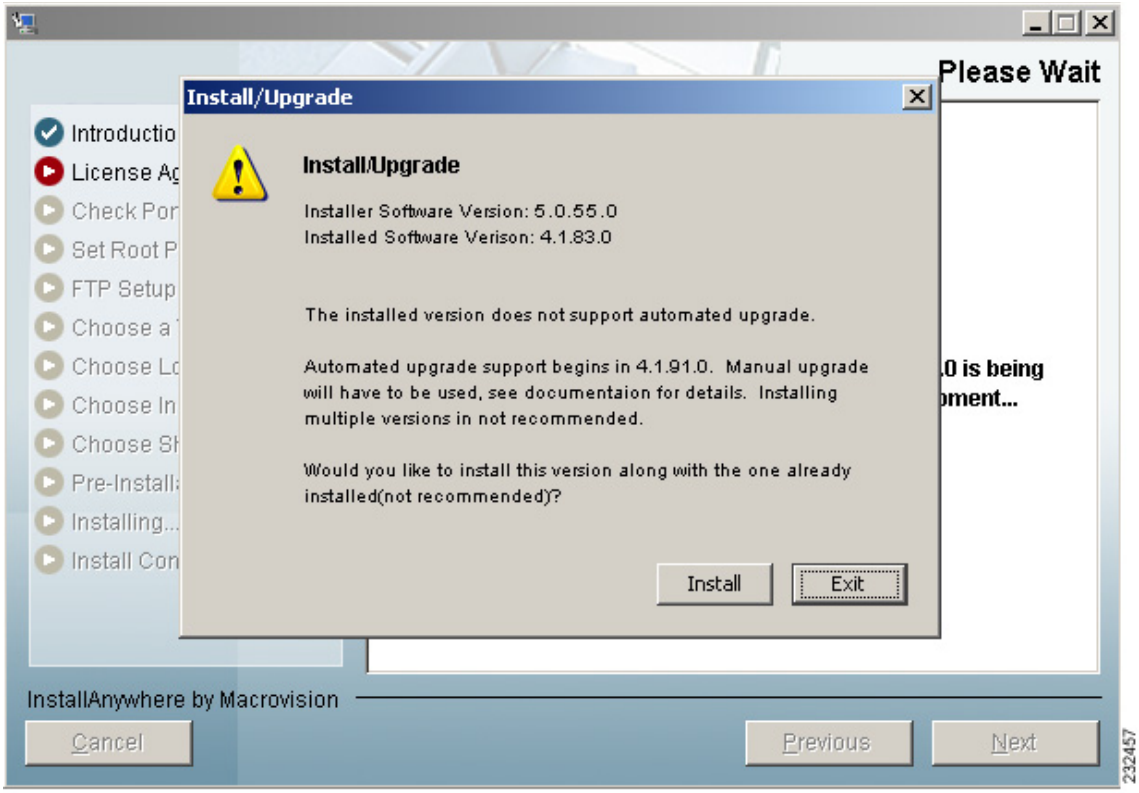
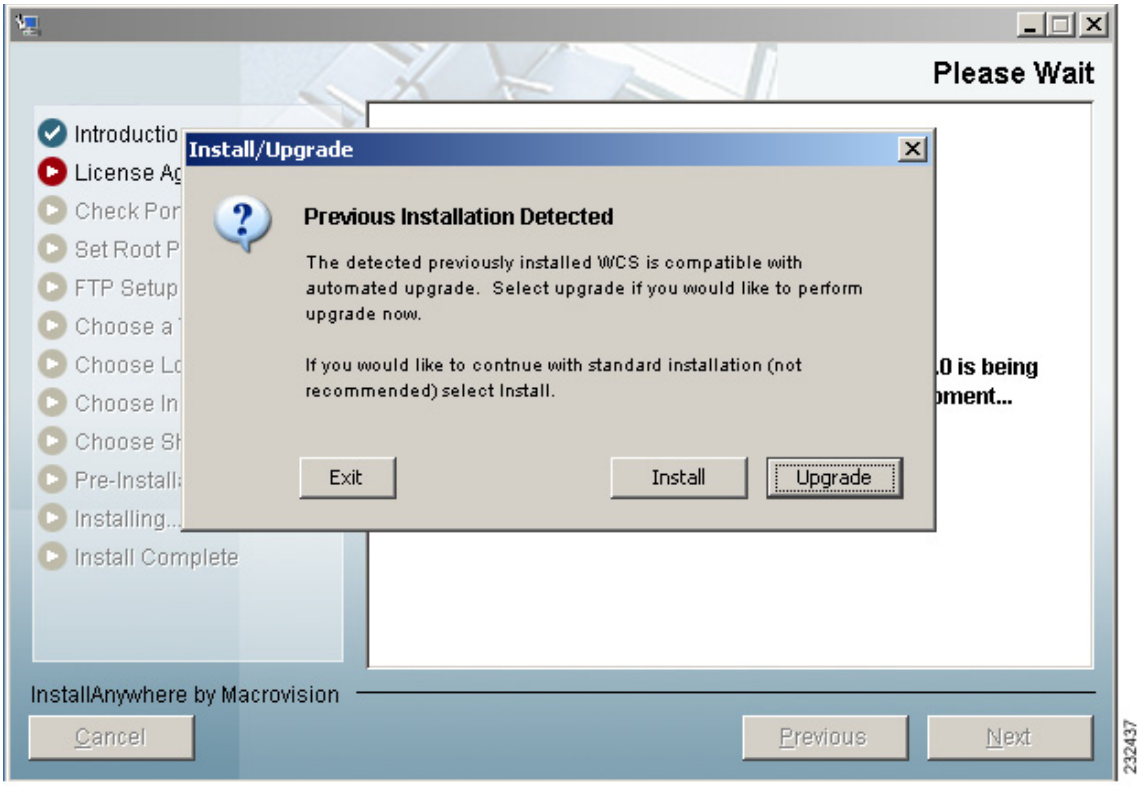


Figure 14-2 Previous Installation Detected



Step 4 If you see a window similar to the one in Figure 14-1 and choose **Install** because you cannot perform the automated upgrade, continue to the "Manually Upgrading WCS on Windows" section on page 14-14. If you see a window similar to the one in Figure 14-2 and choose **Install**, continue to the "Manually Upgrading WCS on Windows" section on page 14-14. If you see a window similar to the one in Figure 14-2 because a previous qualifying version of WCS is detected, choose **Upgrade** and continue to Step 5. This method is preferred.

Step 5 Several of the values from the previous install are retained and carried over as part of the upgrade. These include the following:

- the ports
- the root password
- the root FTP password
- the TFTP server file location
- the FTP server file location
- the multi-homed server interfaces

Step 6 Choose a folder in which to install the Cisco WCS at the Choose Install Folder window. It must be a different location than the previous install. Click **Next** to continue.

Step 7 Choose a folder location to store the shortcuts. It must be a different location than the previous install.

Step 8 Continue to follow the prompts that appear. You are notified of checking for required space, uninstalling of previous versions, backing up files, restoring, and so on. You then see a prompt asking if you are now ready to start WCS as a service. Click **Yes**.

Note The upgrade log is located in the standard log directory (\webnms\logs) if the automated upgrade completes. If the automated upgrade did not complete, the upgrade log is located in the user home directory.

Using the Installer to Upgrade WCS for Linux

Follow these steps to upgrade WCS (on a Linux platform) using the automated upgrade:

Step 1 Using the command line, perform one of the following:

a. If you are installing from a CD, switch to the /media/cdrom directory.

b. If you are installing from Cisco.com, switch to the directory in which the install file was downloaded. For example, if the install file was placed in /root/Desktop, enter **cd /root/Desktop**.

Step 2 Enter **./WCS-STANDARD-K9-7.0.X.Y.bin** (for CD users) or **./WCS-STANDARD-LB-K9-7-0-X-Y.bin** (for Cisco.com users) to start the install script.

Step 3 The Install Anywhere message appears and prepares the system for installation. After a few seconds, the Introduction appears, followed by the license agreement statement. You must accept the license agreement to continue.

Step 4 At this point, the install wizard detects whether a previous version of WCS is installed and specifies whether the current version is eligible for an automated upgrade. You receive a notification whether or not your most recent WCS version is eligible for the automated upgrade.

Step 5 If you cannot continue to the automated upgrade because your current WCS version is not eligible, choose **Install** and continue to the "Manually Upgrading WCS on Linux" section on page 14-14. If you choose to do a manual upgrade rather than the recommended automated upgrade, choose **Install** and continue to the "Manually Upgrading WCS on Linux" section on page 14-14. If your current WCS version is eligible for the recommended automated upgrade, choose **Upgrade** and continue to Step 6.

Step 6 Several of the values from the previous install are retained and carried over as part of the upgrade. These include the following:

- the ports
- the root password
- the root FTP password
- the TFTP server file location
- the FTP server file location
- the multi-homed server interfaces

Step 7 Choose a folder in which to install the Cisco WCS. It must be a different location than the previous install. Click **Next** to continue.

Step 8 Choose a folder location to store the shortcuts. It must be a different location than the previous install.

Step 9 Continue to follow the prompts that appear. You are notified of checking for required space, uninstalling of previous versions, backing up files, restoring, and so on. You then see a prompt asking if you are now ready to start WCS as a service. Click **Yes**.

Note The upgrade log is located in the standard log directory (\webnms\logs) if the automated upgrade completes. For an incomplete automated upgrade, the upgrade log is located in the user home directory.

Manually Upgrading WCS on Windows

Follow these steps to manually upgrade WCS on a Windows server. This type of upgrade is not recommended.

Note When upgrading from software release 4.096.0 to 4.1.82.0, only one "from" e-mail address is restored for the alarm e-mail filters. If you have multiple "from" e-mail addresses defined in the alarm e-mail filters, they are lost. The single "from" e-mail address is configured in Administration > Settings > Mail Server (refer to the "Mail Server Configuration" section on page 18-45).

Step 1 If possible, stop all WCS user interfaces to stabilize the database.

Step 2 Back up the WCS database by following the instructions in the "Backing Up the WCS Database (for Windows)" section on page 14-4.

Step 3 Uninstall the WCS application by following the instructions in the "Uninstalling WCS on Windows" section on page 14-8.

Step 4 Install the new version of WCS by following the instructions in the "Installing WCS for Windows" section on page 2-5.

Step 5 Restore the WCS database by following the instructions in the "Restoring the WCS Database (for Windows)" section on page 14-6.

Manually Upgrading WCS on Linux

Follow these steps to upgrade WCS on a Linux server. This type of upgrade is not recommended.

Step 1 If possible, stop all WCS user interfaces to stabilize the database.

Step 2 Back up the WCS database by following the instructions in the "Backing Up the WCS Database (for Linux)" section on page 14-5.

Step 3 Uninstall the WCS application by following the instructions in the "Uninstalling WCS on Linux" section on page 14-9.

Step 4 Install the new version of WCS by following the instructions in the "Installing WCS for Linux" section on page 2-14.

Step 5 Restore the WCS database by following the instructions in the "Restoring the WCS Database (for Linux)" section on page 14-7.

Upgrading WCS in a High Availability Environment

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

Step 1 You must first upgrade the secondary WCS with the following steps:

a. Shut down the secondary WCS. See the "Stopping WCS" section on page 14-2 for more information.

Note You can use **StopWCS** for a graceful shut down. A graceful shut down does not trigger the automatic failover. Use the CLI command **<WCSROOT>\nmsadmin.bat -switchover stop** to trigger automatic failover when shutting down WCS.

b. Perform an auto upgrade on the secondary WCS. See the "Using the Installer to Upgrade WCS for Windows" section on page 14-10 or the "Using the Installer to Upgrade WCS for Linux" section on page 14-13 for more information.

c. Start the secondary WCS.

Note It will attempt to reconnect to the primary WCS, but a version mismatch error is returned.

Step 2 Upgrade the primary WCS.

a. Shut down the primary WCS. See the "Stopping WCS" section on page 14-2 for more information.

b. Perform an auto upgrade on the primary WCS. See the "Using the Installer to Upgrade WCS for Windows" section on page 14-10 or the "Using the Installer to Upgrade WCS for Linux" section on page 14-13 for more information.

c. Start the primary WCS.

It connects to the Secondary WCS, and all data is resynchronized.

Upgrading the Network

Network upgrades must follow a recommended procedure so that databases can remain synchronized with each other. You cannot for instance upgrade the controller portion of the network to a newer release but maintain the current WCS version and not upgrade it. The supported order of upgrade is WCS 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 ***{install directory}*/bin/dbadmin.(sh|bat) reinitdb** to reinitialize the database.

Recovering the WCS Password

You can change the WCS 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). Follow these steps to recover the passwords and regain access to WCS. For password recovery on a wireless location device, refer to chapters 8 or 9 of the *Cisco 2700 Series Location Appliance Configuration Guide*.

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

Step 1 Change to the WCS bin folder.

Step 2 Perform one of the following:

Enter **passwd root-user *newpassword*** to change the WCS root password. The *newpassword* is the root login password you choose.

or

Enter **passwd location-ftp-user *newuser newpassword*** to change the FTP user and password. The *newuser* and *newpassword* are the FTP user and password you choose.

Step 3 The following options are available with these commands:

- -q — to quiet the output
- -pause — to pause before exiting
- -gui — to switch to the graphical user interface
- -force — to skip prompting for configuration

Step 4 Start WCS.

CHAPTER 15

Configuring Hybrid REAP

This chapter describes hybrid REAP and explains how to configure this feature on controllers and access points. It contains these sections:

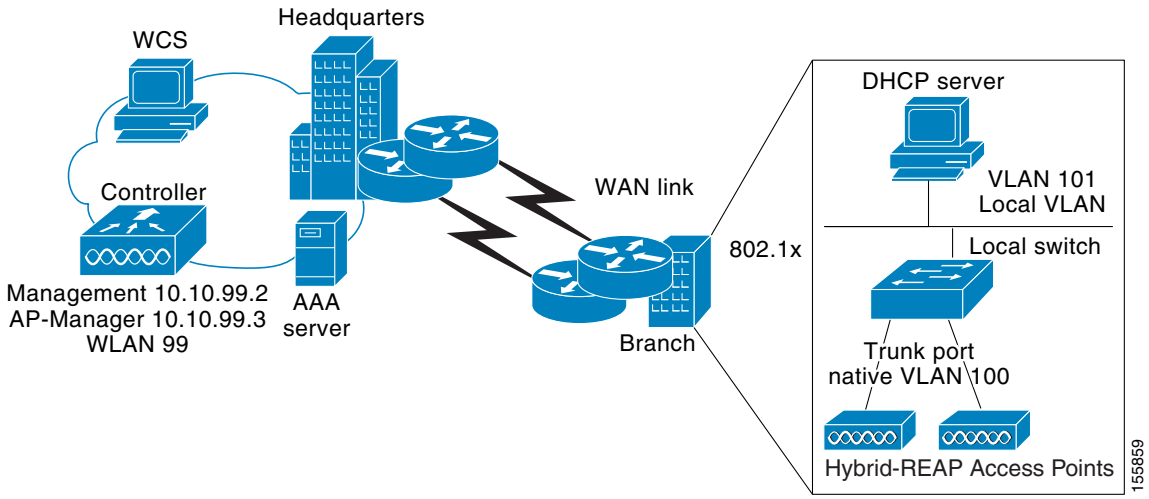
- Overview of Hybrid REAP, page 15-1
- Configuring Hybrid REAP, page 15-4
- Hybrid REAP Access Point Groups, page 15-12

Overview of Hybrid REAP

Hybrid REAP 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 hybrid-REAP access points per location. The hybrid-REAP 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.

Hybrid REAP 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, and the Controller Network Module for Integrated Services Routers, and the controller within the Catalyst 3750G Integrated Wireless LAN Controller Switch. Figure 15-1 illustrates a typical hybrid-REAP deployment.

Figure 15-1 Hybrid REAP Deployment



Hybrid-REAP Authentication Process

When a hybrid-REAP 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 hybrid-REAP access point can learn the controller IP address in one of these 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, Cisco recommends 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 CLI) the controller to which the access point is to connect.

When a hybrid-REAP access point can reach the controller (referred to as *connected mode*), the controller assists in client authentication. When a hybrid-REAP 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 hybrid-REAP modes. See the Hardware Installation Guide for your access point for information on LED patterns.

When a client associates to a hybrid-REAP 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 hybrid-REAP access point switches data packets locally. After the client authenticates successfully, the controller sends a configuration command with a new payload to instruct the hybrid-REAP 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 hybrid-REAP access point handles client authentication and switches client data packets locally. This state is valid only in standalone mode.
- **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 hybrid-REAP 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 hybrid-REAP 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 hybrid-REAP 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 hybrid-REAP 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 hybrid-REAP access point maintains client connectivity even after entering standalone mode. However, once the access point re-establishes a connection with the controller, it disassociates all clients, applies new configuration information from the controller, and reallows client connectivity.

Hybrid REAP Guidelines

Keep these guidelines in mind when using hybrid REAP:

- A hybrid-REAP 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.
- Hybrid REAP supports a 500-byte maximum transmission unit (MTU) WAN link at minimum.
- Roundtrip latency must not exceed 100 milliseconds (ms) between the access point and the controller, and CAPWAP control packets must be prioritized over all other traffic.
- The controller can send multicast packets in the form of unicast or multicast packets to the access point. In hybrid-REAP mode, the access point receives multicast packets only in unicast form.
- Hybrid REAP supports CCKM full authentication but not CCKM fast roaming.
- Hybrid REAP 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 Hybrid REAP

To configure hybrid REAP, you must follow the instructions in these sections in the order provided:

- Configuring the Switch at the Remote Site, page 15-4
- Configuring the Controller for Hybrid REAP, page 15-5
- Configuring an Access Point for Hybrid REAP, page 15-9
- Connecting Client Devices to the WLANs, page 15-12

Configuring the Switch at the Remote Site

Follow these steps to prepare the switch at the remote site.

Step 1 Attach the access point that will be enabled for hybrid REAP to a trunk or access port on the switch.

Note The sample configuration below shows the hybrid-REAP access point connected to a trunk port on the switch.

Step 2 See the sample configuration below to configure the switch to support the hybrid-REAP access point.

In this sample configuration, the hybrid-REAP 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 hybrid-REAP 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.

```
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
 ip address 10.10.101.1 255.255.255.0
 ip helper-address 10.10.101.1
end
```

Configuring the Controller for Hybrid REAP

This section provides instructions for configuring the controller for hybrid REAP. The controller configuration for hybrid REAP consists of creating centrally switched and locally switched s. This procedure uses these three WLANs as examples:

WLAN	Security	Switching	Interface Mapping (VLAN)
employee	WPA1+WPA2	Central	management (centrally switched VLAN)
employee-local	WPA1+WPA2 (PSK)	Local	101 (local switched VLAN)
guest-central	Web authentication	Central	management (centrally switched VLAN)

Step 1 Follow these steps to create a centrally switched WLAN. In our example, this is the first WLAN (employee).

a. Choose **Configure > Controllers**.

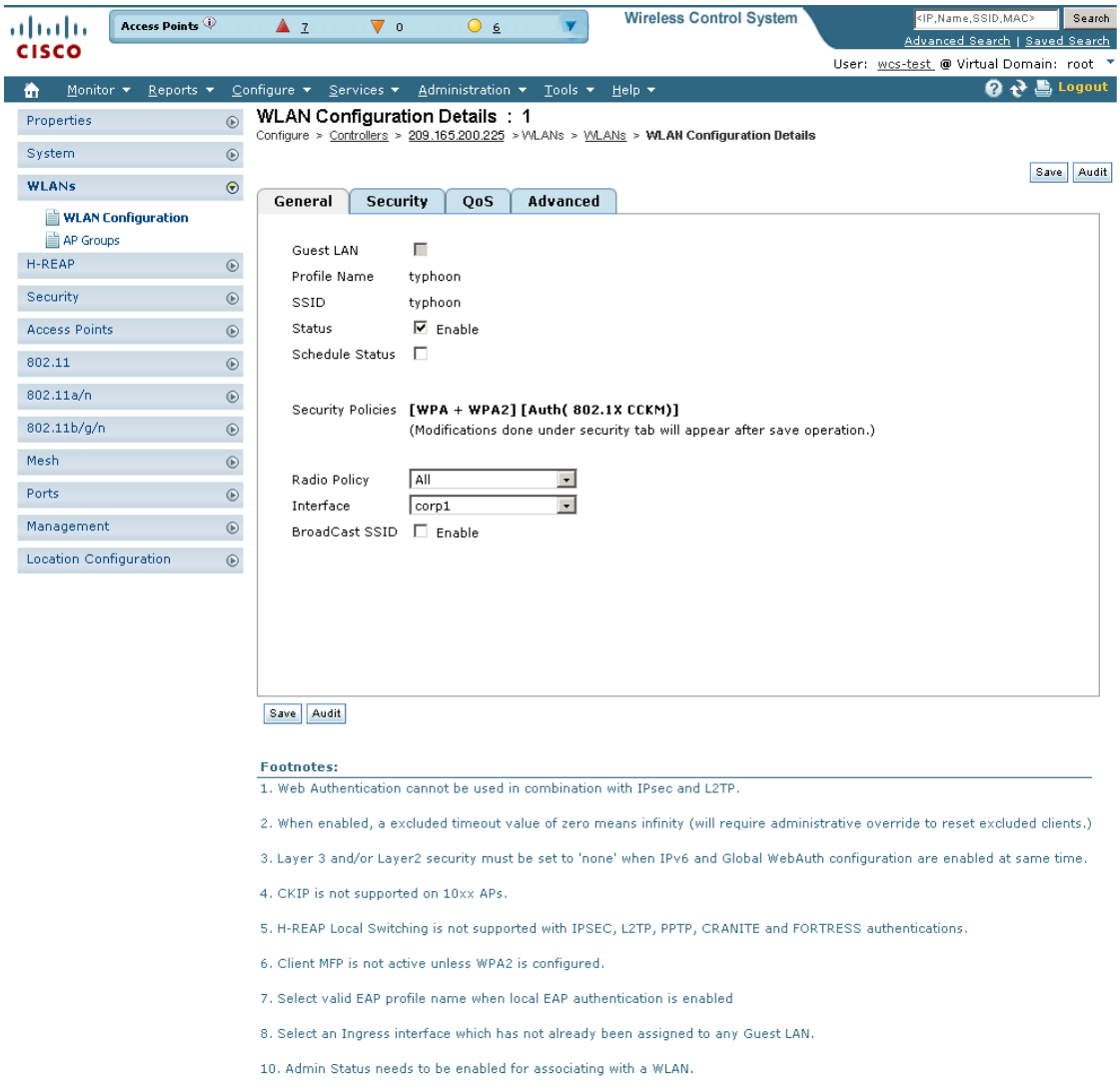
b. Click in the IP Address column for a particular controller.

c. Click **WLANs > WLAN Configuration** to access the s page.

d. Choose **Add a WLAN** from the Select a command drop-down list, and click **Go** (see Figure 15-2).

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.

Figure 15-2 WLANs > New Page



e. If you want to apply a template to this controller, choose a template name from the drop-down list. The parameters populate according to how the template is set. If you want to create a new WLAN template, use the *click here* link to be redirected to the template creation page (see the "Configuring WLAN Templates" section on page 12-18).

f. Modify the configuration parameters for this WLAN. In our employee WLAN example, you would need to choose **WPA1+WPA2** from the Layer 2 Security drop-down box.

g. Be sure to enable this WLAN by checking 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 box under General Policies. Also, select the **Allow AAA Override** check box to ensure that the controller validates a quarantine VLAN assignment.

h. Click **Save** to commit your changes.

Step 2 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 1 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 would need to choose **WPA1+WPA2** from the Layer 2 Security drop-down box. Make sure to choose PSK authentication key management and enter a pre-shared key.

Note Make sure to enable this WLAN by checking the **Admin Status** check box under General Policies. Also, make sure to enable local switching by checking the **H-REAP Local Switching** check box. When you enable local switching, any hybird-REAP access point that advertises this WLAN is able to locally switch data packets (instead of tunneling them to the controller).

Note For hybrid-REAP access points, the interface mapping at the controller for WLANs configured for H-REAP Local Switching is inherited at the access point as the default VLAN tagging. This can be easily changed per SSID and per hybrid-REAP access point. Non-hybrid-REAP access points tunnel all traffic back to the controller, and VLAN tagging is dictated by each WLAN's interface mapping.

c. Click **Save** to commit your changes.

Step 3 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 you can exercise your corporate data policies for unprotected guest traffic from a central site.

a. Follow the substeps in Step 1 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 would need to choose **None** from both the Layer 2 Security and Layer 3 Security drop-down boxes from 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 to enable this by checking the **Status** check box under General Policies.

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 12-64.

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 4 Go to the "Configuring an Access Point for Hybrid REAP" section on page 15-9 to configure two or three access points for hybrid REAP.

Configuring an Access Point for Hybrid REAP

This section provides instructions for configuring an access point for hybrid REAP.

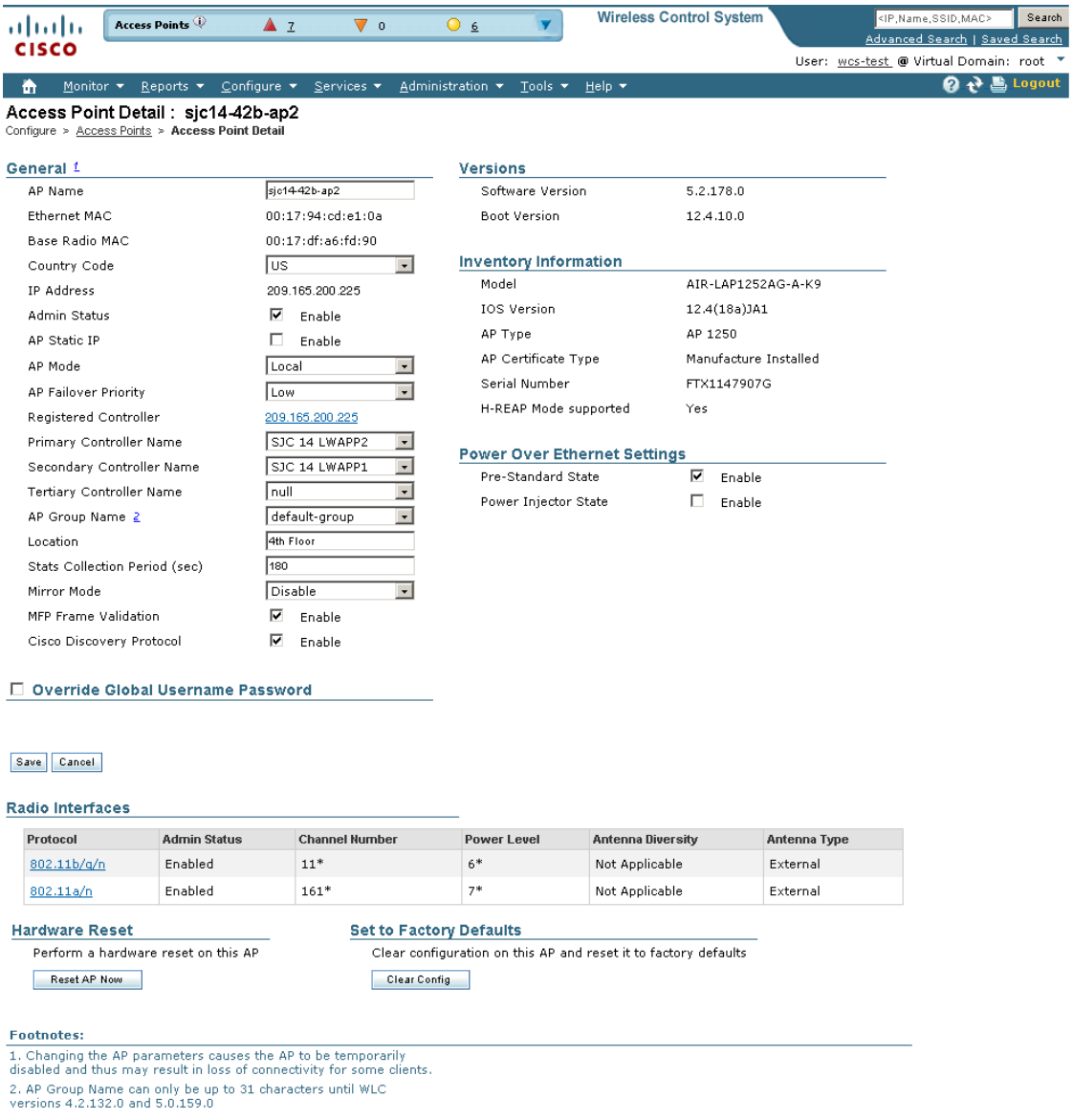
Follow these steps to configure an access point for hybrid REAP.

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 hybrid REAP by clicking one from the AP Name list. The detailed access point page appears (see Figure 15-3).

Figure 15-3 Detailed Access Point Page



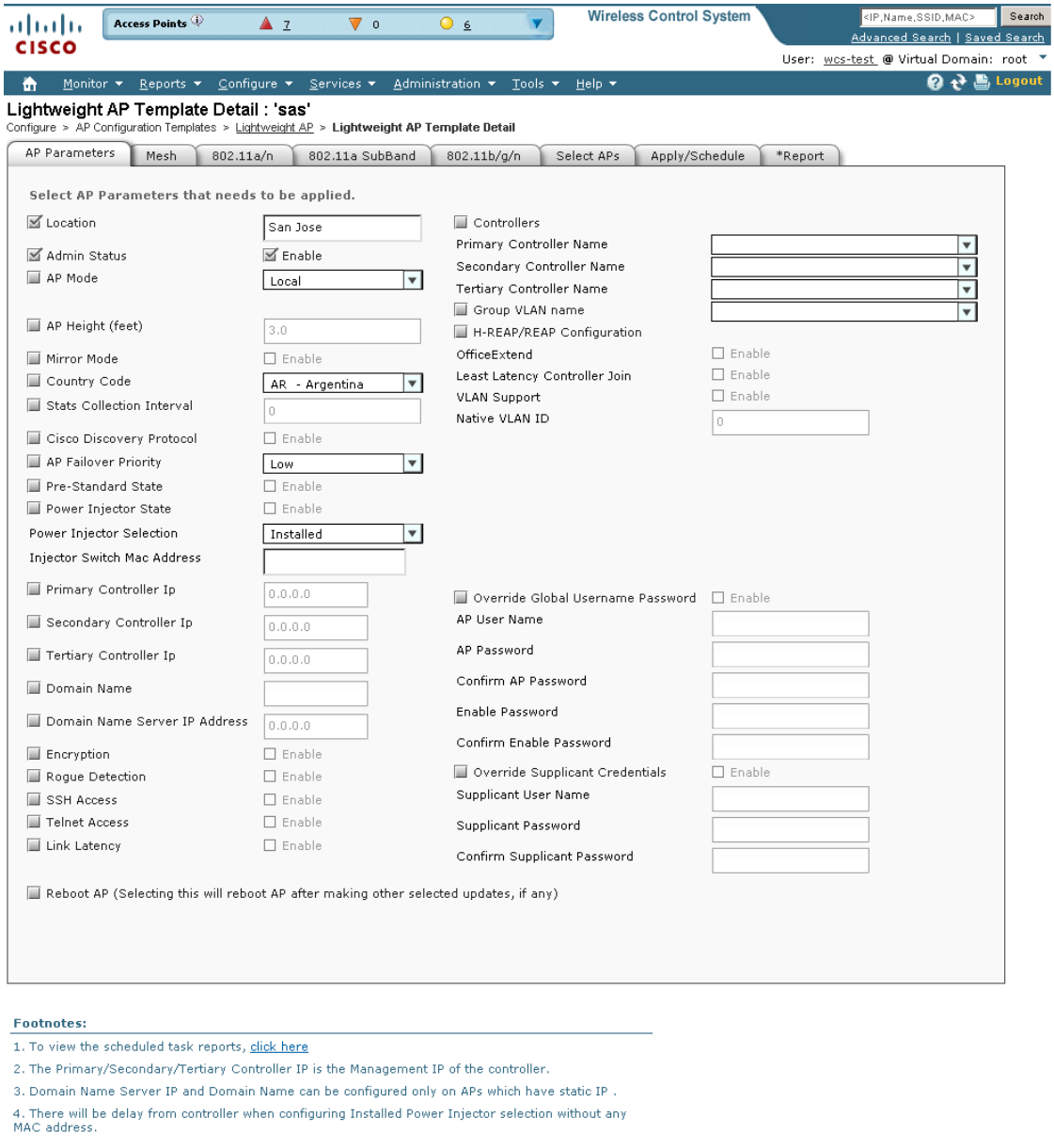
The last parameter under Inventory Information indicates whether this access point can be configured for hybrid REAP. Only the 1130AG and 1240AG access points support hybrid REAP.

Step 4 Verify that the AP Mode parameter displays *H-REAP*. If it does not, continue to Step 5. If H-REAP 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 hybrid REAP by clicking one from the AP Name list. The AP Template Detail page appears (see Figure 15-4).

Figure 15-4 AP/Radio Template Page



Step 7 Click to select the H-REAP/REAP Config check box. Enabling this configuration allows you to view all profile mappings.

Note If you are changing the mode to H-REAP/REAP and if the access point is not already in H-REAP/REAP mode, all other H-REAP/REAP parameters will not be 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.

Note By default, a VLAN is not enabled on the hybrid-REAP access point. When hybrid REAP 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 hybrid-REAP 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 hybrid REAP 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 Hybrid REAP" section on page 15-5.

In our example, you would create three profiles on the client:

1. To connect to the "employee" WLAN, you would 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 "local-employee" WLAN, you would 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 would 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. The user is automatically directed to the controller to complete the web-authentication process. When the web login page appears, the user enters his or her username and password.

To see if a client's data traffic is being locally or centrally switched, click **Monitor > Devices > Clients.**

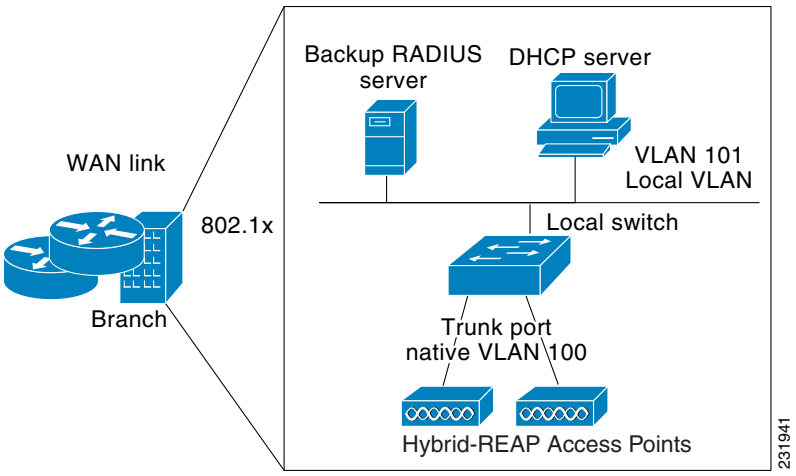
Hybrid REAP Access Point Groups

Hybrid REAP 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 hybrid-REAP access points per location, but you can organize and group the access points per floor and limit them per building, since 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 HREAP 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 HREAP group rather than for all 1000 clients. One particular HREAP 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 HREAP group rather than being configured in each access point.

All of the hybrid-REAP 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 hybrid-REAP 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 hybrid-REAP group rather than having to configure the same server on each access point. Figure 15-5 illustrates a typical hybrid-REAP group deployment with a backup RADIUS server in the branch office.

Figure 15-5 Hybrid-REAP Group Deployment



Hybrid-REAP Groups and Backup RADIUS Servers

You can configure the controller to allow a hybrid-REAP 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.

Hybrid-REAP Groups and CCKM

Hybrid-REAP groups are required for CCKM fast roaming to work with hybrid-REAP 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 hybrid-REAP 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 hybrid-REAP 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 hybrid-REAP and non-bybrid-REAP access points is not supported.

Hybrid-REAP Groups and Local Authentication

You can configure the controller to allow a hybrid-REAP 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 hybrid-REAP 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 an lightweight hybrid-REAP 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 hybrid-REAP backup RADIUS server feature. If a hybrid-REAP group is configured with both a backup RADIUS server and local authentication, the hybrid-REAP 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 hybrid-REAP access point itself (if the primary and secondary are not reachable).

Configuring Hybrid-REAP Groups

Follow these steps to configure HREAP groups. If you want to apply an H-REAP template to multiple controllers, refer to the template instructions in the "Configuring H-REAP AP Groups" section on page 12-34.

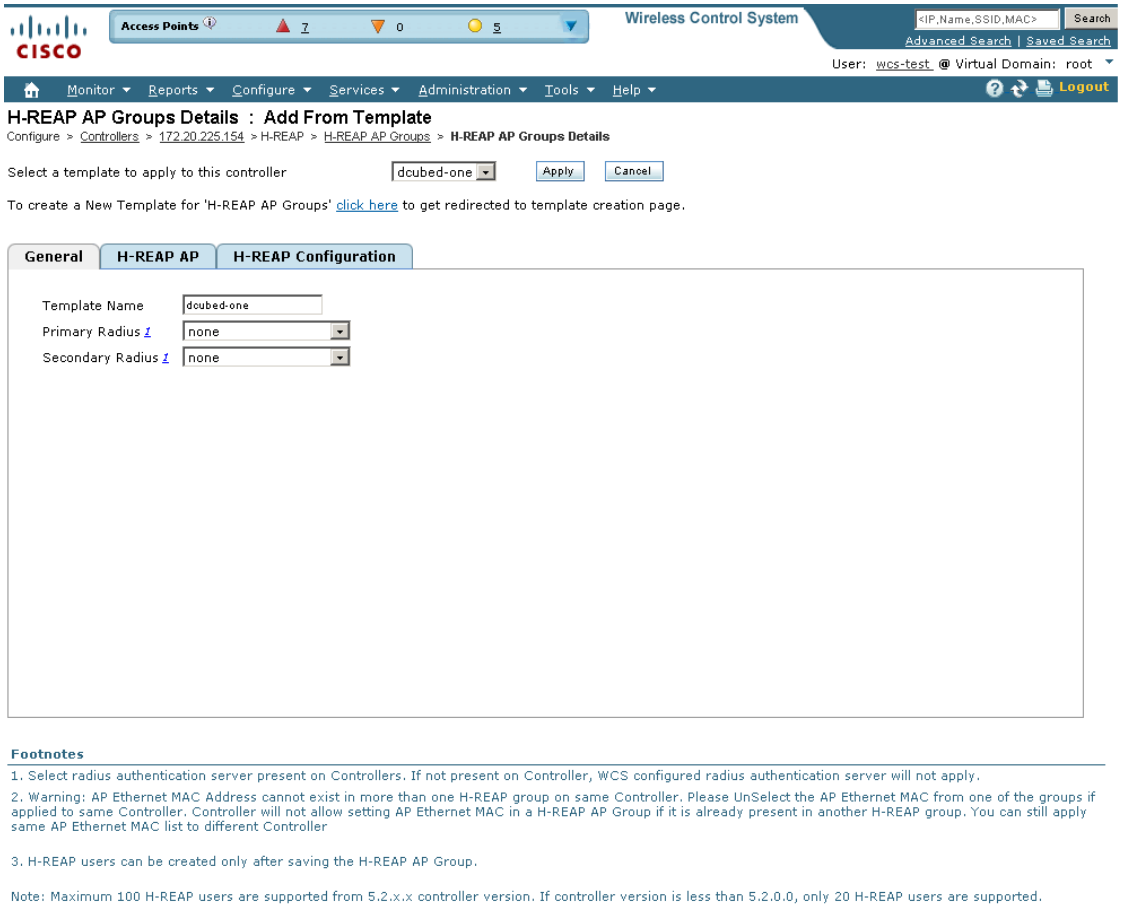
Step 1 Choose **Configure > Controllers**.

Step 2 Choose a specific controller by clicking on the desired IP address.

Step 3 From the left sidebar menu choose **H-REAP > H-REAP AP Groups**. The established HREAP AP groups appear.

Step 4 The Group Name column shows the group names assigned to the HREAP access point groups. If you want to add an additional group, choose **Add H-REAP 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 H-REAP AP Groups template appears (see Figure 15-6).

Figure 15-6 H-REAP AP Groups



Note To delete a group name, click the group name you want to remove and choose **Delete H-REAP AP Group** from the Select a command drop-down list.

The Template Name parameter shows the group name assigned to the H-REAP 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, the WCS configured RADIUS server does not apply.

Note You must configure the RADIUS server configuration on the controller before you apply H-REAP RADIUS server configuration from WCS.

Step 6 Choose the secondary RADIUS authentication servers for each group. If a RADIUS authentication server is not present on the controller, the WCS configured RADIUS server does not apply.

Step 7 If you want to add an access point to the group, click the **H-REAP AP** tab.

Step 8 An access point Ethernet MAC address cannot exist in more than one H-REAP group on the same controller. If more than one group is applied to the same controller, click 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 hybrid-REAP group, click the **H-REAP Configuration** tab. The H-REAP 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 **H-REAP Local Authentication** check box to enable local authentication for this hybrid-REAP 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 hybrid-REAP access point to authenticate clients using LEAP, select the **LEAP** check box. Otherwise, to allow a hybrid-REAP 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 hybrid-REAP group, click the **Users configured in the group** link. It advances you to the H-REAP AP Group screen which shows the names of the groups and the access points that belong in it.

Auditing an H-REAP Group

If the H-REAP configuration changes over a period of time either on WCS or the controller, you can audit the configuration. The changes are visible on subsequent screens. You can choose to synchronize the configuration by refreshing WCS or the controller.

CHAPTER 16

Alarms and Events

This chapter describes the type of events and alarms reported, how to view alarms and events by product or entity and severity, and how to view IDS signature attacks. It contains these sections:

- Using the Alarm Summary, page 16-1
- Monitoring Alarms, page 16-5
- Viewing Alarm Details, page 16-9
- Alarm and Event Dictionary, page 16-26

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 Cisco WCS response to one or more related events. If an event is considered of high enough severity (critical, major, minor, or warning), the WCS raises an alarm until the resulting condition no longer occurs. For example, an alarm may 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 WCS 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, etc.).

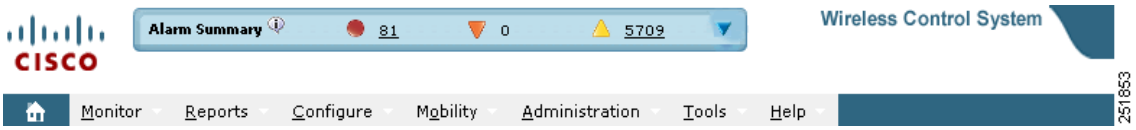
Using the Alarm Summary

When WCS receives an alarm message from a controller, it displays an alarm indicator at the top of the WCS page (see Figure 16-1).

Note The Administration > Settings > Alarms page has a Hide Acknowledged Alarms check box. You must unselect the preference of hiding acknowledged alarms if you want acknowledged alarms to show on the WCS Alarm Summary and alarms lists page. By default, acknowledged alarms are not shown.

Critical (red), Major (orange) and Minor (yellow) alarms are shown in the alarm dashboard, left -to-right.

Figure 16-1 WCS Alarm Summary



Alarms indicate the current fault or state of an element that attention, and they are usually generated by one or more events. The alarm can be cleared but the event remains.

Note Alarm counts refresh every 15 seconds.

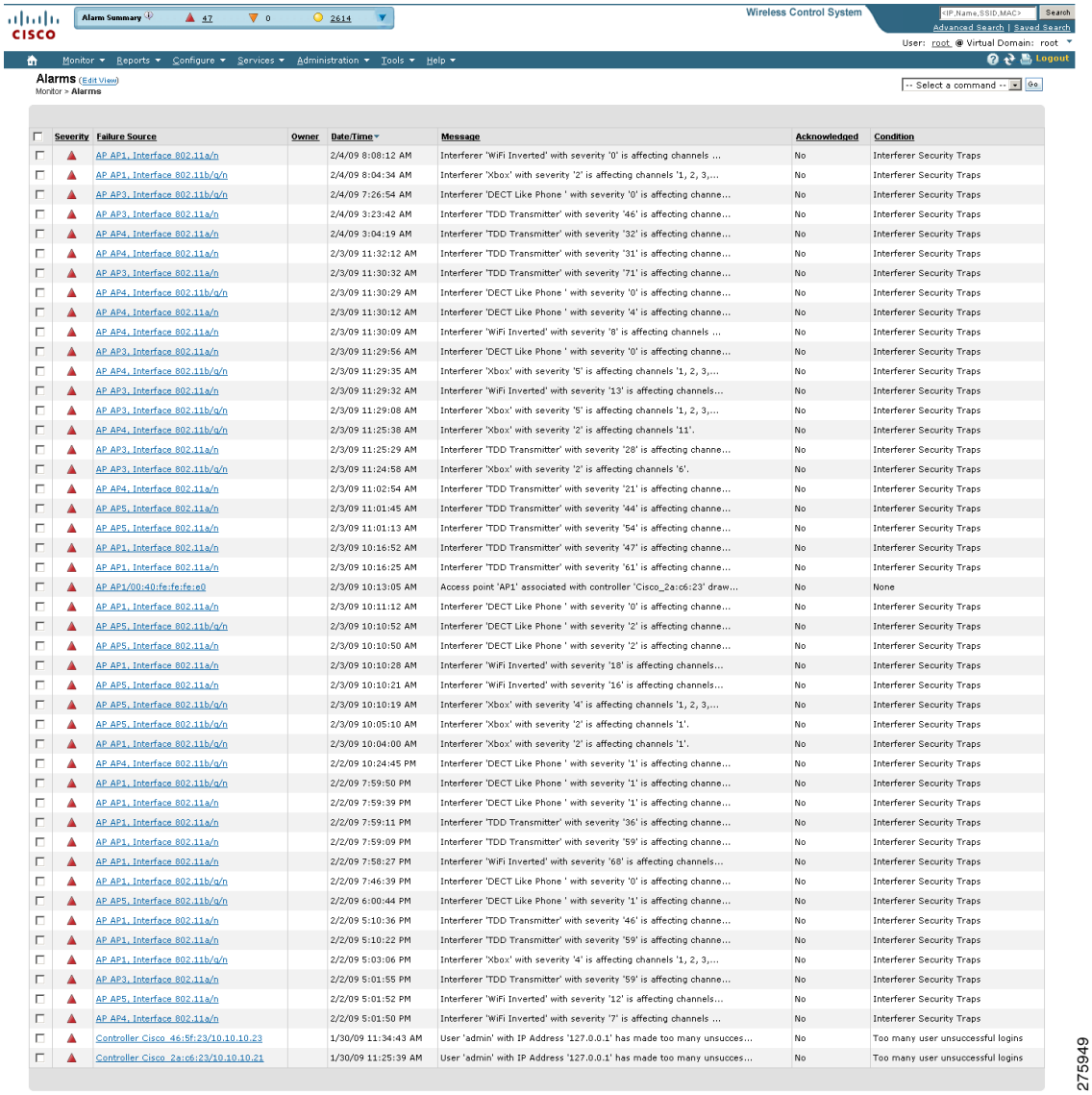
Note If an alarm is acknowledged, it does not appear on the alarm summary page by default. To change this setting, go to Administration > Settings > Alarms and deselect the **Hide acknowledged alarms** check box.

Alarms are color coded as follows:

- Red—Critical Alarm
- Orange—Major Alarm
- Yellow—Minor Alarm

The Alarm Summary displays the number of current critical, major, and minor alarms (see Figure 16-2).

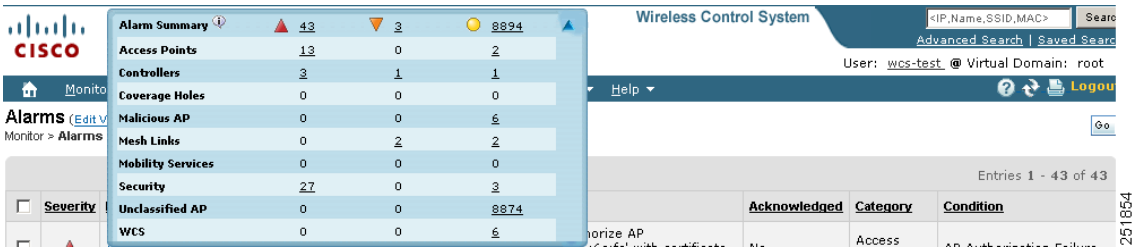
Figure 16-2 Alarm Summary Page for WCS



Click the alarm count number link in the Alarm Summary page to view the Monitor > Alarms page for these alarms.

Click the blue down arrow in the Alarm Summary page to expand the alarm summary (see Figure 16-3).

Figure 16-3 Open Summary Alarm



The expanded summary includes alarm counts for the following:

- Access Points—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. See the "Monitoring Alarms" section on page 16-5 for more information.
- Controllers—Displays counts for controller alarms, such as reachability problems from WCS and other controller failures (fan failure, POE controller failure, AP license expired, link down, temperature sensor failure, and low temperature sensed). See the "Monitoring Alarms" section on page 16-5 for more information.
- 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 Overview" section on page 5-2 for more information.
- Malicious AP—Displays counts for malicious rogue access points alarms. See the "Monitoring Rogue Access Point Alarms" section on page 16-10 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. See the "Monitoring Alarms" section on page 16-5 for more information.
- Mobility—Displays counts for location alarms such as reachability problems from WCS and location notifications (In/Out Area, Movement from Marker, or Battery Level). See the "Monitoring Alarms" section on page 16-5 for more information.
- Security—Displays counts for security alarms such as Signature Attacks, AP Threats/Attacks, and Client Security Events. See the "Monitoring Alarms" section on page 16-5 for more information.
- Unclassified AP—Displays counts for unclassified rogue access point alarms. See the "Monitoring Rogue Access Point Alarms" section on page 16-10 for more information.
- WCS—Displays counts for WCS alarms such as e-mail failures and license violation alarms.

Customizing Alarm Summary Results

If you click **Edit View** from the Alarm Summary page (shown in Figure 16-2), you can customize which results you want to appear in the Alarm Summary page.

Column names appear in one of the following lists:

- Hide Information—Lists columns that do not appear in the table. The **Hide** button points to this list.
- View Information—Lists columns that do appear in the table. The **Show** button points to this list.

To display a column in a table, click it in the Hide Information list, then click **Show**. To remove a column from a table, click it in the View Information list, then click **Hide**. You can select more than one column by holding down the Shift or Control key.

To change the position of a column in the View Information list, click it, then click **Up** or **Down**. The higher a column is in the list, the farther left it appears in the table.

The Alarm Summary items to choose from are as follows:

- Owner
- Date/Time
- Message
- Acknowledged
- Category
- Condition

Monitoring Alarms

This section provides information on the following:

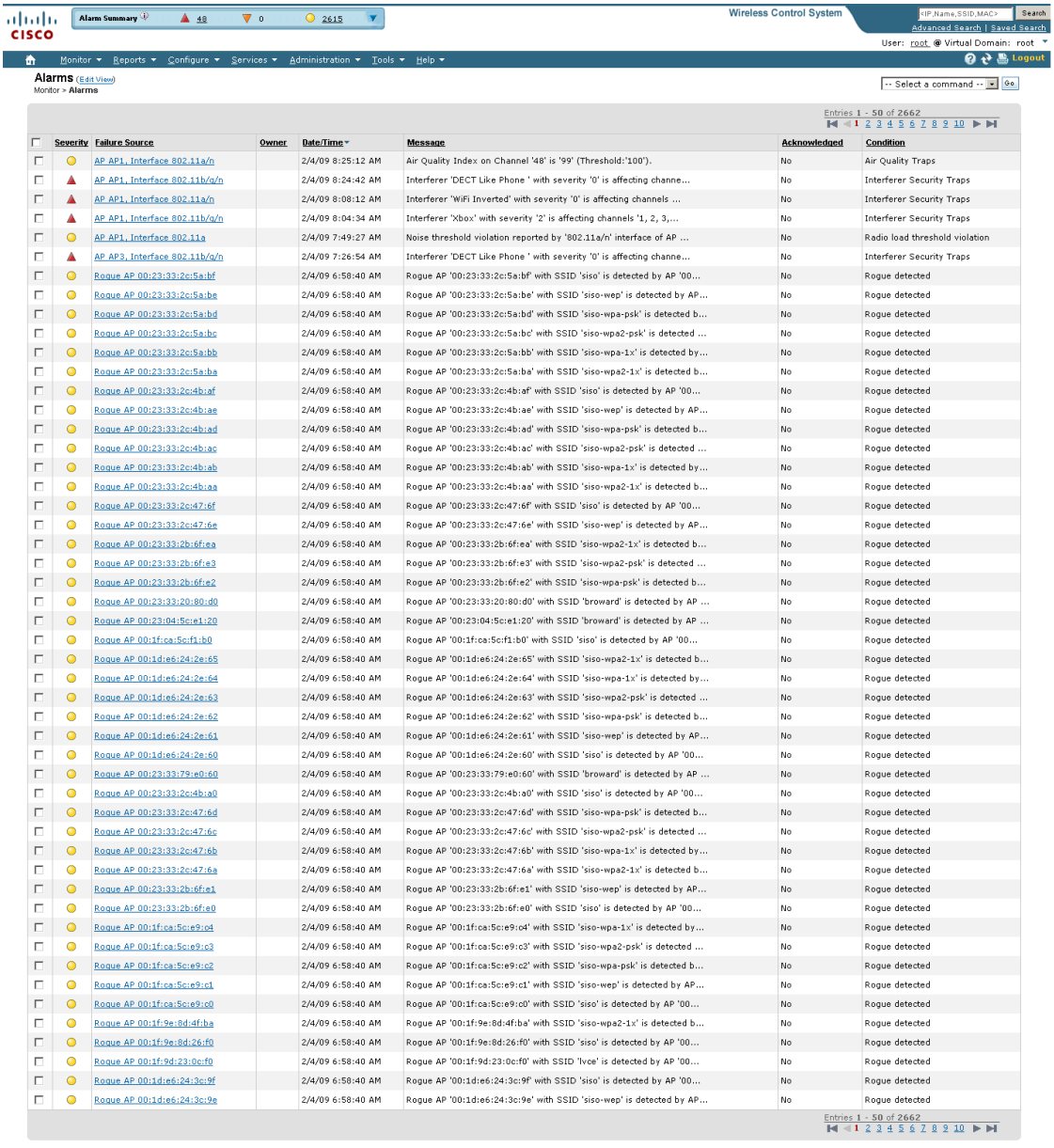
- Monitoring Alarm Overview, page 16-5
- Using Edit View for Alarms, page 16-8
- Viewing Alarm Details, page 16-9
- Monitoring Rogue Access Point Alarms, page 16-10
- Using Advanced Search, page 16-12
- Viewing Rogue Access Point Details, page 16-14
- Acknowledging Alarms, page 16-16
- Monitoring Adhoc Rogue Alarms, page 16-19
- Rogue Access Point Location, Tagging, and Containment, page 16-21
- Monitoring Rogue Alarm Events, page 16-22
- Monitoring E-mail Notifications, page 16-23

Monitoring Alarm Overview

Choose **Monitor > Alarms** to open the Alarms page. This page summarizes the controller alarms (see Figure 16-4).

Note You can search for a specific alarm or type of alarm by using the WCS search feature. See "Using the Search Feature" section on page 2-31 for more information on searching for an alarm or alarm type.

Figure 16-4 Monitor Alarms Page



This page displays a table of logged alarms. For more information, see Table 16-1.

Table 16-1 Monitor Alarms Page

Parameter	Description
(Check box)	Enables you to select one or more alarms. You can take action on selected alarms using the Select a command drop-down list.
Severity	Displays the alarm's level of severity ranging from critical to minor. • Red circle—Critical • Orange downward triangle—Major • Yellow upward triangle—Minor
Failure Source	Indicates the device that triggered the alarm. **Note** When you move your mouse cursor over an individual failure source, additional information regarding the failure and its location displays. The same information appears in the Message column.
Owner	Displays the name of the person to whom this alarm is assigned, if one was entered.
Date/Time	Displays the date and time that the alarm occurred.
Message	Indicates the reason for the alarm.
Acknowledged	Displays whether or not the alarm is acknowledged by the user.
Category	Displays the alarm's assigned category such as rogue AP, controller, switch, and security. This column does not appear by default. You can add this column to the table in the Edit View page. To go to the Edit View page, click **Edit View**. See the "Using Edit View for Alarms" section on page 16-8 for more information.
Condition	Displays the current condition that caused the alarm. This column does not appear by default. You can add this column to the table in the Edit View page. To go to the Edit View page, click **Edit View**. See the "Using Edit View for Alarms" section on page 16-8 for more information.

When there are multiple alarm pages, the page numbers appear 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 **Edit View** to go to the Edit View page.

Select a Command Menu

Using the Select a command drop-down list, you can make the following changes to the selected alarms:

- Assign to me—Assign the selected alarms to the current user.
- Unassign—Unassign the selected alarms.
- Delete—Delete the selected alarms.
- Clear—Clear the selected alarms.
- Acknowledge—You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in WCS 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—Opens the All Alarms > Email Notification page where you can view and configure e-mail notifications.

To make a change to a selected alarm, follow these steps:

Step 1 Select an alarm by checking the check box.

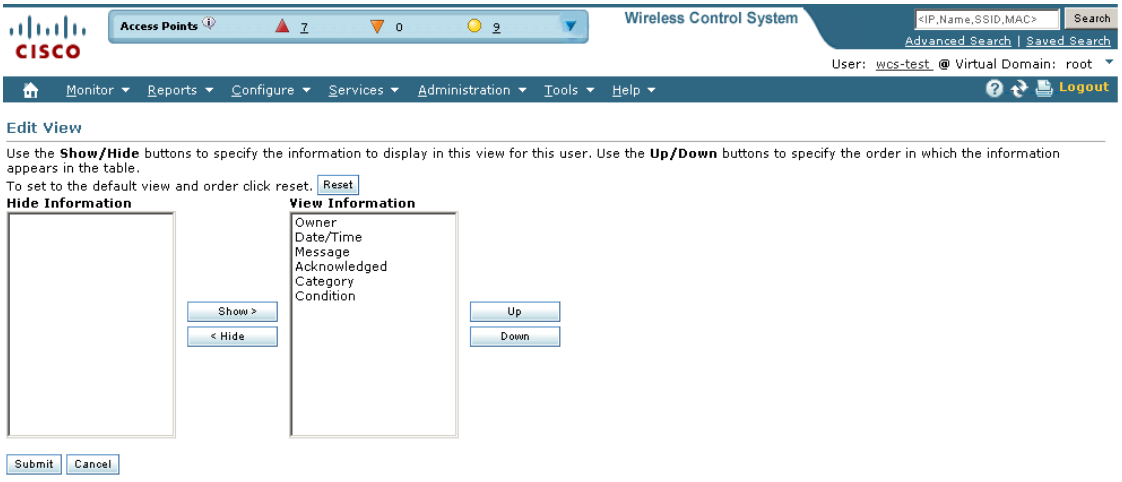
Step 2 From the command drop-down list, select a command.

Step 3 Click **Go**.

Using Edit View for Alarms

The Edit View page allows you to add, remove, or reorder columns in the alarms table (see Figure 16-5).

Figure 16-5 Edit View Page



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

Step 1 Choose **Monitor > Alarms**.

Step 2 Click **Edit View**.

Step 3 To add an additional column to the alarms 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 alarms table.

Step 4 To remove a column from the alarms table, click to highlight the column heading in the right column. Click **Hide** to move the heading to the left column. Not all items in the left column appear in the alarms table.

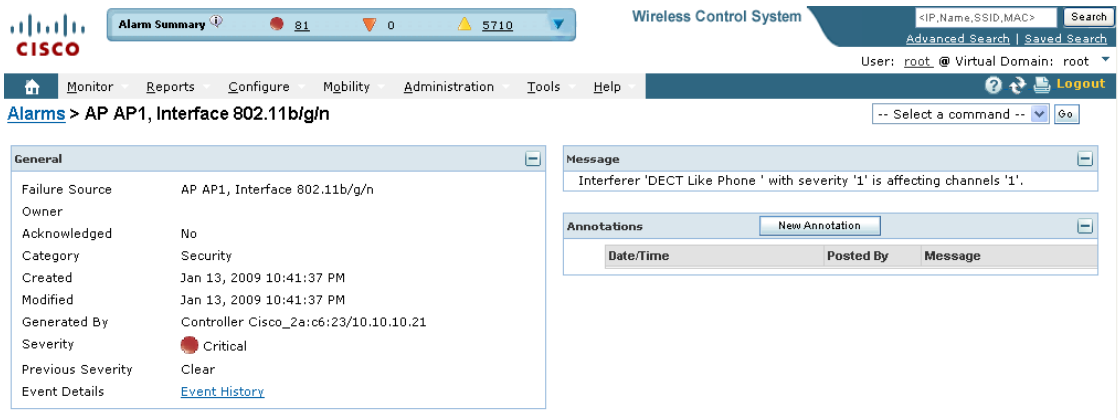
Step 5 Use the **Up/Down** buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click **Up** or **Down** to move it higher or lower in the current list.

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

Viewing Alarm Details

In the Monitor > Alarms page, click an item under Failure Source to access the alarms details page (see Figure 16-6).

Figure 16-6 Alarm Details Page



This page provides the following information (Table 16-2):

Table 16-2 General Parameters

Parameter	Description
Failure Source	Device that generated the alarm.
Owner	Name of person to which this alarm is assigned, or blank.
Acknowledged	Displays whether or not the alarm is acknowledged by the user.

Table 16-2 General Parameters

Parameter	Description
Category	The category of the alarm (for example, AP, Rogue AP, or Security).
Created	Month, day, year, hour, minute, second, AM or PM alarm created.
Modified	Month, day, year, hour, minute, second, AM or PM alarm last modified.
Generated By	Device that generated the alarm.
Severity	Level of security: Critical, Major, Minor, Warning, Clear, Info, Color coded.
Previous Severity	Critical, Major, Minor, Warning, Clear, Info. Color coded.

Note The General information may vary depending on the type of alarm. For example, some alarm details may include location and switch port tracing information.

- Annotations—Enter any new notes in this box and click **Add** to update the alarm. Notes appear in the "Annotations" display area.
- Messages—Displays information about the alarm.
- 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 you to the Monitoring Rogue 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.

Monitoring Rogue Access Point Alarms

Rogue access point radios are unauthorized access points detected by one or more access points.

To open the Rogue AP Alarms page, do one of the following:

- Search for rogue Access Points. See the "Using Advanced Search" section on page 16-12 for more information about the search feature.
- In the WCS home page, click the **Security** tab. 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 box. See the "Using the Alarm Summary" section on page 16-1 for more information.

Note If there are multiple alarm pages, the page numbers appear at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

The Rogue AP Alarms page contains the following parameters:

Table 16-3 Rogue Access Point Alarms

Parameter	Description
Check box	Select the alarms on which you want to take action.
Severity	Indicates the severity of the alarm: Critical, Major, Minor, Clear.
Rogue MAC Address	Indicates the MAC address of the rogue access points. See Monitor Alarms > Rogue AP Details.
Vendor	Rogue access point vendor name or Unknown.
Classification Type	Malicious, Friendly, or Unclassified.
Radio Type	Indicates the radio type for this rogue access point.
Strongest AP RSSI	Indicates the which signal strength indicator that was the strongest for this WCS (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 access point.
Date/Time	Indicates the date and time that the alarm occurred.
State	Indicates the state of the alarm. Includes Alert, Known or Removed.
SSID	Indicates the service set identifier being broadcast by the rogue access point radio. It is blank if 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.

Note The alarm remains in WCS, and you can search for all Acknowledged alarms using the alarm search functionality.

Select a Command

Select one or more alarms by checking their respective check boxes, select one of the following commands from the Select a Command drop-down list, and click **Go**.

- Assign to me—Assign the selected alarms to the current user.
- Unassign—Unassign the selected alarms.
- Delete—Delete the selected alarms.
- Clear—Clear the selected alarms.

- Acknowledge—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See the "Acknowledging Alarms" section on page 16-16 for more information.

Note The alarm remains in WCS and you can search for all Acknowledged alarms using the alarm search functionality.

- Unacknowledge—Unacknowledge an already acknowledged alarm.
- E-mail Notification—Opens the **All Alarms > E-mail Notification** page where you can view and configure e-mail notifications. See Monitor Alarms > E-mail Notification for more information.

Caution Attempting to contain a rogue access point may 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.

Using Advanced Search

When the access points on your wireless LAN are powered up and associated with controllers, WCS immediately starts listening for rogue access points. When a controller detects a rogue access point, it immediately notifies WCS, which creates a rogue access point alarm.

Follow these steps to find rogue access point alarms using Advanced Search.

Step 1 Click **Advanced Search** in the top right-hand corner of the WCS main page.

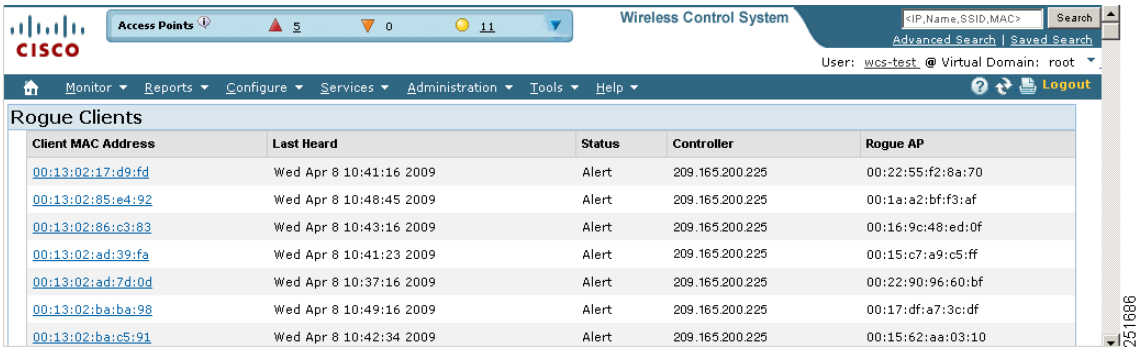
Step 2 Choose **Rogue Client** from the Search Category drop-down list.

Step 3 (optional) You can filter the search even further with the other search criteria if desired.

Step 4 Click **Search**.

Step 5 The list of rogue clients appears (see Figure 16-7).

Figure 16-7 Rogue Clients Page



Step 6 Choose a rogue client by clicking a client MAC address. The Rogue Client detail page appears (see Figure 16-8).

Figure 16-8 Rogue Client Detail Page

General

Client MAC Address	00:13:02:85:e4:92
Number of detecting APs	16
First Heard	Wed Apr 8 07:13:00 2009
Last Heard	Wed Apr 8 11:00:48 2009
Rogue AP MAC Address	00:1a:a2:bf:f3:af
Status	Alert

Location

No Location Information.
Client is not detected by any MSE.

Location Notifications

Absence	0
Containment	0
Distance	0
All	0

APs that detected this Rogue Client

Base Radio MAC	AP Name	Channel Number	Radio Type	RSSI	SNR	Last Heard
00:17:df:a6:83:50	sjc14-31b-ap6	36	802.11a	-82	17	Wed Apr 8 10:51:38 2009
00:17:df:a6:9f:c0	sjc14-41b-ap8	6	802.11b/g	-128	-1	Wed Apr 8 09:59:22 2009
00:17:df:a6:9f:c0	sjc14-41b-ap8	36	802.11a	-128	-1	Wed Apr 8 10:31:17 2009
00:17:df:a6:dc:60	sjc14-31b-ap1	36	802.11a	-63	33	Wed Apr 8 10:57:45 2009
00:17:df:a6:e1:10	sjc14-31b-ap8	36	802.11a	-128	-1	Wed Apr 8 10:31:16 2009
00:17:df:a6:e5:10	sjc14-32b-ap4	36	802.11a	-128	-1	Wed Apr 8 10:28:16 2009
00:17:df:a6:e7:d0	sjc14-31b-ap5	6	802.11b/g	-48	-1	Wed Apr 8 09:59:04 2009
00:17:df:a6:e7:d0	sjc14-31b-ap5	36	802.11a	-71	-1	Wed Apr 8 10:39:38 2009
00:17:df:a6:f2:20	sjc14-31b-ap10	36	802.11a	-87	6	Wed Apr 8 10:52:16 2009
00:17:df:a6:f3:10	sjc14-31b-ap7	6	802.11b/g	-68	25	Wed Apr 8 09:57:32 2009
00:17:df:a6:f3:10	sjc14-31b-ap7	36	802.11a	-128	-1	Wed Apr 8 10:31:16 2009
00:17:df:a6:fd:f0	sjc14-32b-ap5	6	802.11b/g	-73	22	Wed Apr 8 10:02:14 2009
00:17:df:a6:fd:f0	sjc14-32b-ap5	36	802.11a	-80	18	Wed Apr 8 11:00:48 2009
00:17:df:a7:a3:70	sjc14-31b-ap3	11	802.11b/g	-63	30	Wed Apr 8 10:04:40 2009
00:17:df:a7:a3:70	sjc14-31b-ap3	36	802.11a	-43	51	Wed Apr 8 10:57:34 2009
00:17:df:a8:34:60	sjc14-31b-ap2	36	802.11a	-65	28	Wed Apr 8 10:57:35 2009

251688

Step 7 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 on 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.

Configuring Alarm Severity

The 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, select **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, select 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.

Viewing Rogue Access Point Details

Alarm event details for each rogue access point are available from the Rogue AP Alarms page.

Follow these steps to view alarm events for a rogue access point radio.

Step 1 In the Rogue AP Alarms page, click an item under **Rogue MAC Address**.

This page displays alarm events for a rogue access point radio. Rogue access point radios are unauthorized access points detected by access points. The following information is available:

- General—
  - Rogue MAC Address—MAC address of the rogue access points.
  - Vendor—Rogue access point vendor name or Unknown.
  - Rogue Type—Indicates the rogue type such as AP.
  - On Network—Indicates whether or not the rogue access point is located on the network.
  - Owner—Indicates the owner or is left blank.
  - Acknowledged—Indicates whether or not the alarm is acknowledged by the user.
  - Classification Type—Malicious, Friendly, or Unclassified.
  - State—Indicates the state of the alarm: Alert, Known, or Removed.
  - 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.
  - Radio Type—Indicates the radio type for this rogue access point.
  - Strongest AP RSSI—Indicates the strongest received signal strength indicator in dBm.
  - No. of Rogue Clients—Indicates the number of rogue clients associated to this 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.
  - Severity—The severity of the alarm: Critical, Major, Minor, Clear. Color coded.
  - Previous Severity—The previous severity of the alarm: Critical, Major, Minor, Clear. Color coded.
  - Event Details—Click to open the Monitor > Events page.
  - Switch Port Trace Status—Indicates the switch port trace status. See the "Switch Port Trace" section on page 18-60 or the "Using Switch Port Tracing" section on page 10-57 for additional information.
- Switch Port Tracing Details—Provides the most recent switch port tracing details. To view additional trace details, use the **Click here for more details** link.
- Rogue Client—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.
- Message—Describes the alarm.
- 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.

Acknowledging Alarms

You may want to remove certain alarms 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 may 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, click the check box, and choose **Acknowledge** from the Select a command drop-down list.

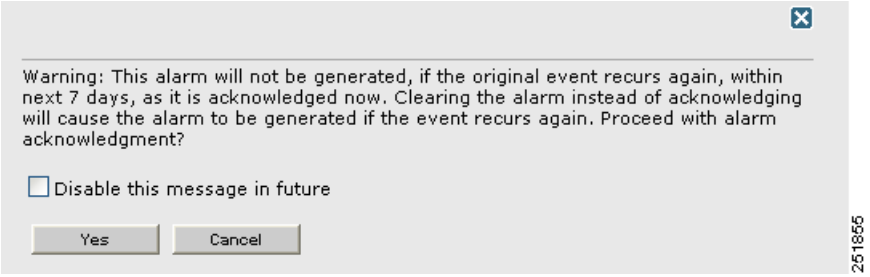
Now if the access point generates a new violation on the same interface, WCS will not create a new alarm, and the Alarm Summary page shows no new alarms. However, if the interference violation is created on another interface, such as 802.11a, a new alarm is created.

Any alarms, once acknowledged, will not show up on either the Alarm Summary 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 cannot be found with any search criteria. To change this default, go to the **Administration > Settings > Alarms** page and disable the **Hide Acknowledged Alarms** preference.

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 (see Figure 16-9).

Figure 16-9 Alarm Warning



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

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 dialog box. See "Using the Alarm Summary" for more information.

The Monitor Air Quality Alarms page contains the following parameters:

- Severity—Indicates the severity of the alarm including:

Icon	Meaning
	Critical
	Major
	Minor
	Warning
	Info
	Clear—Displays if the interferer is no longer detected by any access point.

- 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 WCS alarm browser.
- Acknowledged—Displays whether or not the alarm is acknowledged by the user. See "Acknowledging Alarms" for more information.

Monitor Air Quality Alarms > 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 "Acknowledging Alarms" for more information.

Note The alarm remains in WCS 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 where you can view and configure email notifications. See "Monitoring E-mail Notifications" 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. See "Using the Alarm Summary" for more information.

The Monitor CleanAir Security Alarms page contains the following parameters:

- Severity—Indicates the severity of the alarm including:

Icon	Meaning
	Critical
	Major
	Minor
	Warning
	Info
	Clear—Displays if the interferer is no longer detected by any access point.

- 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 WCS alarm browser.
- Acknowledged—Displays whether or not the alarm is acknowledged by the user. See "Acknowledging Alarms" for more information.

Monitor Security Alarms > Select a Command Menu

Select one or more alarms by checking their respective check boxes, select 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 "Acknowledging Alarms" for more information.

Note The alarm remains in WCS 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 where you can view and configure email notifications. See "Monitoring E-mail Notifications" for more information.

Monitoring Adhoc 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:

- Search for ad hoc rogue alarms. See the "Using the Search Feature" section on page 2-31 for more information.
- In the WCS home page, click the Security tab. 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 appear 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 parameters:

Table 16-4 Adhoc Rogue Alarm Parameters

Parameter	Description
Check box	Choose the alarms on which you want to take action.
Severity	The severity of the alarm including Critical, Major, Minor, and Clear. These severity levels are color-coded.
Adhoc Rogue MAC Address	Indicates the MAC address of the ad hoc rogue.
Vendor	Indicates the ad hoc rogue vendor name or Unknown.
Classification Type	Indicates the classification type of the ad hoc rogue including malicious, friendly, or unclassified.
Radio Type	Indicates this ad hoc rogue's radio type.
Strongest AP RSSI	Indicates the strongest received signal strength indicator in dBm.
No. of Rogue Clients	Indicates the number of rogue clients associated to this ad hoc rogue.
Owner	Indicates the owner of the ad hoc rogue.
Date/Time	Indicates the date and time that the alarm occurred.
State	Indicates the current state of the alarm including alert, known, or removed.
SSID	Service Set Identifier that is being broadcast by the ad hoc rogue 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.

Monitoring Adhoc Rogue Details

Alarm event details for each ad hoc rogue are available from the Adhoc Rogue Alarms page.

Follow these steps to view the alarm events for an ad hoc rogue radio.

Step 1 In the Adhoc Rogue Alarms page, click an item under **Rogue MAC Address**.

This page displays alarm events for a rogue access point radio. Rogue access point radios are unauthorized access points detected by Cisco lightweight access points. The following information is available:

- General
  - Rogue MAC Address—Media Access Control address of the ad hoc rogue.
  - Vendor—Ad hoc rogue vendor name or Unknown.
  - On Network—Indicates whether or not the ad hoc rogue is located on the network.
  - Owner—Indicates the owner or left blank.
  - Acknowledged—Indicates whether or not the alarm is acknowledged by the user.
  - Classification Type—Malicious, Friendly, or Unclassified.
  - State—Indicates the state of the alarm: Alert, Known, or 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—Indicates the radio type for this ad hoc rogue.
  - Strongest AP RSSI—Indicates the strongest received signal strength indicator in dBm.
  - No. of Rogue Clients—Indicates the number of rogue clients associated to this ad hoc.
  - 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.
  - Severity—The severity of the alarm: Critical, Major, Minor, Clear. Color coded.
  - 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 Alarms > Events page.
- Annotations—Lists existing notes for this alarm.

Rogue Access Point Location, Tagging, and Containment

When the Cisco Unified Wireless Network Solution is monitored using WCS, WCS 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:

- Find rogue access points.
- Receive new rogue access point notification, eliminating hallway scans.
- Monitor unknown rogue access points until they are eliminated or acknowledged.
- Find 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 is done for individual rogue access points by MAC address or is 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 disassociating 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

Click a Rogues alarm square in the Alarm Monitor (lower left-hand side of the screen) to access the Monitor Alarms > <failure object> page. In the Monitor Rogue AP Alarms page, click an item under Rogue MAC Address to access the Monitor Alarms > Rogue AP Details page, from the Select a command drop-down list choose **Detecting APs**, and click **Go** to access this page.

Choose **Monitor > Alarms,** then click **New Search** in the left sidebar. Choose **Severity > All Severities** and **Alarm Category > Rogue AP**, and click **Go** to access Monitor Alarms > <Failure Objects>.

In the Monitor Rogue AP Alarms page, click an item under Rogue MAC Address to access Monitor Alarms > Rogue AP Details. In the Monitor Alarms > Rogue - <vendor:MACaddr> page, from the Select a command drop-down list, choose **Detecting APs** to access this page.

This page enables you to view information about the Cisco lightweight access points that are detecting a rogue access point.

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. Events list the sequence of occurrences for an elements over a period of time.

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

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

- Search for rogue access points. See "Using the Search Feature" section on page 2-31 for more information about the search feature.
- In the WCS home page, click the **Security** tab. 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 box. See "Using the Alarm Summary" section on page 16-1 for more information.

Step 2 In the Rogue AP Alarms page, click the Rogue MAC Address for the appropriate rogue access point. The Rogue AP Alarm details page appears.

Step 3 From the Select a command drop-down list, click **Event History**.

Step 4 Click **Go**. The Rogue AP Events page appears.

Note Any Airlink vendors appear as Alpha.

Click the title of each column to reorder the listings:

- Severity—Color coded display of the severity of the event.
- Rogue MAC Address—Click a list item to display information about the entry.
- Vendor—Name of rogue access point manufacturer.
- Type—AP or AD-HOC.
- On Network—Whether or not the rogue access point is on the same subnet as the associated Port.
- On 802.11a—Whether or not the rogue access point is broadcasting on the 802.11a band.
- On 802.11b—Whether or not the rogue access point is broadcasting on the 802.11b/802.11g band.

- Date/Time—Date and time of the alarm.
- Classification Type—Malicious, Friendly, or Unclassified
- State—State of the alarm, such as Alert and Removed.
- SSID—Service Set Identifier being broadcast by the rogue access point radio.

Monitoring E-mail Notifications

You can configure the delivery of e-mail notifications for specific alarm categories and severity levels.

To configure e-mail notifications, follow these steps:

Step 1 Choose **Monitor > Alarms**.

Step 2 From the Select a command drop-down list, choose **E-mail Notification**.

Step 3 Click an **Alarm Category** to edit severity level and e-mail recipients for its e-mail notifications.

Step 4 Choose the severity level check box(es) (Critical, Major, Minor, Warning) for which you want a notification sent.

Step 5 Enter the notification recipient e-mail addresses in the To text box.

Note Separate multiple e-mail addresses with commas.

Step 6 Click **OK**.

Step 7 Click the **Enabled** check box for appropriate alarm categories to activate the delivery of e-mail notifications.

Step 8 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 Choose 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 CleanAir Air Quality Events

You can use Cisco WCS to view the events generated on the air quality of the wireless network.

To view air quality events, follow these steps:

Step 1 Click **Advanced Search** in the top right of the main WCS page.

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 **Performance**.

Step 5 Click **Go**.

The air quality events page displays the following information:

- Severity—Indicates the severity of the alarm including:

Icon	Meaning
	Critical
	Major
	Minor
	Warning
	Info
	Clear—Displays if the interferer is no longer detected by any access point.

- 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:

Step 1 In the Air Quality Events page, click an item under Failure Source to access the alarm details page. See Monitoring CleanAir Air Quality Events.

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, 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 know more about the alarm details.
- Message—Describes the air quality index on this access point.

Monitoring Interferer Security Risk Events

You can use Cisco WCS to view the security events generated on your wireless network.

To view interferer security events, follow these steps:

Step 1 Click **Advanced Search** in the top right of the main WCS page.

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 including:

Icon	Meaning
	Critical
	Major
	Minor
	Warning
	Info
	Clear—Displays if the interferer is no longer detected by any access point.

- 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 Monitoring Interferer Security Risk Events.

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.

Alarm and Event Dictionary

This section describes the event and alarm notifications that the wireless LAN controller, access points, and location appliances can receive. In addition, specific actions an administrator can do to address these alarms and events are described.

Note Not all traps which are seen on the WLC GUI are supported by WCS.

Notification Format

For each alarm and event notification, the following information is provided:

Table 16-5 Notification Format

Field	Description
Title	The notification title is generally picked up from an event property file defined in the NMS.
MIB Name	The MIB Name is the name of the notification as defined in the management information base (MIB). In some cases, if the event is specific only to the NMS, this field is not relevant. You can define multiple events in WCS from the same trap based on the values of the variables present in the trap. In such cases, multiple subentries appear with the same MIB Name. In addition, this field displays the value of the variable that caused WCS to generate this event.

Table 16-5 Notification Format (continued)

Field	Description
WCS Message	The WCS Message is a text string that reflects the message displayed in the WCS alarm or event browser associated with this event. Numbers such as "{0}" reflect internal WCS variables that typically are retrieved from variables in the trap. However, the order of the variables as they appear in the trap cannot be derived from the numbers.
Symptoms	This field displays the symptoms associated with this event.
WCS Severity	This field displays the severity assigned to this event in WCS.
Probable Causes	This field lists the probable causes of the notification.
Recommended Actions	This field lists any actions recommended for the administrator managing the wireless network.

Traps Added in Release 2.0

AP_BIG_NAV_DOS_ATTACK

MIB Name	bsnApBigNavDosAttack.
WCS Message	The AP "{0}" with protocol "{1}" receives a message with a large NAV field and all traffic on the channel is suspended. This is most likely a malicious denial of service attack.
Symptoms	The system detected a possible denial of service attack and suspended all traffic to the affected channel.
WCS Severity	Critical.
Probable Causes	A malicious denial of service attack is underway.
Recommended Actions	Identify the source of the attack in the network and take the appropriate action immediately.

AP_CONTAINED_AS_ROGUE

MIB Name	bsnAPContainedAsARogue.
WCS Message	AP "{0}" with protocol "{1}" on Switch "{2}" is contained as a Rogue preventing service.
Symptoms	An access point is reporting that it is being contained as a rogue.
WCS Severity	Critical.
Probable Causes	Another system is containing this access point.
Recommended Actions	Identify the system containing this access point. You may need to use a wireless sniffer.

AP_DETECTED_DUPLICATE_IP

MIB Name	bsnDuplicateIpAddressReported.
WCS Message	AP "{0}" on Switch "{3}" detected duplicate IP address "{2}" being used by machine with mac address "{1}."
Symptoms	The system detects a duplicate IP address in the network that matches that assigned to an access point.
WCS Severity	Critical.
Probable Causes	Another device in the network is configured with the same IP address as an access point.
Recommended Actions	Correct the misconfiguration of IP addresses in the network.

AP_HAS_NO_RADIOS

MIB Name	bsnApHasNoRadioCards.
WCS Message	**Not supported in WCS yet**.
Symptoms	An access point is reporting that it has no radio cards.
WCS Severity	N/A.
Probable Causes	Manufacturing fault or damage to the system during shipping.
Recommended Actions	Call customer support.

AP_MAX_ROGUE_COUNT_CLEAR

MIB Name	bsnApMaxRogueCountClear.
WCS Message	Fake AP or other attack on AP with MAC address "{0}" associated with Switch "{2}" is cleared now. Rogue AP count is within the threshold of "{1}'."
Symptoms	The number of rogues detected by a switch (controller) is within acceptable limits.
WCS Severity	Informational.
Probable Causes	N/A.
Recommended Actions	None.

AP_MAX_ROGUE_COUNT_EXCEEDED

MIB Name	bsnApMaxRogueCountExceeded.
WCS Message	Fake AP or other attack may be in progress. Rogue AP count on AP with MAC address "{0}" associated with Switch "{2}" has exceeded the severity warning threshold of "{1}."
Symptoms	The number of rogues detected by a switch (controller) exceeds the internal threshold.
WCS Severity	Critical.
Probable Causes	• There may be too many rogue access points in the network. • A fake access point attack may be in progress.
Recommended Actions	Identify the source of the rogue access points.

AUTHENTICATION_FAILURE (From MIB-II standard)

MIB Name	AuthenticationFailure.
WCS Message	Switch "{0}". Authentication failure reported.
Symptoms	There was an SNMP authentication failure on the switch (controller).
WCS Severity	Informational.

Probable Causes	An incorrect community string is in use by a management application.
Recommended Actions	Identify the source of the incorrect community string and correct the string within the management application.

BSN_AUTHENTICATION_FAILURE

MIB Name	bsnAuthenticationFailure.
WCS Message	Switch "{0}." User authentication from Switch "{0}" failed for user name "{1}" and user type "{2}."
Symptoms	A user authentication failure is reported for a local management user or a MAC filter is configured on the controller.
WCS Severity	Minor.
Probable Causes	Incorrect login attempt by an admin user from the controller CLI or controller GUI, or a client accessing the WLAN system.
Recommended Actions	If the user has forgotten the password, the superuser may need to reset it.

COLD_START (FROM MIB-II STANDARD)

MIB Name	coldStart.
WCS Message	Switch "{0}." Cold start.
Symptoms	The switch (controller) went through a reboot.
WCS Severity	Informational.
Probable Causes	• The switch (controller) has power-cycled. • The switch (controller) went through a hard reset. • The switch (controller) went through a software restart.
Recommended Actions	None.

CONFIG_SAVED

MIB Name	bsnConfigSaved.
WCS Message	Switch "{0}." Configuration saved in flash.
Symptoms	A configuration save to flash is performed on the switch (controller).
WCS Severity	Informational.
Probable Causes	The switch (controller) saves the configuration to the flash via a CLI command or entry via the controller GUI or WCS.
Recommended Actions	If you change the configuration using the controller CLI or controller GUI, you may need to refresh the configuration.

IPSEC_IKE_NEG_FAILURE

MIB Name	bsnIpsecIkeNegFailure.
WCS Message	IPsec IKE Negotiation failure from remote IP address "{0}."
Symptoms	Unable to establish an IPsec tunnel between a client and a WLAN appliance.
WCS Severity	Minor.
Probable Causes	Configuration mismatch.
Recommended Actions	Validate configuration, verify that authentication credentials match (preshared keys or certificates); and verify that encryption algorithms and strengths match.

IPSEC_INVALID_COOKIE

MIB Name	bsnIpsecInvalidCookieTrap.
WCS Message	IPsec Invalid cookie from remote IP address "{0}."
Symptoms	Cannot successfully negotiate an IPsec session.
WCS Severity	Minor.
Probable Causes	Synchronization problem. The client believes a tunnel exists while the WLAN appliance does not. This problem often happens when the IPsec client does not detect a disassociation event.
Recommended Actions	Reset the IPsec client and then restart tunnel establishment.

LINK_DOWN (FROM MIB-II STANDARD)

MIB Name	linkDown.
WCS Message	Port "{0}" is down on Switch "{1}."
Symptoms	The physical link on one of the switch (controller) ports is down.
WCS Severity	Critical.
Probable Causes	• An access point or a port was manually disconnected from the network. • A port failure.
Recommended Actions	Troubleshoot physical network connectivity to the affected port.

LINK_UP (FROM MIB-II STANDARD)

MIB Name	linkUp.
WCS Message	Port "{0}" is up on Switch "{1}."
Symptoms	The physical link is up on a switch (controller) port.
WCS Severity	Informational.
Probable Causes	A physical link to the switch (controller) is restored.
Recommended Actions	None.

LRAD_ASSOCIATED

MIB Name	bsnAPAssociated.
WCS Message	AP "{0}" associated with Switch "{2}" on Port number "{1}."
Symptoms	An access point has associated with a switch (controller).
WCS Severity	Informational.
Probable Causes	• A new access point has joined the network. • An access point has associated with a standby switch (controller) due to a failover. • An access point rebooted and reassociated with a switch (controller).
Recommended Actions	None.

LRAD_DISASSOCIATED

MIB Name	bsnAPDisassociated.
WCS Message	AP "{0}" disassociated from Switch "{1}."
Symptoms	The switch (controller) is no longer detecting an access point.
WCS Severity	Informational.
Probable Causes	• A failure in the access point. • An access point is no longer on the network.
Recommended Actions	Check if the access point is powered up and has network connectivity to the switch (controller).

LRADIF_COVERAGE_PROFILE_FAILED

MIB Name	bsnAPCoverageProfileFailed.
WCS Message	AP "{0}," interface "{1}." Coverage threshold of "{3}" is violated. Total no. of clients is "{5}" and no. failed clients is "{4}."
Symptoms	Number of clients experiencing suboptimal performance has crossed the configured threshold.
WCS Severity	Minor.
Probable Causes	Many clients are wandering to the remote parts of the coverage area of this radio interface with no handoff alternative.
Recommended Actions	• If the configured threshold is too low, you may need to readjust it to a more optimal value. • If the coverage profile occurs on a more frequent basis, you may need to provide additional radio coverage. • If the power level of this radio can be manually controlled, you may need to boost it to increase the coverage area.

LRADIF_COVERAGE_PROFILE_PASSED

MIB Name	bsnAPCoverageProfileUpdatedToPass.
WCS Message	AP "{0},” interface "{1}." Coverage changed to acceptable.
Symptoms	A radio interface that was reporting coverage profile failure has reverted to an acceptable level.
WCS Severity	Informational.
Probable Causes	The number of clients on this radio interface with suboptimal performance has dropped below the configured threshold.
Recommended Actions	None.

LRADIF_CURRENT_CHANNEL_CHANGED

MIB Name	bsnAPCurrentChannelChanged.
WCS Message	AP "{0},” interface "{1}." Channel changed to "{2}." Interference Energy before update was "{3}" and after update is "{4}."
Symptoms	The current channel assigned to a radio interface has automatically changed.
WCS Severity	Informational.
Probable Causes	Possible interference on a channel has caused the radio management software on the controller to change the channel.
Recommended Actions	None.

LRADIF_CURRENT_TXPOWER_CHANGED

MIB Name	bsnAPCurrentTxPowerChanged.
WCS Message	AP "{0},” interface "{1}." Transmit Power Level changed to "{2}."
Symptoms	The power level has automatically changed on a radio interface.
WCS Severity	Informational.
Probable Causes	The radio management software on the controller has modified the power level for optimal performance.
Recommended Actions	None.

LRADIF_DOWN

MIB Name	bsnAPIfDown.
WCS Message	AP "{0},” interface "{1}" is down.
Symptoms	A radio interface is out of service.
WCS Severity	Critical if not disabled, otherwise Informational.
Probable Causes	• A radio interface has failed. • An administrator has disabled a radio interface. • An access point has failed and is no longer detected by the controller.
Recommended Actions	If the access point is not administratively disabled, call customer support.

LRADF_INTERFERENCE_PROFILE_FAILED

MIB Name	bsnAPInterferenceProfileFailed.
WCS Message	AP "{0},” interface "{1}.” Interference threshold violated.
Symptoms	The interference detected on one or more channels is violated.
WCS Severity	Minor.
Probable Causes	There are other 802.11 devices in the same band that are causing interference on channels used by this system.
Recommended Actions	• If the interference threshold is configured to be too low, you may need to readjust it to a more optimum value. • Investigate interference sources such as other 802.11 devices in the vicinity of this radio interface. A possible workaround is adding one or more access points to distribute the current load or slightly increasing the threshold of the access point which is displaying this message. To perform this workaround, follow the steps below: 1. Choose **Configure > Controllers**. 2. Click any IP address in that column of the All Controllers page. 3. From the left sidebar menu, choose **802.11a/n** or **802.11b/g/n** and then **RRM Thresholds**. 4. Adjust the Interference Threshold (%) in the Other Thresholds section.

LRADIF_INTERFERENCE_PROFILE_PASSED

MIB Name	bsnAPInterferenceProfileUpdatedToPass.
WCS Message	AP "{0},” interface "{1}." Interference changed to acceptable.
Symptoms	A radio interface reporting interference profile failure has reverted to an acceptable level.
WCS Severity	Informational.
Probable Causes	The interference on this radio interface has dropped below the configured threshold.
Recommended Actions	None.

LRADIF_LOAD_PROFILE_FAILED

MIB Name	bsnAPLoadProfileFailed.
WCS Message	AP "{0},” interface "{1}." Load threshold violated.
Symptoms	A radio interface of an access point is reporting that the client load has crossed a configured threshold.
WCS Severity	Minor.
Probable Causes	There are too many clients associated with this radio interface.
Recommended Actions	• Verify the client count on this radio interface. If the threshold for this trap is too low, you may need to readjust it. • Add new capacity to the physical location if the client count is a frequent issue on this radio.

LRADIF_LOAD_PROFILE_PASSED

MIB Name	bsnAPLoadProfileUpdatedToPass.
WCS Message	AP "{0}," interface "{1}." Load changed to acceptable.
Symptoms	A radio interface that was reporting load profile failure has reverted to an acceptable level.
WCS Severity	Informational.
Probable Causes	The load on this radio interface has dropped below the configured threshold.
Recommended Actions	None.

LRADIF_NOISE_PROFILE_FAILED

MIB Name	bsnAPNoiseProfileFailed.
WCS Message	AP "{0}," interface "{1}." Noise threshold violated.
Symptoms	The monitored noise level on this radio has crossed the configured threshold.
WCS Severity	Minor.
Probable Causes	Noise sources that adversely affect the frequencies on which the radio interface operates.
Recommended Actions	• If the noise threshold is too low, you may need to readjust it to a more optimal value. • Investigate noise sources in the vicinity of the radio interface (for example, a microwave oven).

LRADIF_NOISE_PROFILE_PASSED

MIB Name	bsnAPNoiseProfileUpdatedToPass.
WCS Message	AP "{0}," interface "{1}." Noise changed to acceptable.
Symptoms	A radio interface that was reporting noise profile failure has reverted to an acceptable level.
WCS Severity	Informational.
Probable Causes	The noise on this radio interface has dropped below the configured threshold.
Recommended Actions	None.

LRADIF_UP

MIB Name	bsnAPIfUp.
WCS Message	AP "{0}," interface "{1}" is up.
Symptoms	A radio interface is back up.
WCS Severity	Informational.
Probable Causes	• An administrator has enabled a radio interface. • An access point has turned on. • A new access point has joined the network.
Recommended Actions	None.

MAX_ROGUE_COUNT_CLEAR

MIB Name	bsnMaxRogueCountClear.
WCS Message	Fake AP or other attack is cleared now. Rogue AP count on system "{0}" is within the threshold of "{1}."
Symptoms	The number of rogues detected by a controller is within acceptable limits.
WCS Severity	Informational.
Probable Causes	N/A.
Recommended Actions	None.

MAX_ROGUE_COUNT_EXCEEDED

MIB Name	bsnMaxRogueCountExceeded.
WCS Message	Fake AP or other attack may be in progress. Rogue AP count on system "{0}" has exceeded the severity warning threshold of "{1}."
Symptoms	The number of rogues detected by a controller exceeds the internal threshold.
WCS Severity	Critical.
Probable Causes	• There are too many rogue access points in the network. • A fake access point attack is in progress.
Recommended Actions	Identify the source of the rogue access points.

MULTIPLE_USERS

MIB Name	multipleUsersTrap.
WCS Message	Switch "{0}." Multiple users logged in.
Symptoms	Multiple users with the same login ID are logged in through the CLI.
WCS Severity	Informational.
Probable Causes	The same user has logged in multiple times through the CLI interface.
Recommended Actions	Verify that the expected login sessions for the same user are valid.

NETWORK_DISABLED

MIB Name	bsnNetworkStateChanged (bsnNetworkState set to disabled).
WCS Message	Global "{1}" network status disabled on Switch with IP Address "{0}."
Symptoms	An administrator has disabled the global network for 802.11a/n and 802.11b/g/n.
WCS Severity	Informational.
Probable Causes	Administrative command.
Recommended Actions	None.

NO_ACTIVITY_FOR_ROGUE_AP

MIB Name	This is a WCS-only event generated when no rogue activity is seen for a specific duration.
WCS Message	Rogue AP "{0}" is cleared explicitly. It is not detected anymore.
Symptoms	A rogue access point is cleared from the management system due to inactivity.
WCS Severity	Informational.
Probable Causes	A rogue access point is not located on any managed controller for a specified duration.
Recommended Actions	None.

POE_CONTROLLER_FAILURE

MIB Name	bsnPOEControllerFailure.
WCS Message	The POE controller has failed on the Switch "{0}."
SYMPTOMS	A failure in the Power Over Ethernet (POE) unit is detected.
WCS Severity	Critical.
Probable Causes	The power of the Ethernet unit has failed.
Recommended Actions	Call customer support. The unit may need to be repaired.

RADIOS_EXCEEDED

MIB Name	bsnRadiosExceedLicenseCount.
WCS Message	The Radios associated with Switch "{0}" exceeded license count "{1}." The current number of radios on this switch is "{2}."
Symptoms	The number of supported radios for a switch (controller) has exceeded the licensing limit.
WCS Severity	Major.
Probable Causes	The number of access points associated with the switch (controller) has exceeded the licensing limits.
Recommended Actions	Upgrade the license for the switch (controller) to support a higher number of access points.

RADIUS_SERVERS_FAILED

MIB Name	bsnRADIUSServerNotResponding.
WCS Message	Switch "{0}." RADIUS server(s) are not responding to authentication requests.
Symptoms	The switch (controller) is unable to reach any RADIUS server for authentication.
WCS Severity	Critical.
Probable Causes	Network connectivity to the RADIUS server is lost or the RADIUS server is down.
Recommended Actions	Verify the status of all configured RADIUS servers and their network connectivity.

ROGUE_AP_DETECTED

MIB Name	bsnRogueAPDetected.
WCS Message	Rogue AP or ad hoc rogue "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}" Radio type "{2}" with RSSI "{5}" and SNR "{6}."
Symptoms	The system has detected a rogue access point.
WCS Severity	Minor if not on a wired network; Critical if on a wired network.
Probable Causes	• An illegal access point is connected to the network. • A known internal or external access point unknown to this system is detected as rogue.
Recommended Actions	• Verify the nature of the rogue access point by tracing it using its MAC address or the SSID, or by using location features to locate it physically. • If the access point is a known internal or external access point, acknowledge it or mark it as a known access point. Consider adding it to the known access point template within WCS. • If the access point is deemed to be a severity threat, contain it using the management interface.

ROGUE_AP_ON_NETWORK

MIB Name	bsnRogueAPDetectedOnWiredNetwork
WCS Message	Rogue AP or ad hoc rogue "{0}" is on the wired network.
Symptoms	A rogue access point is found reachable through the wired network.
WCS Severity	Critical.
Probable Causes	An illegal access point was detected as reachable through the wired network.
Recommended Actions	• Determine if this is a known or valid access point in the system. If it is valid, place it in the known access point list. • Contain the rogue. Prevent anyone from accessing it until the access point has been traced down using location or other features.

ROGUE_AP_REMOVED

MIB Name	bsnRogueAPRemoved.
WCS Message	Rogue AP or ad hoc rogue "{0}" is removed; it was detected as Rogue AP by AP "{1}" Radio type "{2}."
Symptoms	The system is no longer detecting a rogue access point.
WCS Severity	Informational.
Probable Causes	A rogue access point has powered off or moved away and therefore the system no longer detects it.
Recommended Actions	None.

RRM_DOT11_A_GROUPING_DONE

MIB Name	bsnRrmDot11aGroupingDone.
WCS Message	RRM 802.11a/n grouping done; the new group leader's MAC address is "{0}."
Symptoms	The radio resource module is finished grouping for the A band, and a new group leader is chosen.
WCS Severity	Informational.
Probable Causes	The older RRM group leader may have gone down.
Recommended Actions	None.

RRM_DOT11_B_GROUPING_DONE

MIB Name	bsnRrmDot11bGroupingDone.
WCS Message	RRM 802.11b/g/n grouping done; the new group leader's MAC address is "{0}."
Symptoms	The radio resource module finished its grouping for the B band and chose a new group leader.
WCS Severity	Informational.
Probable Causes	The older RRM group leader may have gone down.
Recommended Actions	None.

SENSED_TEMPERATURE_HIGH

MIB Name	bsnSensedTemperatureTooHigh.
WCS Message	The sensed temperature on the Switch "{0}" is too high. The current sensed temperature is "{1}."
Symptoms	The system's internal temperature has crossed the configured thresholds.
WCS Severity	Major.
Probable Causes	• Fan failure. • Fault in the device.
Recommended Actions	• Verify the configured thresholds and increase the value if it is too low. • Call customer support.

SENSED_TEMPERATURE_LOW

MIB Name	bsnSensedTemperatureTooLow.
WCS Message	The sensed temperature on the Switch "{0}" is too low. The current sensed temperature is "{1}."
Symptoms	The internal temperature of the device is below the configured limit in the system.
WCS Severity	Major.
Probable Causes	• Operating environment. • Hardware fault.
Recommended Actions	• Verify the configured thresholds and ensure that the limit is appropriate. • Call customer support.

STATION_ASSOCIATE

MIB Name	bsnDot11StationAssociate.
WCS Message	Client "{0}" is associated with AP "{1}," interface "{2}."
Symptoms	A client has associated with an access point.
WCS Severity	Informational.
Probable Causes	A client has associated with an access point.
Recommended Actions	None.

STATION_ASSOCIATE_FAIL

MIB Name	bsnDot11StationAssociateFail.
WCS Message	Client "{0}" failed to associate with AP "{1}," interface "{2}." The reason code is "{3}."
Symptoms	A client station failed to associate with the system.
WCS Severity	Informational.
Probable Causes	The access point was busy.
Recommended Actions	Check whether the access point is busy and reporting load profile failures.

STATION_AUTHENTICATE

MIB Name	bsnDot11StationAssociate (bsnStationUserName is set).
WCS Message	Client "{0}" with user name "{3}" is authenticated with AP "{1}," interface "{2}."
Symptoms	A client has successfully authenticated with the system.
WCS Severity	Informational.
Probable Causes	A client has successfully authenticated with the system.
Recommended Actions	None.

STATION_AUTHENTICATION_FAIL

MIB Name	bsnDot11StationAuthenticateFail.
WCS Message	Client "{0}" has failed authenticating with AP "{1}," interface "{2}." The reason code is "{3}."
Symptoms	The system failed to authenticate a client.
WCS Severity	Informational.
Probable Causes	Failed client authentication.
Recommended Actions	Check client configuration and configured keys or passwords in the system.

STATION_BLACKLISTED

MIB Name	bsnDot11StationBlacklisted.
WCS Message	Client "{0}" which was associated with AP "{1}," interface "{2}" is excluded. The reason code is "{3}."
Symptoms	A client is in the exclusion list and is not allowed to authenticate for a configured interval.
WCS Severity	Minor.
Probable Causes	• Repeated authentication or association failures from the client station. • A client is attempting to use an IP address assigned to another device.
Recommended Actions	• Verify the configuration or the client along with its credentials. • Remove the client from the exclusion list by using the management interface if the client needs to be allowed back into the network.

STATION_DEAUTHENTICATE

MIB Name	bsnDot11StationDeauthenticate.
WCS Message	Client "{0}" is deauthenticated from AP "{1}," interface "{2}" with reason code "{3}."
Symptoms	A client is no longer authenticated by the system.
WCS Severity	Informational.
Probable Causes	A client is no longer authenticated by the system.
Recommended Actions	None.

STATION_DISASSOCIATE

MIB Name	bsnDot11StationDisassociate.
WCS Message	Client "{0}" is disassociated from AP "{1}," interface "{2}" with reason code "{3}."
Symptoms	A client has disassociated with an access point in the system.
WCS Severity	Informational.
Probable Causes	A station may disassociate due to various reasons such as inactivity timeout or a forced action from the management interface.
Recommended Actions	None.

STATION_WEP_KEY_DECRYPT_ERROR

MIB Name	bsnWepKeyDecryptError.
WCS Message	The WEP Key configured at the station may be wrong. Station MAC Address is "{0}," AP MAC is "{1}" and Slot ID is "{2}."
Symptoms	A client station seems to have the wrong WEP key.
WCS Severity	Minor.
Probable Causes	A client has an incorrectly configured WEP key.
Recommended Actions	Identify the client and correct the WEP key configuration.

STATION_WPA_MIC_ERROR_COUNTER_ACTIVATED

MIB Name	bsnWpaMicErrorCounterActivated.
WCS Message	The AP "{1}" received a WPA MIC error on protocol "{2}" from Station "{0}." Counter measures have been activated and traffic has been suspended for 60 seconds.
Symptoms	A client station has detected a WPA MIC error.
WCS Severity	Critical.
Probable Causes	A possible hacking attempt is underway.
Recommended Actions	Identify the station that is the source of this threat.

SWITCH_DETECTED_DUPLICATE_IP

MIB Name	bsnDuplicateIpAddressReported.
WCS Message	Switch "{0}" detected duplicate IP address "{0}" being used by machine with mac address "{1}."
Symptoms	The system has detected a duplicate IP address in the network that is assigned to the switch (controller).
WCS Severity	Critical.
Probable Causes	Another device in the network is configured with the same IP address as that of the switch (controller).
Recommended Actions	Correct the misconfiguration of IP addresses in the network.

SWITCH_DOWN

MIB Name	This is a WCS-only event.
WCS Message	Switch "{0}" is unreachable.
Symptoms	A switch (controller) is unreachable from the management system.
WCS Severity	Critical.
Probable Causes	• The switch (controller) has encountered hardware or software failure. • There are network connectivity issues between the management station and the switch (controller). • The configured SNMP community strings on the management station or the switch (controller) are incorrect.
Recommended Actions	• Check if the switch (controller) is powered up and reachable through the web interface. • Ping the switch (controller) from the management station to verify if there is IP connectivity. • Check the community strings configured on the management station.

SWITCH_UP

MIB Name	This is a WCS-only event.
WCS Message	Switch "{0}" is reachable.
Symptoms	A switch (controller) is now reachable from the management station.
WCS Severity	Informational.
Probable Causes	A switch (controller) is reachable from the management station.
Recommended Actions	None.

TEMPERATURE_SENSOR_CLEAR

MIB Name	bsnTemperatureSensorClear.
WCS Message	The temperature sensor is working now on the switch "{0}." The sensed temperature is "{1}."
Symptoms	The temperature sensor is operational.
WCS Severity	Informational.
Probable Causes	The system is detecting the temperature sensor to be operational now.
Recommended Actions	None.

TEMPERATURE_SENSOR_FAILURE

MIB Name	bsnTemperatureSensorFailure.
WCS Message	The temperature sensor failed on the Switch "{0}." Temperature is unknown.
Symptoms	The system is reporting that a temperature sensor has failed and the system is unable to report accurate temperature.
WCS Severity	Major.
Probable Causes	The temperature sensor has failed due to hardware failure.
Recommended Actions	Call customer support.

TOO_MANY_USER_UNSUCCESSFUL_LOGINS

MIB Name	bsnTooManyUnsuccessLoginAttempts.
WCS Message	User "{1}" with IP Address "{0}" has made too many unsuccessful login attempts.
Symptoms	A management user has made too many login attempts.
WCS Severity	Critical.
Probable Causes	• An admin user has made too many login attempts. • A user attempted to break into the administration account of the management system.
Recommended Actions	• Identify the source of the login attempts and take the appropriate action. • Increase the value of the login attempt threshold if it is too low.

Traps Added in Release 2.1

ADHOC_ROGUE_AUTO_CONTAINED

MIB Name	bsnAdhocRogueAutoContained.
WCS Message	Adhoc Rogue "{0}" was found and is auto contained as per WPS policy.
Symptoms	The system detected an ad hoc rogue and automatically contained it.
WCS Severity	Major.
Probable Causes	The system detected an ad hoc rogue and automatically contained it as configured in the system's wireless prevention policy.
Recommended Actions	Identify the ad hoc rogue through the location application and take the appropriate action.

ADHOC_ROGUE_AUTO_CONTAINED_CLEAR

MIB Name	bsnAdhocRogueAutoContained (bsnClearTrapVariable set to true).
WCS Message	Adhoc Rogue "{0}" was found and was auto contained. The alert state is clear now.
Symptoms	An ad hoc rogue that the system has detected earlier is now clear.
WCS Severity	Informational.
Probable Causes	The system no longer detects an ad hoc rogue.
Recommended Actions	None.

NETWORK_ENABLED

MIB Name	bsnNetworkStateChanged (bsnNetworkState set to enabled).
WCS Message	Global "{1}" network status enabled on Switch with IP Address "{0}."
Symptoms	An administrator has enabled the global network for 802.11a/n or 802.11b/g/n.
WCS Severity	Informational.
Probable Causes	Administrative command.
Recommended Actions	None.

ROGUE_AP_AUTO_CONTAINED

MIB Name	bsnRogueApAutoContained.
WCS Message	Rogue AP "{0}" is advertising our SSID and is auto contained as per WPS policy.
Symptoms	The system has automatically contained a rogue access point.
WCS Severity	Major.
Probable Causes	The system detected an ad hoc rogue and automatically contained it as configured in the system's wireless prevention policy.
Recommended Actions	• Track the location of the rogue and take the appropriate action. • If this is a known valid access point, clear the rogue from containment.

ROGUE_AP_AUTO_CONTAINED_CLEAR

MIB Name	bsnRogueApAutoContained (bsnClearTrapVariable set to true).
Message	Rogue AP "{0}" was advertising our SSID and was auto contained. The alert state is clear now.
Symptoms	The system has cleared a previously contained rogue.
WCS Severity	Informational.
Probable Causes	The system has cleared a previously contained rogue.
Recommended Actions	None.

TRUSTED_AP_INVALID_ENCRYPTION

MIB Name	bsnTrustedApHasInvalidEncryption.
WCS Message	Trusted AP "{0}" is invalid encryption. It is using "{1}" instead of "{2}." It is auto contained as per WPS policy.
Symptoms	The system automatically contained a trusted access point that has invalid encryption.
WCS Severity	Major.
Probable Causes	The system automatically contained a trusted access point that violated the configured encryption policy.
Recommended Actions	Identify the trusted access point and take the appropriate action.

TRUSTED_AP_INVALID_ENCRYPTION_CLEAR

MIB Name	bsnTrustedApHasInvalidEncryption (bsnClearTrapVariable set to true).
WCS Message	Trusted AP "{0}" had invalid encryption. The alert state is clear now.
Symptoms	The system has cleared a previous alert about a trusted access point.
WCS Severity	Informational.
Probable Causes	The trusted access point has now conformed to the configured encryption policy.
Recommended Actions	None.

TRUSTED_AP_INVALID_RADIO_POLICY

MIB Name	bsnTrustedApHasInvalidRadioPolicy.
WCS Message	Trusted AP "{0}" has invalid radio policy. It is using "{1}" instead of "{2}." It has been auto contained as per WPS policy.
Symptoms	The system has contained a trusted access point with an invalid radio policy.
WCS Severity	Major.
Probable Causes	The system has contained a trusted access point connected to the wireless system for violating the configured radio policy.
Recommended Actions	Identify the trusted access point and take the appropriate action.

TRUSTED_AP_INVALID_RADIO_POLICY_CLEAR

MIB Name	bsnTrustedApHasInvalidRadioPolicy (bsnClearTrapVariable set to true).
WCS Message	Trusted AP "{0}" had invalid radio policy. The alert state is clear now.
Symptoms	The system has cleared a previous alert about a trusted access point.
WCS Severity	Informational.
Probable Causes	The trusted access point has now conformed to the configured encryption policy.
Recommended Actions	None.

TRUSTED_AP_INVALID_SSID

MIB Name	bsnTrustedApHasInvalidSsid.
WCS Message	Trusted AP "{0}" has invalid SSID. It was auto contained as per WPS policy.
Symptoms	The system has automatically contained a trusted access point for advertising an invalid SSID.
WCS Severity	Major.
Probable Causes	The system has automatically contained a trusted access point for violating the configured SSID policy.
Recommended Actions	Identify the trusted access point and take the appropriate action.

TRUSTED_AP_INVALID_SSID_CLEAR

MIB Name	bsnTrustedApHasInvalidSsid (bsnClearTrapVariable set to true).
WCS Message	Trusted AP "{0}" had invalid SSID. The alert state is clear now.
Symptoms	The system has cleared a previous alert about a trusted access point.
WCS Severity	Informational.
Probable Causes	The trusted access point has now conformed to the configured policy.
Recommended Actions	None.

TRUSTED_AP_MISSING

MIB Name	bsnTrustedApIsMissing.
WCS Message	Trusted AP "{0}" is missing or has failed.
Symptoms	The wireless system no longer detects a trusted access point.
WCS Severity	Major.
Probable Causes	A trusted access point has left the network or has failed.
Recommended Actions	Track down the trusted access point and take the appropriate action.

TRUSTED_AP_MISSING_CLEAR

MIB Name	bsnTrustedApIsMissing (bsnClearTrapVariable set to true).
WCS Message	Trusted AP "{0}" is missing or has failed. The alert state is clear now.
Symptoms	The system has found a trusted access point again.
WCS Severity	Informational.
Probable Causes	The system has detected a previously missing trusted access point.
Recommended Actions	None.

Traps Added in Release 2.2

AP_IMPERSONATION_DETECTED

MIB Name	bsnAPImpersonationDetected.
WCS Message	AP Impersonation with MAC "{0}" is detected by authenticated AP "{1}" on "{2}" radio and Slot ID "{3}."
Symptoms	A radio of an authenticated access point has heard from another access point whose MAC address neither matches that of a rogue nor is it an authenticated neighbor of the detecting access point.
WCS Severity	Critical.
Probable Causes	A severity breach related to access point impersonation may be under way.
Recommended Actions	Track down the MAC address of the impersonating access point in the network and contain it.

AP_RADIO_CARD_RX_FAILURE

MIB Name	bsnAPRadioCardRxFailure.
WCS Message	Receiver failure detected on the "{0}" radio of AP "{1}" on Switch "{2}."
Symptoms	A radio card is unable to receive data.
WCS Severity	Critical.
Probable Causes	• A radio card is experiencing reception failure. • The antenna of the radio is disconnected.
Recommended Actions	• Check the access point's antenna connection. • Call customer support.

AP_RADIO_CARD_RX_FAILURE_CLEAR

MIB Name	bsnAPRadioCardRxFailureClear.
WCS Message	Receiver failure cleared on the "{0}" radio of AP "{1}" on Switch "{2}."
Symptoms	A radio is no longer experiencing reception failure.
WCS Severity	Informational.
Probable Causes	A malfunction in the access point has been corrected.
Recommended Actions	None.

AP_RADIO_CARD_TX_FAILURE

MIB Name	bsnAPRadioCardTxFailure.
WCS Message	Transmitter failure detected on the "{0}" radio of AP "{1}" on Switch "{2}."
Symptoms	A radio card is unable to transmit.
WCS Severity	Critical.
Probable Causes	• A radio card is experiencing transmission failure. • The antenna of the radio may be disconnected.
Recommended Actions	• Check the antenna of the access point. • Call customer support.

AP_RADIO_CARD_TX_FAILURE_CLEAR

MIB Name	bsnAPRadioCardTxFailureClear.
WCS Message	Transmitter failure cleared on the "{0}" radio of AP "{1}" on Switch "{2}."
Symptoms	A radio is no longer experiencing transmission failure.
WCS Severity	Informational.
Probable Causes	A malfunction in the access point has been corrected.
Recommended Actions	None.

SIGNATURE_ATTACK_CLEARED

MIB Name	bsnSignatureAttackDetected (bsnClearTrapVariable is set to True).
WCS Message	Switch "{0}" is cleared from IDS signature attack. The wireless system is no longer detecting the intrusion.
Symptoms	The switch (controller) no longer detects a signature attack.
WCS Severity	Informational.
Probable Causes	The signature attack that the system previously detected has stopped.
Recommended Actions	None.

SIGNATURE_ATTACK_DETECTED

MIB Name	bsnSignatureAttackDetected
WCS Message	IDS Signature attack detected on Switch "{0}." The Signature Type is "{1}," Signature Name is "{2}," and Signature description is "{3}."
Symptoms	The switch (controller) is detecting a signature attack. The switch (controller) has a list of signatures that it monitors. When it detects a signature, it provides the name of the signature attack in the alert it generates.
WCS Severity	Critical.
Probable Causes	Someone is mounting a malevolent signature attack.
Recommended Actions	Track down the source of the signature attack in the wireless network and take the appropriate action.

TRUSTED_AP_HAS_INVALID_PREAMBLE

MIB Name	bsnTrustedApHasInvalidPreamble.
WCS Message	Trusted AP "{0}" on Switch "{3}" has invalid preamble. It is using "{1}" instead of "{2}." It has been auto contained as per WPS policy.
Symptoms	The system has contained a trusted rogue access point for using an invalid preamble.
WCS Severity	Major.
Probable Causes	The system has detected a possible severity breach because a rogue is transmitting an invalid preamble.
Recommended Actions	Locate the rogue access point using location features or the access point detecting it and take the appropriate actions.

TRUSTED_HAS_INVALID_PREAMBLE_CLEARED

MIB Name	bsnTrustedApHasInvalidPreamble (bsnClearTrapVariable is set to true).
WCS Message	Trusted AP "{0}" on Switch "{3}" had invalid preamble. The alert state is clear now.
Symptoms	The system has cleared a previous alert about a trusted access point.
WCS Severity	Informational.
Probable Causes	The system has cleared a previous alert about a trusted access point.
Recommended Actions	None.

Traps Added in Release 3.0

AP_FUNCTIONALITY_DISABLED

MIB Name	bsnAPFunctionalityDisabled.
WCS Message	AP functionality has been disabled for key "{0}," reason being "{1}" for feature-set "{2}."
Symptoms	The system sends this trap out when the controller disables access point functionality because the license key has expired.
WCS Severity	Critical.
Probable Causes	When the controller boots up, it checks whether the feature license key matches the controller's software image. If it does not, the controller disables access point functionality.
Recommended Actions	Configure the correct license key on the controller and reboot it to restore access point functionality.

AP_IP_ADDRESS_FALLBACK

MIB Name	bsnAPIPAddressFallback.
WCS Message	AP "{0}" with static-ip configured as "{2}" has fallen back to the working DHCP address "{1}."
Symptoms	This trap is sent out when an access point, with the configured static ip-address, fails to establish connection with the outside world and starts using DHCP as a fallback option.
WCS Severity	Minor.
Probable Causes	If the configured IP address on the access point is incorrect or obsolete, and if the AP Fallback option is enabled on the switch (controller), the access point starts using DHCP.
Recommended Actions	Reconfigure the access point's static IP to the correct IP address if desired.

AP_REGULATORY_DOMAIN_MISMATCH

MIB Name	bsnAPRegulatoryDomainMismatch.
WCS Message	AP "{1}" is unable to associate. The Regulatory Domain configured on it "{3}" does not match the Controller "{0}" country code "{2}."
Symptoms	The system generates this trap when an access point's regulatory domain does not match the country code configured on the controller. Due to the country code mismatch, the access point will fail to associate with the controller.
WCS Severity	Critical.
Probable Causes	• If someone changes the controller's country code configuration and some of the existing access points support a different country code, these access points fail to associate. • An access point on the controller's network sends join requests to the controller, but the regulatory domain is outside the domain in which the controller is operating.
Recommended Actions	Either remove the access points that are not meant for inclusion in the controller's domain or correct the controller's country code setting.

RX_MULTICAST_QUEUE_FULL

MIB Name	bsnRxMulticastQueueFull.
WCS Message	CPU Receive Multicast Queue is full on Controller "{0}."
Symptoms	This trap indicates that the CPU's Receive Multicast queue is full.
WCS Severity	Critical.
Probable Causes	An ARP storm.
Recommended Actions	None.

Traps Added in Release 3.1

AP_AUTHORIZATION_FAILURE

MIB Name	bsnAPAuthorizationFailure
WCS Message	• Failed to authorize AP “{0}." Authorization entry does not exist in Controllers “{1}” AP Authorization List. • Failed to authorize AP “{0}." AP’s authorization key does not match with SHA1 key in Controllers “{1}” AP Authorization List. • Failed to authorize AP “{0}." Controller “{1}” could not verify the Self Signed Certificate from the AP. • Failed to authorize AP “{0}." AP has a self signed certificate where as the Controllers “{1}” AP authorization list has Manufactured Installed Certificate for this AP.
Symptoms	An alert is generated when an access point fails to associate with a controller due to authorization issues.
WCS Severity	Critical.
Probable Causes	• The access point is not on the controller's access point authorization list. • The key entry in the controller's access point authorization list does not match the SHA1 key received from the access point. • The access point self-signed certificate is not valid. • The access point has a self-signed certificate and the controller’s access point authorization list (for the given access point) references a manufactured installed certificate.
Recommended Actions	• Add the access point to the controller’s authorization list. • Update the access point’s authorization key to match the controller’s access point key. • Check the accuracy of the access point’s self-signed certificate. • Check the certificate type of the access point in the controller’s access point authorization list.

HEARTBEAT_LOSS_TRAP

MIB Name	heartbeatLossTrap.
WCS Message	Keepalive messages are lost between Master and Controller"{0}.”
Symptoms	This trap is generated when the controller loses connection with the Supervisor Switch (in which it is physically embedded) and the controller cannot hear the heartbeat (keepalives) from the Supervisor.
WCS Severity	Major.
Probable Causes	• Port on the WiSM controller could be down. • Loss of connection with the Supervisor Switch.
Recommended Actions	None.

INVALID_RADIO_INTERFACE

MIB Name	invalidRadioTrap.
WCS Message	Radio with MAC address “{0}” and protocol “{1}” that has joined controller “{2}” has invalid interface. The reason is “{3}.”
Symptoms	If a Cisco access point joins the network but has unsupported radios, the controller detects this and generates a trap. This symptom propogates an alert in WCS.
WCS Severity	Critical.
Probable Causes	The radio hardware is not supported by the controller.
Recommended Actions	None.

RADAR_CLEARED

MIB Name	bsnRadarChannelCleared
WCS Message	Radar has been cleared on channel "{1}" which was detected by AP base radio MAC "{0}" on radio 802.11a/n.
Symptoms	Trap is generated after the expiry of a non-occupancy period for a channel that previously generated a radar trap.
WCS Severity	Informational.
Probable Causes	Trap is cleared on a channel.
Recommended Actions	None.

RADAR_DETECTED

MIB Name	bsnRadarChannelDetected
WCS Message	Radar has been detected on channel "{1}" by AP base radio MAC "{0}" on radio 802.11a/n.
Symptoms	This trap is generated when radar is detected on the channel on which an access point is currently operating.
WCS Severity	Informational.
Probable Causes	Radar is detected on a channel.
Recommended Actions	None.

RADIO_CORE_DUMP

MIB Name	radioCoreDumpTrap
WCS Message	Radio with MAC address “{0}” and protocol “{1}” has core dump on controller “{2}."
Symptoms	When a Cisco radio fails and a core dump occurs, the controller generates a trap and WCS generates an event for this trap.
WCS Severity	Informational.
Probable Causes	Radio failure.
Recommended Actions	Capture the core dump file using the controller’s command line interface and send to TAC support.

RADIO_INTERFACE_DOWN

MIB Name	bsnAPIfDown.
WCS Message	Radio with MAC address “{0}” and protocol “{1}” is down. The reason is “{2}.”
Symptoms	When a radio interface is down, WCS generates an alert. Reason for the radio outage is also noted.
WCS Severity	Critical if not manually disabled. Informational if radio interface was manually disabled.
Probable Causes	• The radio interface has failed. • The access point cannot draw enough power. • The maximum number of transmissions for the access point is reached. • The access point has lost connection with the controller heart beat. • The admin status of the access point admin is disabled. • The admin status of the radio is disabled.
Recommended Actions	None.

RADIO_INTERFACE_UP

MIB Name	bsnAPIfUp.
WCS Message	Radio with MAC address “{0}” and protocol “{1}” is up. The reason is “{2}.”
Symptoms	When a radio interface is operational again, WCS clears the previous alert. Reason for the radio being up again is also noted.
WCS Severity	Informational.
Probable Causes	• Admin status of access point is enabled. • Admin status of radio is enabled. • Global network admin status is enabled.
Recommended Actions	None.

UNSUPPORTED_AP

MIB Name	unsupportedAPTrap.
WCS Message	AP "{0}" tried to join controller "{1}" and failed. The controller does not support this kind of AP.
Symptoms	When unsupported access points try to join 40xx/410x controllers or 3500 controller with 64 MB flash, these controllers generate a trap, and the trap is propagated as an event in WCS.
WCS Severity	Informational.
Probable Causes	Access point is not supported by the controller.
Recommended Actions	None.

Traps Added in Release 3.2

LOCATION_NOTIFY_TRAP

MIB Name	locationNotifyTrap.
WCS Message	Depending on the notification condition reported, the trap is sent out in an XML format and is reflected in WCS with the following alert messages: • Absence of <Element> with MAC <macAddress>, last seen at <timestamp>. • <Element> with MAC <macAddress> is <In | Out> the Area <campus | building | floor | coverageArea>. • <Element> with MAC <macAddress> has moved beyond <specifiedDistance> ft. of marker <MarkerName>, located at a range of <foundDistance> ft. For detailed info on the XML format for the trap content, consult the *2700 Location Appliance Configuration Guide*.
Symptoms	A 2700 location appliance sends this trap out when the defined location notification conditions are met (such at element outside area, elements missing, and elements exceeded specified distance). WCS uses this trap to display alarms about location notification conditions.
WCS Severity	Minor (under the Location Notification dashboard).
Probable Causes	The location notification conditions configured for a 2700 location appliance are met for certain elements on the network.
Recommended Actions	None.

Traps Added In Release 4.0

CISCO_LWAPP_MESH_POOR_SNR

MIB Name	ciscoLwappMeshPoorSNR
WCS Message	Poor SNR.
Symptoms	SNR (signal-to-noise) ratio is important because high signal strength is not enough to ensure good receiver performance. The incoming signal must be stronger than any noise or interference that is present. For example, you can have high signal strength and still have poor wireless performance if there is strong interference or a high noise level.
WCS Severity	Major.
Probable Causes	The link SNR fell below 12 db. The threshold level cannot be changed. If poor SNR is detected on the backhaul link for a child or parent, the trap is generated and contains SNR values and MAC addresses.
Recommended Actions	None.

CISCO_LWAPP_MESH_PARENT_CHANGE

MIB Name	ciscoLwappMeshParentChange
WCS Message	Parent changed.
Symptoms	When the parent is lost, the child joins with another parent, and the child sends traps containing both old and new parent's MAC addresses.
WCS Severity	Info.
Probable Causes	The child moved to another parent.
Recommended Actions	None.

CISCO_LWAPP_MESH_CHILD_MOVED

MIB Name	ciscoLwappMeshChildMoved
WCS Message	Child moved.
Symptoms	When the parent access point detects a child being lost and communication is halted, the child lost trap is sent to WCS, along with the child MAC address.
WCS Severity	Info.
Probable Causes	The child moved from the parent.
Recommended Actions	None.

CISCO_LWAPP_MESH_CONSOLE_LOGIN

MIB Name	ciscoLwappMeshConsoleLogin
WCS Message	Console login successful or failed.
Symptoms	The console port provides the ability for the customer to change the user name and password to recover the stranded outdoor access point. To prevent any unauthorized user access to the access point, WCS sends an alarm when someone tries to log in. This alarm is required to provide protection because the access point is physically vulnerable being located outdoors.
WCS Severity	A login is of critical severity.
Probable Causes	You have successfully logged in to the access point console port or failed on three consecutive tries.
Recommended Actions	None.

CISCO_LWAPP_MESH_AUTHORIZATION_FAILURE

MIB Name	ciscoLwappMeshAuthorizationFailure
WCS Message	Fails to authenticate with controller.
Symptoms	WCS receives a trap from the controller. The trap contains the MAC addresses of those access points that failed authorization.
WCS Severity	Minor.
Probable Causes	The access point tried to join the MESH but failed to authenticate because the MESH node MAC address was not on the MAC filter list.
Recommended Actions	None.

CISCO_LWAPP_MESH_CHILD_EXCLUDED_PARENT

MIB Name	ciscoLwappMeshChildExcludedParent
WCS Message	Parent AP being excluded by child AP.
Symptoms	When a child fails authentication at the controller after a fixed number of attempts, the child can exclude that parent. The child remembers the excluded parent so that when it joins the network, it sends the trap which contains the excluded parent MAC address and the duration of the exclusion period.
WCS Severity	Info.
Probable Causes	A child marked a parent for exclusion.
Recommended Actions	None.

CISCO_LWAPP_MESH_EXCESSIVE_PARENT_CHANGE

MIB Name	ciscoLwappMeshExcessiveParentChange
WCS Message	Parent changed frequently.
Symptoms	When MAP parent-change-counter exceeds the threshold within a given duration, it sends a trap to WCS. The trap contains the number of times the MAP changes and the duration of the time. The threshold is user configurable.
WCS Severity	Major.
Probable Causes	The MESH access point changed its parent frequently.
Recommended Actions	None.

IDS_SHUN_CLIENT_TRAP

MIB Name	CISCO-LWAPP-IDS-MIB. CLIdsNewShunClient.
WCS Message	The Cisco Intrusion Detection System "{0}" has detected a possible intrusion attack by the wireless client "{1}."
Symptoms	This trap is generated in response to a shun client clear alert originated from a Cisco IDS/IPs appliance ("{0}") installed in the data path between the wireless client ("{1}") and the site's intranet.
WCS Severity	Critical.
Probable Causes	The designated client is generating a packet-traffic pattern which shares properties with a well-known form of attack on the customer's network.
Recommended Actions	Investigate the designated client and determine if it is an intruder, a virus, or a false alarm.

IDS_SHUN_CLIENT_CLEAR_TRAP

MIB Name	CISCO-LWAPP-IDS-MIB. cLIdsNewShunClientClear.
WCS Message	The Cisco Intrusion Detection System "{0}" has cleared the wireless client "{1}" from possibly having generated an intrusion attack.
Symptoms	This trap is generated is response to one of two things: 1) a shun client clear alert originated from a Cisco IDS/IPS appliance ("{0}") installed in the data path between the wireless client ("{1"}) and the site's intranet, or 2) a scheduled timeout of the original IDS_SHUN_CLIENT_TRAP for the wireless client.
WCS Severity	Clear.
Probable Causes	The designated client is no longer generating a suspicious packet-traffic pattern.
Recommended Actions	None.

MFP_TIMEBASE_STATUS_TRAP

MIB Name	CISCO-LWAPP-MFP-MIB. ciscoLwappMfpTimebaseStatus.
WCS Message	Controller "{0}" is "{1}" with the Central time server.
Symptoms	This notification is sent by the agent to indicate when the synchronization of the controller's time base with the Central time base last occurred.
WCS Severity	Critical (not in sync trap) and clear (sync trap).
Probable Causes	The controller's time base is not in sync with the Central time base.
Recommended Actions	None.

MFP_ANOMALY_DETECTED_TRAP

MIB Name	CISCO-LWAPP-MFP-MIB. ciscoLwappMfpAnomalyDetected.
WCS Message	MFP configuration of the WLAN was violated by the radio interface "{0}" and detected by the radio interface "{1}" of the access point with MAC address "{2}." The violation is "{3}."
Symptoms	This notification is sent by the agent when the MFP configuration of the WLAN was violated by the radio interface cLApIfSmtDot11Bssid and detected by the radio interface cLApDot11IfSlotId of the access point cLApSysMacAddress. This violation is indicated by cLMfpEventType. When observing the management frame(s) given by cLMfpEventFrames for the last cLMfpEventPeriod time units, the controller reports the occurrence of a total of cLMfpEventTotal violation events of type cLMfpEventType. When the cLMfpEventTotal is 0, no further anomalies have recently been detected, and the NMS should clear any alarm raised about the MFP errors. **Note** This notification is generated by the controller only if MFP was configured as the protection mechanism through cLMfpProtectType.
WCS Severity	Critical.
Probable Causes	The MFP configuration of the WLAN was violated. Various types of violations are invalidMic, invalidSeq, noMic, and unexpectedMic.
Recommended Actions	None.

GUEST_USER_REMOVED_TRAP

MIB Name	CISCO-LWAPP-WEBAUTH-MIB. cLWAGuestUserRemoved.
WCS Message	Guest user "{1}" deleted on controller "{0}."
Symptoms	This notification is generated when the lifetime of the guest user {1} expires and the guest user's accounts are removed from the controller "{0}."
WCS Severity	Critical.
Probable Causes	GuestUserAccountLifetime expired.
Recommended Actions	None.

Traps Added or Updated in Release 4.0.96.0

AP_IMPERSONATION_DETECTED

MIB Name	bsnAPImpersonationDetected.
WCS Message	AP Impersonation with MAC "{0}" using source MAC "{1}" is detected by authenticated AP "{2}" on "{3}" radio and slot ID "{4}."
Symptoms	A radio of an authenticated access point had communication with another access point whose MAC address neither matches that of a rogue nor is an authenticated neighbor of the detecting access point.
WCS Severity	Critical.
Probable Causes	A security breach related to access point impersonation may be occurring.
Recommended Actions	Track down the MAC address of the impersonating access point and contain it.

RADIUS_SERVER_DEACTIVATED

MIB Name	ciscoLwappAAARadiusServerGlobalDeactivated.
WCS Message	RADIUS server "{0}" (port {1}) is deactivated.
Symptoms	The controller detects that the RADIUS server is deactivated in the global list.
WCS Severity	Major.
Probable Causes	RADIUS server is deactivated in the global list.
Recommended Actions	None.

RADIUS_SERVER_ACTIVATED

MIB Name	ciscoLwappAAARadiusServerGlobalDeactivated.
WCS Message	RADIUS server "{0}" (port {1}) is activated.
Symptoms	The controller detects that the RADIUS server is deactivated in the global list.
WCS Severity	Major.
Probable Causes	RADIUS server is deactivated in the global list.
Recommended Actions	None.

RADIUS_SERVER_WLAN_DEACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerWlanDeactivated.
WCS Message	RADIUS server "{0}" (port {1}) is deactivated on WLAN "{2}."
Symptoms	The controller detects that the RADIUS server is deactivated on the WLAN.
WCS Severity	Major.
Probable Causes	RADIUS server is deactivated on the WLAN.
Recommended Actions	None.

RADIUS_SERVER_WLAN_ACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerWlanActivated.
WCS Message	RADIUS server "{0}" (port {1}) is activated on WLAN "{2}."
Symptoms	The controller detects that the RADIUS server is activated on the WLAN.
WCS Severity	Clear.
Probable Causes	RADIUS server is activated on the WLAN.
Recommended Actions	None.

RADIUS_SERVER_TIMEOUT

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusReqTimedOut.
WCS Message	RADIUS server "{0}" (port {1}) failed to respond to request from client "{2}" with MAC "{3}."
Symptoms	The controller detects that the RADIUS server failed to respond to a request from a client or user.
WCS Severity	Informational.
Probable Causes	RADIUS server fails to process the request from the client or user.
Recommended Actions	None.

DECRYPT_ERROR_FOR_WRONG_WPA_WPA2

MIB Name	CISCO-LWAPP-DOT11-CLIENT-MIB. CiscoLwappDot11ClientKeyDecryptError.
WCS Message	Decrypt error occurred at AP with MAC "{0}" running TKIP with wrong WPA/WPA2 by client with MAC "{1}."
Symptoms	The controller detects that a user is trying to connect with an invalid security policy for WPA/WPA2 types.
WCS Severity	Minor.
Probable Causes	The user failed to authenticate and join the controller.
Recommended Actions	None.

Traps Added or Updated in Release 4.1

AP_IMPERSONATION_DETECTED

MIB Name	bsnAPImpersonationDetected.
WCS Message	AP impersonation of MAC "{0}" using source MAC "{1}" is detected by an authenticated AP "{2}" on "{3}" radio and slot ID "{4}."
Symptoms	A radio of an authenticated access point received signals from another access point whose MAC address neither matches that of a rogue nor is an authenticated neighbor of the detecting access point.
WCS Severity	Critical.
Probable Causes	A security breach related to access point impersonation has occurred.
Recommended Actions	Track down the MAC address of the impersonating access point and contain it.

INTERFERENCE_DETECTED

MIB Name	COGNIO-TRAPS-MIB.cognioInterferenceDetected.
WCS Message	Interference detected by type {0} with power {1}.
Symptoms	A Cognio spectrum agent detected interference over its configured thresholds.
WCS Severity	Minor.
Probable Causes	Excessive wireless interference or noise.
Recommended Actions	None.

INTERFERENCE_CLEAR

MIB Name	COGNIO-TRAPS-MIB. cognioInterferenceClear
WCS Message	Interference cleared.
Symptoms	The Cognio spectrum expert agent no longer detects an interference source over its configured threshold.
WCS Severity	Clear.
Probable Causes	Previous excessive wireless interference or noise is gone.
Recommended Actions	None.

ONE_ANCHOR_ON_WLAN_UP

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityOneAnchorOnWlanUp.
WCS Message	Controller "{0}." An anchor of WLAN "{1}" is up.
Symptoms	Successive EoIP and UDP ping to at least one anchor on the WLAN is up.
WCS Severity	Clear.
Probable Causes	At least one anchor is reachable from an EoIP/UDP ping.
Recommended Actions	None.

RADIUS_SERVER_DEACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerGlobalDeactivated.
WCS Message	RADIUS server "{0}" (port {1}) is deactivated.
Symptoms	The controller detects that the RADIUS server is deactivated in the global list.
WCS Severity	Major.
Probable Causes	RADIUS server is deactivated in the global list.
Recommended Actions	None.

RADIUS_SERVER_ACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerGlobalActivated.
WCS Message	RADIUS server "{0}" (port {1}) is activated.
Symptoms	The controller detects that the RADIUS server is activated in the global list.
WCS Severity	Clear.
Probable Causes	RADIUS server is activated in the global list.
Recommended Actions	None.

RADIUS_SERVER_WLAN_DEACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerWlanDeactivated.
WCS Message	RADIUS server "{0}" (port {1}) is deactivated on WLAN "{2}."
Symptoms	The controller detects that the RADIUS server is deactivated on the WLAN.
WCS Severity	Major.
Probable Causes	RADIUS server is deactivated on the WLAN.
Recommended Actions	None.

RADIUS_SERVER_WLAN_ACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerGlobalWlanActivated.
WCS Message	RADIUS server "{0}" (port {1}) is activated on WLAN "{2}."
Symptoms	The controller detects that the RADIUS server is activated on the WLAN.
WCS Severity	Clear.
Probable Causes	RADIUS server is activated on the WLAN.
Recommended Actions	None.

RADIUS_SERVER_TIMEOUT

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusReqTimedOut.
WCS Message	RADIUS server "{0}" (port {1}) failed to respond to request from client "{2}" with MAC "{3}."
Symptoms	The controller detects that the RADIUS server failed to respond to a request from the client or user.
WCS Severity	Informational.
Probable Causes	The RADIUS server fails to process the request from a client or user.
Recommended Actions	None.

MOBILITY_ANCHOR_CTRL_PATH_DOWN

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorControlPathDown.
WCS Message	Controller "{0}." Control path on anchor "{1}" is down.
Symptoms	When successive ICMP ping attempts to the anchor fails, the anchor is conclusively down.
WCS Severity	Major.
Probable Causes	Anchor not reachable by ICMP ping.
Recommended Actions	None.

MOBILITY_ANCHOR_CTRL_PATH_UP

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorControlUp.
WCS Message	Controller "{0}." Control path on anchor "{1}" is up.
Symptoms	The ICMP ping to the anchor is restored, and the anchor is conclusively up.
WCS Severity	Clear.
Probable Causes	The anchor is reachable by an ICMP ping.
Recommended Actions	None.

MOBILITY_ANCHOR_DATA_PATH_DOWN

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorDataPathDown.
WCS Message	Controller "{0}." Data path on anchor "{1}" is down.
Symptoms	Successive EoIP ping attempts to the anchor fails, and the anchor is conclusively down.
WCS Severity	Major.
Probable Causes	The anchor is not reachable by an EoIP ping.
Recommended Actions	None.

MOBILITY_ANCHOR_DATA_PATH_UP

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorDataPathUp.
WCS Message	Controller "{0}." Data path on anchor "{1}" is up.
Symptoms	The EoIP ping to the anchor is restored, and the anchor is conclusively up.
WCS Severity	Clear.
Probable Causes	Anchor is reachable by the EoIP ping.
Recommended Actions	None.

WLAN_ALL_ANCHORS_TRAP_DOWN

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAllAnchorsOnWlanDown.
WCS Message	Controller "{0}." All anchors of WLAN "{1}" are down.
Symptoms	Successive EoIP ping attempts to all the anchors on WLAN is occurring.
WCS Severity	Critical.
Probable Causes	Anchors are not reachable by the EoIP ping.
Recommended Actions	None.

MESH_AUTHORIZATIONFAILURE

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshAuthorizationFailure.
WCS Message	MESH "{0}" fails to authenticate with controller because "{1}"
Symptoms	A mesh access point failed to join the mesh network because its MAC address is not listed in the MAC filter list. The alarm includes the MAC address of the mesh access point that failed to join.
WCS Severity	Minor.
Probable Causes	The mesh node MAC address is not in the MAC filter list, or a security failure from the authorization server occurred.
Recommended Actions	None.

MESH_CHILDEXCLUDEDPARENT

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshChildExcludedParent.
WCS Message	Parent AP being excluded by child AP due to failed authentication, AP current parent MAC address "{0}," previous parent MAC address "{1}."
Symptoms	This notification is sent by the agent when the child access point marks a parent access point for exclusion. When the child fails to authenticate at the controller after a fixed number of times, the child marks the parent for exclusion. The child remembers the excluded MAC address and informs the controller when it joins the network. The child access point marks the MAC address and excludes it for the time determined by MAP node so that it does not try to join this excluded node. The child MAC address is sent as part of the index.
WCS Severity	Info.
Probable Causes	The child access point failed to authenticate to the controller after a fixed number of times.
Recommended Actions	None.

MESH_PARENTCHANGE

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshParentChange.
WCS Message	MESH "{0}" changed its parent. AP current parent MAC address "{1}," previous parent MAC address "{2}."
Symptoms	This notification is sent by the agent when a child moves to another parent. The alarm includes the MAC addresses of the former and current parents.
WCS Severity	Info.
Probable Causes	The child access point has changed its parent.
Recommended Actions	None.

MESH_CHILDMOVED

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshChildMoved.
WCS Message	Parent AP lost connection to this AP. AP neighbor type is "{0}."
Symptoms	This notification is sent by the agent when the parent access point loses connection with its child.
WCS Severity	Info.
Probable Causes	The parent access point lost connection with its child.
Recommended Actions	None.

MESH_EXCESSIVEPARENTCHANGE

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshExcessiveParentChange.
WCS Message	MESH "{0}" changes parent frequently.
Symptoms	This notification is sent by the agent if the number of parent changes for a given mesh access point exceeds the threshold. Each access point keeps count of the number of parent changes within a fixed time. If the count exceeds the threshold defined by c1MeshExcessiveParentChangeThreshold, then the child access point informs the controller.
WCS Severity	Major.
Probable Causes	The child access point has frequently changed its parent.
Recommended Actions	None.

MESH_POORSNR

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshPoorSNR.
WCS Message	MESH "{0}" has SNR on backhaul link as "{1}" which is lower then predefined threshold.
Symptoms	This notification is sent by the agent when the child access point detects a signal-to-noise ratio below 12dB the backhaul link. The alarm includes the SNR value and the MAC addresses of the parent and child.
WCS Severity	Major.
Probable Causes	SNR is lower then the threshold defined by c1MeshSNRThreshold.
Recommended Actions	None.

MESH_POORSNRCLEAR

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshPoorSNRClear.
WCS Message	MESH "{0}" has SNR on backhaul link as "{1}" which is normal now.
Symptoms	This notification is sent by the agent to clear ciscoLwappMeshPoorSNR when the child access point detects SNR on the backhaul link that is higher than the threshold defined by c1MeshSNRThreshold.
WCS Severity	Info.
Probable Causes	SNR on the backhaul link is higher than the threshold defined by c1MeshSNRThreshold.
Recommended Actions	None.

MESH_CONSOLELOGIN

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshConsoleLogin.
WCS Message	MESH "{0}" has console logged in with status "{1}"
Symptoms	This notification is sent by the agent when login on the MAP console is successful or when a failure occurred after three attempts.
WCS Severity	Critical.
Probable Causes	Login on the MAP console was successful, or a failure occurred after three attempts.
Recommended Actions	None.

LRADIF_REGULATORY_DOMAIN

MIB Name	ciscoLwappApIfRegulatoryDomainMismatchNotif
WCS Message	Access Point "{0}" is unable to associate. The Regulatory Domain "{1}" configured on interface "{2}" does not match the controller "{3}" regulatory domain "{4}."
Symptoms	The system generates this trap when the regulatory domain configured on the access point radios does not match the country code configured on the controller.
WCS Severity	Critical.
Probable Causes	If the controller's country code configuration is changed, and some access points support a different country code, then these access points fail to associate. An access point on the controller's network sends join requests to the controller, but the regulatory domain is outside the domain in which the controller is operating.
Recommended Actions	Either remove the access points that are not meant for inclusion in the controller's domain or correct the controller's country code setting.

LRAD_CRASH

MIB Name	ciscoLwappApCrash
WCS Message	Access Point "{0}" crashed and has a core dump on controller "{1}."
Symptoms	An access point has crashed.
WCS Severity	Info.
Probable Causes	Access point failure.
Recommended Actions	Capture the core dump file using the controller's CLI and send it to TAC support.

LRAD_UNSUPPORTED

MIB Name	ciscoLwappApUnsupported
WCS Message	Access Point "{0}" tried to join controller "{1}" and failed. Associate failure reason "{2}."
Symptoms	An access point tried to associate to a controller to which it is not supported.
WCS Severity	Info.
Probable Causes	The access point is not supported by the controller.
Recommended Actions	None.

Traps Added or Updated in Release 4.2

GUEST_USER_ADDED

MIB Name	CISCO-LWAPP-WEBAUTH-MIB. cLWAGuestUserAdded
WCS Message	Guest user "{0}" created on the controller "{1}."
Symptoms	This notification is sent by the agent when the GuestUser account is created successfully.
WCS Severity	Info.
Probable Causes	The guest user account was created on the agent by either CLI, Web UI, or WCS.
Recommended Actions	None.

GUEST_USER_AUTHENTICATED

MIB Name	CISCO-LWAPP-WEBAUTH-MIB. cLWAGuestUserLogged
WCS Message	Guest user "{0}" logged into controller "{1}."
Symptoms	This notification is sent by the agent when the GuestUser logged into the network through webauth successfully.
WCS Severity	Info.
Probable Causes	The guest user was successful with webauth authentication.
Recommended Actions	None.

IOSAP_LINK_UP

MIB Name	linkUp
WCS Message	Autonomous AP “{0},” Interface “{1}” is {2} up.
Symptoms	The physical link is up on an autonomous access point radio port.
WCS Severity	Clear.
Probable Causes	A physical link has been restored to the autonomous access point.
Recommended Actions	None.

IOSAP_LINK_DOWN

MIB Name	linkDown
WCS Message	Autonomous AP “{0},” Interface “{1}” is {2} down.
Symptoms	The physical link is down on an autonomous access point radio port.
WCS Severity	Critical.
Probable Causes	The radio port of an autonomous access point was disabled manually or a port failure occurred.
Recommended Actions	Check the administrative status of the port. If the port administrative status is not down, check other port settings.

IOSAP_UP

MIB Name	None.
WCS Message	The autonomous AP "{0}" is reachable.
Symptoms	The autonomous AP is SNMP reachable.
WCS Severity	Clear.
Probable Causes	The autonomous access point starts to respond to SNMP queries.
Recommended Actions	None.

IOSAP_DOWN

MIB Name	None.
WCS Message	Autonomous AP "{0}" is unreachable.
Symptoms	The autonomous AP is SNMP unreachable.
WCS Severity	Critical.
Probable Causes	• Network connectivity to the autonomous access point is broken. • Ethernet port of the autonomous access point is down. • SNMP agent is not running in the autonomous access point. • SNMP credentials on the WCS do not match the SNMP credentials configured on the autonomous access point. • SNMP version on the WCS does not match the SNMP version configured on the autonomous access point.
Recommended Actions	First, check the IP connectivity to the access point. Next, check the port status of the access point. Finally, check SNMP credentials on both the WCS and the access point.

WCS_EMAIL_FAILURE

MIB Name	None.
WCS Message	WCS with IP Address "{0}" failed to send e-mail.
Symptoms	This notification is generated by WCS when it fails to send e-mails.
WCS Severity	Major.
Probable Causes	The SNMP server is either not configured or not reachable from WCS.
Recommended Actions	Check Administration > Settings > Mail Server settings. Send a test e-mail from the mail server settings to see if it is successful.

AUDIT_STATUS_DIFFERENCE

MIB Name	None.
WCS Message	Switch “{0}” Audit done at “(1).” Config differences found between WCS and controller.
Symptoms	This notification is generated by WCS when audit differences are detected while auditing a controller during a network audit background task or per controller audit.
WCS Severity	Minor.
Probable Causes	The WCS and controller configuration are not synchronized.
Recommended Actions	Refresh the configuration from the controller so that it synchronizes with the controller configuration on WCS.

LRAD_POE_STATUS

MIB Name	ciscoLwappApPower
WCS Message	Access point “{0}” draws low power from Ethernet. Failure reason: “{1}”
Symptoms	This notification is generated when the access point draws low power from the Ethernet connection.
WCS Severity	Critical.
Probable Causes	The access point receives low power from the Ethernet connection.
Recommended Actions	Check the power status of the access point and the device connected to the access point.

ROGUE_AP_NOT_ON_NETWORK

MIB Name	bsnRogueAPDetectedOnWiredNetwork (bsnRogueAPOnWiredNetwork is set to false).
WCS Message	Rogue AP or ad hoc rogue "{0}" is not able to connect to the wired network.
Symptoms	A rogue access point is no longer on the wired network.
WCS Severity	Informational.
Probable Causes	The rogue access point is no longer reachable on the wired network.
Recommended Actions	None.

Traps Added or Updated in Release 5.0

GUEST_USER_LOGOFF

MIB Name	CISCO-LWAPP-WEBAUTH-MIB. cLWAGuestUserLoggedOut
WCS Message	Guest user "{1}" logged out from the controller "{0}."
Symptoms	This notification is sent by the agent when a GuestUser who was previously logged into the network logs out.
WCS Severity	Informational.
Probable Causes	The GuestUser logs off from the network.
Recommended Actions	None.

WCS_NOTIFICATION_FAILURE

MIB Name	None.
WCS Message	WCS with IP Address "{0}" failed to send notification.
Symptoms	This notification is generated by WCS when a notification sent to a northbound receiver fails. Currently only guest user related notifications (such as creation, deletion, log in, and log off) can be sent to a northbound receiver.
WCS Severity	Major.
Probable Causes	The notification receiver is either not configured or not reachable from WCS.
Recommended Actions	Check Administration > Settings > Notification Receiver settings. Make sure the server IP is correct, and the server is reachable from WCS.

WCS_LOW_DISK_SPACE

MIB Name	None.
WCS Message	WCS "{0}" does not meet the minimum hardware requirements for disk space. Available: "{3}." Minimum requirement: "{4}" Mb.
Symptoms	This notification is generated by WCS when the free disk space where WCS is installed does not meet minimum hardware requirements. This event is of major severity if minimum requirements are not met. This event is of critical severity when the available disk space is less than half of the minimum requirement.
WCS Severity	Major/Critical.
Probable Causes	The disk is out of free space.
Recommended Actions	Free up disk space.

WCS_OK_DISK_SPACE

MIB Name	None.
WCS Message	WCS "{0}" meets the minimum hardware requirements for disk space. Available: "{3}." Minimum requirement: "{4}" Mb.
Symptoms	This notification is generated by WCS when the free disk space where WCS is installed has met the minimum hardware requirements.
WCS Severity	Clear.
Probable Causes	A low disk space condition has been cleared.
Recommended Actions	None.

WCS_LOW_DISK_SPACE_BACKUP

MIB Name	None.
WCS Message	WCS "{0}" does not have sufficient disk space in directory "{1}" for backup. Space needed: "{2}," space free: "{3}."
Symptoms	This notification is generated by WCS when a previously created WCS_LOW_DISK_SPACE_BACKUP event is cleared or when the disk contains enough space for a backup.
WCS Severity	Clear.
Probable Causes	A low disk space condition has been cleared.
Recommended Actions	None.

STATION_ASSOCIATE_DIAG_WLAN

MIB Name	CISCO-LWAPP-DOT11-CCX-CLIENT-MIB.cldccDiagClientAssociatedToDiagWlan
WCS Message	Client "{0}" is associated to diagnostic WLAN with reason "{1}."
Symptoms	This notification is sent by the agent when a v5 client associates to a diagnostic channel.
WCS Severity	Info.
Probable Causes	When a CCXv5 client gets associated to the diagnostic channel WLAN on WLC, this trap is raised.
Recommended Actions	If you wish to automatically perform client troubleshooting, you must enable Client Troubleshooting in Administration > Settings > client. After it is enabled, the series of V5 tests are carried out on the client upon trap arrival, and the client is updated with the test status via pop-up messages. The report is placed in the logs directory. The log filename is shown in the Client Details page in the Automated Troubleshooting Report section. You can export all automated troubleshooting logs.

WLAN_SHUT_FAILED

MIB Name	None.
WCS Message	Wlan "{0}" shutdown failed on controller "{1}."
Symptoms	This notification is generated by WCS during scheduled operations for a given WLAN Config object. It notifies the user that the WLAN status did not change at the scheduled time.
WCS Severity	Major.
Probable Causes	The controller for the selected WLAN is not reachable, or the WLAN object does not exist.
Recommended Actions	Check the WCS logs at the time of event generation and verify if the WLAN exists on the controller.

WLAN_SHUT_SUCCESS

MIB Name	None.
WCS Message	Wlan "{0}" successfully shutdown on controller "{1}."
Symptoms	This notification is generated by WCS during scheduled operation for each given WLAN configuration object. It notifies the user that the admin status has been successfully completed.
WCS Severity	Info.
Probable Causes	Verify the admin status for the displayed WLAN on the controller.
Recommended Actions	Remove the event from the event list page.

RADIO_SHUT_FAILED

MIB Name	None.
WCS Message	Radio shutdown failed for AP "{0}" connected to controller "{1}."
Symptoms	This notification is generated by WCS during a scheduled operation for a given list of access point radios. It notifies the user that the status for certain radios has failed to change.
WCS Severity	Major.
Probable Causes	The controllers for the selected access point are not reachable, or the radio configurations are changed on the controller.
Recommended Actions	Check the WCS logs at the time of event generation and verify that the access point is associated with the controller.

RADIO_SHUT_SUCCESS

MIB Name	None.
WCS Message	Radio successfully shutdown for AP "{0}" connected to controller "{1}."
Symptoms	This notification is generated by WCS during scheduled operation for a given list of access point radios. It notifies the user that the admin status has been successfully changed.
WCS Severity	Info.
Probable Causes	None.
Recommended Actions	Verify the status of the specified radio on the controller.

Traps Added or Updated in Release 5.1

CONFIGAUDITSET_ENFORCEMENT_SUCCESS

MIB Name	None.
WCS Message	Successfully enforced Config Group “0” on controllers “1.”
Symptoms	This notification is generated by WCS during network audit when all the templates from the config group (which are opted to be enforced) are successfully enforced.
WCS Severity	Minor.
Probable Causes	The config group (which are opted to be enforced) templates are not in sync with the device values.
Recommended Actions	Look at the controller audit report for the list of enforced values. An alarm is cleared when no enforcements are found during the next network audit cycle.

CONFIGAUDITSET_ENFORCEMENT_FAIL

MIB Name	None.
WCS Message	Failed to enforce Config Group “0” on controllers “1.”
Symptoms	This notification is generated by WCS during network audit when some failures are encountered during enforcement of the templates from the config groups (which as opted to be enforced).
WCS Severity	Critical.
Probable Causes	The config group (which are opted to be enforced) templates are not in sync with the device values.
Recommended Actions	Look at the controller audit report for the list of enforced values and for the failed enforcements. An alarm is cleared upon successful enforcements during the next network audit cycle.

Traps Added or Updated in Release 6.0

STATION_AUTHENTICATED

MIB Name	ciscoLwappDot11ClientMovedToRunState
WCS Message	Client “{0}” is authenticated with interface “{2}” of AP “{1}.”
Symptoms	A client has completed a security policy and has moved to Run state. It can start to send or receive data.
WCS Severity	Informational.
Probable Causes	A client has completed security policy and moved to Run state.
Recommended Actions	None.

WCS_CLIENT_TRAP_DISABLED

MIB Name	None.
WCS Message	Client traps are disabled on controller(s) {0}.
Symptoms	This notification is generated by WCS when required client traps are disabled in one or more controllers. These traps are needed for WCS to detect client sessions in a timely and efficient manner. The required traps are: • 802.11 Association • 802.11 Disassociation • 802.11 Authentication • 802.11 Deauthentication • 802.11 Failed Association • 802.11 Failed Authentication
WCS Severity	Minor.
Probable Causes	When a controller is added to WCS, WCS enables the required client traps. If WCS does not have the correct SNMP read-write community, it could fail. The trap controls can also be changed by pushing the SNMP trap control template or using controller GUI/CLI.
Recommended Actions	Use the WCS template to enable the required client traps on the controller list.

WLC_LICENSE_NOT_ENFORCED

MIB Name	clmgmtLicenseNotEnforced
WCS Message	Controller {0} has AP with unlicensed feature {1} version {2} attempting to join.
Symptoms	An access point with a licensed feature is trying to join a controller without the proper license.
WCS Severity	Critical.
Probable Causes	An access point with a WPLUS feature like indoor mesh or OfficeExtend AP is trying to join a controller without a WPLUS license.
Recommended Actions	You must add a WPLUS license to the controller or fix the primary, secondary, or tertiary controller configuration to have controllers with WPLUS licenses.

WLC_LICENSE_COUNT_EXCEEDED

MIB Name	clmgmtLicenseUsageCountExceeded
WCS Message	Controller {0} with license {1} version {2} and counted feature {4} with limit {3} has been exceeded {5}.
Symptoms	The access point cannot join a controller.
WCS Severity	Critical.

Probable Causes	The controller has reached the maximum licensed access point capacity.
Recommended Actions	Add a license capacity to the controller or move the access point to a controller with more capacity.

VOIP_CALL_FAILURE

MIB Name	ciscoLwappVoipCallfailureNotif
WCS Message	VoIP Call failure of {4} (Error Code {3}) occurred on Client {0} with phone number {5} calling {6} which was associated with AP {1} on interface {2}.
Symptoms	VoIP snooping is enabled on a WLAN.
WCS Severity	Informational.
Probable Causes	A SIP error is detected by an access point.
Recommended Actions	The actions depend on the type of error that is being reported. Errors can range from “dialed number does not exist,” “busy,” “service unavailable,” to “service timeout.”

MSE_EVAL_LICENSE

MIB Name	None
WCS Message	Evaluation license for {0} is expired.
Symptoms	The tracking for clients or tags stops, or service does not start.
WCS Severity	Critical.
Probable Causes	The evaluation period for the service has expired.
Recommended Actions	Add a permanent license for the service using License Center or the appropriate third-party vendor application.

MSE_LICENSING_ELEMENT_LIMIT

MIB Name	None
WCS Message	{0} limit for {1} is reached or exceeded.
Symptoms	Elements are not tracked beyond a certain limit.
WCS Severity	Critical.
Probable Causes	Limit for the specified service has been reached.
Recommended Actions	Add a license with higher licensed capacity to the particular service.

Traps Added or Updated in Release 7.0

- SI_AQ_TRAPS
- SI_SECURITY_TRAPS
- SI_SENSOR_CRASH_TRAPS

SI_AQ_TRAPS

MIB Name	CISCO-LWAPP-SI-MIB.my
WCS Message	Air Quality Index on Channel {0} is {1} (Threshold: {2}).
Symptoms	Too Many interferers (Wi-Fi / non-Wi-Fi).
WCS Severity	Minor.
Probable Causes	Air Quality Index has gone below the threshold.
Recommended Actions	Reduce interference.

SI_SECURITY_TRAPS

MIB Name	CISCO-LWAPP-SI-MIB.my
WCS Message	Security-Risk Interferer {0} is detected by {3}.
Symptoms	Interferers detected which are defined as threat to the network.
WCS Severity	Critical.
Probable Causes	Interference detected by SI chip.
Recommended Actions	Reduce interference.

SI_SENSOR_CRASH_TRAPS

MIB Name	CISCO-LWAPP-SI-MIB.my
WCS Message	CleanAir Sensor Status: {0} Error Code: {1}.
Symptoms	CleanAir Sensor Software stopped working.
WCS Severity	Critical.
Probable Causes	CleanAir sensor is not operational due to crash.
Recommended Actions	Reset AP to resolve the problem.

Unsupported Traps

- BROADCAST_STORM_START: broadcastStormStartTrap
- FAN_FAILURE: fanFailureTrap
- POWER_SUPPLY_STATUS_CHANGE: powerSupplyStatusChangeTrap
- BROADCAST_STORM_END: broadcastStormEndTrap
- VLAN_REQUEST_FAILURE: vlanRequestFailureTrap
- VLAN_DELETE_LAST: vlanDeleteLastTrap
- VLAN_DEFAULT_CFG_FAILURE: vlanDefaultCfgFailureTrap
- VLAN_RESTORE_FAILURE_TRAP: vlanRestoreFailureTrap
- IPSEC_ESP_AUTH_FAILURE: bsnIpsecEspAuthFailureTrap
- IPSEC_ESP_REPLAY_FAILURE: bsnIpsecEspReplayFailureTrap
- IPSEC_ESP_INVALID_SPI: bsnIpsecEspInvalidSpiTrap

- LRAD_UP: bsnAPUp
- LRAD_DOWN: bsnAPDown
- STP_NEWROOT: stpInstanceNewRootTrap
- STP_TOPOLOGY_CHANGE: stpInstanceTopologyChangeTrap
- IPSEC_SUITE_NEG_FAILURE: bsnIpsecSuiteNegFailure
- BSN_DOT11_ESS_CREATED: bsnDot11EssCreated
- BSN_DOT11_ESS_DELETED BSNDOT11ESSDELETED
- LRADIF_RTS_THRESHOLD_CHANGED
- LRADIF_ED_THRESHOLD_CHANGED
- LRADIF_FRAGMENTATION_THRESHOLD_CHANGED
- WARM_START: warmStart
- LINK_FAILURE: linkFailureTrap

CHAPTER 17

Running Reports

Cisco WCS 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 the 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.

Reports are saved in either CSV or PDF format and are either saved to a file on WCS for later download or e-mailed to a specific e-mail address.

The reporting types include the following:

- Current, which provides a snap shot of the data from the last polling cycle without continuously polling
- Historical, which retrieves data from the device periodically and stores it in the WCS database
- Trend, which generates a report using aggregated data. Data can be periodically collected based from devices on user-defined intervals, and a schedule can be established for report generation.

With WCS, you also have the ability to export any report that you can view, sort reports into logical groups, and archive for long-term storage.

Note The number of rows visible in a report depends on the size of the html file, the number of database records, the size of the exported page, the size of the scheduled report, and the WCS server memory size. If you want the report to print as it appears on the page display, you must choose landscape mode. The detailed limitations are as follows:

Maximum number of graphs for a single report—500
Maximum size of an HTTP report (displayed in the Results parameter)—65 Mbs
Maximum number of records for a non-scheduled report—100,000 records
Maximum number of records for a scheduled report—Up to 200,000 records (when physical memory is greater than 1 GB)

The Reports menu provides access to all WCS reports as well as currently saved and scheduled reports.

- Report Launch Pad—The hub for all WCS reports. From this page, you can access specific types of reports and create new reports. See the "Report Launch Pad" section on page 17-2 for more information.
- Scheduled Run Results—Allows you to access and manage all currently scheduled runs in WCS. See the "Managing Scheduled Run Results" section on page 17-9 for more information.

- Saved Reports—Allows you to access and manage all currently saved reports in WCS. See the "Managing Saved Reports" section on page 17-11 for more information.

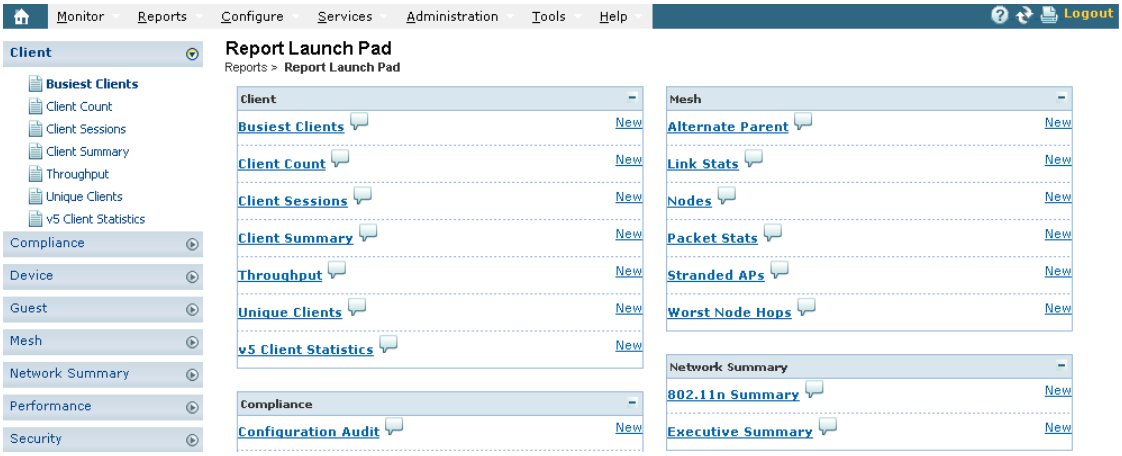
Note See the "Specific WCS Reports" section on page 17-13 for additional information for each report type.

Report Launch Pad

The report launch pad provides access to all WCS reports from a single page. From this page, you can view current reports, open specific types of reports, create and save new reports, and manage scheduled runs (see Figure 17-1).

Tip Hold your mouse cursor over the tool tip next to the report type to view more report details.

Figure 17-1 Report Launch Pad



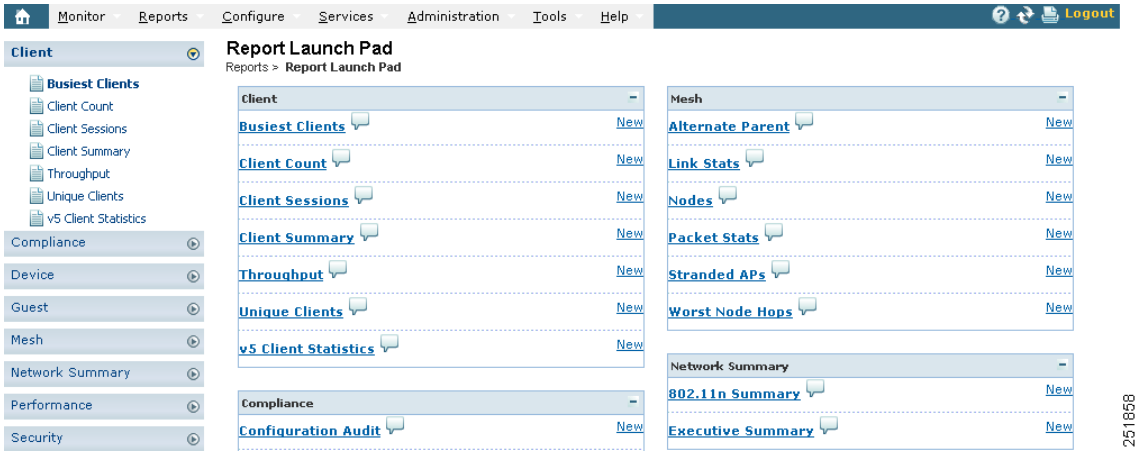
Creating and Running a New Report

To create and run a new report, follow these steps:

Step 1 Choose **Reports > Report Launch Pad**.

The reports are listed by category in the main section of the page and on the left sidebar menu (see Figure 17-2).

Figure 17-2 Report Launch Pad

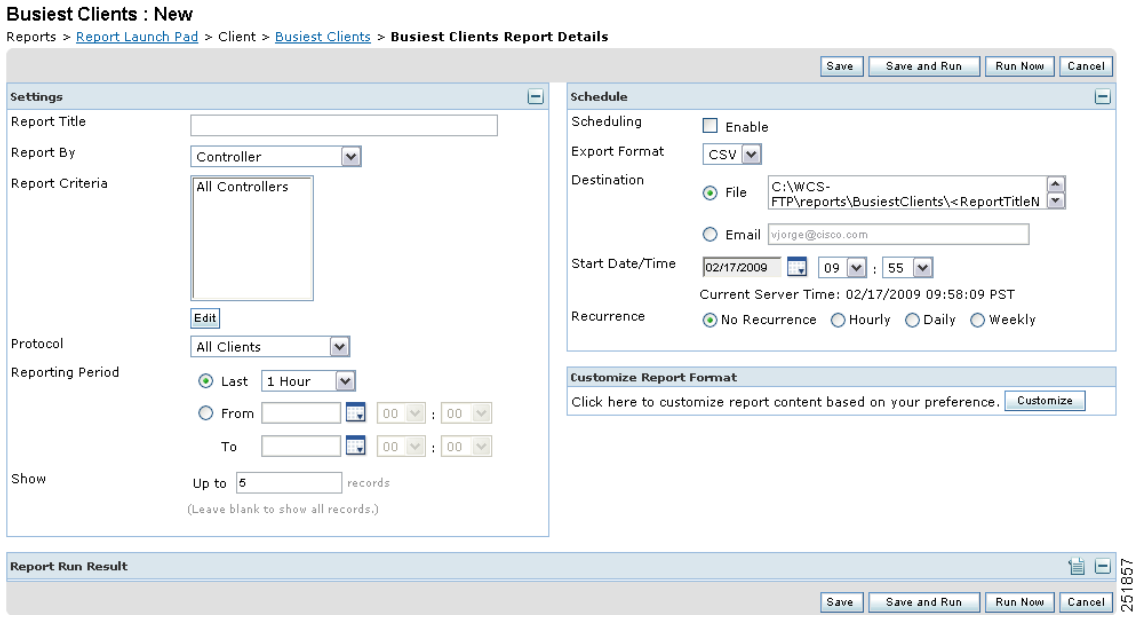


Step 2 Find the appropriate report in the main section of the Report Launch Pad.

Note Click the report name from the Report Launch Pad or use the navigation on the left side of the Report Launch Pad page to view any currently saved reports for that report type.

Step 3 Click **New** to the right of the report. The Report Details page appears (see Figure 17-3).

Figure 17-3 Report Details Page



Step 4 In the Report Details page, enter the following Settings parameters:

Note Certain parameters may or may not appear depending on the report type.

- Report Title—If you plan to use this as a saved report, enter a report name.
- Report By—Select the appropriate Report By category from the drop-down list.
- Report Criteria—The parameter allows you to sort your results depending on the previous Report By selection made. Click **Edit** to open the Filter Criteria page.

Note Click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select 802.11a/n, 802.11b/g/n, or both.
- Report Period
  - Last—Select the **Last** radio button and period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.
- Show—Enter the number of records that you want displayed on each page.

Note Leave the text box blank to display all records.

Step 5 If you plan to run this report at a later time or as a recurring report, enter the Schedule parameters. The Schedule parameters allow you to control when and how often the report runs.

- Enable Schedule—Select the check box to run the report on the set schedule.
- Export Format—Choose your format for exported files (CSV or PDF).
- Destination—Select your destination type (File or Email). Enter the applicable file location or the email address.

Note The default file locations for CSV and PDF files are:

/wcs-ftp/reports/Inventory/<ReportTitleName>_<yyyymmdd>_<HHMMSS>.csv
/wcs-ftp/reports/Inventory/<ReportTitleName>_<yyyymmdd>_<HHMMSS>.pdf

Note To set the mail server setup for emails, choose **Administration > Settings**, then click **Mail Server** in the sidebar menu to open the Mail Server Configuration page. Enter the SMTP and other required information.

- Start 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. Select the time from the hours and minutes drop-down lists. The report will begin running on this data and at this time.
- Recurrence—Enter the frequency of this report.
  - No Recurrence—The report runs only once (at the time indicated for the Start Date/Time).
  - Hourly—The report runs on the interval indicated by the number of hours you enter in the Entry text box.
  - Daily—The report runs on the interval indicated by the number of days you enter in the Every text box.

– Weekly—The report runs on the interval indicated by the number of weeks you enter in the Every text box and on the days specified by the selected check boxes.

The Create Custom Report page allows you to customize the report results. Table 17-1 specifies which reports are customizable, which have multiple sub-reports, and which report views are available. In future releases, all reports will be customizable.

Table 17-1 Report Customization

Report	Customizable	Multiple Sub-Reports?	Report Views	Report View Customizable?
Air Quality vs Time	Yes	No	Tabular	No
Security Risk Interferers	Yes	No	Tabular	No
Worst Air Quality APs	Yes	No	Tabular	No
Worst Interferers	Yes	No	Tabular	No
Busiest Clients	Yes	No	Tabular	No
Client Count	Yes	No	Graphical	No
Client Session	Yes	No	Tabular	No
Client Summary	Yes	Yes	Various	Yes
Client Traffic Stream Metrics	Yes	No	Tabular[1]	No
Throughput	No	No	Tabular	No
Unique Clients	Yes	No	Tabular	No
v5 Client Statistics	No	No	Tabular	No
Configuration Audit	Yes	No	Tabular	No
PCI	Yes	No	Tabular	No
AP Profile Status	Yes	No	Tabular	No
Device Summary	Yes	No	Tabular	No
Busiest APs	Yes	No	Tabular	No
Inventory - Combined Inventory	Yes	Yes	Various[2]	Yes
Inventory - APs	Yes	Yes	Various	Yes
Inventory - Controllers	Yes	Yes	Various	Yes
Inventory - MSEs	Yes	Yes	Various	Yes
Up Time	Yes	No	Tabular	No
Utilization - Controllers	No	No	Graphical	No
Utilization - MSEs	No	No	Graphical	No
Utilization - Radios	No	No	Graphical	No
Guest Account Status	Yes	No	Tabular	No
Guest Association	Yes	No	Tabular	No
Guest Count	No	No	Tabular	No

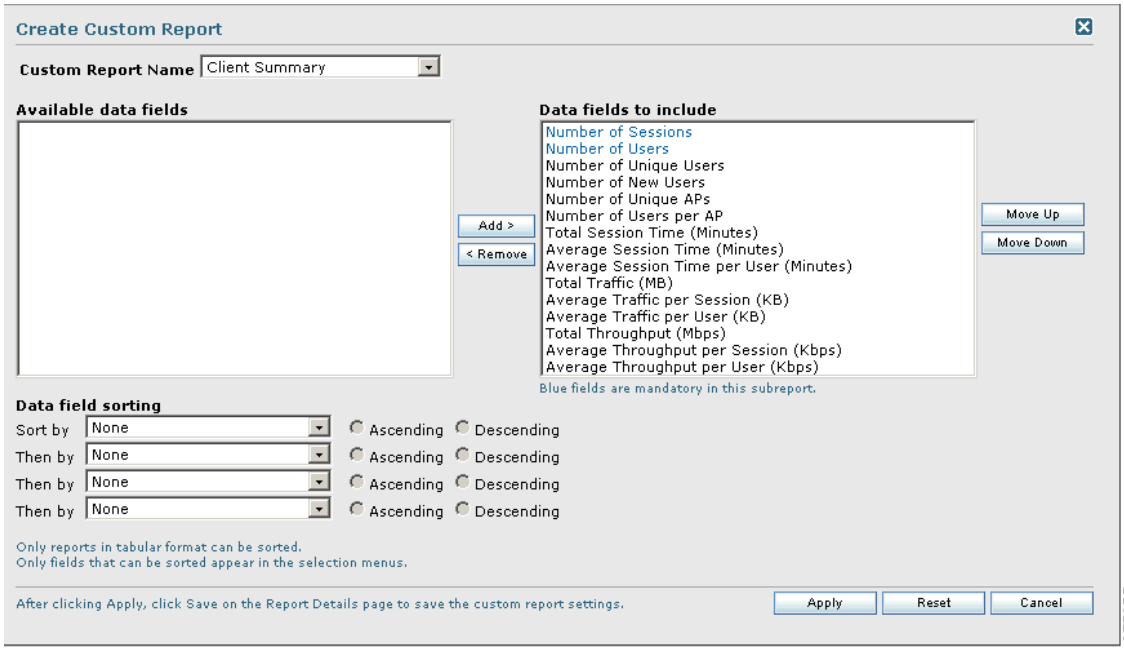
Table 17-1 Report Customization

Report	Customizable	Multiple Sub-Reports?	Report Views	Report View Customizable?
Guest User Sessions	Yes	No	Tabular	No
WCS Guest Operations	Yes	No	Tabular	No
Alternate Parent	Yes	No	Tabular	No
Link Stats - Link Stats	Yes	No	Tabular	No
Link Stats - Node Hops	Yes	No	Graphical	No
Nodes	Yes	No	Tabular	No
Packet Stats - Packet Stats	No	No	Graphical	No
Packet Stats - Packet Error Stats	No	No	Graphical	No
Packet Stats - Packet Queue Stats	No	No	Graphical	No
Stranded APs	No	No	Tabular	No
Worst Node Hops - Worst Node Hop	Yes	Yes	Various	No
Worst Node Hops - Worst SNR Link	Yes	Yes	Various	No
802.11n Summary	No	Yes	Graphical	No
Executive Summary	No	Yes	Various	No
802.11 Counters	Yes	No	Both	Yes
Coverage Holes	Yes	No	Tabular	No
Network Utilization	Yes	Yes	Both	Yes
Traffic Stream Metrics	Yes	Yes	Both	Yes
Tx Power and Channel	No	No	Graphical	No
VoIP Calls Graph	No	No	Graphical	No
VoIP Calls Table	No	No	Tabular	No
Voice Statistics	No	No	Graphical	No
Adaptive wIPS Alarm	Yes	No	Tabular	No
Adaptive wIPS Top 10 APs	Yes	No	Tabular	No
Adhoc Rogue Events	Yes	No	Tabular	No
Adhoc Rogues	Yes	No	Tabular	No
New Rogue APs	Yes	No	Tabular	No
New Rogue AP Count	No	No	Graphical	No
Rogue AP Events	Yes	No	Tabular	No
Rogue APs	Yes	No	Tabular	No
Security Summary	Yes	No	Tabular	No

1. Sub-report Client Summary view is tabular only. The rest of the sub-reports such as Client Summary by Protocol have both report views and are customizable to show either tabular, graphical, or both.
2. Combined inventory (similar to other inventory reports: APs/Controllers/MSEs) consists of multiple sub-reports. Reports that are by model or version have both views. These views are customizable with setting such as Count of Controllers by Model. Other reports, such as Controller Inventory, are tabular only.

Step 6 Click **Customize** to open a separate Create Custom Report page (see Figure 17-4).

Figure 17-4 Customize Report View Page



a. From the Custom Report Name drop-down list, select the report you intend to run. The Available and Selected column heading selections may change depending on the report selected.

b. From the Report View drop-down list, specify if the report will appear in tabular, graphical, or combined form (both). This option is not available on every report.

c. Use the **Add >** and **< Remove** buttons to move highlighted column headings between the two panels (Available data fields and Data fields to include).

Note Column headings in blue are mandatory in the current subreport. They cannot be removed from the Selected Columns area.

d. Use the **Change Order** buttons (Move Up or Move Down) to determine the order of the columns in the results table. The higher the column heading appears in the Selected Columns list, the farther left it appears in the results table.

e. In the **Data field Sorting** section, indicate your sorting preference (Ascending or Descending). Determine how the report data is sorted.

- You can select four data fields for which you can specify sorting order. Use the Sort by and Then by drop-down lists to select each data field for sorting.
- For each sorted data field, select whether you want it sorted in Ascending or Descending order.

Note Only reports in table form (rather than graphs or combined) can be sorted. Only fields that can be sorted appear in the Data field sorting drop-down lists.

f. Click **Apply** to confirm the changes, **Reset** to return columns to the default, or **Cancel** to close this page with no changes made.

Note The changes made in the Create Custom Report page are not saved until you click Save from the Report Details page.

Step 7 When all report parameters have been set, choose one of the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run Now—Click to run the report without saving the report setup.
- Cancel—Click to return to the previous page without running nor saving this report.

Managing Current Reports

If a report has been saved for a specific report type, you can access the current reports from the Report Launch Pad.

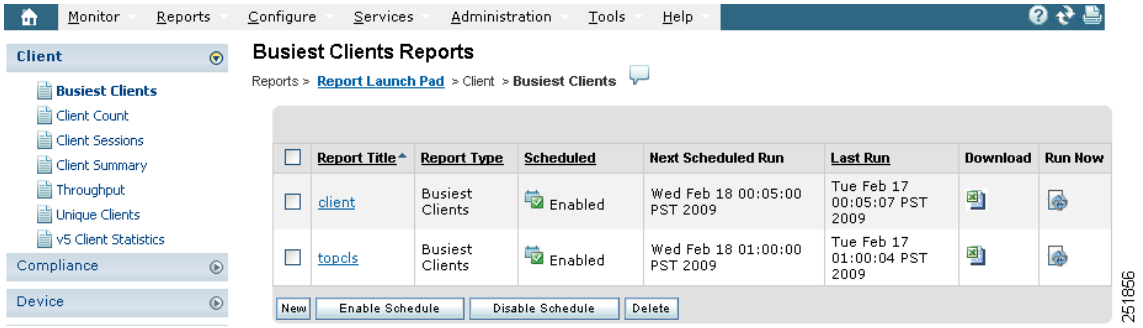
To access current or saved reports from the Report Launch Pad, follow these steps:

Step 1 Choose **Reports > Report Launch Pad**.

Step 2 Choose the specific report from the left sidebar menu or from the main section of the Report Launch Pad. The page displays a list of current reports for this report type (see Figure 17-5).

Note To view a list of saved reports, choose **Reports > Saved Reports**. See the "Managing Saved Reports" section on page 17-11 for more information.

Figure 17-5 Current Reports Page

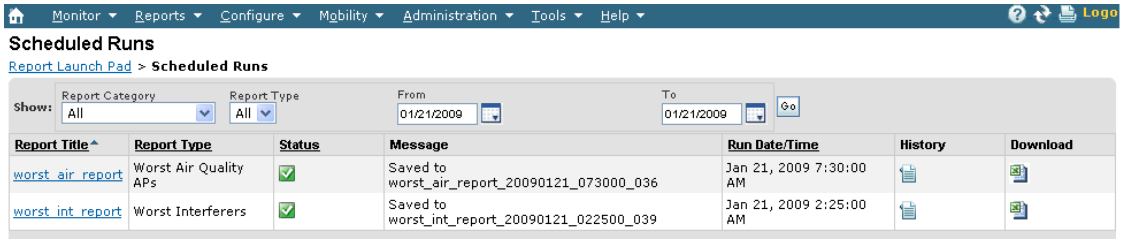


Managing Scheduled Run Results

To view all currently scheduled runs in WCS, choose **Report > Scheduled Run Results** (see Figure 17-6).

Note The list of scheduled runs can be sorted by report category, report type, and time frame.

Figure 17-6 Scheduled Run Results Page



The Scheduled Run Results page displays the following information:

- Report Title—Identifies the user-assigned report name.

  Note Click the report title to view the details for this report.

- Report Type—Identifies the specific report type.
- Status—Indicates whether or not the report ran successfully.
- Message—Indicates whether or not this report was saved and the file name for this report (if saved).
- Run Date/Time—Indicates the date and time that the report is scheduled to run.
- History—Click the History icon to view all scheduled runs and their details for this report.
- Download—Click the Download icon to open or save a .csv/.pdf file of the report results.

Select one of the following links for additional information on scheduled run results:

- Sorting Scheduled Run Results
- Viewing or Editing Scheduled Run Details

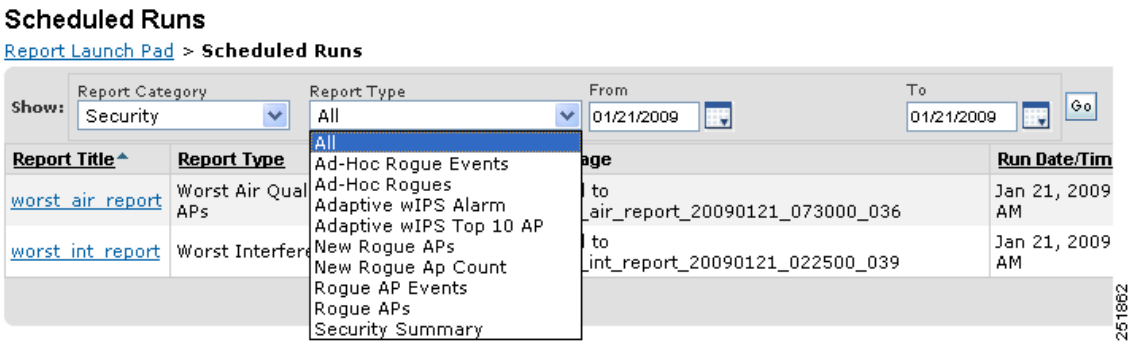
Sorting Scheduled Run Results

You can use the Show drop-down lists to sort the Scheduled Run Results by category, type, and time frame (see Figure 17-7):

- Report Category—Select the appropriate report category from the drop-down list or select **All**.
- Report Type—Select the appropriate report type from the drop-down list or select **All**. The report Type selections change depending on the selected report category.
- From/To—Type the report start (From) and end (To) dates in the text boxes or click the calendar icons to select the start and end dates.

Click **Go** to sort this list. Only reports that match your criteria appear.

Figure 17-7 Sorting Scheduled Run Results



Viewing or Editing Scheduled Run Details

To view or edit a saved report, follow these steps:

Step 1 Select **Report > Scheduled Run Results**.

Step 2 Click the Report Title link for the appropriate report to open the Report Details page.

Step 3 From this page, you can view or edit the details for the scheduled run.

Step 4 When all scheduled run parameters have been edited (if necessary), select from the following:

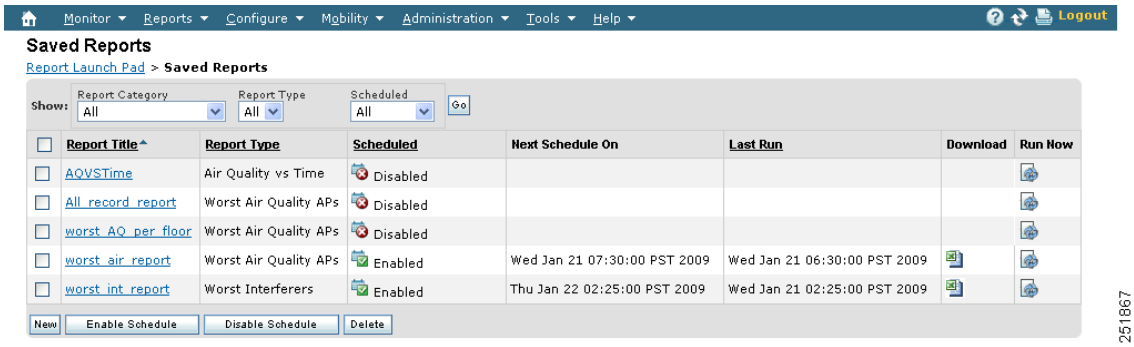
- Save—Click to save this schedule run without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this scheduled run and to immediately run the report.
- Cancel—Click to return to the previous page without running nor saving this report.
- Delete—Click to delete the current saved report.

Managing Saved Reports

In the Saved Reports page, you can create and manage saved reports (see Figure 17-8). To open this page in WCS, choose **Reports > Saved Reports**.

Note The list of saved reports can be sorted by report category, report type, and scheduled status (enabled, disabled, or expired).

Figure 17-8 Saved Reports Page



The Saved Reports page displays the following information:

- Report Title—Identifies the user-assigned report name.

  Note Click the report title to view the details for this report.

- Report Type—Identifies the specific report type.
- Scheduled—Indicates whether this report is enabled or disabled.
- Next Schedule On—Indicates the date and time of the next scheduled run for this report.
- Last Run—Indicates the date and time of the most recent scheduled run for this report.
- Download—Click the **Download** icon to open or save a .csv file of the report results.
- Run Now—Click the **Run Now** icon to immediately run the current report.

Select one of the following links for additional information on saved reports:

- Sorting Saved Reports
- Viewing or Editing Saved Report Details
- Running a Saved Report

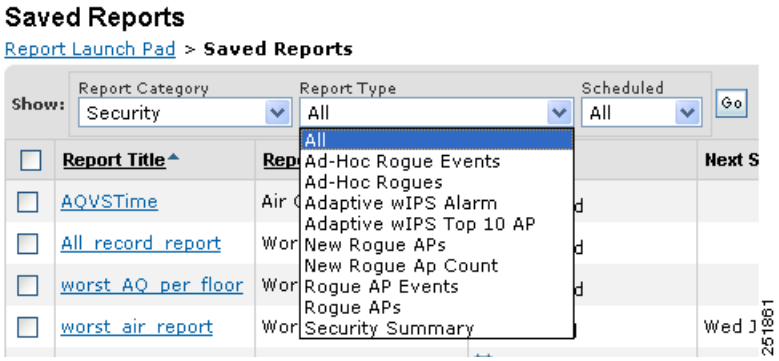
Sorting Saved Reports

You can use the Show drop-down lists to sort the Saved Reports list by category, type, and scheduled status (see Figure 17-9).

- Report Category—Select the appropriate report category from the drop-down list or select **All**.

- Report Type—Select the appropriate report type from the drop-down list or select **All**. The Report Type selections change depending on the selected report category.
- Scheduled—Select **All**, **Enabled**, **Disabled**, or **Expired** to sort the Saved Reports list by scheduled status.

Figure 17-9 Sorting Saved Reports



Click **Go** to sort this list. Only reports that match your criteria appear.

Viewing or Editing Saved Report Details

To view or edit a saved report, follow these steps:

Step 1 Select **Report > Saved Reports**.

Step 2 Click the Report Title link for the appropriate report to open the Report Details page.

Step 3 From this page, you can view or edit the details for the saved report.

Step 4 When all report parameters have been edited, choose one of the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run Now—Click to run the report without saving the report setup.
- Cancel—Click to return to the previous page without running nor saving this report.
- Delete—Click to delete the current saved report.

Running a Saved Report

In the Reports > Saved Reports page, click **Run Now** for the appropriate report.

Specific WCS Reports

- CleanAir Reports
  - Air Quality vs Time
  - Security Risk Interferers
  - Worst Air Quality APs
  - Worst Interferers
- Client Reports
  - Busiest Clients
  - Client Count
  - Client Sessions
  - Client Summary
  - Client Traffic Stream Metrics
  - Unique Clients
  - V5 Client Statistics
- Compliance Reports
  - Configuration Audit
  - Payment Card Industry (PCI)
- Device Reports
  - AP Profile Status
  - Busiest APs
  - AP Summary
  - Inventory Reports
  - Uptime
  - Utilization
- Guest Reports
  - Guest Accounts Status
  - Guest Association
  - Guest Count
  - Guest User Sessions
  - WCS Guest Operations
- Mesh Reports
  - Alternate Parent
  - Link Stats
  - Nodes
  - Packet Stats
  - Stranded APs
  - Worst Node Hops

- Network Summary
  - 802.11n Summary
  - Executive Summary
- Performance Reports
  - 802.11 Counters
  - Coverage Hole
  - Network Utilization
  - Traffic Stream Metrics
  - Tx Power and Channel
  - VoIP Calls Graph
  - VoIP Calls Table
  - Voice Statistics
- Security Reports
  - Adaptive wIPS Alarms
  - Adaptive wIPS Top 10 Access Points
  - Adhoc Rogue Events
  - Adhoc Rogues
  - New Rogue Access Points
  - New Rogue Access Point Count
  - Rogue Access Points Events
  - Rogue Access Points
  - Security Summary

CleanAir Reports

Click **New** for CleanAir report type to create a new report. See "Creating and Running a New Report" for more information.

Click a report type to view currently saved reports. From this page, you can enable, disable, delete, or run currently saved reports. See "Managing Current Reports" for more information.

The following are available CleanAir reports:

- Air Quality vs Time
- Security Risk Interferers
- Worst Air Quality APs
- Worst Interferers

Air Quality vs Time

This report displays the air quality index distributions over a period of time for access points on your wireless networks.

Click **Air Quality vs Time** from the Report Launch Pad to open the Air Quality vs Time page. From this page, you can enable, disable, delete, or run currently saved reports. See "Managing Current Reports" for more information.

To create a new report, click **New** from the Report Launch Pad or from the Air Quality vs Time page. See "Configuring a AirQuality vs Time Report" and "Air Quality vs Time Report Results" for more information.

Configuring a AirQuality vs Time Report

Settings

The following settings can be configured for a Air Quality vs Time report:

- Report Title—If you plan to use this as a saved report, type an appropriate name.
- Report By
  - AP By Controller—Choose **All Controllers > All Access Points** or click **Edit** to select specific access points.
  - AP By Floor Area—Choose **System Campus > All Access Points** or click **Edit** to select specific access points.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** or click **Edit** to select specific locations or access points.
- Protocol—Select the radio type by selecting the check box specific to a radio frequency.
- Reporting Period—You can configure the reporting period in two ways:
  - Last— Select the first radio button to generate reports for a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.
- Show—Enter the number of records you want displayed in each page.

Note Leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See "Creating and Running a New Report" for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See "Creating and Running a New Report" for more information on customizing report results.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.

- Save and Run—Click to save this report setup and to immediately run the report.
- Run Now—Click to run the report without saving the report setup.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See "Creating and Running a New Report" for additional information on running or scheduling a report.

Air Quality vs Time Report Results

Note Use the Create Custom Report page to customize the displayed results. See "Creating and Running a New Report" for more information on customizing report results.

The following are potential results for a Air Quality vs Time report, depending on how the report is customized:

- AP Name
- Basic Radio MAC
- Radio Type
- Time
- AQ Minimum Index
- AQ Average Index

Security Risk Interferers

This report displays the security risk interferers on your wireless network.

Click **Security Risk Interferers** from the Report Launch Pad to open the Security Risks Interferers page. From this page, you can enable, disable, delete, or run currently saved reports. See "Managing Current Reports" for more information.

To create a new report, click **New** from the Report Launch Pad or from the Security Risk Interferers page. See "Configuring a Security Risk Interferers Report" and "Security Risks Interferers Report Results" for more information.

Configuring a Security Risk Interferers Report

Settings

The following settings can be configured for a Security Risks Interferers report:

- Report Title—If you plan to use this as a saved report, type an appropriate name.
- Report By
  - AP By Controller—Choose **All Campuses>All Buildings > All Floors > All Access Points** or click **Edit** to select specific access points.
  - AP By Floor Area—Choose **All Campuses>All Buildings > All Floors > All Access Points** or click **Edit** to select specific access points.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** or click **Edit** to select specific locations or access devices.

- Protocol—Select the radio type by selecting the check box specific to a radio frequency.
- Reporting Period—You can configure the reporting period in two ways:
  - Last— Select the first radio button to generate reports for a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.
- Show—Enter the number of records you want displayed on each page.

Note Leave the text box blank to display all records.

Note The information in this report will be available only if you set a security alarm on the interferer.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See "Creating and Running a New Report" for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See "Creating and Running a New Report" for more information on customizing report results.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run Now—Click to run the report without saving the report setup.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See "Creating and Running a New Report" for additional information on running or scheduling a report.

Security Risks Interferers Report Results

Note Use the Create Custom Report page to customize the displayed results. See "Creating and Running a New Report" for more information on customizing report results.

The following are potential results for a Security Risks Interferers report, depending on how the report is customized:

- Interferer Type
- Affected Channels

- Discovered
- Last Updated
- Detected AP Name
- Affected Band

Worst Air Quality APs

This report displays the access points with the lowest air quality index.

Click **Worst Air Quality APs** from the Report Launch Pad to open the Worst Air Quality APs page. From this page, you can enable, disable, delete, or run currently saved reports. See "Managing Current Reports" for more information.

To create a new report, click **New** from the Report Launch Pad or from the Worst Air Quality APs page. See "Configuring a Worst Air Quality APs Report" and "Worst Air Quality APs Report Results" for more information.

Configuring a Worst Air Quality APs Report

Settings

The following settings can be configured for a Worst Air Quality APs report:

- Report Title—If you plan to use this as a saved report, type an appropriate name.
- Report By
  - AP By Controller—Choose **All Campuses>All Buildings > All Floors > All Access Points** or click **Edit** to select specific access points.
  - AP By Floor Area—Choose **All Campuses>All Buildings > All Floors > All Access Points** or click **Edit** to select specific access points.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** or click Edit to select specific locations or access devices.
- Protocol—Select the radio type by selecting the check box specific to a radio frequency.
- Reporting Period—You can configure the reporting period in two ways:
  - Last— Select the first radio button to generate reports for a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.
- Show—Enter the number of records you want displayed on each page.

Note Leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See "Creating and Running a New Report" for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See "Creating and Running a New Report" for more information on customizing report results.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run Now—Click to run the report without saving the report setup.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See "Creating and Running a New Report" for additional information on running or scheduling a report.

Worst Air Quality APs Report Results

Note Use the Create Custom Report page to customize the displayed results. See "Creating and Running a New Report" for more information on customizing report results.

The following are potential results for a Worst Air Quality APs report, depending on how the report is customized:

- AP Name
- Radio Type
- Worst Air Quality Value
- Channel Number
- Most Recent Reported Time
- Interferer Count

Worst Interferers

This report displays the worst interferers on your wireless network.

Click **Worst Interferers** from the Report Launch Pad to open the Worst Air Quality APs page. From this page, you can enable, disable, delete, or run currently saved reports. See "Managing Current Reports" for more information.

To create a new report, click **New** from the Report Launch Pad or from the Worst Interferers page.

Configuring a Worst Interferers Report

Settings

The following settings can be configured for a Worst Interferers report:

- Report Title—If you plan to use this as a saved report, type an appropriate name.

- Report By
  - Cluster Center AP
  - Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the report criteria area or click **Edit** to select specific locations.
  - Outdoor Area—Choose **All Campuses > All Outdoor Area** from the report criteria area or click **Edit** to select specific locations.
- Protocol—Select the radio type by selecting the check box specific to a radio frequency.
- Reporting Period—You can configure the reporting period in two ways:
  - Last— Select the first radio button to generate reports for a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.
- Show—Enter the number of records you want displayed on each page.

Note Leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See "Creating and Running a New Report" for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See "Creating and Running a New Report" for more information on customizing report results.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run Now—Click to run the report without saving the report setup.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See "Creating and Running a New Report" for additional information on running or scheduling a report.

Worst Interferers Report Results

Note Use the Create Custom Report page to customize the displayed results. See "Creating and Running a New Report" for more information on customizing report results.

The following are potential results for a Worst Interferers report, depending on how the report is customized:

- Device Type
- Severity
- Worst Severity Time
- Duty Cycle (%)
- Affected Channels
- Cluster Center APs
- Map Location
- Discovered

Note Severity value N/A means that the severity value for this device is not available. A value of 1 means that the severity is minimal and a value of 100 means very severe.

Note Interferers with unknown location are not listed if the **Report By** criteria is Floor Area or **Outdoor Area**.

Client Reports

The report structure has changed in Release 6.0 or later:

- The Client Association and Detailed Client Report are replaced by the Client Session report.
- Any saved Detailed Client reports are migrated to the Client Session report.
- Client Association Data from 5.1 or earlier is not migrated.

  Note After migration to 6.0 or later, you cannot see previous Client Association information that was presented in the Client Association Report.

- The Client Count report that was under 802.11 Scaling in release 5.2 is now consolidated into one Client Count report.

The following types of client reports are available:

- Busiest Clients
- Client Count
- Client Sessions
- Client Summary
- Client Traffic Stream Metrics
- Client Traffic Stream Metrics
- Unique Clients
- V5 Client Statistics

Busiest Clients

This report displays the busiest and least busy clients on the wireless network by throughput, utilization, and other statistics. You can sort this report by location, by band, or by other parameters.

Note Busiest Clients reports do ***not*** include autonomous clients.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - Controller—Choose **All Controllers** from the Report Criteria page or click **Edit** to select specific devices.
  - Floor Area—Choose **All Campuses > All Buildings > All Floors** from the Report Criteria page or click **Edit** to select specific locations.
  - Outdoor Area—Choose **All Campuses > All Outdoor Areas** from the Report Criteria page or click **Edit** to select specific locations.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All APs** from the Report Criteria page or click **Edit** to select specific locations or devices.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All APs** from the Report Criteria page or click **Edit** to select specific locations or devices.
  - SSID—Choose **All SSIDs** from the Report Criteria page or click **Edit** to select a specific or multiple SSIDs.
  - AP by RAP Mesh Role—Choose **All RAP APs** from the Report Criteria page or click **Edit** to select a specific RAP access point.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select **All Clients**, **Wired Clients**, or a specific radio type from the drop-down list.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

  Note The reporting period is based on the clients last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for the Busiest Client report results includes:

- Client MAC Address—The MAC address of the client.
- Client IP Address—The IP address of the client.
- Username
- Protocol—802.11a, 802.11b, 802.11g, 802.11n_5 GHz, or 802.11n_2.4 GHz
- Throughput (Mbps)—The average throughput (in Mbps) for the client.
- Utilization (%)—The average percentage of use for this client.
- On Controller—The controller on which the client is located.
- Bytes Sent—The number of bytes sent.
- Bytes Received—The number of bytes received.
- Packets Sent—The number of packets sent.
- Packets Received—The number of packets received.

Busiest Client Report Results

Note Use the Customize Report Format to customize the displayed results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

The following potential results occur, depending on how the report is customized. See Figure 17-10 for potential results for the Busiest Client report.

- Client MAC address, IP address, and username
- Protocol—802.11a/n or 802.11b/g/n
- Throughput—Either Mbps or kbps

  Note If throughput is less than 0.1 kbps, you see <0.1 kbps.

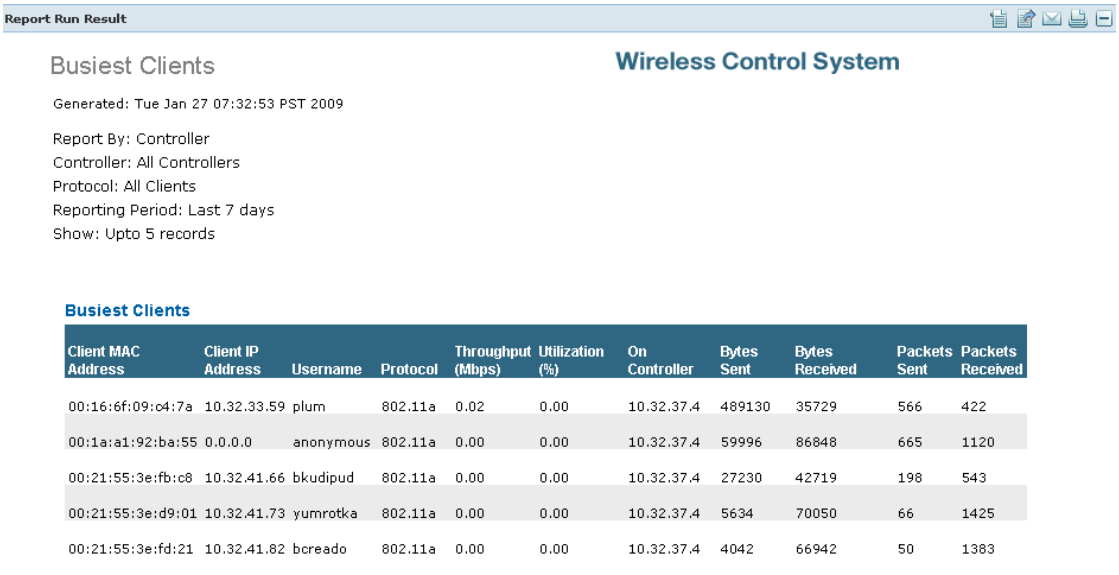
- Utilization (%)
- On Controller—The controller on which the client is located.
- Bytes sent and received

Note If the value is greater than 1,000,000,000, a G is appended at the end of the value (such as 3.45 G). If the value is greater than 1,000,000 but less than 1,000,000,000, an M is appended at the end of the value (such as 456.8 M).

- Packets sent and received

Note If the value is greater than 1,000,000,000, a G is appended at the end of the value (such as 3.45 G). If the value is greater than 1,000,000 but less than 1,000,000,000, an M is appended at the end of the value (such as 456.8 M).

Figure 17-10 Busiest Client Report Results


Report Run Result

Busiest Clients

Wireless Control System

Generated: Tue Jan 27 07:32:53 PST 2009

Report By: Controller
Controller: All Controllers
Protocol: All Clients
Reporting Period: Last 7 days
Show: Upto 5 records

Busiest Clients

Client MAC Address	Client IP Address	Username	Protocol	Throughput (Mbps)	Utilization (%)	On Controller	Bytes Sent	Bytes Received	Packets Sent	Packets Received
00:16:6f:09:c4:7a	10.32.33.59	plum	802.11a	0.02	0.00	10.32.37.4	489130	35729	566	422
00:1a:a1:92:ba:55	0.0.0.0	anonymous	802.11a	0.00	0.00	10.32.37.4	59996	86848	665	1120
00:21:55:3e:fb:c8	10.32.41.66	bkudipud	802.11a	0.00	0.00	10.32.37.4	27230	42719	198	543
00:21:55:3e:d9:01	10.32.41.73	yumrotka	802.11a	0.00	0.00	10.32.37.4	5634	70050	66	1425
00:21:55:3e:fd:21	10.32.41.82	bcreado	802.11a	0.00	0.00	10.32.37.4	4042	66942	50	1383

251877

Client Count

This trending report displays the total number of active clients on your wireless network.

The Client Count report displays data on the numbers of clients that connected to the network through a specific device, in a specific geographical area, or through a specific or multiple SSIDs.

Note Client Count reports include clients connected to autonomous Cisco IOS access points.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by

- Controller—Select **All Controllers** from the Report Criteria page or click **Edit** to select specific devices.
- Floor Area—Select **All Campuses > All Buildings > All Floors** from the Report Criteria page or click **Edit** to select specific locations.
- Outdoor Area—Select **All Campuses > All Outdoor Areas** from the Report Criteria page or click **Edit** to select specific locations.
- AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All APs** from the Report Criteria page or click **Edit** to select specific locations or devices.
- AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All APs** from the Report Criteria page or click **Edit** to select specific locations or devices.
- SSID—Select **All SSIDs** from the Report Criteria page or click **Edit** to select a specific or multiple SSIDs.
- AP by RAP Mesh Role—Select **All RAP APs** from the Report Criteria page or click **Edit** to select a specific RAP access point.

Note In the Report Criteria page, click **Select** to confirm your sort criteria or **Close** to return to the previous page.

- Protocol—Select **All Clients** or a specific radio type from the drop-down list.

Note Wired clients and clients associated to Cisco IOS access points are not included as part of this report.

- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Client Count report results includes:

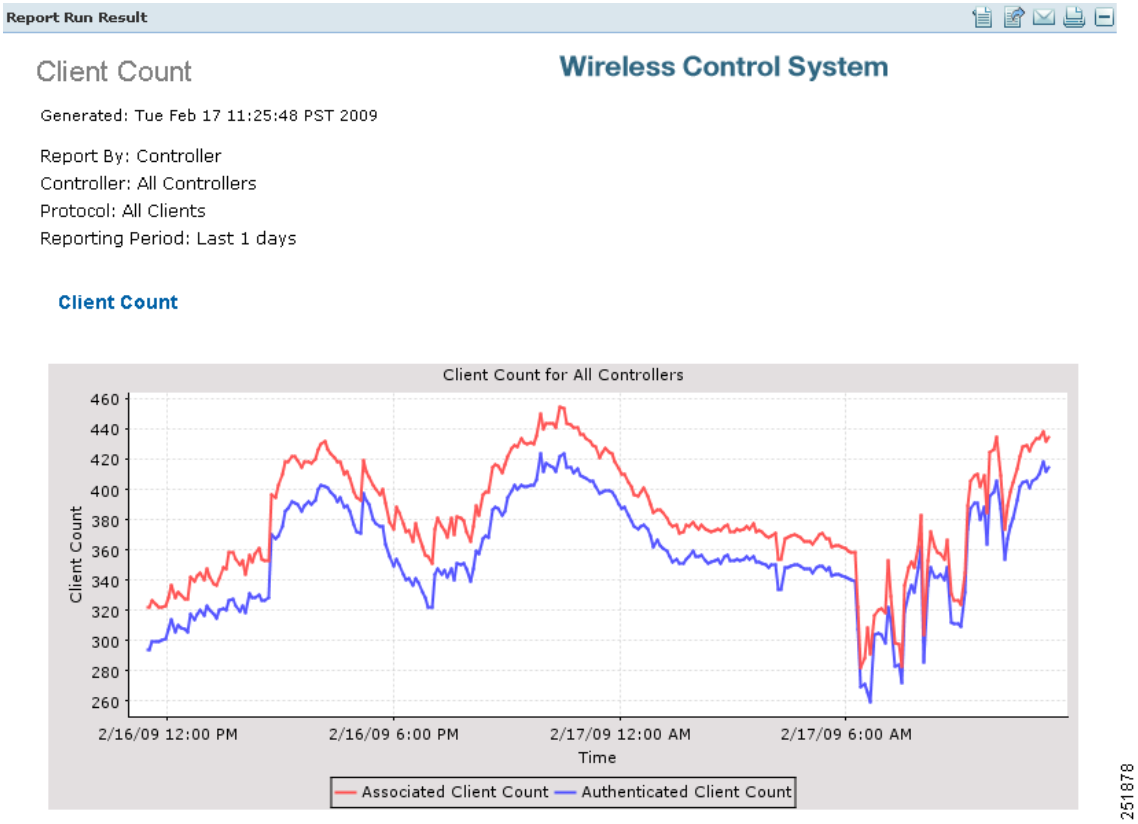
- Controller IP—The IP address of the controller.
- Time—The time the client count occurred.
- Associated Client Count—The number of associated clients for the specified period of time.
- Authenticated Client Count—The number of authenticated clients for the specified period of time.

Client Count Report Results

Note Use the Customize Report Format to customize the displayed results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

The Client Count report displays the following graph for the results (Figure 17-11):

Figure 17-11 Client Count Report Results



Client Sessions

This report displays the clients on the network, client statistics, and the access points to which they are connected.

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - Controller—Select **All Controllers** from the Report Criteria page or click **Edit** to select specific devices.
  - Floor Area—Select **All Campuses > All Buildings > All Floors** from the Report Criteria page or click **Edit** to select specific locations.
  - Outdoor Area—Select **All Campuses > All Outdoor Areas** from the Report Criteria page or click **Edit** to select specific locations.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All APs** from the Report Criteria page or click **Edit** to select specific locations or devices.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All APs** from the Report Criteria page or click **Edit** to select specific locations or devices.
  - SSID—Select **All SSIDs** from the Report Criteria page or click **Edit** to select a specific or multiple SSIDs.
  - AP by RAP Mesh Role—Select **All RAP APs** from the Report Criteria page or click **Edit** to select a specific RAP access point.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

  - VLAN
  - Client MAC Address
  - Client Username
- Reporting Period
  - Last—Select the Last radio button and a period of time from the drop-down list.
  - From—Select the From radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Client Sessions report results includes:

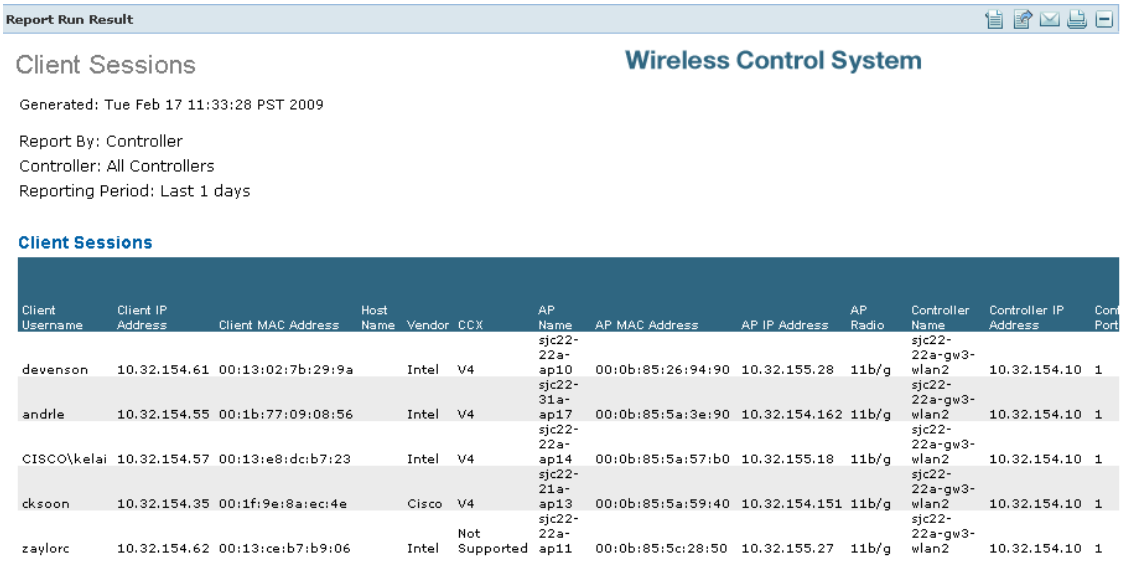
- Client Username
- Client IP Address—The IP address of the client.
- Client MAC Address—The MAC address of the client.
- Association Time —The date and time the client associated.
- Vendor—The vendor name for this client.
- AP Name—The access point to which this client is associated.
- Controller Name—The name of the controller to which this client is associated.
- Map Location—The building, floor area, or outdoor area (as applicable) where the client is located.
- SSID—The SSID to which this client is associated.
- Profile—The name of the profile to which this client is associated.
- VLAN ID—The VLAN Identifier. The range is 1 to 4096.
- Protocol—802.11a, 802.11b, 802.11g, 802.11n_5 GHz, or 802.11b_2.4 GHz.
- Session Duration—The length of time of the client session in hours, minutes, and seconds.
- Policy Type—The type of security policy for this client session.
- Average Session Throughput (kbps)—The average throughput in kbps for this client session.
- Host Name—The DNS host name of the device the client is on. WCS does a DNS lookup to resolve the host name from the client's IP address. The IP address to host name mapping must be defined in a DNS server. By default, the host name lookup is disabled. Use Administration > Settings > Clients to enable host name lookup.
- CCX—The Cisco Client Extension version number.
- AP MAC Address
- IP address
- AP Radio—The radio type of the access point.
- Controller IP Address—The IP address of the controller to which this client is associated.
- Controller Port—The port number for the controller to which this client is associated.
- Anchor Controller—The IP address of the anchor or foreign controller for the mobility client.
- Association ID
- Disassociation Time—The date and time this client disassociated.
- Authentication—The authentication method for this client.
- Encryption Cipher
- EAP Type
- Authentication Algorithm
- Web Security
- Tx and Rx (bytes)—The approximate number of bytes transmitted or received during the session.

Client Sessions Report Results

Note Use the Customize Report Format to customize the displayed results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

The following image (Figure 17-12) displays potential results for the Client Sessions report, depending on how the report is customized:

Figure 17-12 Client Sessions Report Results



Report Run Result

Client Sessions

Wireless Control System

Generated: Tue Feb 17 11:33:28 PST 2009

Report By: Controller
Controller: All Controllers
Reporting Period: Last 1 days

Client Sessions

Client Username	Client IP Address	Client MAC Address	Host Name	Vendor	CCX	AP Name	AP MAC Address	AP IP Address	AP Radio	Controller Name	Controller IP Address	Cont Port
devenson	10.32.154.61	00:13:02:7b:29:9a		Intel	V4	sjc22-22a-ap10	00:0b:85:26:94:90	10.32.155.28	11b/g	sjc22-22a-gw3-wlan2	10.32.154.10	1
andrle	10.32.154.55	00:1b:77:09:08:56		Intel	V4	sjc22-31a-ap17	00:0b:85:5a:3e:90	10.32.154.162	11b/g	sjc22-22a-gw3-wlan2	10.32.154.10	1
CISCO\kelai	10.32.154.57	00:13:e8:dc:b7:23		Intel	V4	sjc22-22a-ap14	00:0b:85:5a:57:b0	10.32.155.18	11b/g	sjc22-22a-gw3-wlan2	10.32.154.10	1
cksoon	10.32.154.35	00:1f:9e:8a:ec:4e		Cisco	V4	sjc22-21a-ap13	00:0b:85:5a:59:40	10.32.154.151	11b/g	sjc22-22a-gw3-wlan2	10.32.154.10	1
zaylorc	10.32.154.62	00:13:ce:b7:b9:06		Intel	Not Supported	sjc22-22a-ap11	00:0b:85:5c:28:50	10.32.155.27	11b/g	sjc22-22a-gw3-wlan2	10.32.154.10	1

251879

Client Summary

The Client Summary is a detailed report that displays various client statistics.

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Note A Client Summary report includes summary results sorted by protocol, SSID, VLAN, and vendor. To customize report results for a particular section, select the applicable section from the Customizable Report drop-down list.

The Client Summary report contains four sub reports. Each of them can be independently customized. The following information is default information available from a Client Summary report depending on the customizable report selected:

- Number of Sessions
- Number of Total Users
- Number of Unique Users
- Number of New Users
- Number of Unique APs
- Number of Users per AP
- Total Traffic (MB)
- Average Traffic per Session (KB) and per user (in KB)
- Total Throughput (Mbps)
- Average Throughput per Session and per user (Mbps)

  Note When WCS does not receive client traps, it relies on client status polling to discover client associations (The task runs every 5 minutes by default.). However, WCS cannot accurately determine when the client was actually associated. WCS assumes the association started at the polling time which may be later than the actual association time. Therefore the calculation of the average client throughput can give inaccurate results, especially for short client sessions.

- Protocol—802.11a/n or 802.11b/g/n.
- SSID—The user-defined Service Set Identifier name
- VLAN
- Vendor
- User Count

- Time Used (Minutes)
- Traffic (MB)
- Session Count
- % of Users
- % of Time
- % of Traffic
- % of Session
- Total Time of a session

Client Summary Report Results

Note Use the Customize Report Format to customize the displayed results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

The Client Summary report contains the following potential results (see Figure 17-13), depending on how the report is customized:

Figure 17-13 Client Summary Report Results

Report Run Result

Client Summary

Wireless Control System

Generated: Tue Feb 17 11:44:43 PST 2009

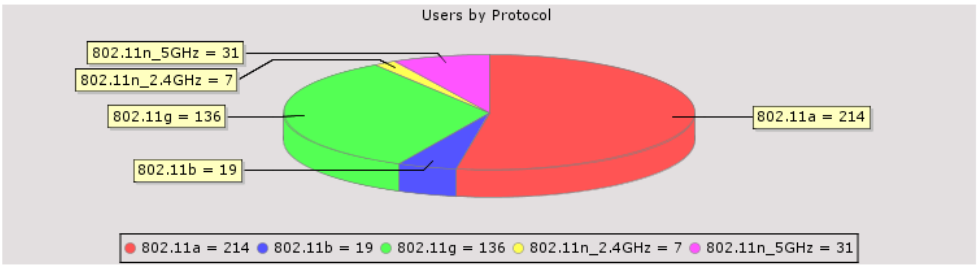
Reporting Period: Last 6 hours

Client Summary

Number of Sessions	Number of Total Users	Number of Unique Users	Number of New Users	Number of Unique APs	Number of Users per AP	Total Traffic (Mb)	Average Traffic per Session (Kb)	Average Traffic per User (Kb)	Total Throughput (MBPS)	Average Throughput per Session (Mbps)	Average Throughput per User (Mbps)
2207	318	318	96	230	1	47387.47	21471.44	149.02	381928.15	173.05	1201.03

Client Summary by Protocol

Protocol	User Count	Time Used (Minutes)	Traffic (MB)	Session Count	% of Users	% of Time	% of Traffic	% of Sessions
802.11a	214	20240.04	23342.38	1729	52.58	67.93	67.93	81.52
802.11b	19	691.15	335.50	20	4.67	2.32	0.98	0.94
802.11g	136	7323.95	7188.50	316	33.42	24.58	20.92	14.90
802.11n_2.4GHz	7	245.41	150.19	11	1.72	0.82	0.44	0.52



251880

Client Traffic Stream Metrics

The Client Traffic Stream Metrics report displays client or SSID based traffic stream metric (TSM) information.

Click **Client Traffic Stream Metrics** from the Report Launch Pad to open the Client Traffic Stream Metrics Reports page. From this page, you can enable, disable, delete, or run currently saved reports. See the "Managing Current Reports" section on page 17-8 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Client Traffic Stream Metrics Reports page.

Note The traffic stream metrics and radio performance background tasks must be running prior to generating this report.

Settings

The following settings can be configured for a Client Traffic Stream Metrics report:

- Report Title—If you plan to use this as a saved report, enter a report name.
- Report by
  - SSID—Choose **All SSIDs** from the Report Criteria page or click **Edit** to select a specific or multiple SSIDs.
  - Client MAC Address—Choose **All Clients** from the Report Criteria page or click **Edit** to select specific clients.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the Last radio button and a period of time from the drop-down list.
  - From—Select the From radio button and enter the From and To dates and times. You can type a date in the text box or client the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Schedule

If you play to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Mandatory columns are displayed in blue font and cannot be moved to Available Columns. Time, Client MAC address, and QoS are mandatory columns for the Client Traffic Stream Metrics report.

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

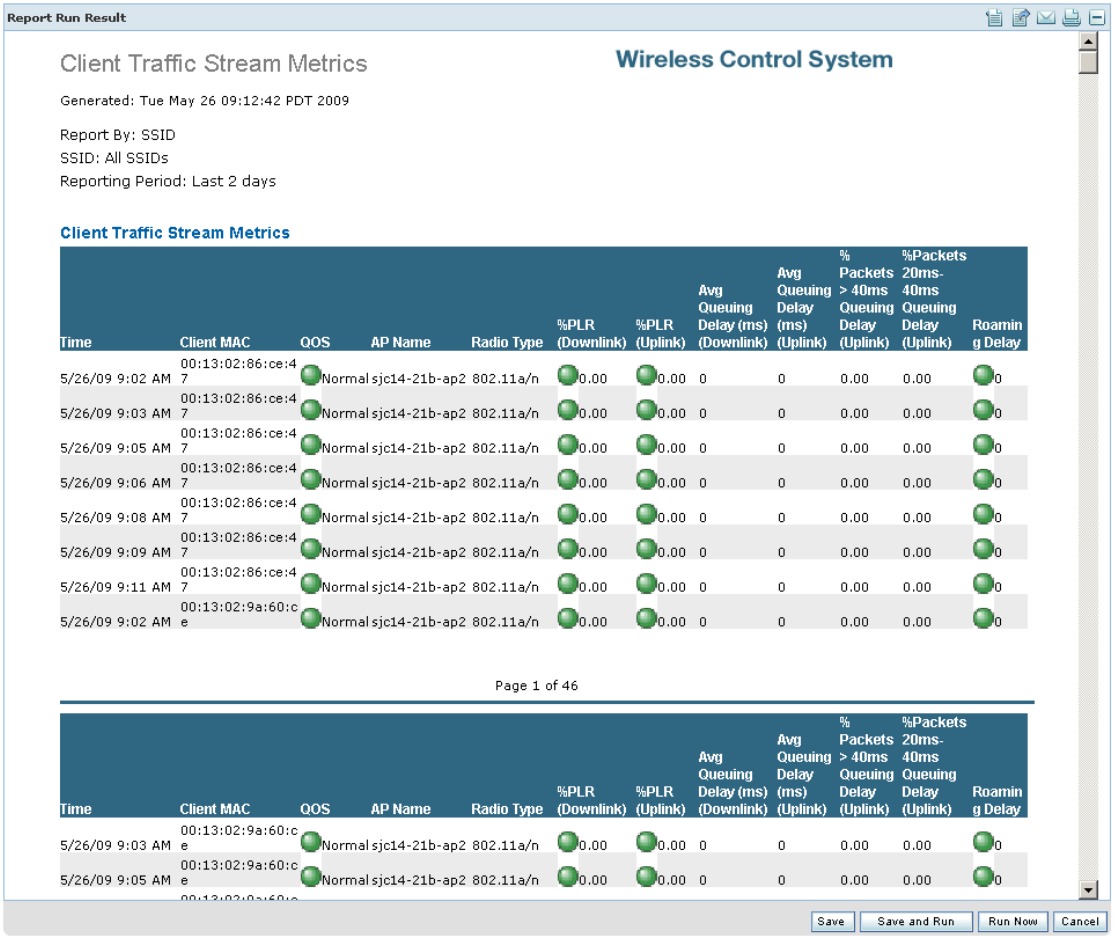
The following are potential results for a Client Traffic Stream Metrics report, depending on how the report is customized:

- Time (mandatory column)
- Client MAC (mandatory column)
- QoS (mandatory column)—QoS values (packet latency, packet jitter, packet loss, roaming time) which can affect how 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.
- AP Name (mandatory column)
- Radio Type (mandatory column)
- Avg Queuing Delay (ms) (Downlink) (mandatory column)—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 the time for re-tries, if needed.
- Avg Queuing Delay (ms) (Uplink) (mandatory column)—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.
- % 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.
- % Packets > 40ms Queuing Delay (Uplink)—Percentage of queuing delay packets greater than 40 ms.
- % Packets 20ms-40ms Queuing Delay (Uplink)—Percentage of queuing delay packets between 20 ms and 40 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 he first packet is received from the new access point after a successful roam.
- Time—Time that the statistics were gathered from the access point(s).
- Client MAC—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, or PDA and refers to any client attached to the access point collecting measurements.

Client Traffic Stream Metrics Report Results

The Client Traffic Stream Metrics Report contains the following results (see Figure 17-14).

Figure 17-14 Client Traffic Stream Metrics Report Results



Throughput

This report displays the ongoing bandwidth used by the wireless clients on your network.

Note The Throughput report does not include wired clients or clients connected to Autonomous Cisco IOS access points.

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - Controller—Select **All Controllers** from the Report Criteria page or click **Edit** to select specific devices.
  - Floor Area—Select **All Campuses > All Buildings > All Floors** from the Report Criteria page or click **Edit** to select specific locations.

  - Outdoor Area—Select **All Campuses > All Outdoor Areas** from the Report Criteria page or click **Edit** to select specific locations.
  - AP by Controller—Select **All Controllers > All Access Points** or click **Edit** to select specific devices.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All APs** from the Report Criteria page or click **Edit** to select specific locations or devices.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All APs** from the Report Criteria page or click **Edit** to select specific locations or devices.
  - Criteria page or click **Edit** to select specific locations or devices.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select **All Clients** or a specific radio type from the drop-down list.

Note Wired clients and clients associated to Cisco IOS access points are not included as part of this report.

- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

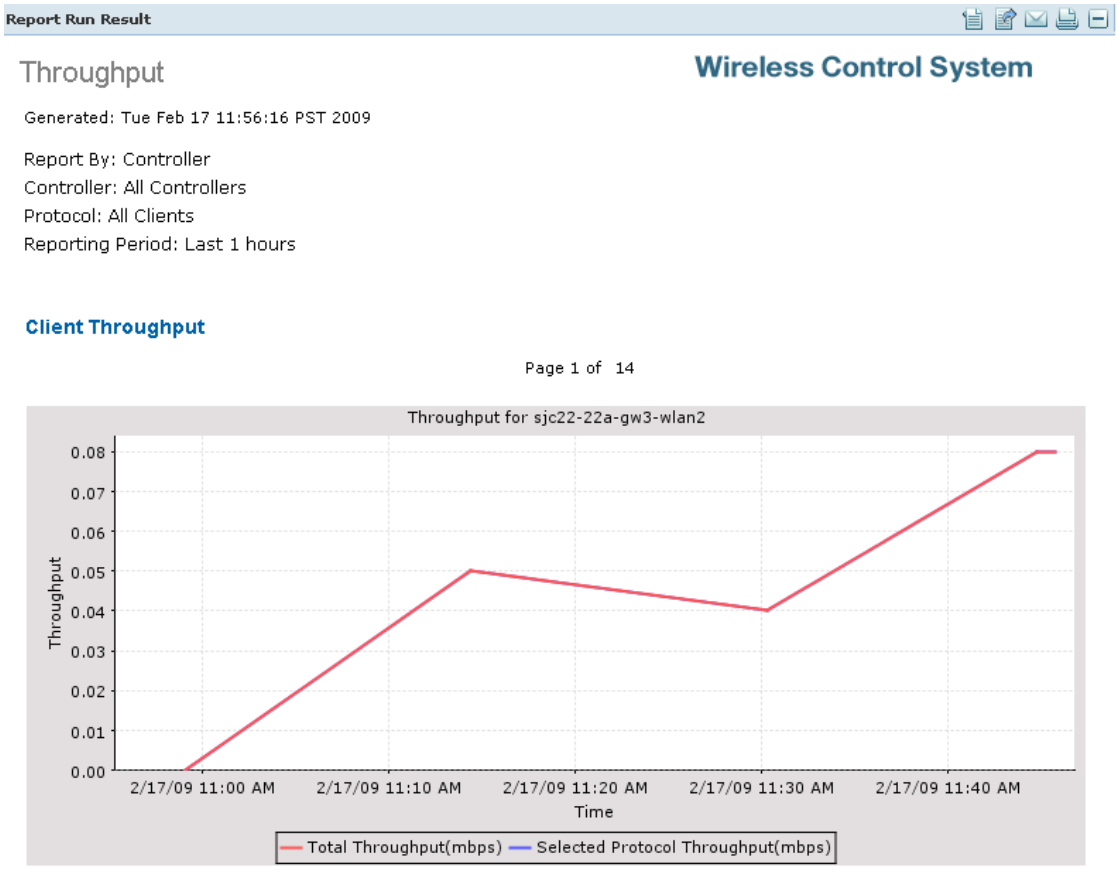
Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Throughput Report Results

The Throughput report displays the following results (Figure 17-15):

Figure 17-15 Throughput Report Results



Unique Clients

This report displays all unique clients by the time, protocol, and controller filters that you select. A unique clients is determined by the MAC address of the client device. These clients are sorted by controller in this report.

A new First Seen column is added in release 6.0. It is the time that WCS first learned of the client MAC address. For existing clients, WCS sets the First Seen column with the timestamp currently in the database, which is the time the record was last updated.

Note Unique Clients reports do ***not*** include autonomous clients.

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by

  - Controller—Select **All Controllers** from the Report Criteria page or click **Edit** to select specific devices.
  - Floor Area—Select **All Campuses > All Buildings > All Floors** from the Report Criteria page or click **Edit** to select specific locations.
  - Outdoor Area—Select **All Campuses > All Outdoor Areas** from the Report Criteria page or click **Edit** to select specific locations.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All APs** from the Report Criteria page or click **Edit** to select specific locations or devices.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All APs** from the Report Criteria page or click **Edit** to select specific locations or devices.
  - SSID—Select **All SSIDs** from the Report Criteria page or click **Edit** to select a specific or multiple SSIDs.
  - AP by RAP Mesh Role—Select **All RAP APs** from the Report Criteria page or click **Edit** to select a specific RAP access point.
  - Select a specific RAP access point.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select **All Clients**, **Wired Clients**, or a specific radio type from the drop-down list.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Mandatory columns are displayed in blue font and cannot be moved to Available data fields Column. Last Seen, User, and MAC address are mandatory columns for the Unique Client report.

The following information is available on the unique client report:

- Host Name
- AP MAC Address

- IP Address—The IP address of the controller to which this client is associated.
- Controller IP Address
- Port
- Last Session Length
- VLAN ID—The VLAN Identifier. The range is 1 to 4096.
- CCX—The Cisco Client Extension version number.
- E2E
- Vendor—The vendor name for this client.
- IP Address
- AP Name—The access point to which this client is associated.
- Controller—The name of the controller to which this client is associated.
- 802.11 State—Client association status.
- SSID—The SSID to which this client is associated.
- Profile—The name of the profile to which this client is associated.
- Authenticated
- Protocol—802.11a, 802.11b, 802.11g, 802.11n_5 GHz, or 802.11b_2.4 GHz.
- Map Location

Unique Client Report Results

The following results appear for the Throughput report (Figure 17-16):

Figure 17-16 Unique Client Report Results


Report Run Result

Unique Clients

Wireless Control System

Generated: Tue Feb 17 13:51:31 PST 2009

Report By: Floor Area
Floor: Root Area -> WNBU -> 4th Floor
Protocol: All Clients
Reporting Period: Last 1 days

Unique Clients

Last Seen	First Seen	User	Vendor	IP Address	MAC Address	AP Name	Controller	Port	802.11 State	SSID	Authenticat
2/16/09 2:16 PM	2/2/09 11:13 AM	gbeach	Unknown	10.32.33.76	00:24:36:94:92:82	SJC14-41A-AP-A5	Cisco_32:1b:23	29	Disassociated	alpha	Yes
2/16/09 6:13 PM	2/16/09 10:03 AM	CISCO\anukala	Intel	10.32.33.83	00:16:6f:0a:89:0f	SJC14-41A-AP-A5	Cisco_32:1b:23	29	Disassociated	alpha	Yes
2/16/09 6:51 PM	1/15/09 12:02 PM	CISCO\ajmadhav	Intel	10.32.33.61	00:1d:e0:6b:86:f1	SJC14-41A-AP-A2	Cisco_32:1b:23	29	Disassociated	alpha	Yes
2/17/09 11:13 AM	2/16/09 12:42 PM	tdimacch	Apple	10.32.33.82	00:23:12:61:78:26	SJC14-41A-AP-A5	Cisco_32:1b:23	29	Disassociated	alpha	Yes
2/17/09 12:30 PM	2/16/09 11:10 AM	mkranz	Apple	10.32.41.134	00:21:e9:aa:f8:93	SJC14-41A-AP-A2	Cisco_32:1b:23	29	Disassociated	alpha_iptv	Yes

251903

V5 Client Statistics

This report displays the 802.11 and security statistics for Cisco Compatible Extensions v5 clients.

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

V5 Client Statistics Report Results

This report displays the following results for the v5 Client Statistics report (Figure 17-17):

Figure 17-17 V5 Client Statistics Report Results


Report Run Result

v5 Client Statistics

Wireless Control System

Generated: Tue Feb 17 13:56:01 PST 2009

Dot11 Counters

Reporting Period: Last 1 days

Dot11 Counters

Client MAC	Trans Fragment Count	Multicast Transmitted Frame Count	Failed Count	Retry Count	Multi Retry Count	Frame Duplicate Count	RTS Success Count	RTS Fail Count	ACK Fail Count	Rcv. Fragment Count	Multi Rcv. Frame Count	FCS Error Count	Trans Frame Count
00:1b:9e:33:e2:3f	22.50	0.00	0.00	2.00	0.00	0.00	0.00	0.00	5.00	147.50	0.00	0.00	15.00
00:40:96:a8:ca:73	66.40	0.00	4.20	0.20	4.20	0.00	0.00	14.40	8.00	156.00	0.00	7.00	44.20
00:40:96:aa:93:ad	14.89	0.00	0.00	1.11	0.00	0.00	0.00	0.00	1.56	187.44	0.00	5.11	6.22
00:40:96:b2:78:fb	29.00	0.00	0.00	0.25	0.00	0.00	0.00	0.00	0.25	105.50	0.00	0.75	16.00
00:40:96:b2:80:87	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	150.00	0.00	0.00	0.00

251906

Compliance Reports

The Configuration Audit report displays the differences between WCS and its controllers. The PCI DSS Compliance report summarizes your Wireless LAN Security components with reference to the Payment Card Industry (PCI) Data Security Standard (DSS) requirements. PCI DSS compliance is required for all merchants and service providers that store, process, or transmit cardholder data. You can find PCI DSS standards at https://www.pcisecuritystandards.org.

- Configuration Audit
- Payment Card Industry (PCI)

Configuration Audit

This report displays the configuration differences between WCS and its controllers. You must configure audit mode on the Administration > Settings page. In audit mode, you can perform an audit based on templates or the stored configuration. The report shows the last time an audit was performed using the Configuration Sync background task.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Controller—Select **All Controllers** or a specific controller from the available list.
- Audit Time—Select **Latest** or a specific date and time from the available list.

Note The available audit times are based on when the Configuration Sync background task was run.

- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Note A Configuration Audit report includes the following sections: Audit Summary, Applied Templates and Config Group Template Discrepancies, Enforced Values, Failed Enforcements, and WCS Config Discrepancies. Select the applicable report from the Customizable Report drop-down list.
To customize report results for a particular section, select the applicable section from the Customizable Report drop-down list.

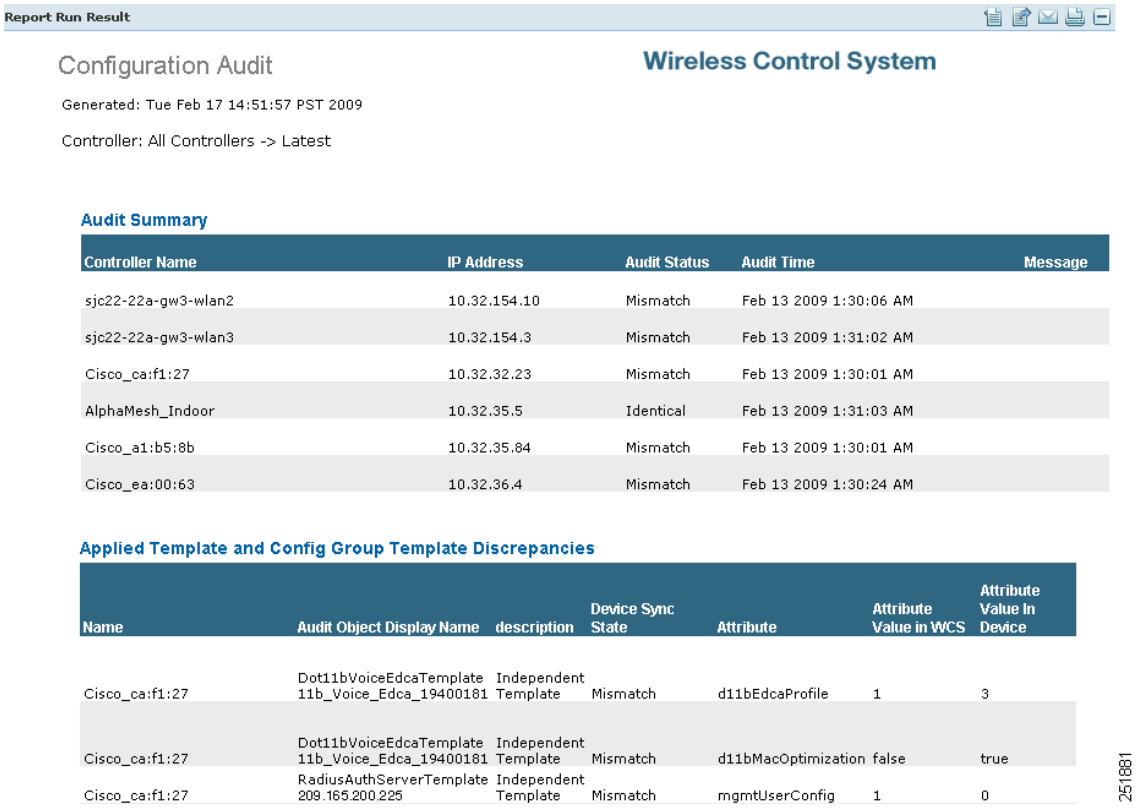
A Configuration Audit report contains the following default information, depending on which customized report is selected:

- Controller Name
- Audit Status
- Audit Time
- Name
- Audit Object Display Name
- Device Sync State
- Time
- Client MAC Address
- IP Address
- Message
- Description
- Attribute
- Attribute Value in WCS
- Attribute Value in Device
- Enforced Value
- Instance Name
- Description
- Error Message
- Attribute Value in DB

Configuration Audit Results

The Configuration Audit report contains the following results (Figure 17-18):

Figure 17-18 Configuration Audit Report Results


Report Run Result

Configuration Audit

Wireless Control System

Generated: Tue Feb 17 14:51:57 PST 2009

Controller: All Controllers -> Latest

Audit Summary

Controller Name	IP Address	Audit Status	Audit Time	Message
sjc22-22a-gw3-wlan2	10.32.154.10	Mismatch	Feb 13 2009 1:30:06 AM	
sjc22-22a-gw3-wlan3	10.32.154.3	Mismatch	Feb 13 2009 1:31:02 AM	
Cisco_ca:f1:27	10.32.32.23	Mismatch	Feb 13 2009 1:30:01 AM	
AlphaMesh_Indoor	10.32.35.5	Identical	Feb 13 2009 1:31:03 AM	
Cisco_a1:b5:8b	10.32.35.84	Mismatch	Feb 13 2009 1:30:01 AM	
Cisco_ea:00:63	10.32.36.4	Mismatch	Feb 13 2009 1:30:24 AM	

Applied Template and Config Group Template Discrepancies

Name	Audit Object Display Name	description	Device Sync State	Attribute	Attribute Value in WCS	Attribute Value In Device
Cisco_ca:f1:27	Dot11bVoiceEdcaTemplate 11b_Voice_Edca_19400181	Independent Template	Mismatch	d11bEdcaProfile	1	3
Cisco_ca:f1:27	Dot11bVoiceEdcaTemplate 11b_Voice_Edca_19400181	Independent Template	Mismatch	d11bMacOptimization	false	true
Cisco_ca:f1:27	RadiusAuthServerTemplate 209.165.200.225	Independent Template	Mismatch	mgmtUserConfig	1	0

251881

Payment Card Industry (PCI)

This report displays the PCI Data Security Standard (DSS) version 1.1 requirements that are relevant to your wireless network security.

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Note A PCI report includes the following sections: New Rogue APs, Adhoc Rogues, Config Compliance, Location Server/Mobility Service Engine, Auth Enc Violations, Client Association, Access Points, Controllers, Autonomous Access Points, MSEs, and Threats and Attacks.
To customize report results for a particular section, select the appropriate section from the Customizable Report drop-down list.

New Rogue APs report results include:

- Created Time
- Rogue MAC Address
- Detecting AP Name
- Radio Type
- Controller IP Address
- SSID—The user-defined Service Set Identifier name.
- State
- Map Location—The building, floor area, or outdoor area (as applicable) where the new rogue access point is located.
- Channel Number
- RSSI (dBm)
- Classification Type

Adhoc Rogues report results include:

- Modified Time
- Rogue MAC Address
- Detecting AP Name
- Radio Type
- Controller IP Address
- Map Location—The building, floor area, or outdoor area (as applicable) where the ad hoc rogue is located.
- SSID—The user-defined Service Set Identifier name.
- Channel Number

- RSSI (dBm)
- State

Config Compliance, Location Server/ Mobility Services Engine, and Auth Enc Violations report results include:

- IP Address
- Device Security Issues
- Device Name
- Device Type—Indicates the device type as MSE 3310, MSE 3350, or 2710 Location Server.

Client Association report results include:

- Time
- Client MAC Address—The MAC address of the client.
- Controller IP Address
- AP Name—The access point name.
- Client Username
- Status
- Session Duration
- Reason

Access Point report results include:

- AP Name—The access point name.
- Ethernet MAC Address
- IP Address
- Model
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- Controller Name
- Base radio MAC Address
- Software Version
- Detailed Location
- Primary Controller
- Secondary Controller Name
- Tertiary Controller Name
- Admin Status
- AP Mode
- 802.11a/n Status
- 802.11b/g/n Status
- Gateway
- Netmask
- IOS version

- Boot version
- Certificate type
- Serial number
- Local interface
- Neighbor name
- Neighbor address
- Neighbor port
- Neighbor Advt version

Controller report results include:

- Controller name
- Location
- Model
- Reachability status
- IP address
- Serial number
- Software version
- Mobility group

Autonomous Access Point reports results include:

- AP Name—The access point name.
- Ethernet MAC address
- Model
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- Reachability status
- 802.11a/n MAC address
- 802.11b/g/n MAC address
- IP address—The IP address of the MSE or Location Server.
- Software version
- Location
- 802.11a/n status
- 802.11b/g/n status
- Serial number

MSE report results include:

- Device name
- Start time—The start time of the MSE or Location Server.
- HTTP/HTTPS port—The port numbers for HTTP and HTTPS.
- HTTPS—Whether HTTPS is enabled or disabled.
- Version

- IP address
- Device type

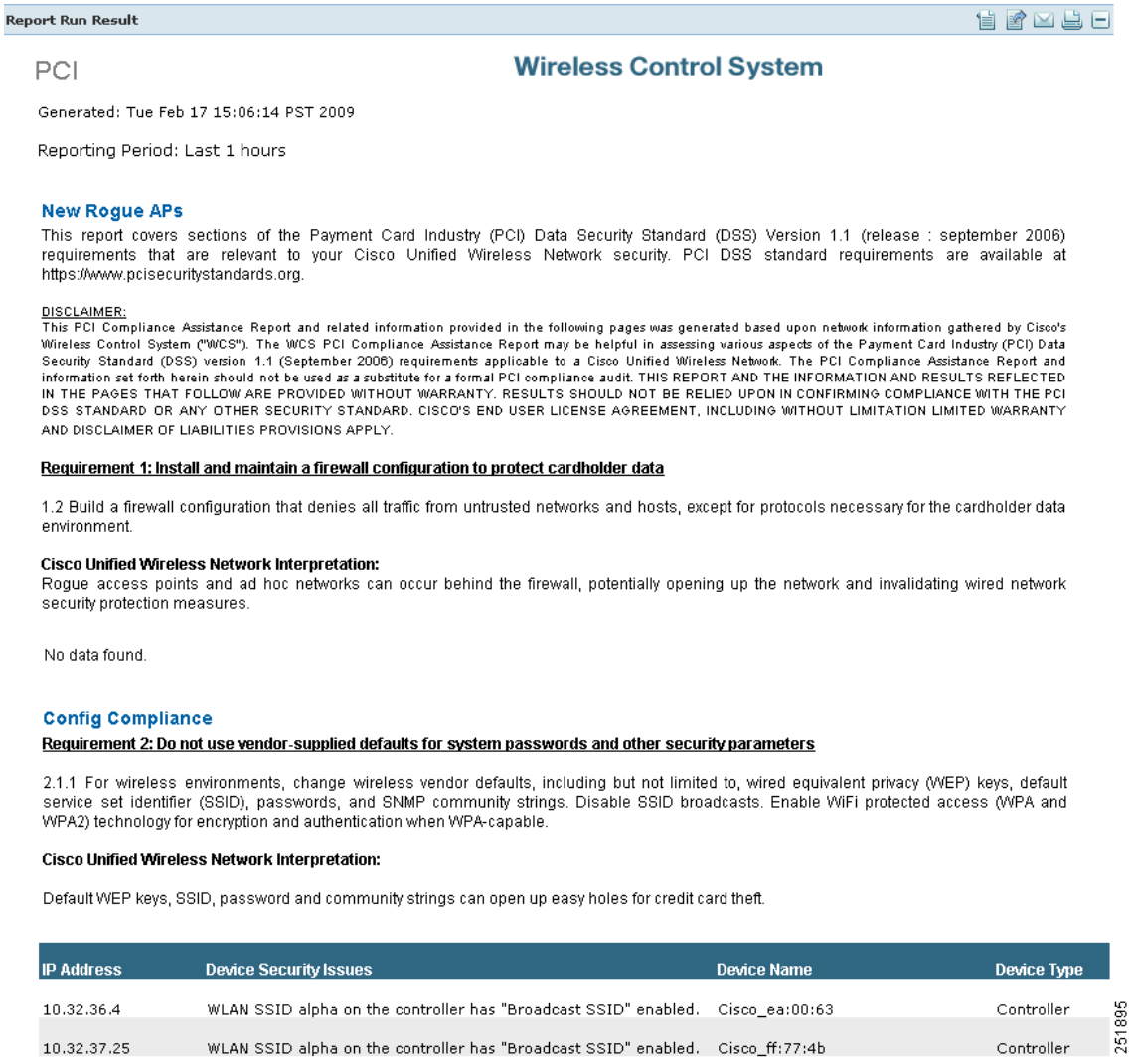
Threats and Attacks report results include:

- Severity
- Date/Time
- Message
- Failure Object

PCI Report Results

The PCI report contains the following results (Figure 17-19):

Figure 17-19 PCI Report Results



Device Reports

You can create the following device reports:

- AP Image Predownload
- AP Profile Status
- Busiest APs
- AP Summary
- Inventory Reports
- Uptime
- Utilization

AP Image Predownload

This report displays scheduled download software task status.

Click AP Image Predownload from the Report Launch Pad to open the AP Image Predownload page. From this page, you can enable, disable, delete, or run currently saved reports. See "Managing Current Reports" for more information.

To create a new report, click **New** from the Report Launch Pad or from the AP Image Predownload Reports page. See "Configuring a AP Image Predownload Report" and "AP Image Predownload Report Results" for more information.

Configuring a AP Image Predownload Report

Settings

The following settings can be configured for a AP Image Predownload report:

- Report Title—If you plan to use this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select specific devices.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select specific locations or devices.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select specific locations or devices.

Note In the Report Criteria page, you can select **All Access Points** or **All OfficeExtend Access Points**.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Show—Enter a number between 10 and 50, or leave blank to show all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See "Creating and Running a New Report" for more information on scheduling a report.

Creating a Custom Report

The Create Custom Report page allows you to customize the report results. See "Creating and Running a New Report" for more information on customizing report results.

Note Mandatory columns are displayed in blue font and cannot be moved to Available Columns. AP Name, Primary Image, Backup Image, Predownload Version, and Predownload Status are mandatory columns for the AP Image Predownload report.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run Now—Click to run the report without saving the report setup.
- Export Now—Click to export the report results. The supported export formats is PDF and CSV.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See "Creating and Running a New Report" for additional information on running or scheduling a report.

AP Image Predownload Report Results

The following are potential results for an AP Image Predownload report, depending on how the report is customized:

- AP Name—Access point name.
- Primary Image—Current Primary Image present in the AP.
- Backup Image—Current Backup Image present in the AP.
- Predownload Version—The image version that is currently downloading to the AP from the controller as part of the predownload process.
- Predownload Status—The current status of the image download as part of the predownload process.
- MAC Address—MAC Address of the AP.
- Controller IP Address—IP address of the controller to which the access point is associated.

AP Profile Status

This report displays access point load, noise, interference, and coverage profile status.

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select specific devices.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select specific locations or devices.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select specific locations or devices.

Note In the Reports Criteria page, you can select **All Access Points** or All OfficeExtend Access Points.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select 802.11 a/n, 802.11 b/g/n, or both.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

AP Profile Status report results include:

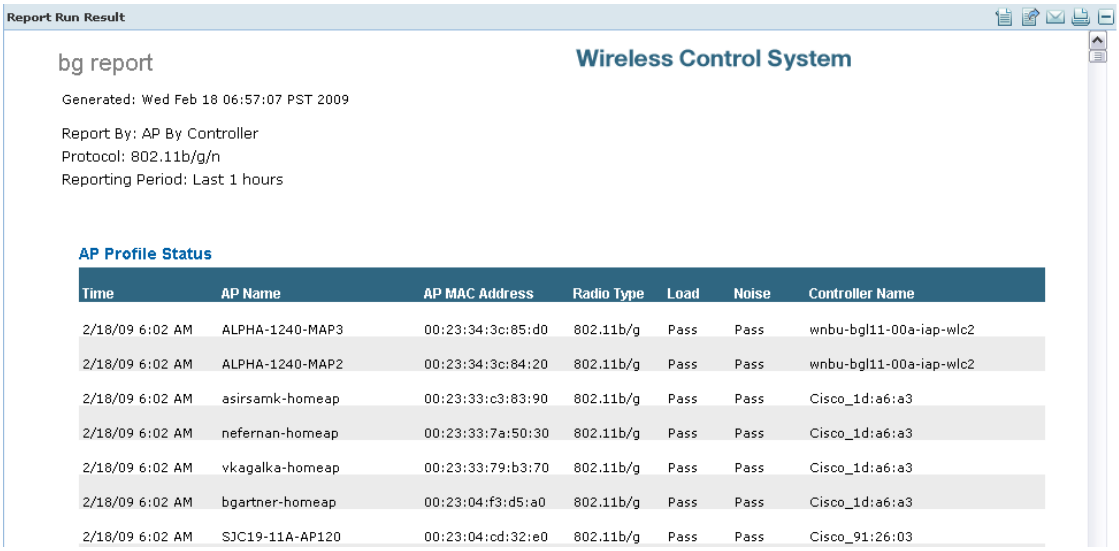
- Time—The date and time at which AP Profile Status is collected.
- AP Name—The access point name.
- AP MAC address—The MAC address of the access point.

- Radio Type—802.11a/n or 802.11b/g/n.
- Load—*True* if the load level exceeds a threshold level, otherwise *false*.
- Noise—*True* if the noise level exceeds a threshold level, otherwise *false*.
- Controller Name—The controller to which the access point is associated.
- Interference—*True* if the interference level exceeds a threshold level, otherwise *false*.
- Coverage—*True* if the coverage level exceeds a threshold level, otherwise *false*.
- Controller IP Address—The IP address of the controller to which the access point is associated.

AP Profile Status Report Results

The AP Profile Status report contains the following results (Figure 17-20):

Figure 17-20 AP Profile Status Report Results



Busiest APs

This report displays the access points with the highest total usage (transmitting, receiving, and channel utilization) on your wireless network.

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Protocol—Select 802.11 a/n or 802.11 b/g/n from the drop-down list.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.

  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

- Show—Enter the number of records that you want displayed on each page.

Note Leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Busiest APs report results include:

- AP Name—The access point name.
- Radio Type
- Rx Utilization (%)—The percentage of time that the access point receiver is busy operating on packets. The percentage (0 to 100%) represents a load from 0 to 1.
- Tx Utilization (%)—The percentage of time that the access point transmitter is busy operating on packets. The percentage (0 to 100%) represents a load from 0 to 1.
- Channel Utilization (%)—The percentage of time that an access point channel is busy operating on packets. The percentage (0 to 100%) represents a load from 0 to 1.
- Controller Name
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- Controller IP Address

Busiest APs Report Results

The Busiest APs report contains the following results (Figure 17-21):

Figure 17-21 Busiest APs Report Results

AP Summary

This report displays the distribution of devices on your wireless network. This report enables you to sort the devices by RF group name, mobility group name, access point group name, SSID, location, and other statistics.

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - Floor Area—Select **All Campuses > All Builders > All Floors** from the Report Criteria page or click **Edit** to select specific locations.
  - Outdoor Area—Select **All Campuses > All Outdoor Areas** from the Report Criteria page or click **Edit** to select specific locations.
  - OfficeExtend AP—Select **Enable** from the Report Criteria page or click **Edit** to select **Enable** or **Disable**.
  - AP by Controller—Select **All Controllers > All APs** from the Report Criteria page or click **Edit** to select specific devices.
  - AP Group—Select **All AP Groups** from the Report Criteria page or click **Edit** to select a specific access point group.
  - RF Group—Select **All RF Groups** from the Report Criteria page or click **Edit** to select a specific radio frequency group.
  - AP Mode—Select **All AP Modes** from the Report Criteria page or click **Edit** to select a specific access point mode.

Note This report only returns monitor mode access points if **Report by AP Mode** is selected. Reports run by any other **Report by** selection drop all monitor mode access points from the results.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- SSID—Select the appropriate SSID from the list. You can choose *None* to show all access points with no SSIDs configured.

Note The SSID filter is tied to all the criteria in the Report By category. This limits the scope for getting a report of access points by any scope listed in the Report By criteria. For this report to be able to retrieve access points by any Report By criteria, the default selection of All SSIDs should be used.

Note Access points must be broadcasting SSID(s) in order to satisfy the "All SSID" default filter of the report.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

AP Summary report results include:

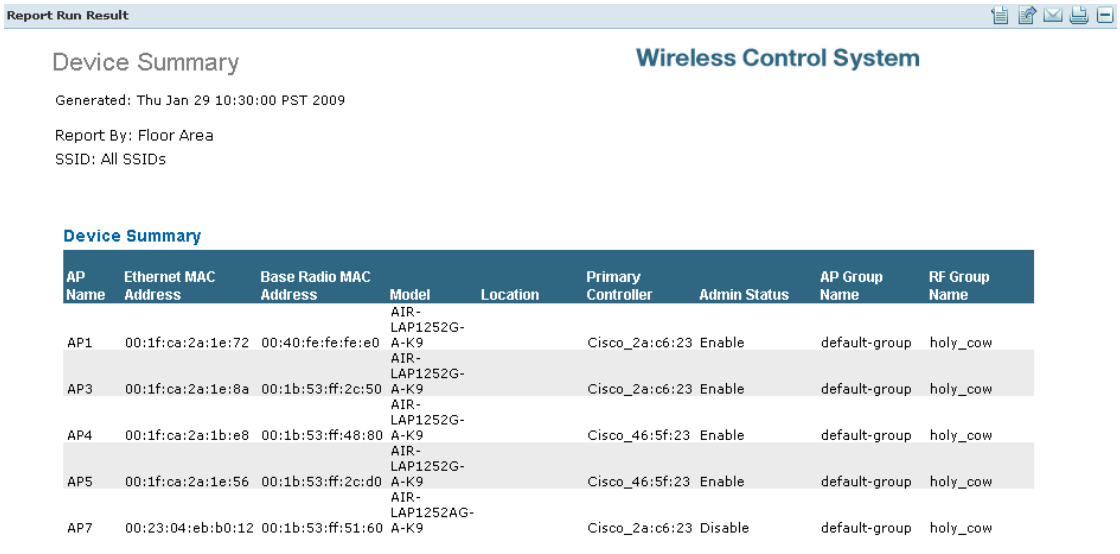
- AP Name—The access point name.
- Ethernet MAC Address
- Base radio MAC Address
- Model
- Location
- Primary Controller
- Admin Status—Enable/Disable.
- AP group Name
- RF group Name
- Software Version

- Controller Version
- AP Mode—Local, Bridge, Rogue Detector, or H-REAP.
- Associated WLANs—Associated SSIDs.
- 802.11a/n and 802.11b/g/n Status—Up/Down.
- Serial Number

AP Summary Report Results

The AP Summary report contains the following results (Figure 17-22):

Figure 17-22 AP Summary Report Results - NEED SCREENSHOT WITH AP SUMMARY


Report Run Result

Device Summary

Wireless Control System

Generated: Thu Jan 29 10:30:00 PST 2009

Report By: Floor Area
SSID: All SSIDs

Device Summary

AP Name	Ethernet MAC Address	Base Radio MAC Address	Model	Location	Primary Controller	Admin Status	AP Group Name	RF Group Name
AP1	00:1f:ca:2a:1e:72	00:40:fe:fe:fe:e0	AIR-LAP1252G-A-K9		Cisco_2a:c6:23	Enable	default-group	holy_cow
AP3	00:1f:ca:2a:1e:8a	00:1b:53:ff:2c:50	AIR-LAP1252G-A-K9		Cisco_2a:c6:23	Enable	default-group	holy_cow
AP4	00:1f:ca:2a:1b:e8	00:1b:53:ff:48:80	AIR-LAP1252G-A-K9		Cisco_46:5f:23	Enable	default-group	holy_cow
AP5	00:1f:ca:2a:1e:56	00:1b:53:ff:2c:d0	AIR-LAP1252G-A-K9		Cisco_46:5f:23	Enable	default-group	holy_cow
AP7	00:23:04:eb:b0:12	00:1b:53:ff:51:60	AIR-LAP1252AG-A-K9		Cisco_2a:c6:23	Disable	default-group	holy_cow

251883

Inventory Reports

This report allows you to generate inventory-related information for controllers, access points, and MSEs managed by WCS. This information includes hardware type and distribution, software distribution, CDP information, and other statistics.

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report Type—Choose **Combined Inventory**, **APs**, **Controllers**, or **MSEs** from the drop-down list.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Note An Inventory report includes the following sections: Count of Controllers by Model, Count of Controllers by Software Version, Controller Inventory, Count of APs by Model, Count of APs by Software Version.
To customize report results for a particular section, select the appropriate section from the Customizable Report drop-down list.

Available information for Count of Controllers by Model results includes:

- Model Name—The name of the model of the controller.
- Number of Controllers—The controller count for each model name.

Available information for Count of Controllers by Model results includes:

- Software Version—The software version of the controller.
- Number of Controllers—The controller count for each software version.

Available information for Controller Inventory results includes:

- Controller Name
- IP Address—The IP address of the controller.
- Location—The user-specified physical location of the controller.
- Interfaces—The names of the interfaces of the controller combined together by commas.
- Reachability Status—*Reachable* if the controller is currently manageable.
- Serial Number—The serial number of the controller.
- Model—The model name of the controller.
- Software Version—The software version of the controller.
- Mobility Group—The name of the mobility group to which the controller is assigned.
- RF Group—The name of the RF group to which the controller is assigned.
- Neighbor Name, Port, and Address—CDP neighbor information including the name, port, and IP address of the neighbor.
- Duplex—The CDP neighbor interface's duplex mode.

Available information for Count of APs by Model results includes:

- Model Name—The name of the model of the access point.
- Number of APs—The access point count for each model name.

Available information for Count of APs by Software Version results includes:

- Software Version—The software version of the access point.
- Number of APs—The access point count for each software version.

Available information for AP Inventory results includes:

- AP Name—The access point name.
- Ethernet MAC Address—The Ethernet MAC address of the access point.
- IP Address—The IP address of the access point.
- Model—The name of the model of the access point.
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- Controller Name—The name of the controller to which the access point is associated.
- Base radio MAC Address—The MAC address of an access point.
- Software Version—The software version of an access point.
- Location—The user-specified physical location of an access point.
- Primary Controller—The name of the primary controller to which the access point should associate. When the access point is not directly connected to a controller, it tries to find the primary controller and associates with it. If this attribute is empty or an access point is unable to find the controller with this name, it associates with the secondary controller.
- Secondary Controller—The name of the secondary controller to which the access point should associate if the primary controller is unavailable. If the primary and secondary controllers are not available, the access point associates with the tertiary controller.
- Tertiary Controller—The name of the tertiary controller to which the access point should associate if the primary and secondary controller is unavailable. If the primary, secondary, and tertiary switch are unavailable, it associates with the master controller.
- Admin Status—The admin status of the access point.
- AP Mode—The monitor only mode setting of the access point. The options are local, monitor, H-REAP, rogue detector, sniffer, and bridge.
- 802.11 a/n and 802.11 b/g/n Status—The operation state of the respective radio. The options are down, up, not associated, and unknown.
- Gateway—The gateway for the access point.
- Netmask—The netmask of the access point's IP address.
- IOS and Boot Versions—The version of the IOS Cisco access point, and the major/minor boot version of the access point.
- Certificate Type—The access point certification type options are unknown, manufacture installed, self signed, or local significance.
- Serial Number—The serial number of the access point.
- Neighbor Name, Address, Port, and Advertised Version—The access point's CDP neighbor's name, IP address, port, and advertised version information.

Available information for Count of MSEs by Version results includes:

- Version—The MSE version.
- Number of MSEs—The count of both MSE and Location Servers.

Available information for MSEs results includes:

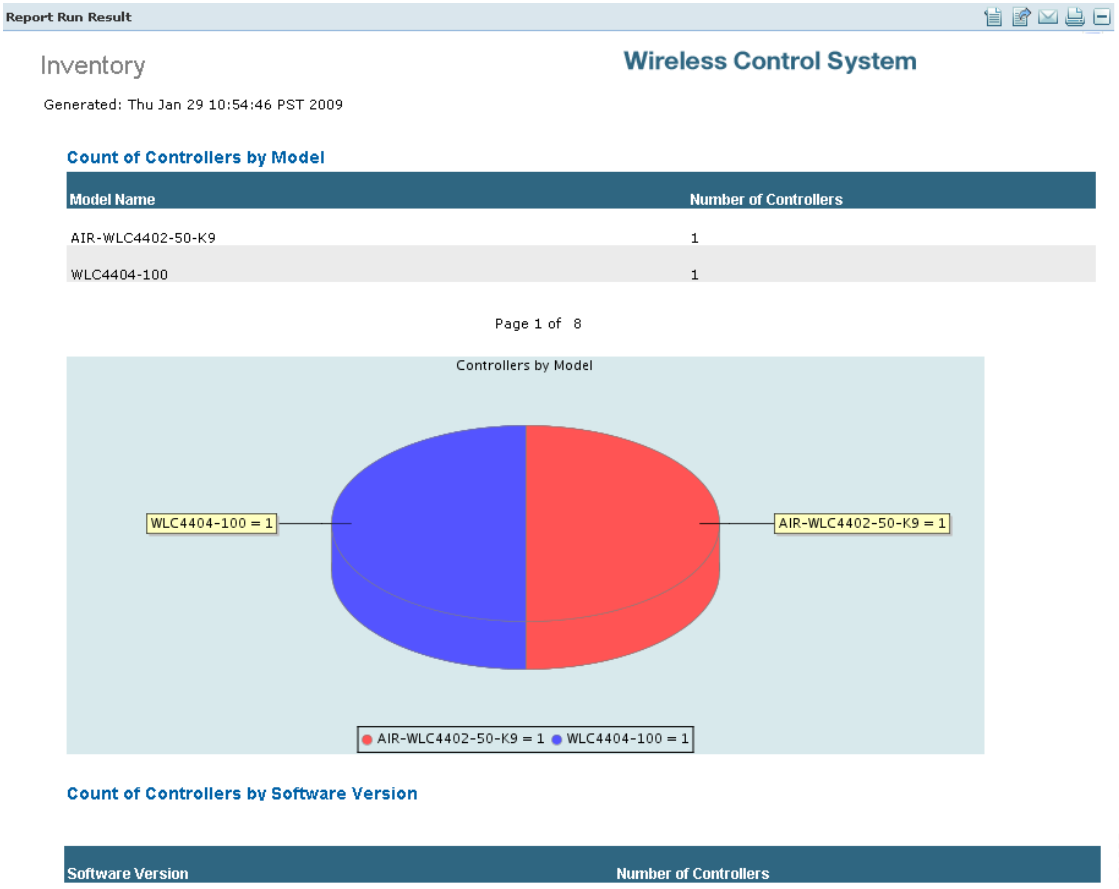
- Device Name—The name of the MSE or Location Server.
- IP Address
- Device Type

- HTTP/HTTPS Port
- HTTPS
- Version
- Start Time

Inventory Report Results

The following is an example of Inventory report results (Figure 17-23):

Figure 17-23 Inventory Report Results



Uptime

This report displays the access point uptime, the LWAPP uptime, and the LWAPP join time.

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Show—Enter the number of records that you want displayed on each page.

Note Leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Uptime report results includes:

- AP Name—The access point name.
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- AP Uptime—The time duration since the last access point reboot.
- LWAPP Uptime—The time duration since the last access point joined the controller.
- LWAPP Join Taken Time—The time it took for the access point to join the controller. This value could be significant in Mesh environments.

Uptime Report Results

The Uptime report displays the following results (Figure 17-24):

Figure 17-24 Uptime Report Results


Report Run Result

Up Time

Wireless Control System

Generated: Thu Jan 29 13:15:51 PST 2009

Show: Upto 5 records

Up Time

AP Nam	Map Location	AP Up Time	LWAPP Up Time	LWAPP Join
AP7		1 days 1 hrs 33 mins 29 secs	1 days 1 hrs 32 mins 6 secs	
AP3	Area 51 > Alien Den	1 days 1 hrs 33 mins 30 secs	1 days 1 hrs 31 mins 56 secs	
AP1	Area 51 > Alien Den	1 days 1 hrs 33 mins 35 secs	1 days 1 hrs 32 mins 1 secs	
AP5	Area 51 > Alien Den	1 days 8 hrs 31 mins 24 secs	1 days 8 hrs 30 mins 7 secs	
AP4	Area 51 > Alien Den	1 days 8 hrs 32 mins 12 secs	1 days 8 hrs 30 mins 39 secs	

251904

Utilization

This report displays the controller, AP, and MSE usage on your wireless network. These statistics (such as CPU usage, memory usage, link utilization, and radio utilization) can help you monitor performance and plan for future expansion.

This report display the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report Type—Select **Controllers**, **MSEs**, or **Radios** from the drop-down list.
- Report by (Report by options change depending on the report type selected)
  - Controller—If the report type is Controllers, select **All Controllers** from the Report Criteria page or click **Edit** to select specific devices. Depending on the report type selected, you receive either radio or controller utilization results. See the "Radio, Controller, and MSE Utilization Results" section on page 17-61.
  - MSEs—If the report type is MSEs, select **All MSEs** from the Report Criteria page or click **Edit** to select specific devices. Depending on the report type selected, you receive either radio or controller utilization results. See the "Radio, Controller, and MSE Utilization Results" section on page 17-61.
  - Radios—If the report type is Radio, select **AP by Controller**, **AP by Floor Area**, or **AP by Outdoor Area** from the Report by drop-down list and the appropriate selection from the Report Criteria page (or click **Edit** to select specific devices). Depending on the report type selected, you receive either radio or controller utilization results. See the "Radio, Controller, and MSE Utilization Results" section on page 17-61.

Note In the Radios Report Criteria page, you can select **All Access Points** or **All OfficeExtend Access Points**.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select 802.11 a/n, 802.11 b/g/n, or both. This parameter only appears if the report type is Radios.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Radio, Controller, and MSE Utilization Results

Depending on the report type selected, you receive either radio, controller, or MSE utilization results.

- Radio Utilization
  - Rx Utilization (%)—The percentage of time that the access point receiver is busy operating on packets. The percentage (from 0 to 100%) represents a load from 0 to 1.
  - Tx Utilization (%)—The percentage of time the access point transmitter is busy operating on packets. The percentage (from 0 to 100%) represents a load from 0 to 1.
  - Channel Utilization (%)—The percentage of time an access point channel is busy operating on packets. The percentage (from 0 to 100%) represents a load from 0 to 1.
- Controller Utilization
  - CPU Utilization—The percentage of CPU utilization.
  - Memory Utilization—The percentage of memory utilization.
  - Port Utilization—The percentage of (totalDeltaBits/bandwidth) on a port.
- MSE Utilization
  - CPU Utilization—The percentage of CPU utilization.
  - Memory Utilization—The percentage of memory utilization.

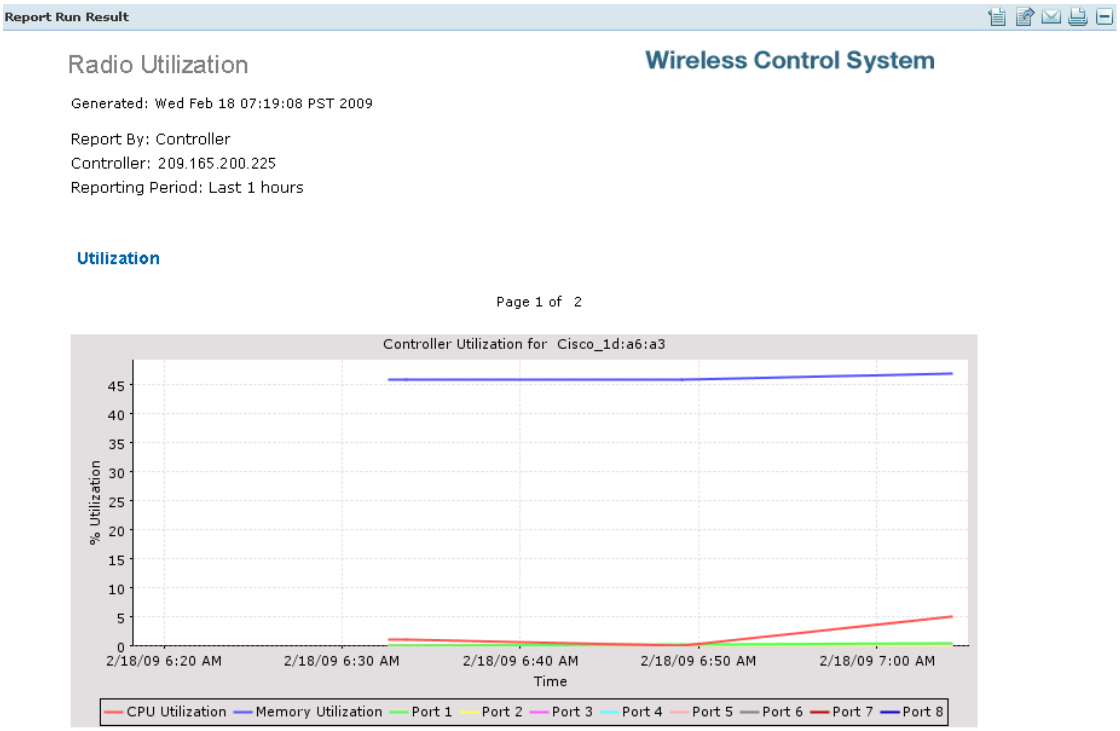
Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Utilization Report Results

The Utilization report displays the following results (Figure 17-25):

Figure 17-25 Utilization Report Results



Guest Reports

You can create the following guest reports:

- Guest Accounts Status
- Guest Association
- Guest Count
- Guest User Sessions
- WCS Guest Operations

Guest Accounts Status

This report displays guest account status changes in chronological order. The report filters guest accounts by the guest user who created them. One example of a status change is Scheduled to Active to Expired.

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by

  - WCS User—Select **All WCS Users** from the Report Criteria page or click **Edit** to select a specific WCS user.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Guest Account Status report results includes:

- Time
- Guest username
- Created by
- Status

Guest Account Status Report Results

The following are potential results for a Guest Account Status report, depending on how the report is customized:

- Time
- Guest Username
- Created by
- Status

Guest Association

This report displays when a guest client associated to and disassociated from a guest profile/SSID over a customizable period of time.

This report displays the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - Guest Profile—Select **All Profiles** from the Report Criteria page or click **Edit** to select a specific profile.
  - specific profile.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Guest Association report results includes:

- Time
- Guest user
- Guest MAC address
- Controller IP Address
- AP MAC Address

- Login and Logout Times
- Guest IP address
- Bytes Received
- Bytes Sent

Guest Association Report Results

The following are potential results for a Guest Association report, depending on how the report is customized:

- Time
- Guest MAC address and username
- Device IP address
- Guest profile
- Status
- AP Name
- Guest IP address
- Session Duration
- Reason—Reason for the disassociation

Guest Count

This report displays the number of guest clients logged into the network per guest profile/SSID over a customizable period of time.

This report display the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - Guest Profile—Select **All Profiles** from the Report Criteria page or click **Edit** to select a specific profile.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select 802.11 a/n, 802.11 b/g/n, or both.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Guest Count Report Results

The Guest Count results contain the following information:

- Authenticated Guest Count—Indicates the number of authenticated guests for each specified guest profile and protocol during the specified period of time.

Guest User Sessions

This report displays historic session data for a guest user. The session data, such as amount of data passed, login and logout time, guest IP address, and guest MAC address, is available for one month by default. The data retention period is configured from the Administration > Background Tasks page. This report is generated for guest users who are associated to controllers running software version 5.2 or above.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - Guest User—Select **All Guest Users** from the Report Criteria page or click **Edit** to select a specific guest user.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

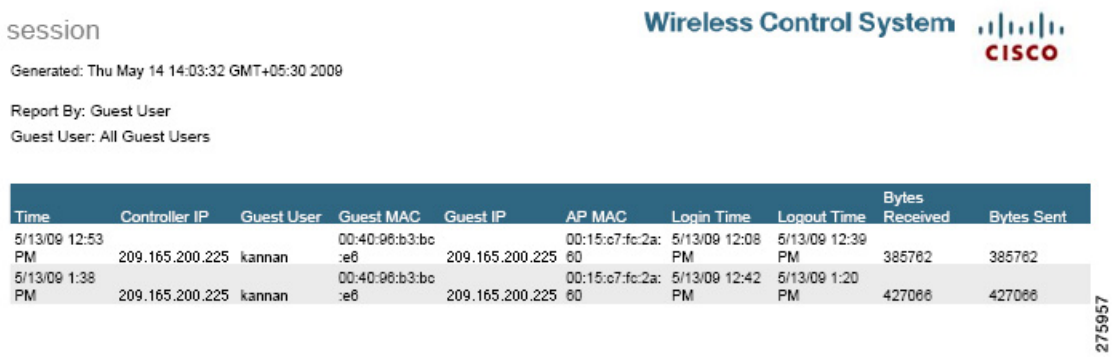
Guest User Sessions Report Results

The Guest User Sessions report contains the following information (refer to Figure 17-26):

- Controller IP Address
- Guest User
- Guest MAC Address

- Guest IP Address
- AP MAC
- Login Time
- Logout Time
- Bytes Received
- Bytes Sent

Figure 17-26 Guest User Sessions Report Results


session

Wireless Control System

Generated: Thu May 14 14:03:32 GMT+05:30 2009

Report By: Guest User
Guest User: All Guest Users

Time	Controller IP	Guest User	Guest MAC	Guest IP	AP MAC	Login Time	Logout Time	Bytes Received	Bytes Sent
5/13/09 12:53 PM	209.165.200.225	kannan	00:40:96:b3:bc :e6	209.165.200.225	00:15:c7:fc:2a: 60	5/13/09 12:08 PM	5/13/09 12:39 PM	385762	385762
5/13/09 1:38 PM	209.165.200.225	kannan	00:40:96:b3:bc :e6	209.165.200.225	00:15:c7:fc:2a: 60	5/13/09 12:42 PM	5/13/09 1:20 PM	427066	427066

275957

WCS Guest Operations

This report displays all activities performed by one or all guests, such as creating, deleting, or updating guest user accounts. If a guest user is deleted from WCS, the activity performed by the deleted guest user still shows for up to one week after the activity occurred.

The following settings and scheduling parameters are available for this report:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - WCS User—Select **All WCS Users** from the Report Criteria page or click **Edit** to select a specific user.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Guest Operation report results includes:

- Time
- Reason
- WCS User
- Guest User
- Operation
- Status

WCS Guest Operation Report Results

The following are potential results for a WCS Guest Operations report, depending on how the report is customized:

- Time
- WCS User
- Guest User
- Operation
- Status
- Reason

Mesh Reports

- Alternate Parent
- Link Stats
- Nodes
- Packet Stats
- Stranded APs

- Worst Node Hops

Alternate Parent

This report displays the number of alternate parents with the same configured mesh group for each mesh access point. This report can be used to determine an access point's capability to handle failures in the mesh path.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

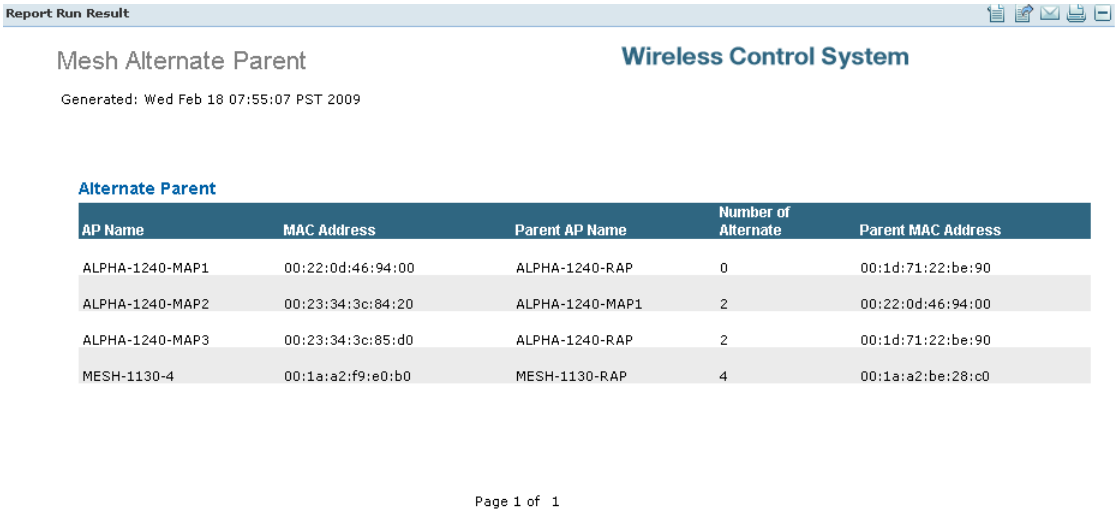
Available information for Alternate Parent report results includes:

- AP Name—The access point name.
- MAC address
- Parent AP name
- Number Alternate parents
- Parent MAC address

Alternate Parent Report Results

The Alternate Parent report contains the following results (Figure 17-27):

Figure 17-27 Alternate Parent Report Results



Report Run Result

Mesh Alternate Parent

Wireless Control System

Generated: Wed Feb 18 07:55:07 PST 2009

Alternate Parent

AP Name	MAC Address	Parent AP Name	Number of Alternate	Parent MAC Address
ALPHA-1240-MAP1	00:22:0d:46:94:00	ALPHA-1240-RAP	0	00:1d:71:22:be:90
ALPHA-1240-MAP2	00:23:34:3c:84:20	ALPHA-1240-MAP1	2	00:22:0d:46:94:00
ALPHA-1240-MAP3	00:23:34:3c:85:d0	ALPHA-1240-RAP	2	00:1d:71:22:be:90
MESH-1130-4	00:1a:a2:f9:e0:b0	MESH-1130-RAP	4	00:1a:a2:be:28:c0

Page 1 of 1

251887

Link Stats

This report displays mesh link and node statistics such as parent access point, link SNR, packet error rate, parent changes, node hops, total transmit packets, mesh path, connected access points, mesh group, data rate, and channel. The mesh link and mesh node statistics can be run individually or combined.

The following settings and scheduling parameters are available for this report:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report Type—Select **Link Stats** or **Node Hops** from the drop-down list.
- Report by—Select **AP by Controller**, **AP by Floor Area**, or **AP by Outdoor Area** from the Report by drop-down list and the appropriate selection from the Report Criteria page (or click **Edit** to select specific devices).

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

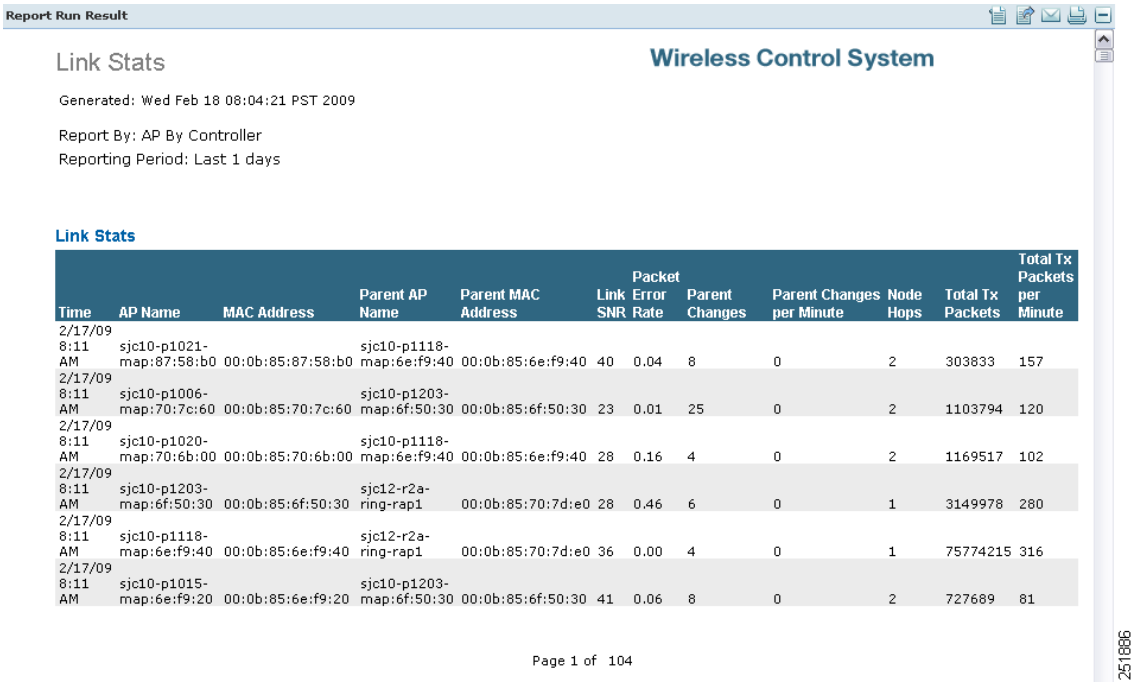
Available information for Link Stats report results includes:

- Time
- MAC address
- Parent MAC address
- AP Name—The access point name.
- Parent AP name
- Link SNR
- Packet Error Rate
- Parent changes
- Parent changes per minute
- Node hops
- Total Tx Packets
- Total Tx Packets per minute

Link Stats Report Results

The Link Stats report contains the following results (Figure 17-28):

Figure 17-28 Link Stats Report Results



Report Run Result

Link Stats

Wireless Control System

Generated: Wed Feb 18 08:04:21 PST 2009

Report By: AP By Controller
Reporting Period: Last 1 days

Link Stats

Time	AP Name	MAC Address	Parent AP Name	Parent MAC Address	Link SNR	Packet Error Rate	Parent Changes	Parent Changes per Minute	Node Hops	Total Tx Packets	Total Tx Packets per Minute
2/17/09 8:11 AM	sjc10-p1021-map:87:58:b0	00:0b:85:87:58:b0	sjc10-p1118-map:6e:f9:40	00:0b:85:6e:f9:40	40	0.04	8	0	2	303833	157
2/17/09 8:11 AM	sjc10-p1006-map:70:7c:60	00:0b:85:70:7c:60	sjc10-p1203-map:6f:50:30	00:0b:85:6f:50:30	23	0.01	25	0	2	1103794	120
2/17/09 8:11 AM	sjc10-p1020-map:70:6b:00	00:0b:85:70:6b:00	sjc10-p1118-map:6e:f9:40	00:0b:85:6e:f9:40	28	0.16	4	0	2	1169517	102
2/17/09 8:11 AM	sjc10-p1203-map:6f:50:30	00:0b:85:6f:50:30	sjc12-r2a-ring-rap1	00:0b:85:70:7d:e0	28	0.46	6	0	1	3149978	280
2/17/09 8:11 AM	sjc10-p1118-map:6e:f9:40	00:0b:85:6e:f9:40	sjc12-r2a-ring-rap1	00:0b:85:70:7d:e0	36	0.00	4	0	1	75774215	316
2/17/09 8:11 AM	sjc10-p1015-map:6e:f9:20	00:0b:85:6e:f9:20	sjc10-p1203-map:6f:50:30	00:0b:85:6f:50:30	41	0.06	8	0	2	727689	81

Page 1 of 104

251886

Nodes

This report displays mesh tree information for each mesh access point such as hop count, number of directly connected children, number of connected access points, and mesh path.

The following settings and scheduling parameters are available for this report:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

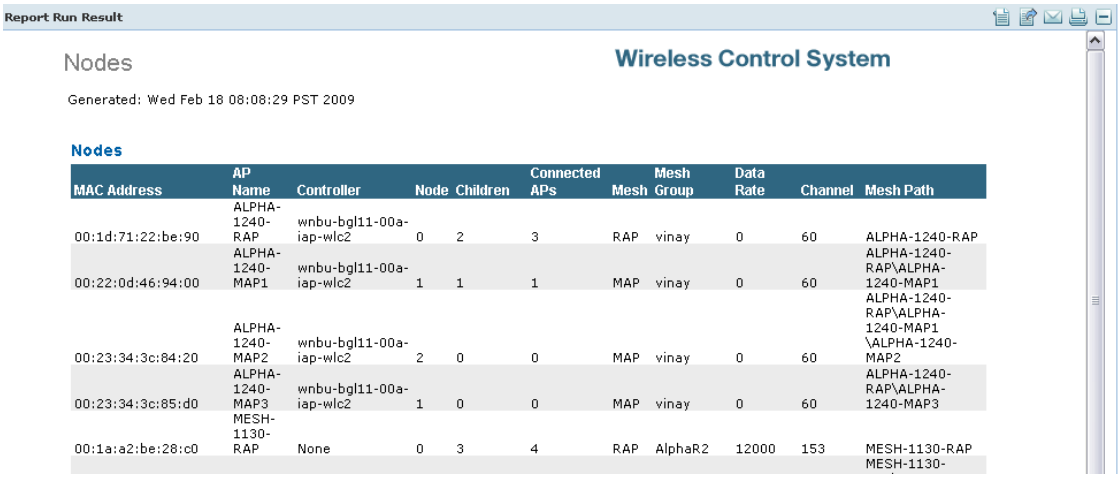
Available information for Node report results includes:

- MAC Address—The MAC address of the mesh access point.
- AP Name—The name of the mesh access point.
- Node Hops—The number of node hops for this mesh group.
- Children—The number of children for this access point.
- Connected APs—The number of access points connected to this access point.
- Mesh Path—The path of the mesh access point.
- Controller—The controller to which the mesh access point is associated.
- Mesh Role—Mesh access point (MAP) or Root access point (RAP).
- Mesh Group—The name of the mesh group to which this access point belongs.
- Data Rate—The data rate for this access point.
- Channel—The channel on which this access point is located.

Nodes Report Results

The Node report contains the following results (Figure 17-29):

Figure 17-29 Node Report Results


Report Run Result

Nodes

Wireless Control System

Generated: Wed Feb 18 08:08:29 PST 2009

Nodes

MAC Address	AP Name	Controller	Node	Children	Connected APs	Mesh	Mesh Group	Data Rate	Channel	Mesh Path
00:1d:71:22:be:90	ALPHA-1240-RAP	wnbu-bgl11-00a-iap-wlc2	0	2	3	RAP	vinay	0	60	ALPHA-1240-RAP
00:22:0d:46:94:00	ALPHA-1240-MAP1	wnbu-bgl11-00a-iap-wlc2	1	1	1	MAP	vinay	0	60	ALPHA-1240-RAP\ALPHA-1240-MAP1
00:23:34:3c:84:20	ALPHA-1240-MAP2	wnbu-bgl11-00a-iap-wlc2	2	0	0	MAP	vinay	0	60	ALPHA-1240-RAP\ALPHA-1240-MAP1 \ALPHA-1240-MAP2
00:23:34:3c:85:d0	ALPHA-1240-MAP3	wnbu-bgl11-00a-iap-wlc2	1	0	0	MAP	vinay	0	60	ALPHA-1240-RAP\ALPHA-1240-MAP3
00:1a:a2:be:28:c0	MESH-1130-RAP	None	0	3	4	RAP	AlphaR2	12000	153	MESH-1130-RAP
										MESH-1130-

251893

Packet Stats

This report displays the total number of packets transmitted, packets transmitted per minute, packet queue average, packet dropped count, packets dropped per minute, and errors for packets transmitted by neighbor access points.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to use this as a saved report, enter a report name.
- Report Type—Select **Packet Stats** from the drop-down list.

- Report by—Select **AP by Controller**, **AP by Floor Area**, or **AP by Outdoor Area** from the Report by drop-down list and the appropriate selection from the Report Criteria page (or click **Edit** to select specific devices).

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Graph Type—Select the type of graph you want displayed for these report results (Packet Counts or Packets Per Minute).
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

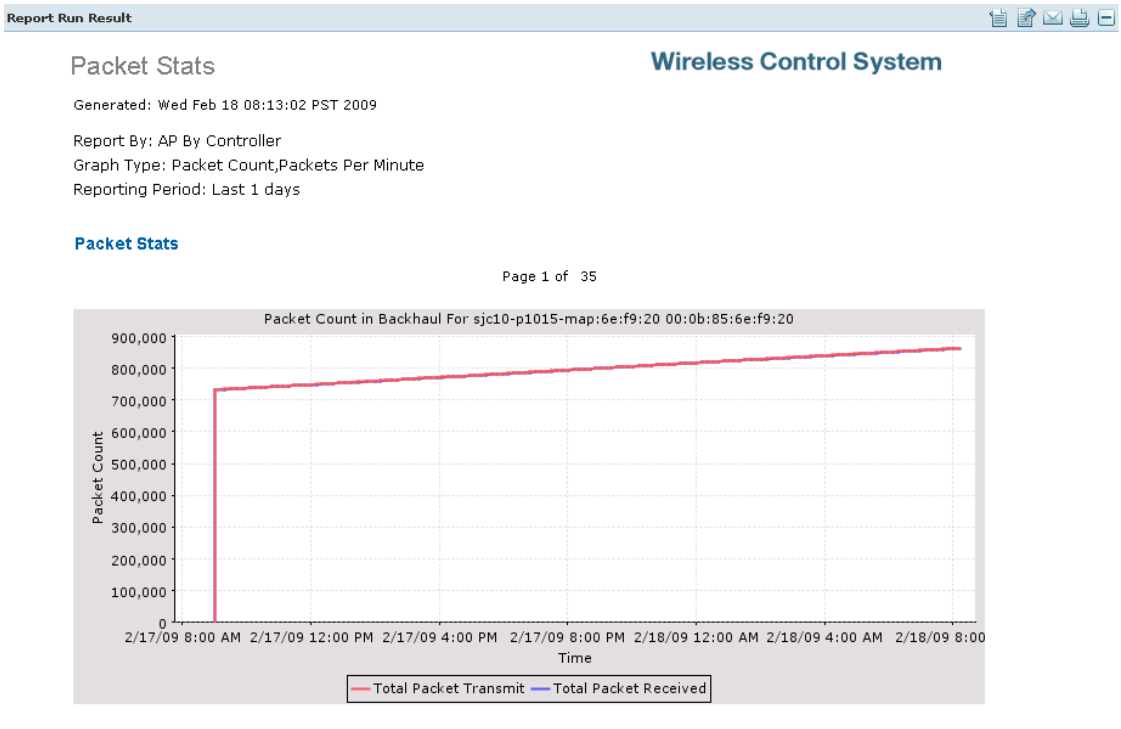
Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Packet Stats Report Results

The Packet Stats report contains the following results (Figure 17-30):

Figure 17-30 Packet Stats Report Results



Packet Error Statistics

This report notes the percentages of packet errors for packets transmitted by the neighbor mesh access point. The packet error rate percentage is 1 minus the number of successfully transmitted packets/numbers of total packets transmitted.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to use this as a saved report, enter a report name.
- Report Type—Select **Packet Error Stats** from the drop-down list.
- Report by—Select **AP by Controller**, **AP by Floor Area**, or **AP by Outdoor Area** from the Report by drop-down list and the appropriate selection from the Report Criteria page (or click **Edit** to select specific devices).

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Neighbor Type—Select All Neighbors or Parent/Children Only.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.

– From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

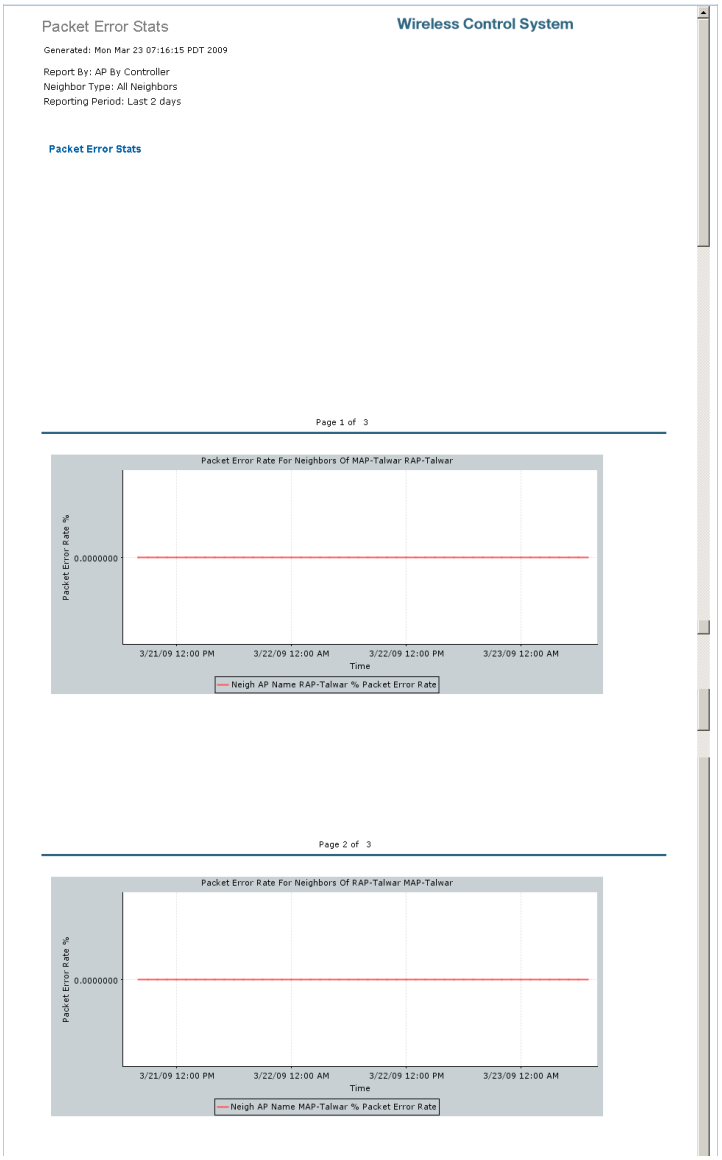
Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Packet Error Stats Report Results

The Packet Error Statistics report contains the following results (Figure 17-31):

Figure 17-31 Packet Error Stats Report Results



Packet Queue Statistics

This report generates a graph of the total number of packets transmitted and the total number of packets successfully transmitted by the neighbor mesh access point.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report Type—Select **Packet Queue Stats** from the drop-down list.

- Report by—Select **AP by Controller**, **AP by Floor Area**, or **AP by Outdoor Area** from the Report by drop-down list and the appropriate selection from the Report Criteria page (or click **Edit** to select specific devices).

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Graph Type—Select the type of graph you want displayed for these report results (Packet Queue Average, Packets Dropped Count, Packets Dropped Per Minute).
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

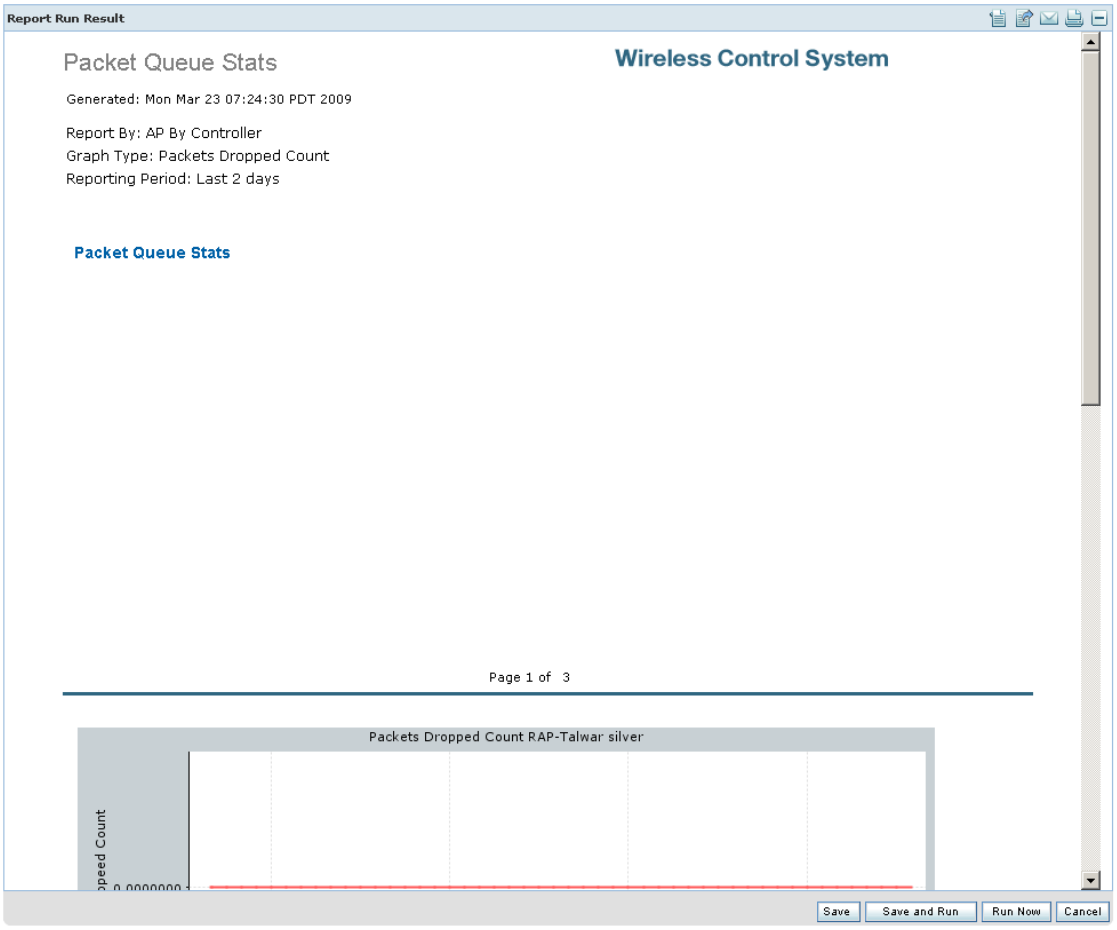
Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Packet Queue Statistics Report Results

The Packet Queue Statistics report contains the following results (Figure 17-32):

Figure 17-32 Packet Queue Statistics Report Results



Stranded APs

This report displays access points that appear to be stranded. These access points might have joined a controller at one time and are no longer joined to a controller managed by WCS, or they might have never joined a controller managed by WCS.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Stranded States—Select **APs Managed by WCS** or **All**.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

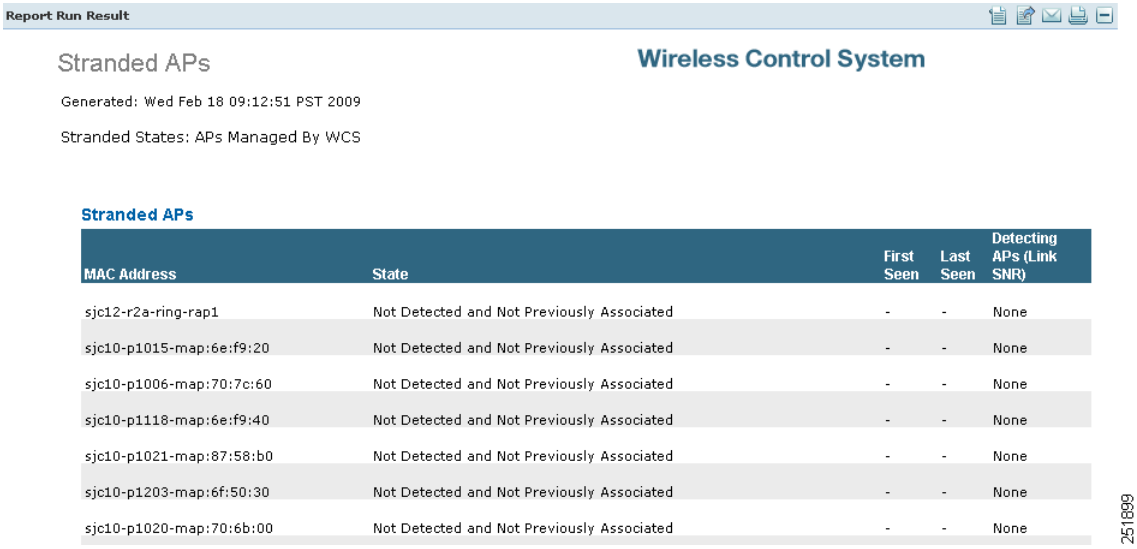
Available information for Link Stats report results includes:

- MAC Address—The MAC address of the stranded access point.
- State—The state of the stranded access point (such as Not Detected and Not Previously Associated).
- First Seen—The date and time this access point was first detected.
- Last Seen—The date and time this access point was last seen.
- Detecting APs (Link SNR)—The access point(s) that detected this stranded access point.

Stranded APs Report Results

The Stranded APs report contains the following results (Figure 17-33):

Figure 17-33 Stranded APs Report Results


Report Run Result

Stranded APs

Wireless Control System

Generated: Wed Feb 18 09:12:51 PST 2009

Stranded States: APs Managed By WCS

Stranded APs

MAC Address	State	First Seen	Last Seen	Detecting APs (Link SNR)
sjc12-r2a-ring-rap1	Not Detected and Not Previously Associated	-	-	None
sjc10-p1015-map:6e:f9:20	Not Detected and Not Previously Associated	-	-	None
sjc10-p1006-map:70:7c:60	Not Detected and Not Previously Associated	-	-	None
sjc10-p1118-map:6e:f9:40	Not Detected and Not Previously Associated	-	-	None
sjc10-p1021-map:87:58:b0	Not Detected and Not Previously Associated	-	-	None
sjc10-p1203-map:6f:50:30	Not Detected and Not Previously Associated	-	-	None
sjc10-p1020-map:70:6b:00	Not Detected and Not Previously Associated	-	-	None

251899

Worst Node Hops

This report displays the worst node hops or backhaul SNR links for the specified reporting period. The information displays in both table and graph form. Report types include worst node hops, worst SNR links for all neighbors, and worst SNR links for parent/children only.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report Type—Select **Worst Node Hops** or **Worst SNR Links** from the drop-down list.
- Report Type—When **Worst Node Hops** is selected from the Report Type above, select **Table Only** or **Table and Graph** to determine how the report results display.
- Neighbor Type—When **Worst SNR Links** is selected from the Report Type, select **All Neighbors (Table Only)**, **Parent/Children Only (Table Only)**, **All Neighbors (Table and Graph)**, or **Parent/Children Only (Table and Graph)** to determine how the report results display.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

- Show—Enter the number of records that you want displayed on each page.

Note Leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Note Worst Node Hops and Worst SNR Links reports are available in both table and graph reports. To customize report results for a particular section, select the applicable section from the Customizable Report drop-down list.

Available information for Worst Node Hops report results includes:

- AP Name—The access point name.
- Node Hops—The number of node hops.
- MAC Address—The MAC address of the access point.
- Parent AP Name—The name of the parent access point.

- Parent MAC Address—The MAC address of the parent access point.
- Time (graph only)—The time of the node hop count.

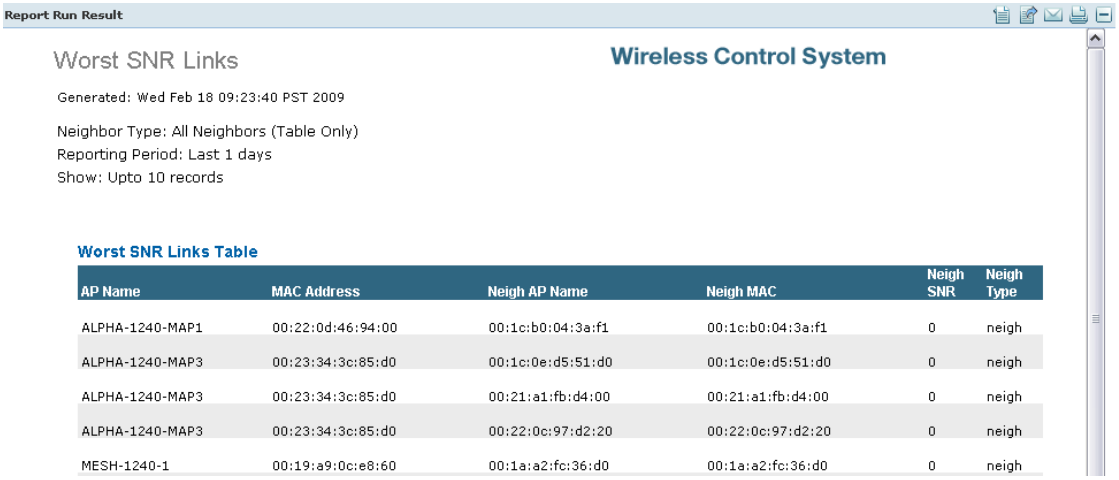
Available information for Worst SNR Links report results includes:

- AP Name—The access point name.
- MAC Address—The MAC address of the access point.
- Neigh SNR—The neighbor signal-to-noise ratio.
- Neigh AP Name—The name of the neighbor access point.
- Neigh MAC Address—The MAC address of the neighbor access point.
- Neigh Type—The neighbor type.
- Time (graph only)—The time of the current report statistics.

Worst Node Hops Report Results

The Worst Node Hops report contains the following results (Figure 17-34):

Figure 17-34 Worst Node Hops Report Results


Report Run Result

Worst SNR Links

Wireless Control System

Generated: Wed Feb 18 09:23:40 PST 2009

Neighbor Type: All Neighbors (Table Only)
Reporting Period: Last 1 days
Show: Upto 10 records

Worst SNR Links Table

AP Name	MAC Address	Neigh AP Name	Neigh MAC	Neigh SNR	Neigh Type
ALPHA-1240-MAP1	00:22:0d:46:94:00	00:1c:b0:04:3a:f1	00:1c:b0:04:3a:f1	0	neigh
ALPHA-1240-MAP3	00:23:34:3c:85:d0	00:1c:0e:d5:51:d0	00:1c:0e:d5:51:d0	0	neigh
ALPHA-1240-MAP3	00:23:34:3c:85:d0	00:21:a1:fb:d4:00	00:21:a1:fb:d4:00	0	neigh
ALPHA-1240-MAP3	00:23:34:3c:85:d0	00:22:0c:97:d2:20	00:22:0c:97:d2:20	0	neigh
MESH-1240-1	00:19:a9:0c:e8:60	00:1a:a2:fc:36:d0	00:1a:a2:fc:36:d0	0	neigh

251910

Network Summary

- 802.11n Summary
- Executive Summary

802.11n Summary

This report displays a summary of 802.11n clients and client bandwidth usage for a customizable period of time.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

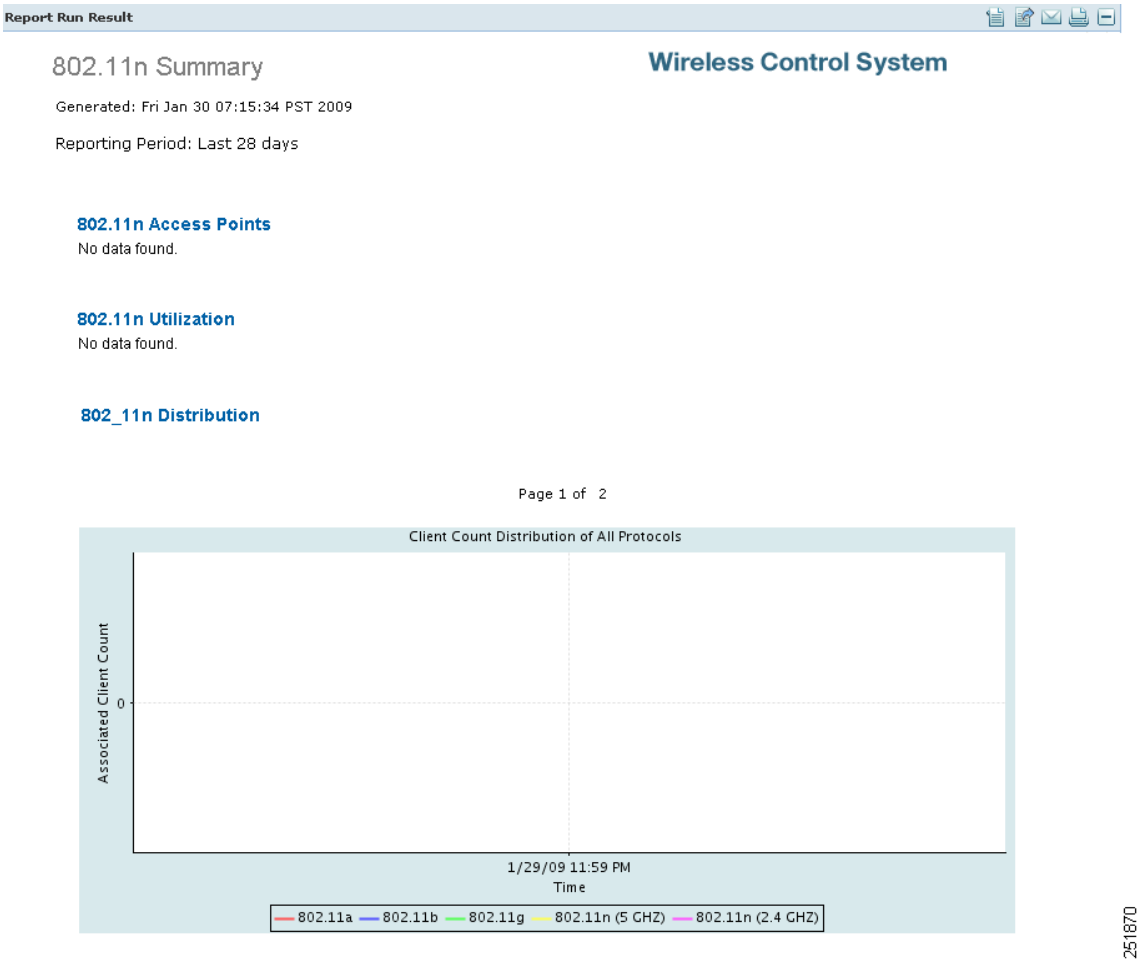
Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

802.11n Summary Report Results

The 802.11n Summary report contains the following results (Figure 17-35):

Figure 17-35 802.11n Summary Report Results



Executive Summary

This report displays a quick view of your wireless network. It provides details on LWAPP versus autonomous access point usage, associated client counts in the network, and guest client counts in the network.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

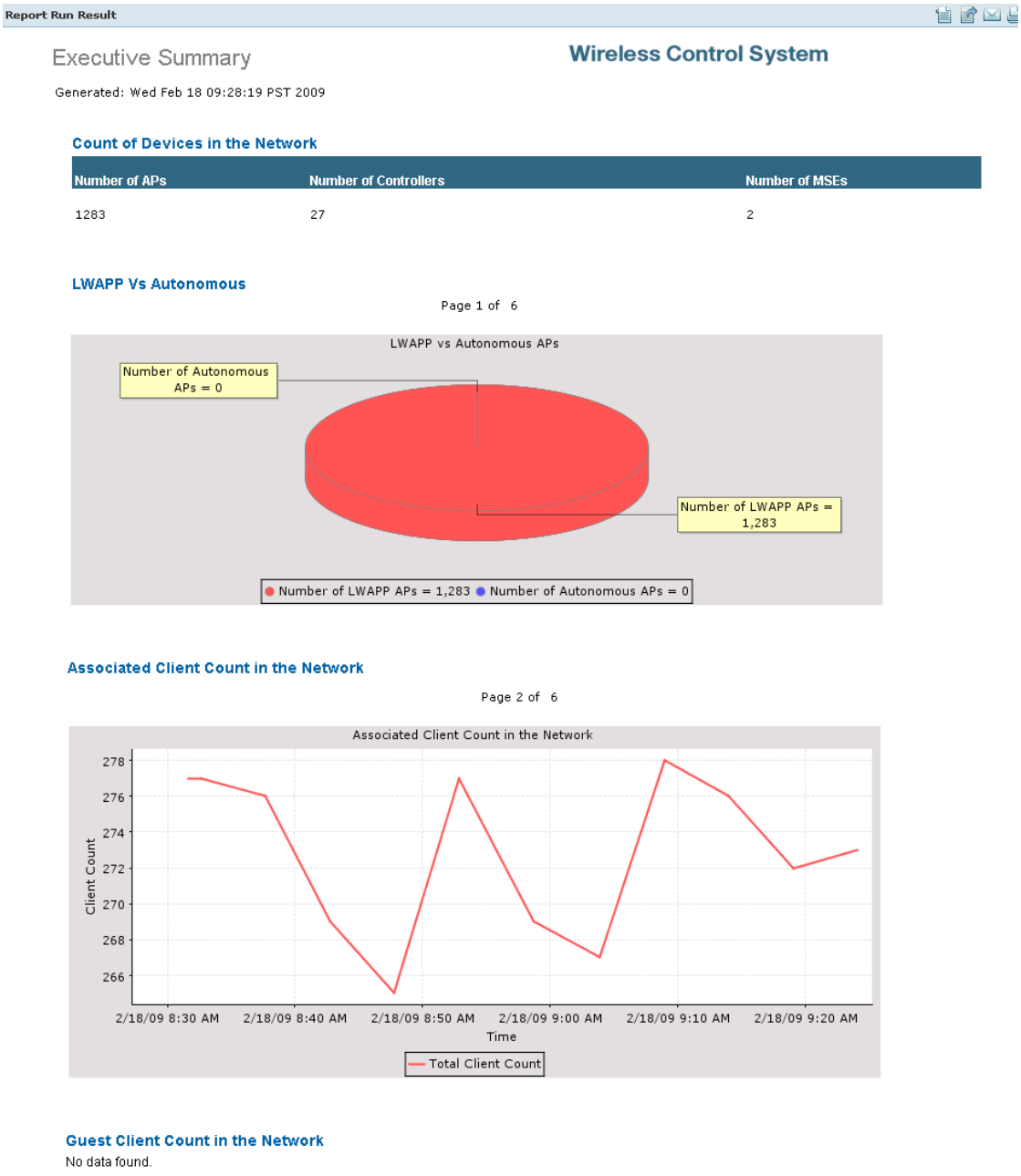
Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Executive Summary Report Results

The Executive Summary report results contain the following (Figure 17-36):

Figure 17-36 Executive Summary Report Results



Performance Reports

You can create the following performance reports:

- 802.11 Counters
- Coverage Hole
- Network Utilization
- Traffic Stream Metrics

- Tx Power and Channel
- VoIP Calls Graph
- VoIP Calls Table
- Voice Statistics

802.11 Counters

This report 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.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select 802.11 a/n, 802.11 b/g/n, or both.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

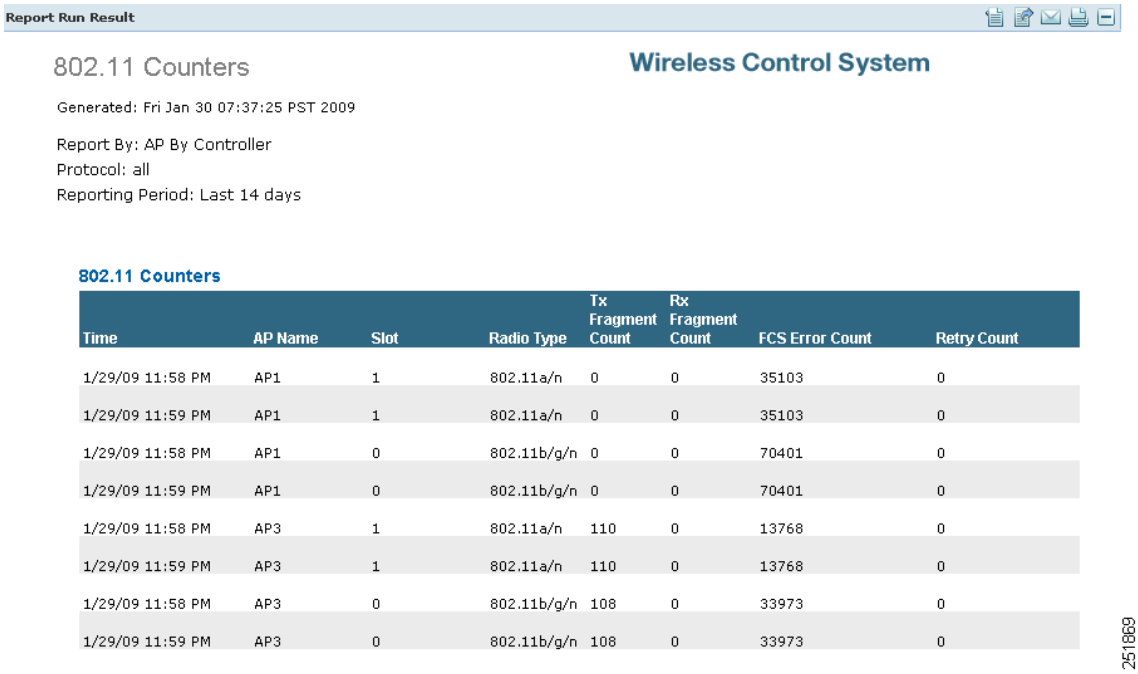
Available information for 802.11 Counters report results includes:

- Time—The date and time of the count.
- AP Name—The name of the applicable access point.
- Slot—The slot number.
- Radio Type—802.11a/n or 802.11b/g/n.
- Tx Fragment Count—The number of successfully received MPDUs of type Data or Management.
- Rx Fragment Count—The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
- FCS Error Count—The number of FCS errors detected in a received MPDU.
- Retry Count—The number of MSDUs successfully transmitted after one or more retransmissions.
- Multicast Rx Frame Count—The number of MSDUs received with the multicast bit set in the destination MAC address.
- Multicast Tx Frame Count—The number of times a multicast bit is set in the destination MAC address of a successfully transmitted MSDU. Operating as an STA in an ESS, where these frames are directed to the access point, implies having received an acknowledgment to all associated MPDUs.
- Tx Failed Count—The number of MSDUs successfully transmitted after one or more retransmissions.
- Multiple Retry Count—The number of MSDUs successfully transmitted after more than one retransmission.
- Frame Duplicate Count—The number of times a frame is received that the Sequence Control field indicates is a duplicate.
- Tx Frame Count—The number of successfully transmitted MSDUs.
- RTS Success Count—The number of times a CTS is received in response to an RTS.
- RTS Failure Count—The number of times a CTS is not received in response to an RTS.
- ACK Failure Count—The number of times an ACK is not received when expected.
- WEP Undecryptable Count—The number of times a frame is received with the WEP subfield of the Frame Control field set to one and the WEPOn value for the key mapped to the AT's 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.

802.11 Counters Report Results

The 802.11 Counter report contains the following results (Figure 17-37):

Figure 17-37 802.11 Counters Report Results



Report Run Result

802.11 Counters

Wireless Control System

Generated: Fri Jan 30 07:37:25 PST 2009

Report By: AP By Controller
Protocol: all
Reporting Period: Last 14 days

802.11 Counters

Time	AP Name	Slot	Radio Type	Tx Fragment Count	Rx Fragment Count	FCS Error Count	Retry Count
1/29/09 11:58 PM	AP1	1	802.11a/n	0	0	35103	0
1/29/09 11:59 PM	AP1	1	802.11a/n	0	0	35103	0
1/29/09 11:58 PM	AP1	0	802.11b/g/n	0	0	70401	0
1/29/09 11:59 PM	AP1	0	802.11b/g/n	0	0	70401	0
1/29/09 11:58 PM	AP3	1	802.11a/n	110	0	13768	0
1/29/09 11:59 PM	AP3	1	802.11a/n	110	0	13768	0
1/29/09 11:58 PM	AP3	0	802.11b/g/n	108	0	33973	0
1/29/09 11:59 PM	AP3	0	802.11b/g/n	108	0	33973	0

251869

Coverage Hole

This report identifies the location of potential coverage holes in your network and whether they occur more frequently at a given spot. This report can help you modify RRM settings or decide whether you need additional access points to provide coverage in sparsely deployed areas. It runs on the alarm table and both the alarm generation time, the cleared time (if cleared), and the state of the alarm (active or cleared).

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period

- Last—Select the **Last** radio button and a period of time from the drop-down list.
- From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

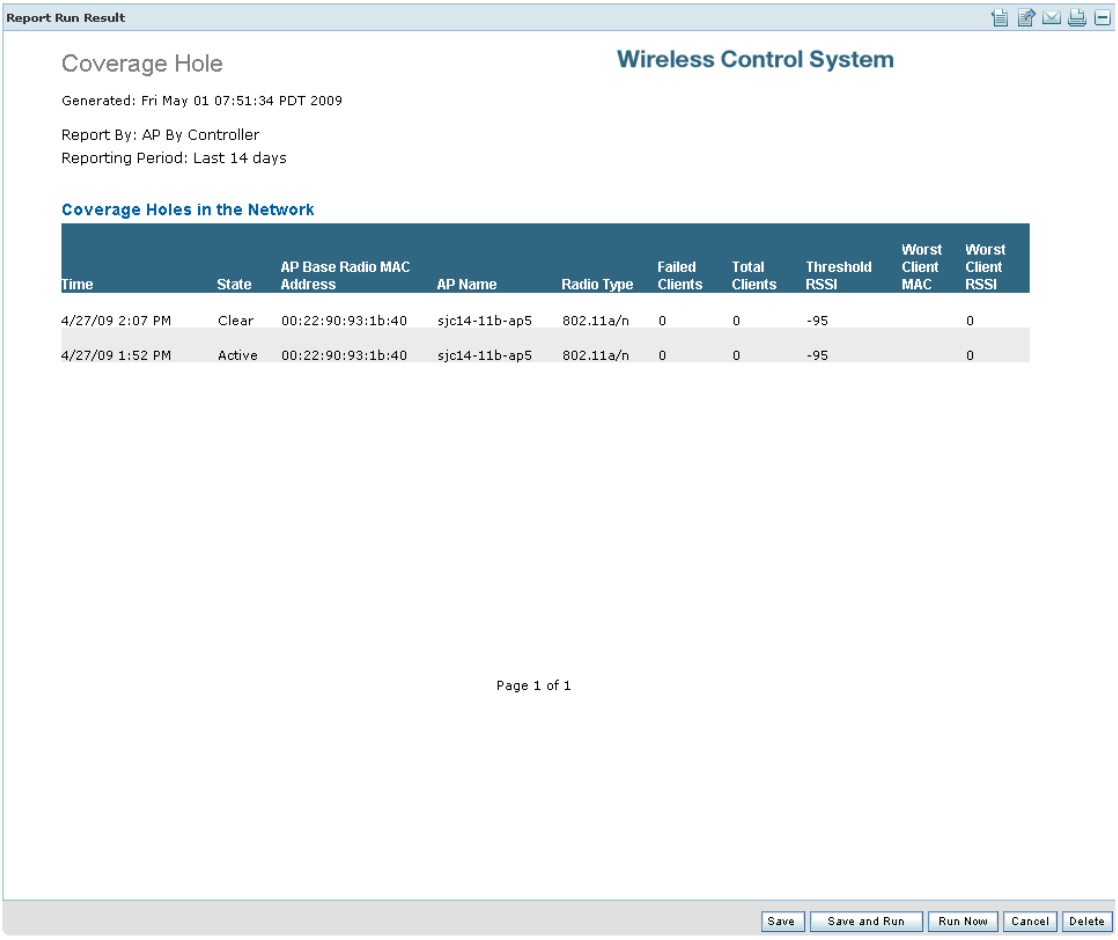
Available information for Coverage Hole report results includes:

- Time—The date and time the coverage hole was detected.
- State—Clear or Active.
- AP Base Radio MAC Address—The MAC address of the access point base radio.
- AP Name—The name of the access point on which the coverage hole was detected.
- Radio Type—802.11a/n or 802.11b/g/n.
- Failed Clients
- Total Clients
- Threshold RSSI
- Worst Client MAC
- Worst Client RSSI

Coverage Hole Report Results

The Coverage Hole report contains the following results (Figure 17-38):

Figure 17-38 Coverage Hole Report Results



Network Utilization

This report shows the overall network use based on the aggregated port use of all controllers on your network. With these statistics, you can assess current network performance and plan for future scalability needs.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available data fields column.

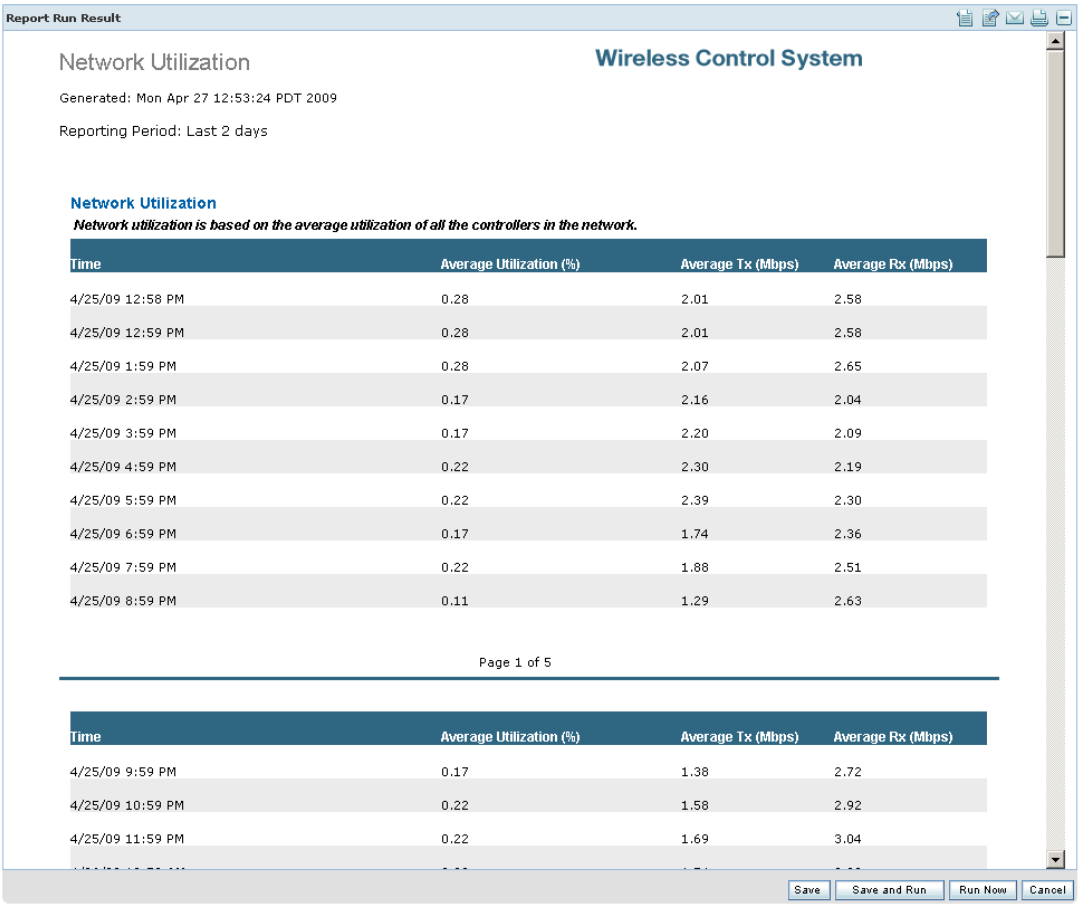
Available information for the Network Utilization report results includes:

- Time
- Average Utilization (%)—The average aggregated (totalDeltaBits/bandwidth) on all controllers.
- Average Tx (Mbps)—The average aggregated received Mbs of all ports on all controllers.
- Average Rx (Mbps)—The average aggregated (totalDeltaBits/bandwidth) on all controllers.

Network Utilization Report Results

The Network Utilization report contains the following results (Figure 17-39):

Figure 17-39 Network Utilization Report Results



Traffic Stream Metrics

This report can help you identify 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.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select 802.11 a/n, 802.11 b/g/n, or both.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

Available information for Traffic Stream Metrics report results includes:

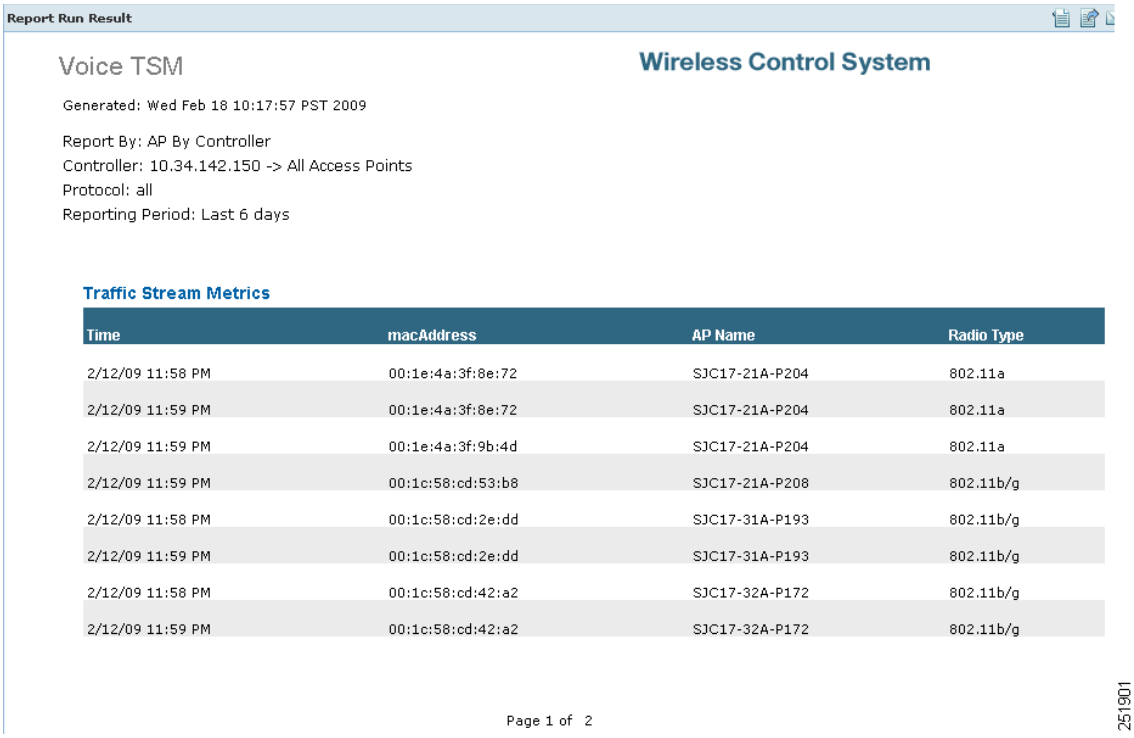
- Time—Date and time the statistics were recorded.
- MAC address—The MAC address of the access point.
- AP Name—The access point name.
- Radio Type—802.11a/n or 802.11b/g/n.
- Average Queuing Delay (Downlink)—The average queuing delay for downlinks.
- Average Queuing Delay (Uplink)—The average queuing delay for uplinks.
- % Packet with less than 10 ms delay (downlink)—The percentage of packets that have a queuing delay of less than 10 milliseconds for a downlink.
- % Packet with less than 10 ms delay (uplink)—The percentage of packets that have a queuing delay of less than 10 milliseconds for an uplink.
- % Packet with more than 10 < 20 ms delay (downlink)—The percentage of packets that have a queuing delay of more than 10 but less than 20 milliseconds for a downlink.
- % Packet with more than 10 < 20 ms delay (uplink)—The percentage of packets that have a queuing delay of more than 10 but less than 20 milliseconds for an uplink.
- % Packet with more than 20 < 40 ms delay (downlink)—The percentage of packets that have a queuing delay of more than 20 but less than 40 milliseconds for a downlink.

- % Packet with more than 20 < 40 ms delay (uplink)—The percentage of packets that have a queuing delay of more than 20 but less than 40 milliseconds for an uplink.
- % Packet with more than 40 ms delay (downlink)—The percentage of packets that have a queuing delay of more than 40 milliseconds for a downlink.
- % Packet with more than 40 ms delay (uplink)—The percentage of packets that have a queuing delay of more than 40 milliseconds for an uplink.
- Packet Loss Ratio (Downlink)—The ratio of lost packets for downlinks.
- Packet Loss Ratio (Uplink)—The ratio of lost packets for uplinks.
- Total Packet Count (Downlink)—The total number of downlink packets.
- Total Packet Count (Uplink)—The total number of uplink packets.
- Roaming Count—Number of packets exchanged for roaming negotiations in this 90-second metrics page.
- Roaming Delay—Roaming delay in milliseconds.

Traffic Stream Metrics Report Results

The Traffic Stream Metrics report contains the following results (Figure 17-40):

Figure 17-40 Traffic Stream Metrics Report Results


Report Run Result

Voice TSM

Wireless Control System

Generated: Wed Feb 18 10:17:57 PST 2009

Report By: AP By Controller
Controller: 10.34.142.150 -> All Access Points
Protocol: all
Reporting Period: Last 6 days

Traffic Stream Metrics

Time	macAddress	AP Name	Radio Type
2/12/09 11:58 PM	00:1e:4a:3f:8e:72	SJC17-21A-P204	802.11a
2/12/09 11:59 PM	00:1e:4a:3f:8e:72	SJC17-21A-P204	802.11a
2/12/09 11:59 PM	00:1e:4a:3f:9b:4d	SJC17-21A-P204	802.11a
2/12/09 11:59 PM	00:1c:58:cd:53:b8	SJC17-21A-P208	802.11b/g
2/12/09 11:58 PM	00:1c:58:cd:2e:dd	SJC17-31A-P193	802.11b/g
2/12/09 11:59 PM	00:1c:58:cd:2e:dd	SJC17-31A-P193	802.11b/g
2/12/09 11:58 PM	00:1c:58:cd:42:a2	SJC17-32A-P172	802.11b/g
2/12/09 11:59 PM	00:1c:58:cd:42:a2	SJC17-32A-P172	802.11b/g

Page 1 of 2

251901

Tx Power and Channel

This report 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 network performance problems.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select 802.11 a/n, 802.11 b/g/n, or both.
- Reporting Period
  - Last—Select the Last radio button and a period of time from the drop-down list.
  - From—Select the From radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

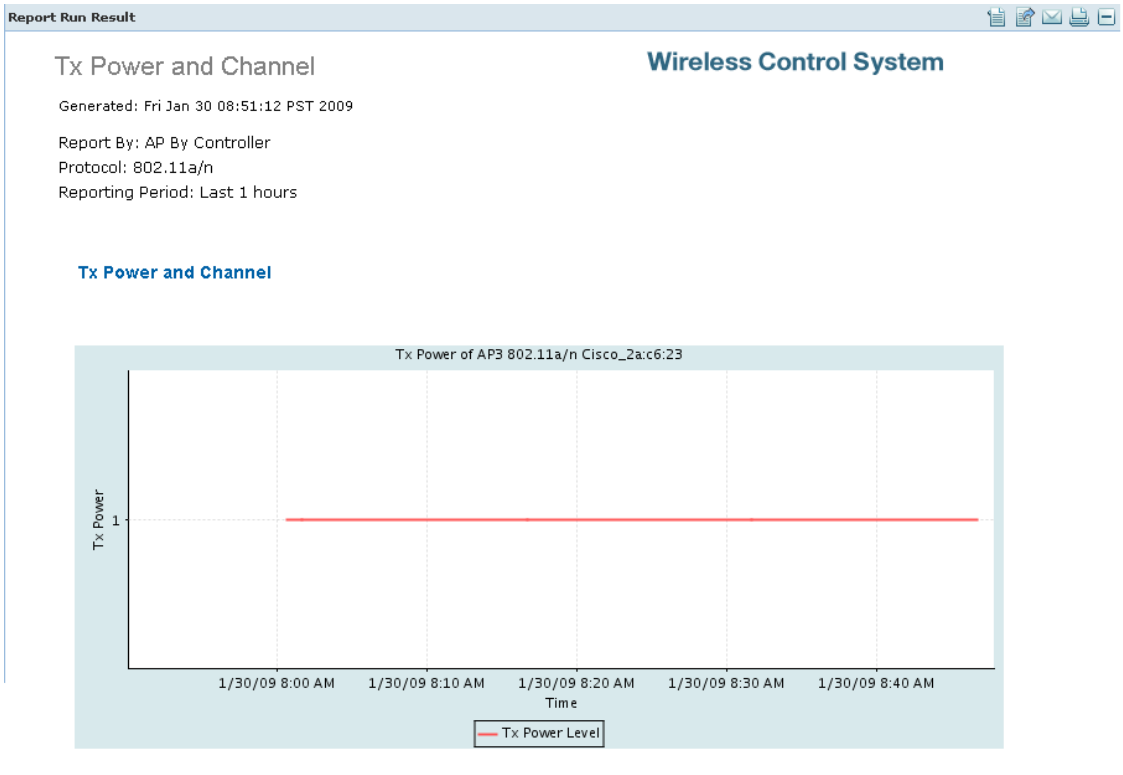
Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Tx Power and Channel Report Results

The Tx Power and Channel report contains the following results (Figure 17-41):

Figure 17-41 Tx Power and Channel Report Results



VoIP Calls Graph

This report helps you 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, you must enable Media Session Snooping on the WLAN. This report displays information in a graph.

Note MSA only supports SIP calls.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select 802.11 a/n, 802.11 b/g/n, or both.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

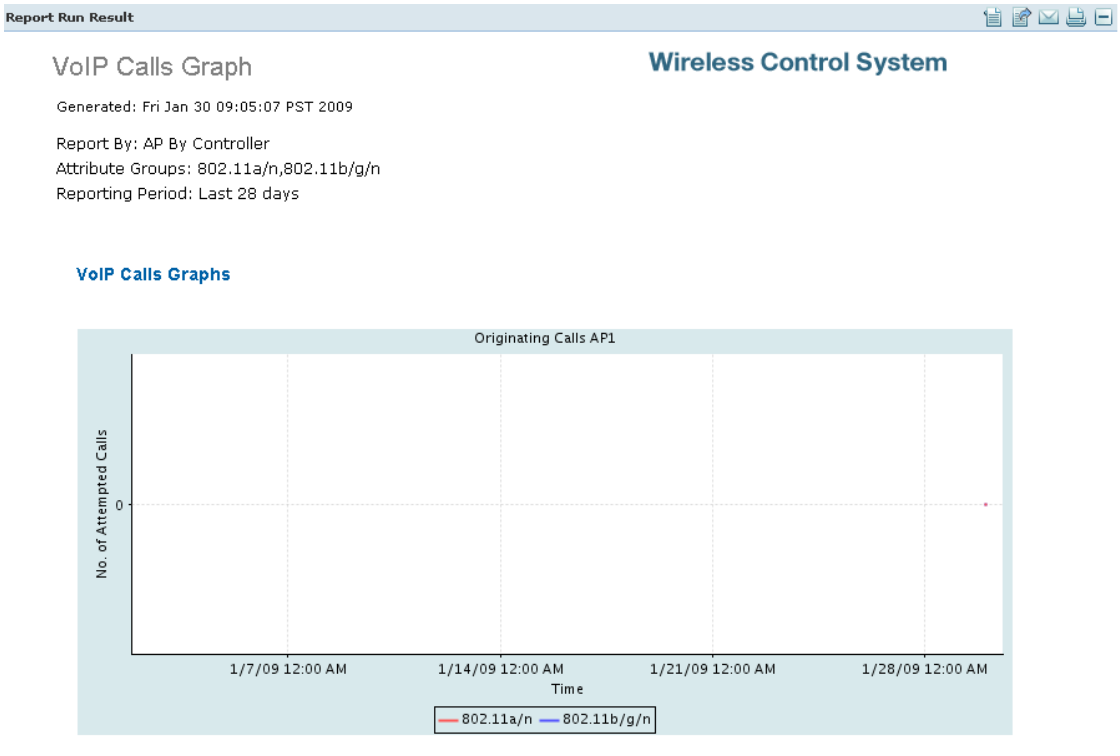
Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

VoIP Calls Report Results

The VoIP Calls report contains the following results (Figure 17-42):

Figure 17-42 VoIP Calls Graph Results



VoIP Calls Table

This report helps you 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, you must enable VoIP snooping (also called Media Session Aware or MSA) on the WLAN. This report displays information in a table.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select 802.11 a/n, 802.11 b/g/n, or both.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

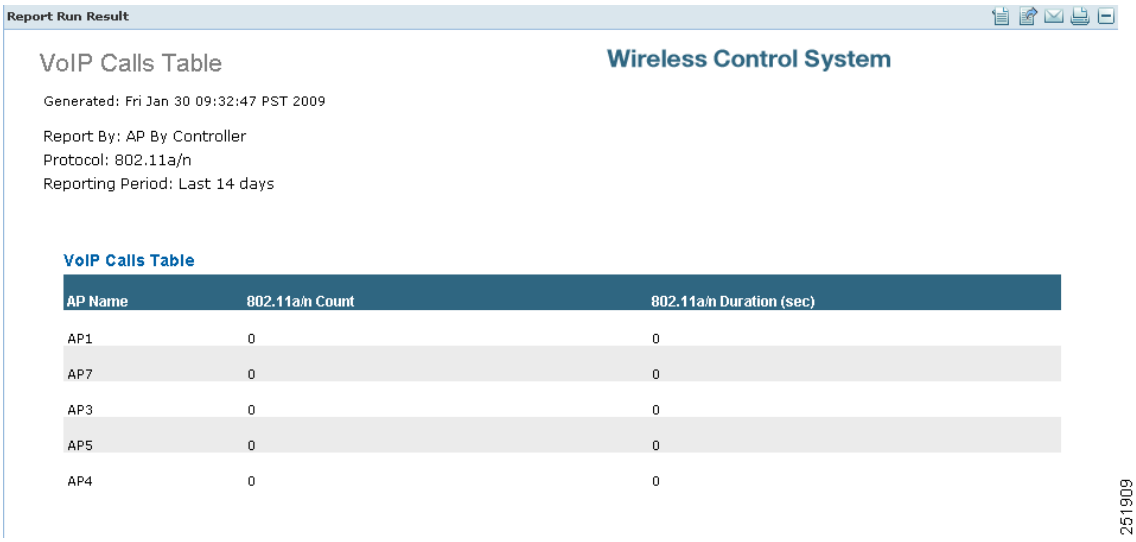
Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

VoIP Calls Table Results

The VoIP Table report contains the following results (Figure 17-43):

Figure 17-43 VoIP Calls Table Results



Voice Statistics

This report helps you analyze wireless network usage from a voice perspective by providing details such as percentage of bandwidth used by voice clients, voice calls, roaming calls, non-roaming calls, and rejected calls (per radio) on the network. To gather useful data from this report, you must make sure that call admission control (CAC) is supported on voice clients.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select 802.11 a/n, 802.11 b/g/n, or both.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

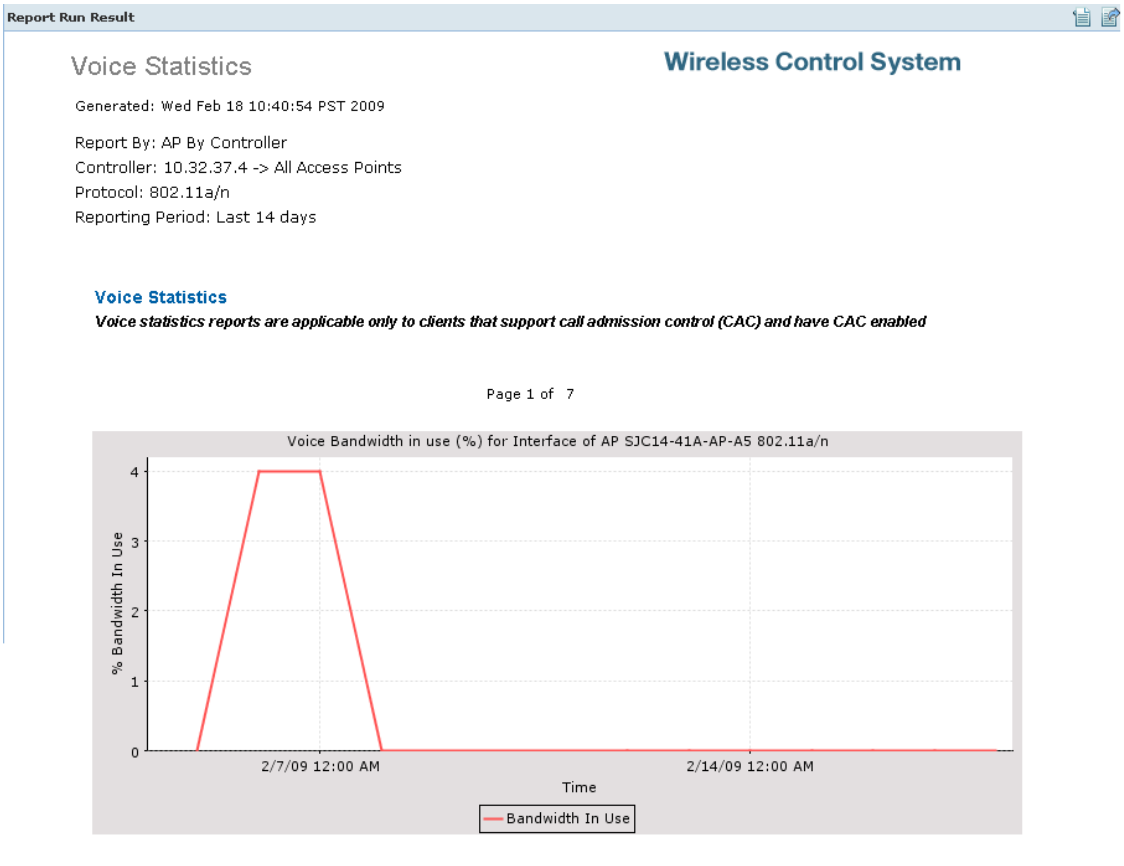
Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Voice Statistics Results

The Voice Statistics report contains the following results (Figure 17-44):

Figure 17-44 Voice Statistics Results



251907

Security Reports

You can create the following security reports:

- Adaptive wIPS Alarms
- Adaptive wIPS Top 10 Access Points
- Adhoc Rogue Events
- Adhoc Rogues
- New Rogue Access Points
- New Rogue Access Point Count
- Rogue Access Points Events
- Rogue Access Points
- Security Summary

Adaptive wIPS Alarms

This report displays wIPS events by selected MSEs, controllers, and access points for each alarm type. This report can take awhile to generate if you set the reporting criteria to collect a substantial number of events. It is best to give a short duration time or run it as a scheduled report.

This report contains thee following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - MSE with Adaptive wIPS Service—Select **All MSEs with Adaptive wIPS Service** from the Report Criteria page or click **Edit** to select a specific MSE.
  - Controller by MSE—Select **All MSEs > All Controllers** from the Report Criteria page or click **Edit** to select a specific controller.
  - AP by MSE—Select **All MSEs > All Controllers > All APs** from the Report Criteria page or click **Edit** to select a specific access point.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Alarm Category—Select **All Types**, **Denial of Service (DoS)**, or **Security Penetration** to determine the types of wIPS alarms to display in the results.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are shown in WCS server local time.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

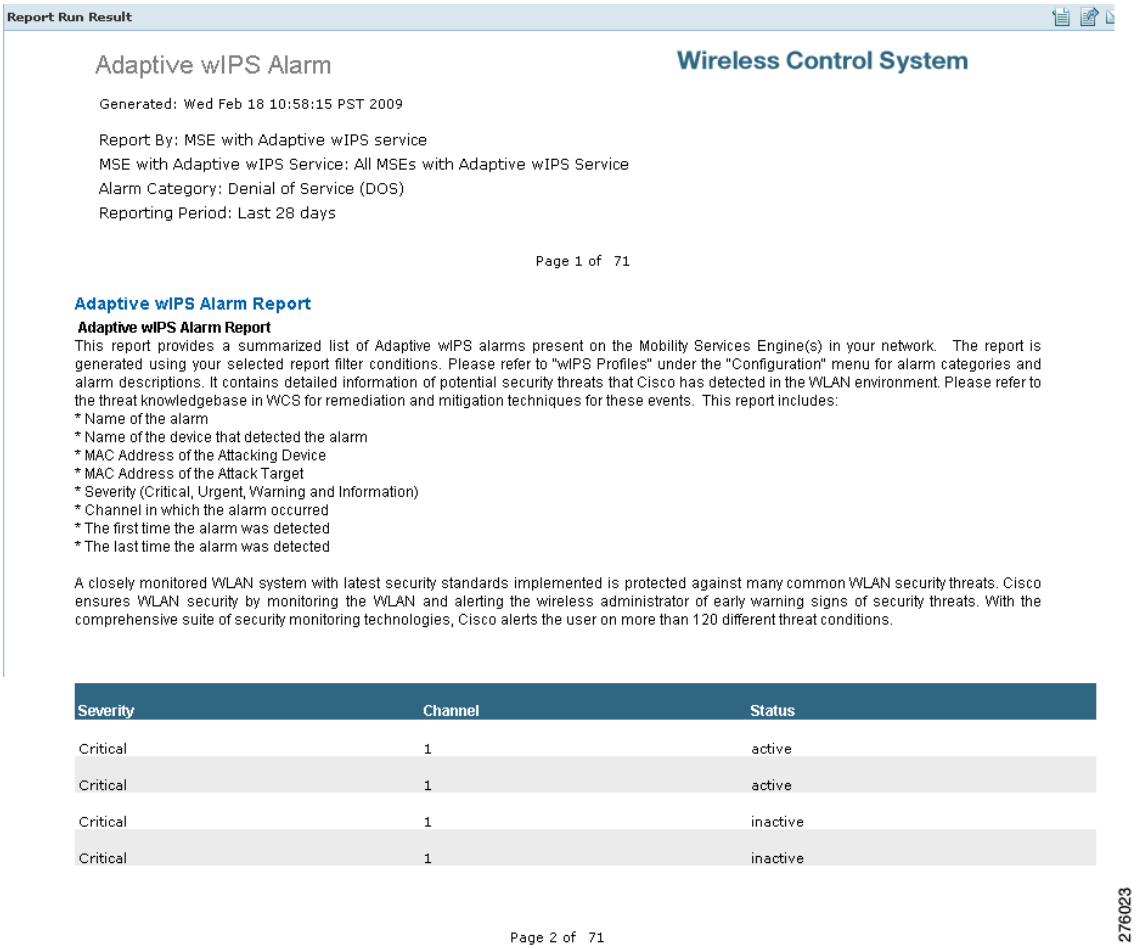
The following information is available for an Adaptive wIPS Alarms report:

- Alarm Name—The name of the alarm.
- AP Name—The name of the device that detected the alarm.
- Source Device—Identifies the device that initiated the potential attack.
- Target Device—Identifies the device targeted by the potential attack.
- Severity—Indicates the severity of the attack (Critical, Urgent, Warning, Information).
- Channel—The channel on which the alarm occurred.
- Status—The current status of the alarm (Active or Inactive).
- First Seen—The date and time the alarm was first detected.
- Last Seen—The date and time the alarm was last detected.
- AP MAC Address—The MAC address of this access point.
- Target SSID—The Service Set Identifier of the targeted device.
- Alarm Category—The type of alarm.
- MSE Name—The name of the MSE to which this device is associated.

Adaptive wIPS Alarms Report Results

The Adaptive wIPS Alarms report contains the following results (Figure 17-45):

Figure 17-45 Adaptive wIPS Alarms Report


Report Run Result

Adaptive wIPS Alarm

Wireless Control System

Generated: Wed Feb 18 10:58:15 PST 2009

Report By: MSE with Adaptive wIPS service
MSE with Adaptive wIPS Service: All MSEs with Adaptive wIPS Service
Alarm Category: Denial of Service (DOS)
Reporting Period: Last 28 days

Page 1 of 71

Adaptive wIPS Alarm Report

Adaptive wIPS Alarm Report

This report provides a summarized list of Adaptive wIPS alarms present on the Mobility Services Engine(s) in your network. The report is generated using your selected report filter conditions. Please refer to "wIPS Profiles" under the "Configuration" menu for alarm categories and alarm descriptions. It contains detailed information of potential security threats that Cisco has detected in the WLAN environment. Please refer to the threat knowledgebase in WCS for remediation and mitigation techniques for these events. This report includes:
* Name of the alarm
* Name of the device that detected the alarm
* MAC Address of the Attacking Device
* MAC Address of the Attack Target
* Severity (Critical, Urgent, Warning and Information)
* Channel in which the alarm occurred
* The first time the alarm was detected
* The last time the alarm was detected

A closely monitored WLAN system with latest security standards implemented is protected against many common WLAN security threats. Cisco ensures WLAN security by monitoring the WLAN and alerting the wireless administrator of early warning signs of security threats. With the comprehensive suite of security monitoring technologies, Cisco alerts the user on more than 120 different threat conditions.

Severity	Channel	Status
Critical	1	active
Critical	1	active
Critical	1	inactive
Critical	1	inactive

Page 2 of 71

276023

Adaptive wIPS Top 10 Access Points

This report displays the ten access points with the highest number of generated Adaptive wIPS alarms.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - MSE with Adaptive wIPS Service—Select **All MSEs with Adaptive wIPS Service** from the Report Criteria page or click **Edit** to select a specific MSE.
  - Controller by MSE—Select **All MSEs > All Controllers** from the Report Criteria page or click **Edit** to select a specific controller.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Alarm Category—Select **All Types**, **Denial of Service (DoS)**, or **Security Penetration** to determine the types of wIPS alarms to display in the results.

Note See the wIPS Policy Alarm Encyclopedia for more information regarding wIPS alarm types.

- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

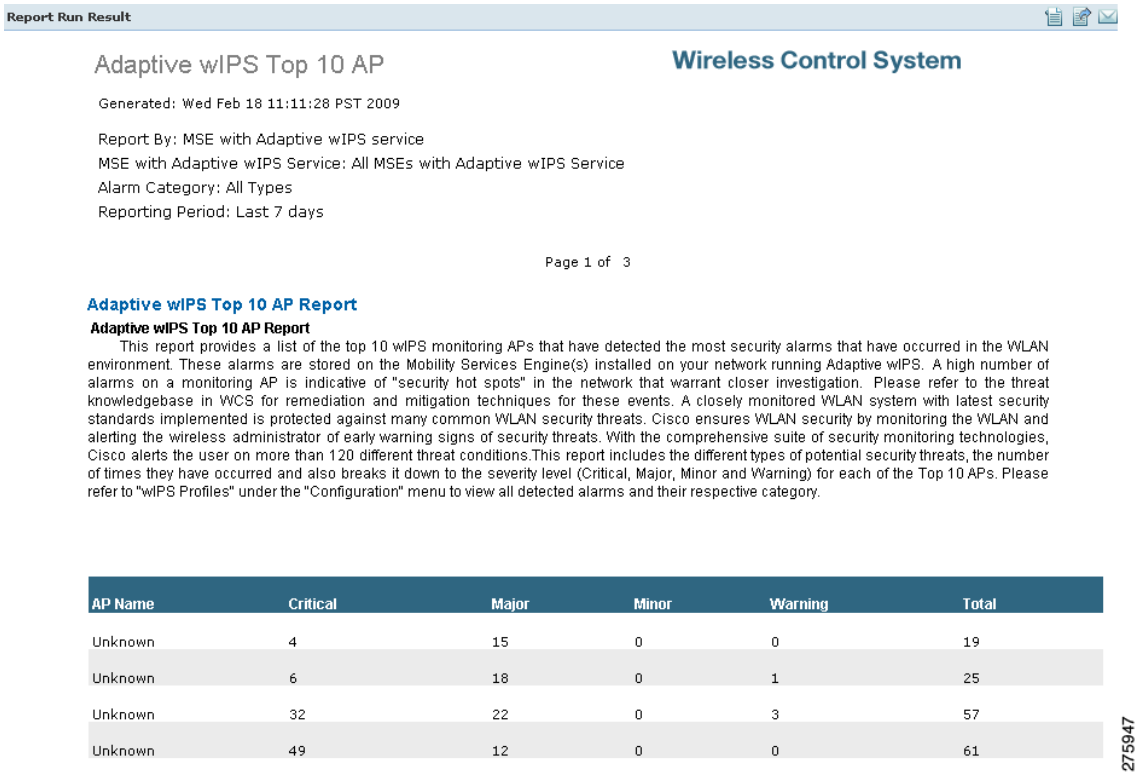
The following information is available for an Adaptive wIPS Top 10 Access Points report:

- AP Name—The name of the access point that generated the alarm.
- Critical—The number of critical alarms for this access point.
- Major—The number of major alarms for this access point.
- Minor—The number of minor alarms for this access point.
- Warning—The number of warning alarms for this access point.
- Total—The number of total alarms for this access point.
- AP MAC Address—The MAC address of this access point.
- MSE Name—The name of the MSE to which this access point is associated.

Adaptive wIPS Top 10 Access Points Report Results

The following is an example of an Adaptive wIPS Top 10 Access Points report (Figure 17-46):

Figure 17-46 Adaptive wIPS Top 10 APs Report


Report Run Result

Adaptive wIPS Top 10 AP

Wireless Control System

Generated: Wed Feb 18 11:11:28 PST 2009

Report By: MSE with Adaptive wIPS service
MSE with Adaptive wIPS Service: All MSEs with Adaptive wIPS Service
Alarm Category: All Types
Reporting Period: Last 7 days

Page 1 of 3

Adaptive wIPS Top 10 AP Report

Adaptive wIPS Top 10 AP Report

This report provides a list of the top 10 wIPS monitoring APs that have detected the most security alarms that have occurred in the WLAN environment. These alarms are stored on the Mobility Services Engine(s) installed on your network running Adaptive wIPS. A high number of alarms on a monitoring AP is indicative of "security hot spots" in the network that warrant closer investigation. Please refer to the threat knowledgebase in WCS for remediation and mitigation techniques for these events. A closely monitored WLAN system with latest security standards implemented is protected against many common WLAN security threats. Cisco ensures WLAN security by monitoring the WLAN and alerting the wireless administrator of early warning signs of security threats. With the comprehensive suite of security monitoring technologies, Cisco alerts the user on more than 120 different threat conditions.This report includes the different types of potential security threats, the number of times they have occurred and also breaks it down to the severity level (Critical, Major, Minor and Warning) for each of the Top 10 APs. Please refer to "wIPS Profiles" under the "Configuration" menu to view all detected alarms and their respective category.

AP Name	Critical	Major	Minor	Warning	Total
Unknown	4	15	0	0	19
Unknown	6	18	0	1	25
Unknown	32	22	0	3	57
Unknown	49	12	0	0	61

275947

Adhoc Rogue Events

This report displays all ad hoc rogue events received by WCS.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.

– From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

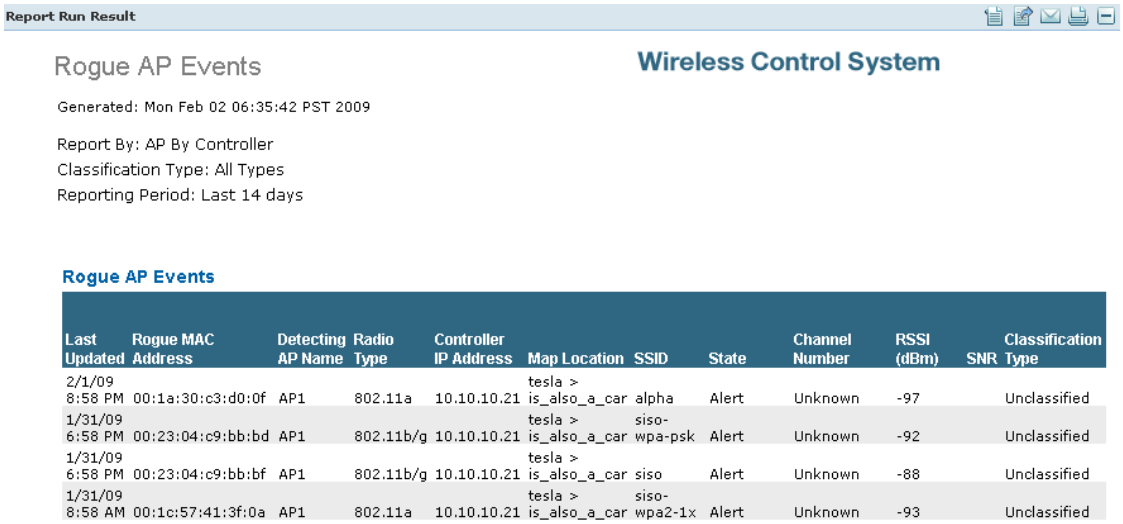
The following information is available for an Adhoc Rogue Events report:

- Last Seen Time—Date and time the ad hoc rogue was last seen.
- Rogue MAC Address—The MAC address of the rogue access point.
- Detecting AP Name—The name of the access point that detected the rogue.
- Radio Type—802.11a or 802.11b/g.
- Controller IP Address—The IP address of the controller on which the ad hoc rogue is located.
- Map Location—The building, floor area, or outdoor area (as applicable) where the ad hoc rogue was detected.
- SSID—The user-defined Service Set Identifier name.
- State—The radio state relative to the network or port. Ad hoc rogue radios appear as "Alert" when first scanned by the port, or as "Pending" when operating system identification is still underway.
- Channel Number—The channel number of the ad hoc rogue.
- RSSI (dBm)—The received signal strength indicator in dBm.

Adhoc Rogue Events Report Results

The Adhoc Rogue Events report contains the following results (Figure 17-47):

Figure 17-47 Adhoc Rogue Events Results



Report Run Result

Rogue AP Events

Wireless Control System

Generated: Mon Feb 02 06:35:42 PST 2009

Report By: AP By Controller
Classification Type: All Types
Reporting Period: Last 14 days

Rogue AP Events

Last Updated	Rogue MAC Address	Detecting AP Name	Radio Type	Controller IP Address	Map Location	SSID	State	Channel Number	RSSI (dBm)	SNR	Classification Type
2/1/09 8:58 PM	00:1a:30:c3:d0:0f	AP1	802.11a	10.10.10.21	tesla > is_also_a_car	alpha	Alert	Unknown	-97		Unclassified
1/31/09 6:58 PM	00:23:04:c9:bb:bd	AP1	802.11b/g	10.10.10.21	tesla > is_also_a_car	siso-wpa-psk	Alert	Unknown	-92		Unclassified
1/31/09 6:58 PM	00:23:04:c9:bb:bf	AP1	802.11b/g	10.10.10.21	tesla > is_also_a_car	siso	Alert	Unknown	-88		Unclassified
1/31/09 8:58 AM	00:1c:57:41:3f:0a	AP1	802.11a	10.10.10.21	tesla > is_also_a_car	siso-wpa2-1x	Alert	Unknown	-93		Unclassified

251896

Adhoc Rogues

WCS gets updates about ad hoc rogues from the controller by using traps or polling. The Last Seen Time is updated anytime a trap for the ad hoc rogue is received or the ad hoc rogue was seen during the last polling cycle of WCS. This report is based on the last seen time of the ad hoc rogue. It includes those rogue access point alarms with clear severity.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

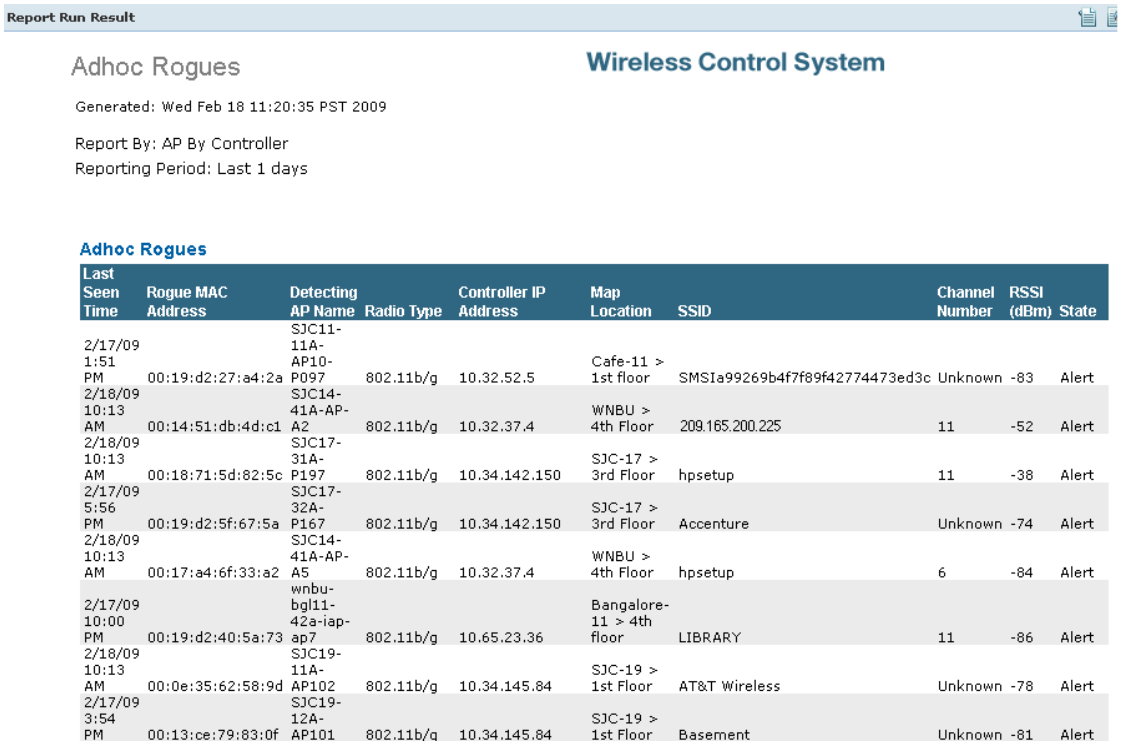
The following information is available for an Adhoc Rogues report:

- Last Seen Time—Date and time the ad hoc rogue was last seen.
- Detecting AP Name—The access point that last detected the rogue, when a rogue is detected by multiple access points on one controller. This last detected access point name comes from the controller that supports maximum RSSI.
- Radio Type—802.11a/n or 802.11b/g/n.
- Controller IP Address—The IP address of the controller on which the ad hoc rogue is located.
- Map Location—The building, floor area, or outdoor area (as applicable) where the ad hoc rogue was detected.
- SSID—The user-defined Service Set Identifier name.
- State—The radio state relative to the network or port. Ad hoc rogue radios appear as "Alert" when first scanned by the port, or as "Pending" when operating system identification is still underway.
- Rogue MAC Address—The MAC address of the ad hoc rogue.
- Channel Number—The channel number of the ad hoc rogue.
- RSSI (dBm)—The maximum received signal strength indicator ever reported by any controller for this rogue.

Adhoc Rogues Report Results

The Adhoc Rogues report contains the following results (Figure 17-48):

Figure 17-48 Adhoc Rogues Results



Report Run Result

Adhoc Rogues

Wireless Control System

Generated: Wed Feb 18 11:20:35 PST 2009

Report By: AP By Controller
Reporting Period: Last 1 days

Adhoc Rogues

Last Seen Time	Rogue MAC Address	Detecting AP Name	Radio Type	Controller IP Address	Map Location	SSID	Channel Number	RSSI (dBm)	State
2/17/09 1:51 PM	00:19:d2:27:a4:2a	SJC11-11A-AP10-P097	802.11b/g	10.32.52.5	Cafe-11 > 1st floor	SMSIa99269b4f7f89f42774473ed3c	Unknown	-83	Alert
2/18/09 10:13 AM	00:14:51:db:4d:c1	SJC14-41A-AP-A2	802.11b/g	10.32.37.4	WNBU > 4th Floor	209.165.200.225	11	-52	Alert
2/18/09 10:13 AM	00:18:71:5d:82:5c	SJC17-31A-P197	802.11b/g	10.34.142.150	SJC-17 > 3rd Floor	hpsetup	11	-38	Alert
2/17/09 5:56 PM	00:19:d2:5f:67:5a	SJC17-32A-P167	802.11b/g	10.34.142.150	SJC-17 > 3rd Floor	Accenture	Unknown	-74	Alert
2/18/09 10:13 AM	00:17:a4:6f:33:a2	SJC14-41A-AP-A5	802.11b/g	10.32.37.4	WNBU > 4th Floor	hpsetup	6	-84	Alert
2/17/09 10:00 PM	00:19:d2:40:5a:73	wnbu-bgl11-42a-iap-ap7	802.11b/g	10.65.23.36	Bangalore-11 > 4th floor	LIBRARY	11	-86	Alert
2/18/09 10:13 AM	00:0e:35:62:58:9d	SJC19-11A-AP102	802.11b/g	10.34.145.84	SJC-19 > 1st Floor	AT&T Wireless	Unknown	-78	Alert
2/17/09 3:54 PM	00:13:ce:79:83:0f	SJC19-12A-AP101	802.11b/g	10.34.145.84	SJC-19 > 1st Floor	Basement	Unknown	-81	Alert

251874

New Rogue Access Points

This report displays all new rogues detected for the first time within a selected timeframe on your network. This report is based on the first seen time of the rogue and is sorted as such. The report includes those rogue access point alarms with clear severity. The value in the Created Time column indicates the time the rogue was first detected.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Classification Type—Select **All Types**, **Malicious**, **Friendly**, or **Unclassified** to determine the type of rogue access point to display in the report results.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

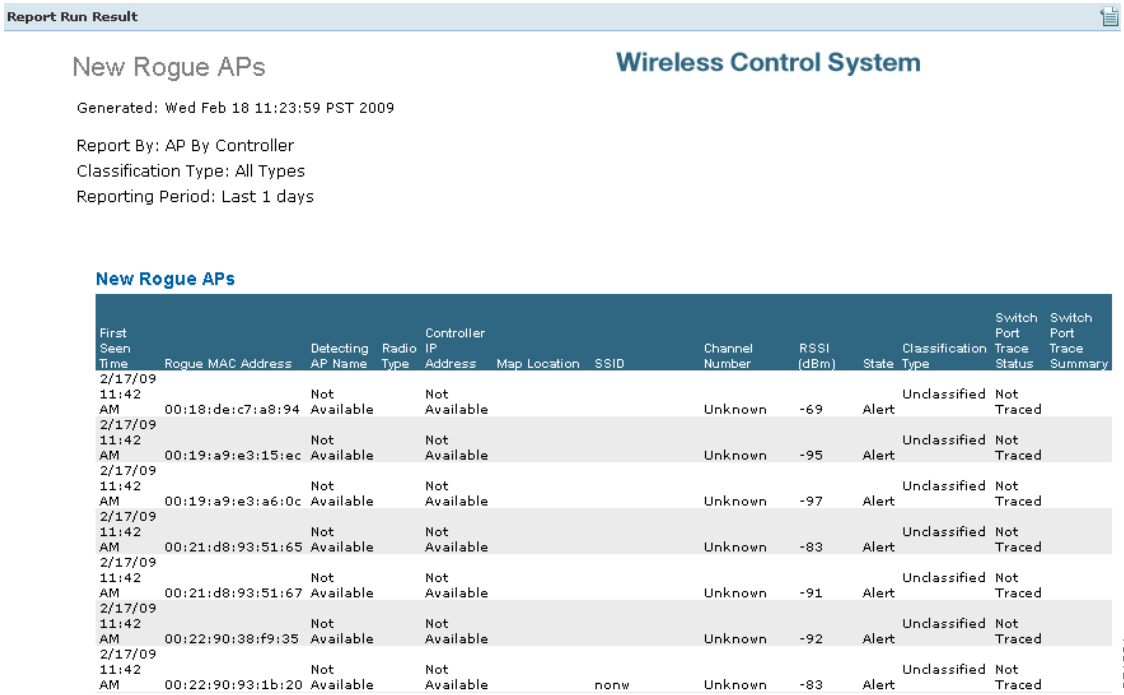
The following information is available for a New Rogue Access Points report:

- First Seen Time—The date and time the rogue access point was first seen.
- Rogue MAC Address—The MAC address of the rogue access point.
- Detecting AP Name—The access point that last detected the rogue, when a rogue is detected by multiple access points on one controller. This last detected access point name comes from the controller that supports maximum RSSI.
- Radio Type—802.11a/n or 802.11b/g/n.
- Controller IP Address—The IP address of the controller on which the rogue access point is located.
- Map Location—The building, floor area, or outdoor area (as applicable) where the rogue access point was detected.
- SSID—The user-defined Service Set Identifier name.
- State—The radio state 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.
- Channel Number—The channel number of the rogue access point.
- RSSI (dBm)—The received signal strength indicator in dBm.
- Classification Type—The type of rogue access point (malicious, friendly, or unclassified).
- Switch Port Trace Status—Indicates whether or not the switch port was traced.
- Switch Port Trace Summary—Provides a summary of the switch port trace or remains blank if no switch port was traced.

New Rogue APs Report Results

The New Rogue Access Points report contains the following results (Figure 17-49):

Figure 17-49 New Rogue Access Points Report



Report Run Result

New Rogue APs

Wireless Control System

Generated: Wed Feb 18 11:23:59 PST 2009

Report By: AP By Controller
Classification Type: All Types
Reporting Period: Last 1 days

New Rogue APs

First Seen Time	Rogue MAC Address	Detecting AP Name	Radio Type	Controller IP Address	Map Location	SSID	Channel Number	RSSI (dBm)	State	Classification Type	Switch Port Trace Status	Switch Port Trace Summary
2/17/09 11:42 AM	00:18:de:c7:a8:94	Not Available		Not Available			Unknown	-69	Alert	Unclassified	Not Traced	
2/17/09 11:42 AM	00:19:a9:e3:15:ec	Not Available		Not Available			Unknown	-95	Alert	Unclassified	Not Traced	
2/17/09 11:42 AM	00:19:a9:e3:a6:0c	Not Available		Not Available			Unknown	-97	Alert	Unclassified	Not Traced	
2/17/09 11:42 AM	00:21:d8:93:51:65	Not Available		Not Available			Unknown	-83	Alert	Unclassified	Not Traced	
2/17/09 11:42 AM	00:21:d8:93:51:67	Not Available		Not Available			Unknown	-91	Alert	Unclassified	Not Traced	
2/17/09 11:42 AM	00:22:90:38:f9:35	Not Available		Not Available			Unknown	-92	Alert	Unclassified	Not Traced	
2/17/09 11:42 AM	00:22:90:93:1b:20	Not Available		Not Available		nonw	Unknown	-83	Alert	Unclassified	Not Traced	

251891

New Rogue Access Point Count

This report provides a graphical display of the count of new rogue access points detected for the first time within the specified time interval. The report includes those rogue access point alarms with clear severity.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Classification Type—Select **All Types**, **Malicious**, **Friendly**, or **Unclassified** to determine the type of rogue access point to display in the report results.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

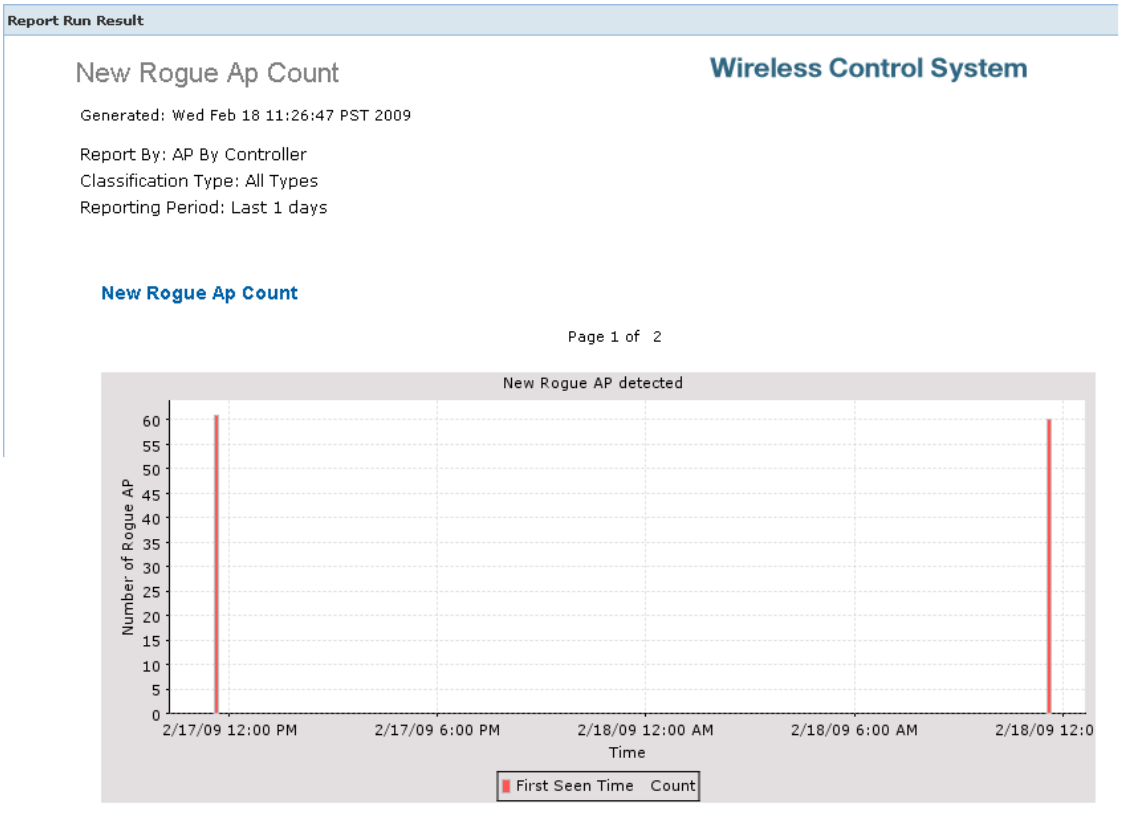
Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

New Rogue Access Point Count Report Results

The New Rogue Access Point Count report contains the following results (Figure 17-50):

Figure 17-50 New Rogue Access Point Count Report



Rogue Access Points Events

This report displays all rogue access point events received by WCS based on the event time of the rogue access points. Any rogue-related trap received by WCS is logged as a rogue event in WCS. A new rogue access point event is created by WCS based on polled data when there is a newly detected rogue access point. In addition, an event is also created by WCS when the user changes the state and classification of the rogue access point through the WCS user interface. One rogue can have multiple events. This report is sorted based on the timestamp of the event.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Classification Type—Select **All Types**, **Malicious**, **Friendly**, or **Unclassified** to determine the type of rogue access point to display in the report results.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

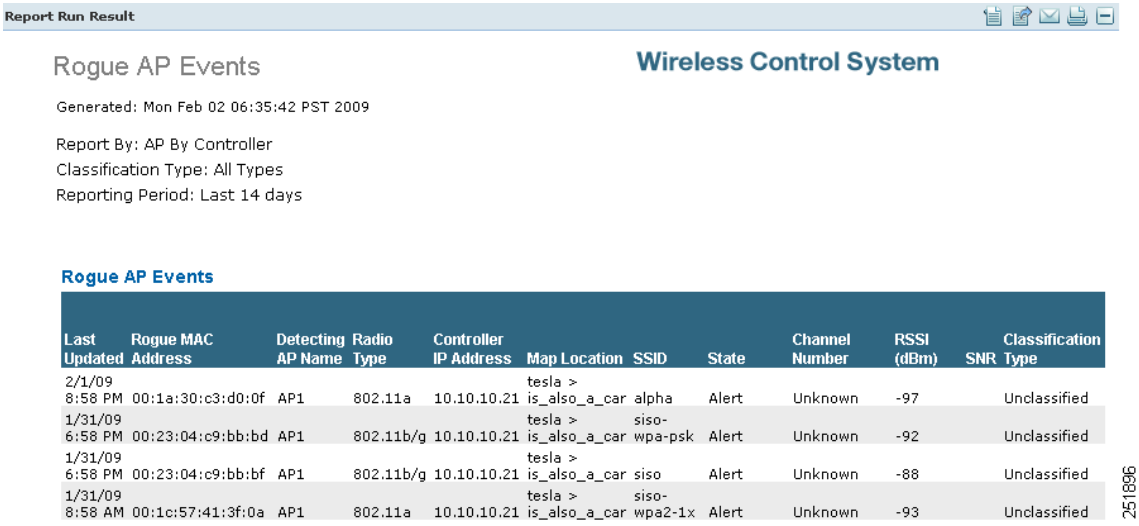
The following information is available for a Rogue Access Point Events report:

- Last Seen Time—The date and time the rogue access point was last detected.
- Rogue MAC Address—The MAC address of the rogue access point.
- Detecting AP Name—The access point that last detected the rogue, when a rogue is detected by multiple access points on one controller. This last detected access point name comes from the controller which supports maximum RSSI.
- Radio Type—802.11a/n or 802.11b/g/n.
- Controller IP Address—The IP address of the controller on which the rogue is located.
- Map Location—The building, floor area, or outdoor area (as applicable) where the rogue access point was detected.
- SSID—The user-defined Service Set Identifier name.
- State—The radio state 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.
- Channel Number—The channel number of the rogue access point.
- RSSI (dBm)—The maximum received signal strength indicator ever reported by any controller for this rogue.
- SNR—The Signal-to-Noise Ratio.
- Classification Type—The type of rogue access point (malicious, friendly, or unclassified).

Rogue AP Events Report Results

The Rogue Access Point Events report contains the following results (Figure 17-51):

Figure 17-51 Rogue Access Point Events Report


Report Run Result

Rogue AP Events

Wireless Control System

Generated: Mon Feb 02 06:35:42 PST 2009

Report By: AP By Controller
Classification Type: All Types
Reporting Period: Last 14 days

Rogue AP Events

Last Updated	Rogue MAC Address	Detecting AP Name	Radio Type	Controller IP Address	Map Location	SSID	State	Channel Number	RSSI (dBm)	SNR	Classification Type
2/1/09 8:58 PM	00:1a:30:c3:d0:0f	AP1	802.11a	10.10.10.21	tesla > is_also_a_car	alpha	Alert	Unknown	-97		Unclassified
1/31/09 6:58 PM	00:23:04:c9:bb:bd	AP1	802.11b/g	10.10.10.21	tesla > is_also_a_car	siso-wpa-psk	Alert	Unknown	-92		Unclassified
1/31/09 6:58 PM	00:23:04:c9:bb:bf	AP1	802.11b/g	10.10.10.21	tesla > is_also_a_car	siso	Alert	Unknown	-88		Unclassified
1/31/09 8:58 AM	00:1c:57:41:3f:0a	AP1	802.11a	10.10.10.21	tesla > is_also_a_car	siso-wpa2-1x	Alert	Unknown	-93		Unclassified

251896

Rogue Access Points

WCS gets updates about rogues from controllers using traps or polling. The last seen time is updated whenever a trap for the rogue is received or rogue was detected during the last polling cycle of WCS. This report is based on the last seen time of the rogue access point. It includes those rogue access point alarms with clear severity.

This report contains the following settings and scheduling parameters:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Report by
  - AP by Controller—Select **All Controllers > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Floor Area—Select **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.
  - AP by Outdoor Area—Select **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page or click **Edit** to select a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Classification Type—Select **All Types**, **Malicious**, **Friendly**, or **Unclassified** to determine the type of rogue access point to display in the report results.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

The following information is available for a Rogue APs report:

- Last Seen Time—The date and time the rogue access point was last detected.
- Rogue MAC Address—The MAC address of the rogue access point.
- Detecting AP Name—The access point that last detected the rogue, when a rogue is detected by multiple access points on one controller. This last detected access point name comes from the controller which supports maximum RSSI.
- Radio Type—802.11a or 802.11b/g.
- Controller IP Address—The IP address of the controller on which the rogue is located.
- Map Location—The building, floor area, or outdoor area (as applicable) where the rogue access point is located.
- SSID—The user-defined Service Set Identifier name.
- State—The radio state 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.
- Channel Number—The channel number of the rogue access point.
- RSSI (dBm)—The maximum received signal strength indicator ever reported by any controller for this rogue.
- Classification Type—The type of rogue access point (malicious, friendly, or unclassified).
- Switch Port Trace Status—Indicates whether or not the switch port was traced.
- Switch Port Trace Summary—Provides a summary of the switch port trace or remains blank if no switch port was traced.

Rogue APs Report Results

The Rogue Access Points report contains the following results (Figure 17-52):

Figure 17-52 Rogues APs Report

Report Run Result

Rogue APs

Wireless Control System

Generated: Mon Feb 02 06:46:45 PST 2009

Report By: AP By Controller
Classification Type: All Types
Reporting Period: Last 14 days

Rogue APs

Last Updated	Rogue MAC Address	Detecting AP Name	Radio Type	Controller IP Address	Map Location	SSID	State	Channel Number	RSSI (dBm)	Classification Type	Switch Port Trace Status	Switch Port Trace Sum
2/2/09 4:58 AM	00:23:33:2b:6f:ea	AP1	802.11b/g	10.10.10.21	tesla > is_also_a_car	siso-wpa2-1x	Alert	Unknown	-98	Unclassified	Not Traced	
2/2/09 4:58 AM	00:23:33:2c:47:6e	AP1	802.11a	10.10.10.21	tesla > is_also_a_car	siso-wep	Alert	Unknown	-94	Unclassified	Not Traced	
2/2/09 4:58 AM	00:23:33:2c:47:6f	AP1	802.11b/g	10.10.10.21	tesla > is_also_a_car	siso	Alert	Unknown	-94	Unclassified	Not Traced	
2/2/09 4:58 AM	00:23:33:2c:4b:aa	AP1	802.11b/g	10.10.10.21	tesla > is_also_a_car	siso-wpa2-1x	Alert	Unknown	-96	Unclassified	Not Traced	

251897

Security Summary

This report displays the number of association failures, rogue access points, ad hocs, and access point connections or disconnections over one month.

The following settings and scheduling parameters are available for this report:

Settings

- Report Title—If you plan to used this as a saved report, enter a report name.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Select the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 17-2 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 17-2 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to Available Columns.

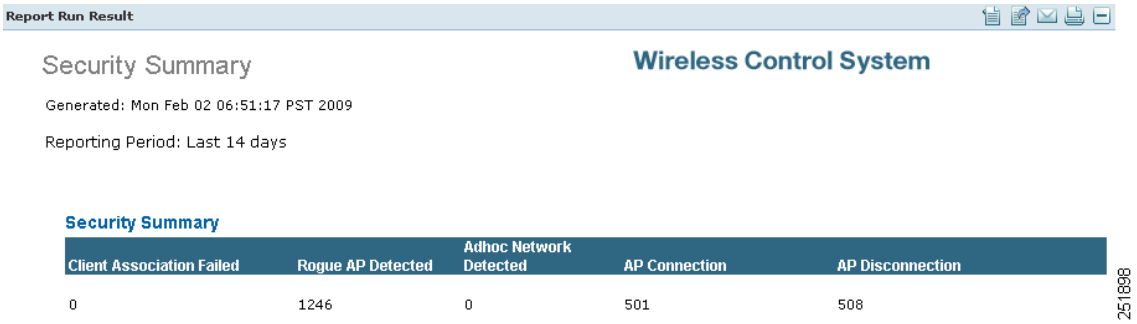
The following information is available for a Security Summary report:

- Client Association Failed—The number of client association failures during the specified period of time.
- Rogue AP Detected—The number of rogue access points detected during the specified period of time.
- Adhoc Network Detected—The number of ad hoc networks detected during the specified period of time.
- AP Connection—The number of access point connections during the specified period of time.
- AP Disconnection—The number of access point disconnections during the specified period of time.

Security Summary Report Results

The Security Summary report contains the following results (Figure 17-53):

Figure 17-53 Security Summary Report



CHAPTER 18

Administrative Tasks

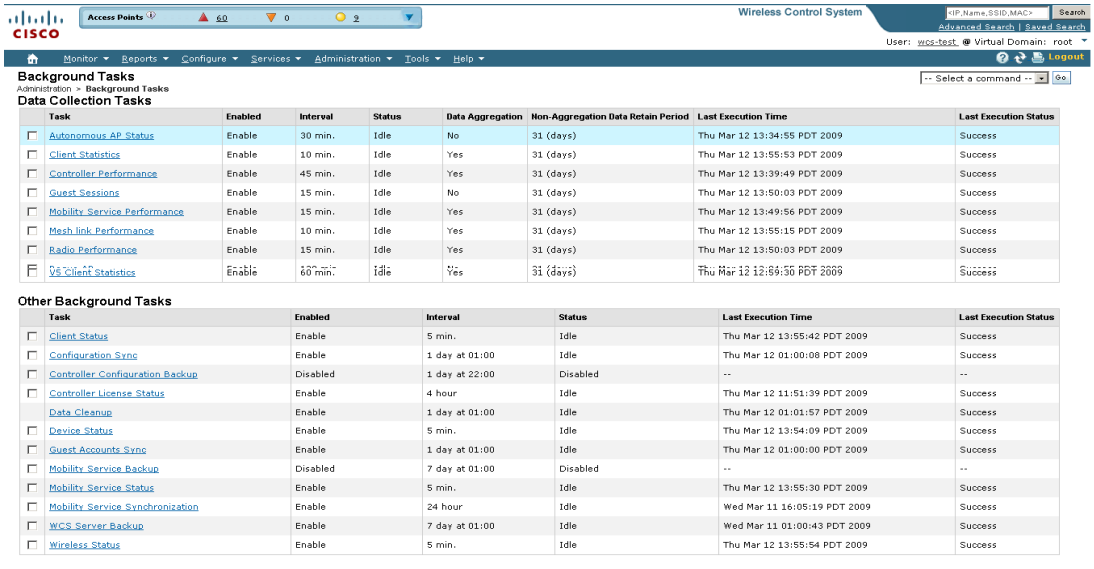
This chapter describes administrative tasks to perform with Cisco WCS. It contains the following sections:

- Running Background Tasks, page 18-1
- Performing a Task, page 18-2
- Importing Tasks Into ACS, page 18-8
- Setting AAA Mode, page 18-18
- Auto Provisioning, page 18-19
- Turning Password Rules On or Off, page 18-29
- Configuring TACACS+ Servers, page 18-29
- Configuring RADIUS Servers, page 18-31
- Establishing Logging Options, page 18-32
- Performing Data Management Tasks, page 18-34
- High Availability, page 18-62
- Setting User Preferences, page 18-66
- Accessing the License Center, page 18-67
- Configuring ACS 5.x, page 18-76

Running Background Tasks

Choose **Administration > Background Tasks** to view several scheduled tasks. The Background Tasks page appears (see Figure 18-1).

Figure 18-1 Background Tasks Page



You can view the administrative and operating status, task interval, and time of day in which the task occurs. To execute a particular task, click the check box of the desired task and choose **Execute Now** from the Select a command drop-down list. The task executes based on what you have configured for the specific task.

Performing a Task

Follow these steps to perform a task (such as scheduling an automatic backup of the WCS database). Data collection tasks are data-set tasks that collect and organize information that may be useful for creating reports.

Note All tasks related to collecting data or any other background task would be handled in a similar manner.

Step 1 Choose **Administration > Background Tasks** to display the Background Tasks page (see Figure 18-1). This page displays the following information:

- Enabled—Whether the tasks have been enabled or disabled.
- Interval—Indicates the time period (in minutes) between task executions. You can set the interval from the task's data collection configuration page.
- Status—The present state of the task.
- Data Aggregation (Data Collection Tasks only)—If set to Yes, the data set combines data.
- Non-Aggregation Data Retain Period (Days) (Data Collection Tasks only)—The number of days that the non-aggregated data is retained. You can set the retention period from the task's data collection configuration page.
- Last Execution Time—The time and date when the task was last run.
- Last Execution Status—The status after the last task was run.

Step 2 On this page, perform one of the following:

- Execute the task now.

  Click the check box of the task you want to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**.

- Enable the task.

  Click the check box of the task you want to enable. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task changes from unavailable to active after enabling is complete.

- Disable the task.

  Click the check box of the task you want to disable. From the Select a command drop-down list, choose **Disable Task, and click Go**. The task is grayed out after the disabling is complete.

- View details of a task.

  Click a URL in the Data Collection Tasks or Other Background Tasks column to view a specific task. The details on that task appear. Data collections are data-set tasks that collect and organize a specific type of information useful for creating reports.

To go to a data set's configuration page, click the name of the data set in the Data Collection page. Each data set configuration page displays a table of the data set's executions. The table has following columns:

- Executed task information including:
  - Last Execution Start Time—Indicates the date and time that the data-set task began running.
  - End Time—Indicates the date and time that the data-set task stopped running.
  - Elapsed Time (secs)—Indicates the amount of time (in seconds) it took to complete the task.
  - Result—Indicates the success or failure of the task.
  - Additional Information—Provides any additional information regarding a specific task.

Each data set configuration page contains the following parameters and information under Collection Set Details:

- Description—Provides a brief read-only description of the data set.
- Data Aggregation—Indicates whether or not data collected by the data set is aggregated.
- Used By Report(s)—Displays names of the reports that use the data set.
  - CleanAir Air Quality—This data set is used for Worst Air Quality APs and Air Quality versus Time reports.
  - Interferers—This data set us used for Worst Interferers reports.
- Collection Status—Select the **Enabled** check box to enable data collection.
- Interval (min.)—Enter the time (in minutes) for the data set execution interval.

Each data set configuration page contains the following parameters under Data Management:

- Non-Aggregation Data Retain Period (Days)—Enter the number of days to retain non-aggregated data collected by the data set.
- Retain Aggregation Raw Data—Select the **Enable** check box to enable the retention of aggregated raw data.

Note The Aggregation Raw Data Retain Period setting is for polled raw data. To configure the retention period for aggregated trend data, go to **Administration > Settings**, then click **Data Management** from the left sidebar.

Note See "WCS Historical Data" section on page 18-7 for more information on aggregated and non-aggregated data.

Note For this example, performing a WCS server backup was selected as the task. The screens and fields to enter on the detailed screens vary based on the task you choose.

Step 3 Select the **Enabled** check box to enable it.

Step 4 Select the **Report History Backup** check box.

Step 5 In the Max Backups to Keep text box, enter the maximum number of backup files to save on the server.

Range: 7 to 50

Default: 7

Note To prevent the WCS platform from running out of disk space, the server automatically deletes old backup files when the number of files exceeds the value entered for this text box.

Step 6 In the Interval (Days) text box, enter 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 7 In the Time of Day text box, enter the back-up start time. It must be in this format: *hh*:*mm AM/PM* (for example: 03:00 AM). If no AM/PM notation is designated, the entered hour is always AM. If you want to specify 5PM, you could enter 17:00 or 5:00 PM. When the page is revisited after saving, the time is display as hh:mm (in this case 17:00), without the PM designation.

Note Backing up a large database affects the performance of the WCS server. Therefore, Cisco recommends that you schedule backups to run when the WCS server is idle (such as, in the middle of the night).

Step 8 Click **Submit** to save your settings. The backup file is saved as a .zip file in the *ftp-install-dir*/ftp-server/root/WCSBackup directory using this format: *dd-mmm-yy_ hh-mm-ss*.zip (for example, 11-Nov-05_10-30-00.zip).

Configuration Sync

Configuration sync is a new task added in software release 5.1. It allows you to poll all configuration data from the controllers. Any audit (such as a network audit, security index calculation, or RRM audit) performed on the polled and database data is secondary to the configuration sync and can only be performed if this configuration sync task is enabled.

Each of the audits can be enabled separately and run independently of the other audits. If a particular audit requires an immediate run, it can be enabled when the Configuration Sync task is run.

Note If you plan to run the configuration sync task daily, you should enable all audits.

Follow these steps to perform a configuration sync.

Step 1 Choose **Administration > Background Tasks** to display the Background Tasks page (see Figure 18-1).

Step 2 On this page, perform one of the following:

- Execute the task now.

  Click the **Configuration Sync** 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.

  Click the **Configuration Sync** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from grayed out to active in the Enabled column.

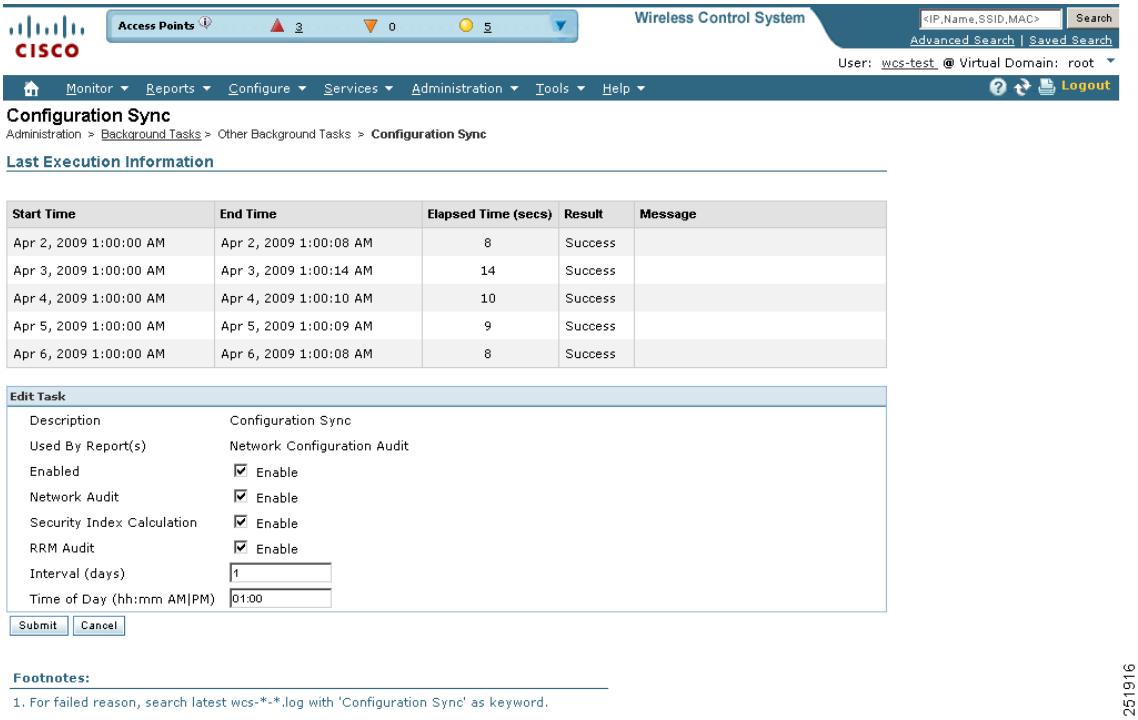
  <OR>

- Disable the task.

  Click the **Configuration Sync** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task is grayed out in the Enabled column after the disabling is complete.

Step 3 To modify the task, click the **Configuration Sync** link in the Background Tasks column. The Task > Configuration Sync page appears (see Figure 18-2).

Figure 18-2 Task > Configuration Sync



Step 4 In this page you can set the interval and time of day for the task and enable the secondary network audit, security index calculation, and RRM audits tasks.

Step 5 Click **Submit**.

Controller License Status

Controller license status is available from release 6.0 or later. It resets the controller license file state so that WCS shows correct information.

Follow these steps to update the controller license status.

Step 1 Choose **Administration > Background Tasks** to display the Background Tasks page (see Figure 18-1).

Step 2 On this page, perform one of the following:

- Execute the task now.

  Click the **Controller License 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.

  Click the **Controller License Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from grayed out to active in the Enabled column.

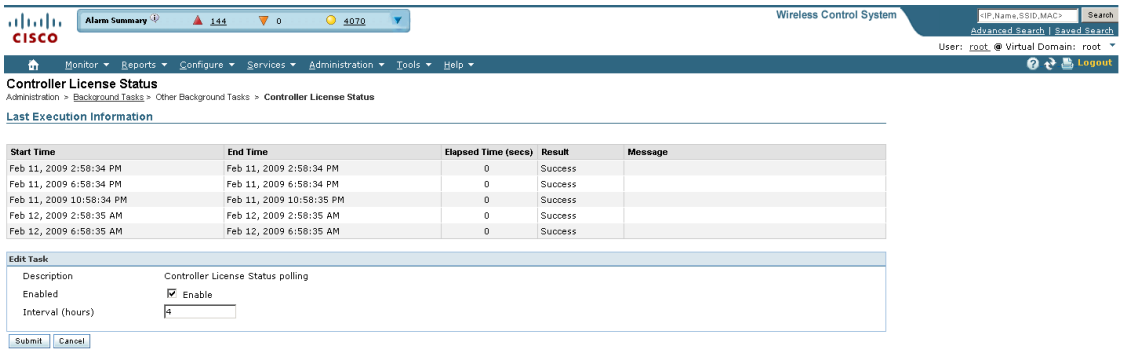
  <OR>

- Disable the task.

  Click the **Controller License Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task converts from grayed out to active in the Enabled column after the disabling is complete.

Step 3 To modify the controller license reset task, click the **Controller License Status** link in the Background Tasks column. The Controller License Status page appears (see Figure 18-3).

Figure 18-3 Controller License Status Page



251925

This page shows when the latest license resynchronizations occurred. By default, it runs every 4 hours. From this page, you can disable this task or change the interval.

WCS Historical Data

There are two types of historical data in WCS, including:

- Aggregated historical data—Numeric data that can be gathered as a whole and aggregated to minimum, maximum, or average. Client count is one example of aggregated historical data.

  Use the Administration > Settings > Data Management page to define the aggregated data retention period. Aggregation types include hourly, daily, and weekly.

  The retention period for these aggregation types are defined as Default, Minimum, and Maximum (see Table 18-1).

Table 18-1 Aggregated Data Retention Periods

Aggregated Data	Default	Minimum	Maximum
Hourly	31 days	1 day	31 days

Table 18-1 Aggregated Data Retention Periods

Aggregated Data	Default	Minimum	Maximum
Daily	90 days	7 days	365 days
Weekly	54 weeks	2 weeks	108 weeks

- Non-aggregated historical data—Numeric data that cannot be gathered as a whole (or aggregated). Client association history is one example of non-aggregated historical data.

  You can define a non-aggregated retention period in each data collection task and other settings.

  For example, you define the retention period for client association history in Administration > Settings > Client. By default, the retention period is 31 days or 1 million records. This retention period can be increased to 365 days.

Importing Tasks Into ACS

To import tasks into Cisco Secure ACS server, you must add WCS to an ACS server (or non-Cisco ACS server).

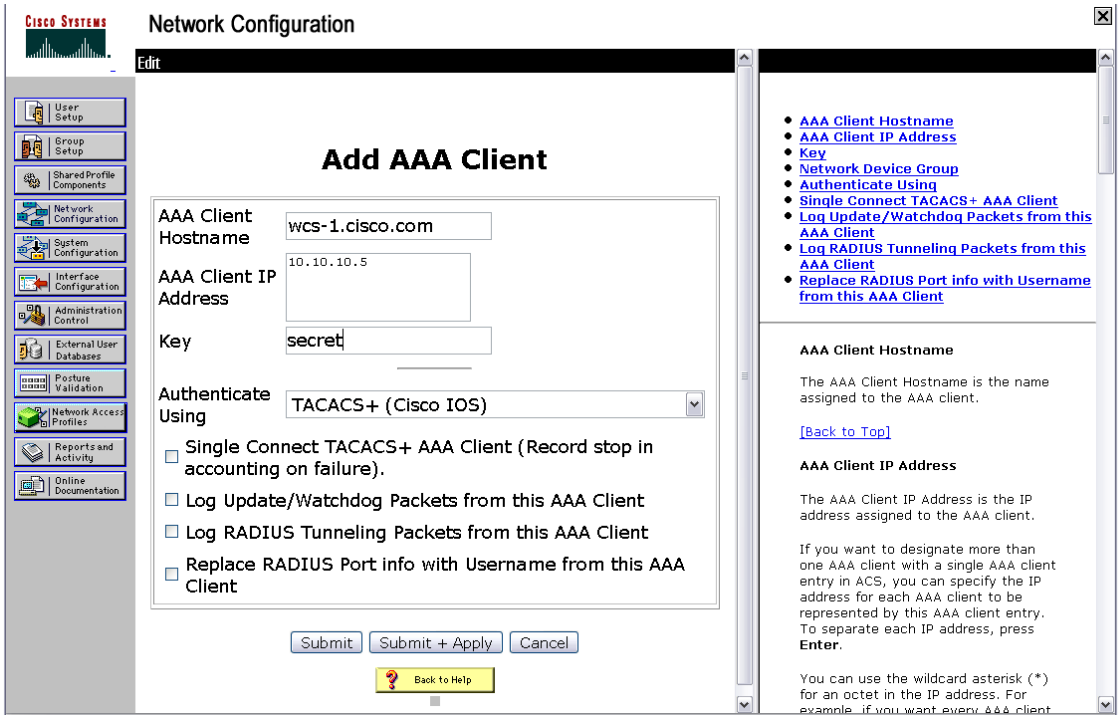
Adding WCS to an ACS Server

Follow these steps to add WCS to an ACS server.

Note The instructions and illustrations in this section pertain to ACS version 4.1 and may vary slightly for other versions or other vendor types. See the CiscoSecure ACS documentation or the documentation for the vendor you are using.

Step 1 Click **Add Entry** on the Network Configuration page of the ACS server (see Figure 18-4).

Figure 18-4 ACS Server Network Configuration Page



Step 2 In the AAA Client Hostname text box, enter the WCS hostname.

Step 3 Enter the WCS IP address into the AAA Client IP Address text box.

Step 4 In the Key text box, enter the shared secret that you wish to configure on both the WCS and ACS servers.

Step 5 Choose **TACACS+** in the Authenticate Using drop-down list.

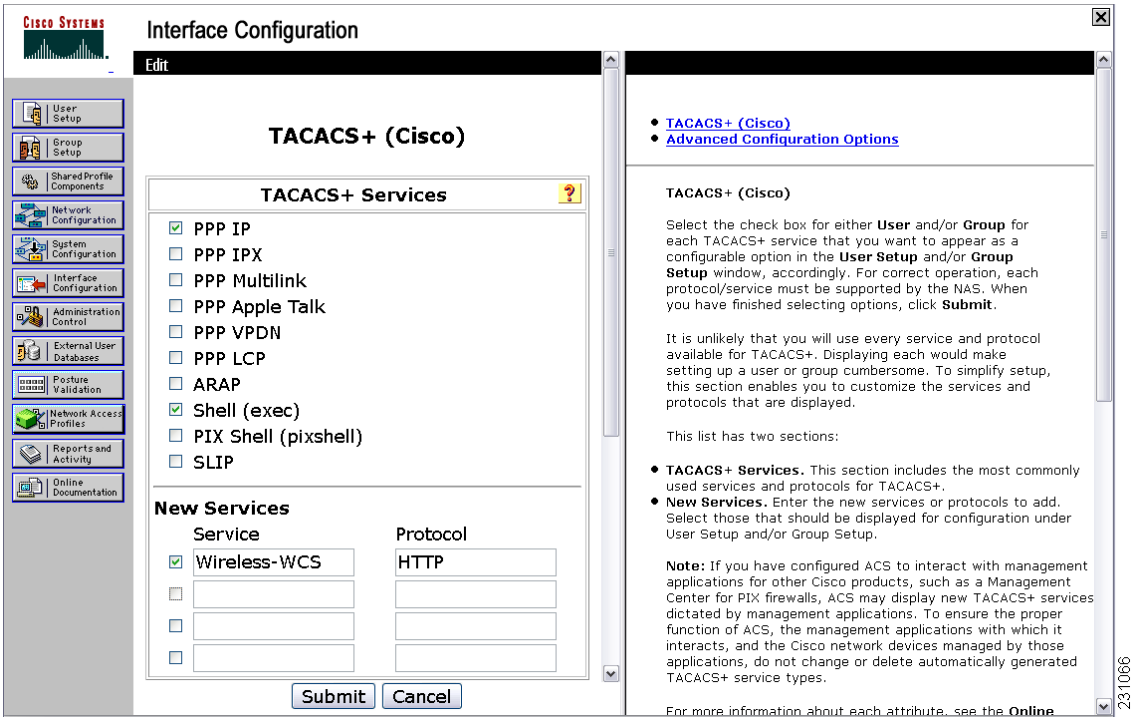
Step 6 Click **Submit + Apply**.

Adding WCS as a TACACS+ Server

Follow these steps to add WCS to a TACACS+ server.

Step 1 Go to the TACACS+ (Cisco IOS) Interface Configuration page (see Figure 18-5).

Figure 18-5 TACACS+ Cisco IOS Interface Configuration Page



Step 2 In the New Services portion of the page, add Wireless-WCS in the Service column heading.

Step 3 Enter HTTP in the Protocol column heading.

Note HTTP must be in uppercase.

Step 4 Click the check box in front of these entries to enable the new service and protocol.

Step 5 Click **Submit**.

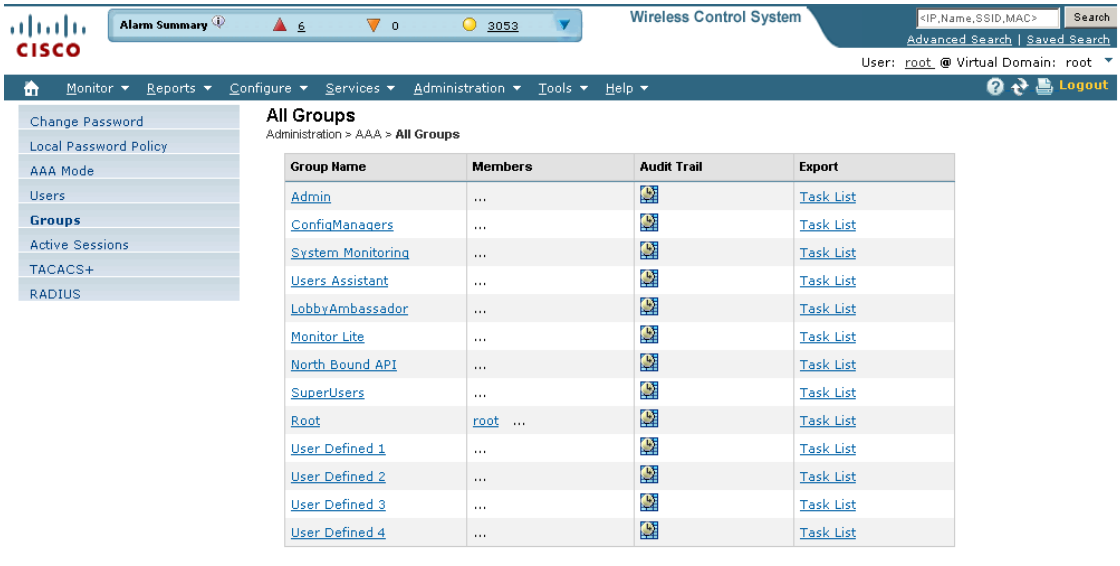
Adding WCS UserGroups into ACS for TACACS+

Follow these steps to add WCS UserGroups into an ACS Server for use with TACACS+ servers.

Step 1 Log into WCS.

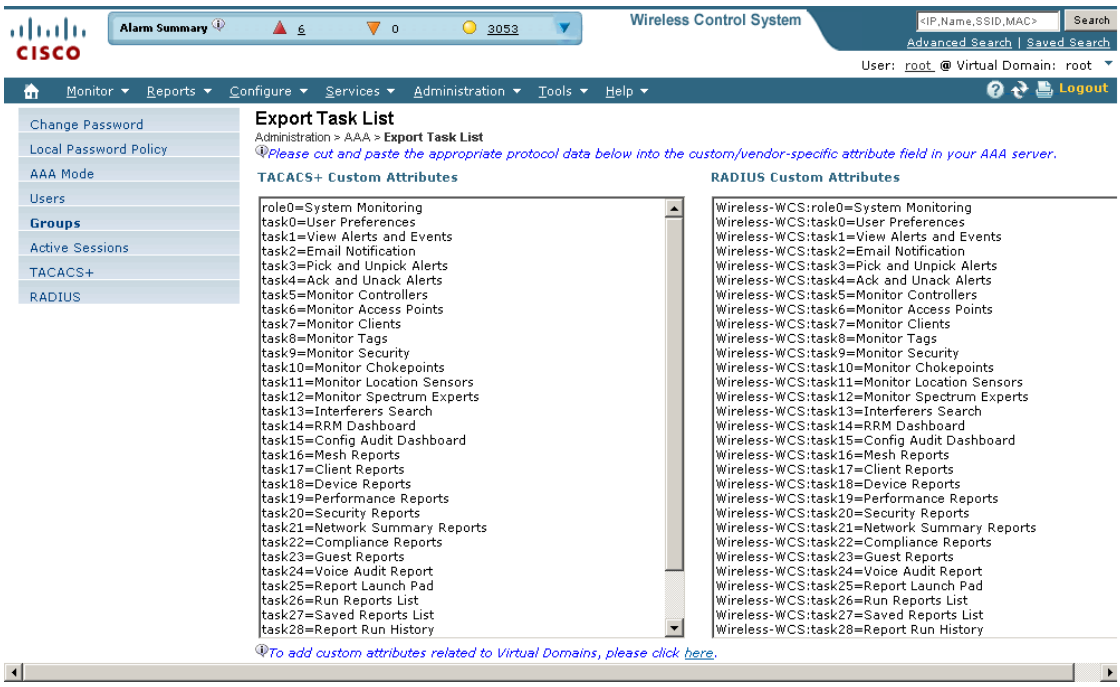
Step 2 Choose Administration > AAA > Groups. The All Groups page appears (see Figure 18-6).

Figure 18-6 All Groups Page



Step 3 Click the Task List URL (the Export right-most column) of the User Group that you wish to add to ACS. The Export Task List page appears (see Figure 18-7).

Figure 18-7 Export Task List Page

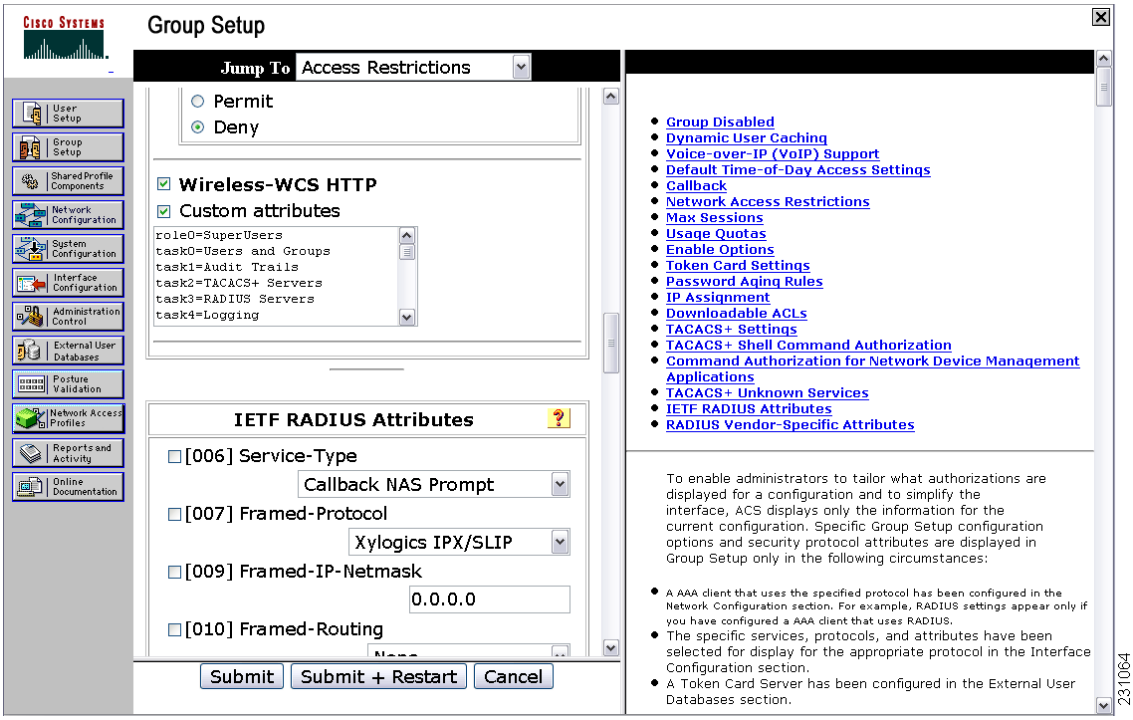


Step 4 Highlight the text inside of the TACACS+ Custom Attributes, go to your browser's menu, and choose **Edit > Copy**.

Step 5 Log in to ACS.

Step 6 Go to Group Setup. The Group Setup page appears (see Figure 18-8).

Figure 18-8 Group Setup Page on ACS Server



Step 7 Choose which group to use and click **Edit Settings**. Wireless-WCS HTTP appears in the TACACS+ setting.

Step 8 Use your browser's Edit > Paste sequence to place the TACACS+ custom attributes from WCS into this text box.

Note When you upgrade WCS, any permissions on the TACACS+ or RADIUS server must be re-added.

Step 9 Click the check boxes to enable these attributes.

Step 10 Click **Submit + Restart**.

You can now associate ACS users with this ACS group.

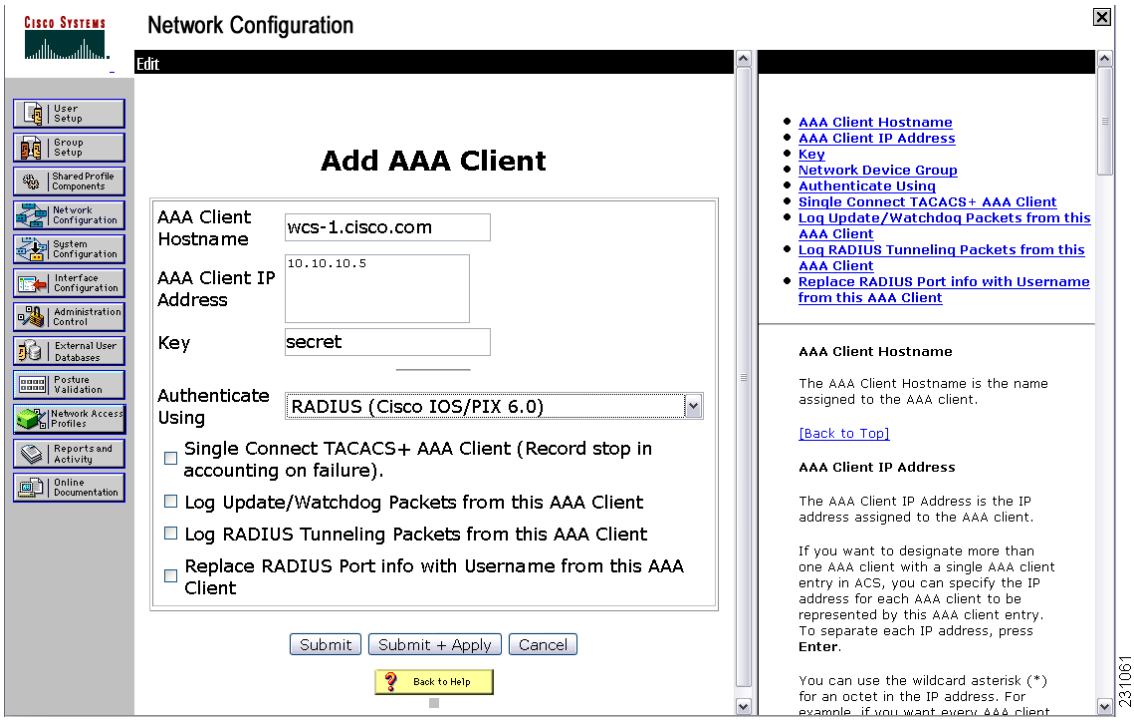
Note To enable TACACS+ in WCS, refer to the "Configuring TACACS+ Servers" section on page 18-29. For information on configuring ACS view server credentials, refer to the "Configuring ACS View Server Credentials" section on page 6-2. For information on adding WCS Virtual Domains into ACS for TACACS+, refer to the "Virtual Domain RADIUS and TACACS+ Attributes" section on page 20-9.

Adding WCS to ACS server for Use with RADIUS

Follow these steps to add WCS to an ACS server for use with RADIUS servers. If you have a non-Cisco ACS server, refer to the "Adding WCS to a Non-Cisco ACS Server for Use with RADIUS" section on page 18-17.

Step 1 Go to Network Configuration on the ACS server (see Figure 18-9).

Figure 18-9 Network Configuration Page on ACS Server



Step 2 Click **Add Entry**.

Step 3 In the AAA Client Hostname text box, enter the WCS hostname.

Step 4 In the AAA Client IP Address text box, enter the WCS IP address.

Step 5 In the Key text box, enter the shared secret that you wish to configure on both the WCS and ACS servers.

Step 6 Choose **RADIUS (Cisco IOS/PIX 6.0)** from the Authenticate Using drop-down list.

Step 7 Click **Submit + Apply**.

You can now associate ACS users with this ACS group.

Note To enable RADIUS in WCS, refer to the "Configuring RADIUS Servers" section on page 18-31. For information on configuring ACS view server credentials, refer to the "Configuring ACS View Server Credentials" section on page 6-2.

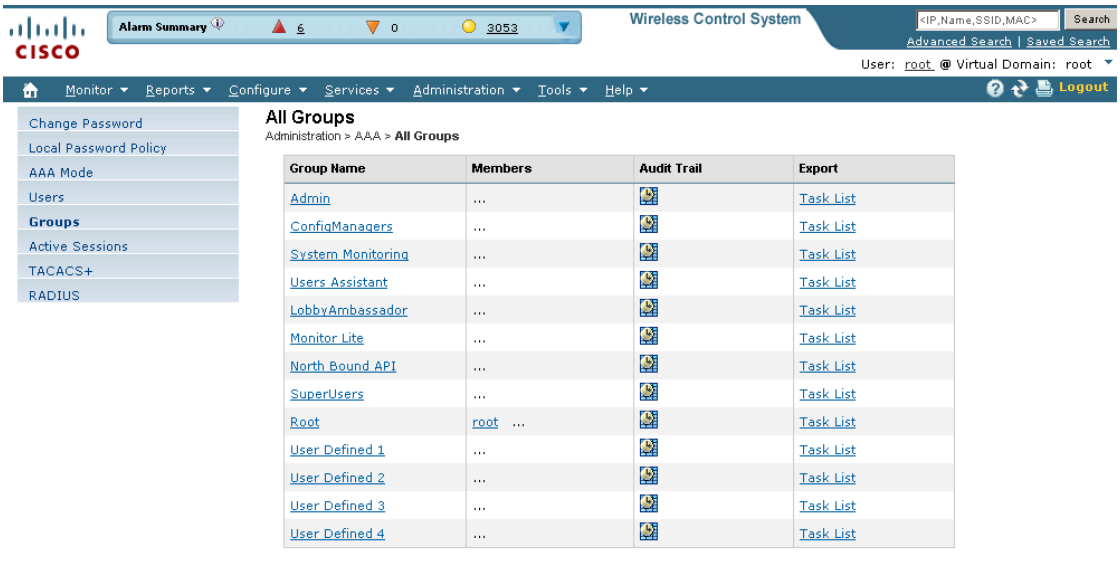
Adding WCS UserGroups into ACS for RADIUS

Follow these steps to add WCS UserGroups into an ACS Server for use with RADIUS servers.

Step 1 Log into WCS.

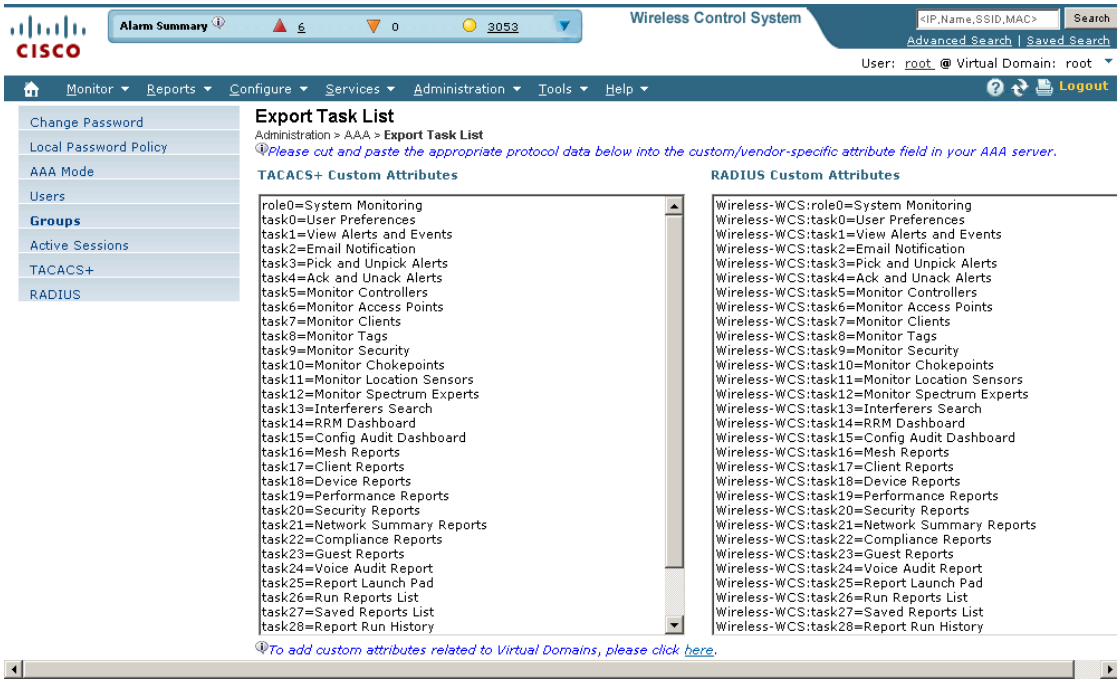
Step 2 Choose Administration > AAA > Groups. The All Groups page appears (see Figure 18-10).

Figure 18-10 All Groups Page



Step 3 Click the Task List URL (the Export right-most column) of the User Group that you wish to add to ACS. The Export Task List page appears (see Figure 18-11).

Figure 18-11 Export Task List Page



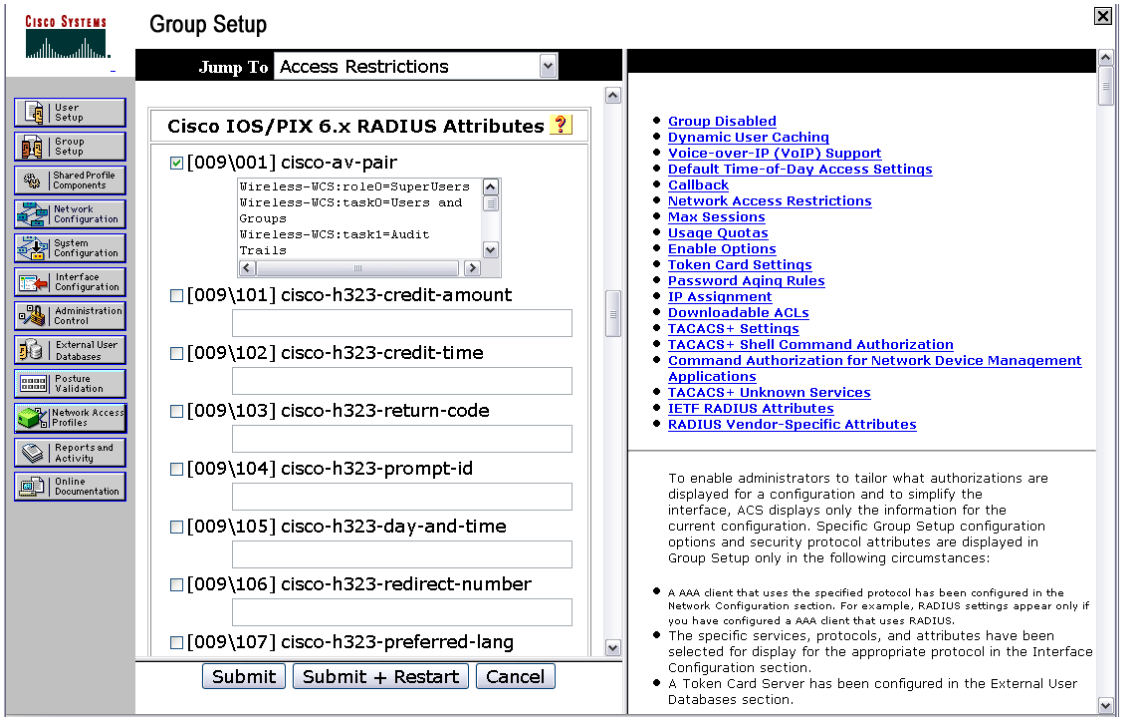
Step 4 Highlight the text inside of the RADIUS Custom Attributes, go to your browser's menu, and choose **Edit > Copy**.

Note When you upgrade WCS, any permissions on the TACACS+ or RADIUS server must be re-added.

Step 5 Log in to ACS.

Step 6 Go to Group Setup. The Group Setup page appears (see Figure 18-12).

Figure 18-12 Group Setup Page on ACS Server



Step 7 Choose which group to use and click **Edit Settings**. Find [009\001]cisco-av-pair under Cisco IOS/PIX 6.x RADIUS Attributes.

Step 8 Use your browser's Edit > Paste sequence to place the RADIUS custom attributes from WCS into this text box.

Note When you upgrade WCS, any permissions on the TACACS+ or RADIUS server must be re-added.

Step 9 Click the check boxes to enable these attributes.

Step 10 Click **Submit + Restart**.

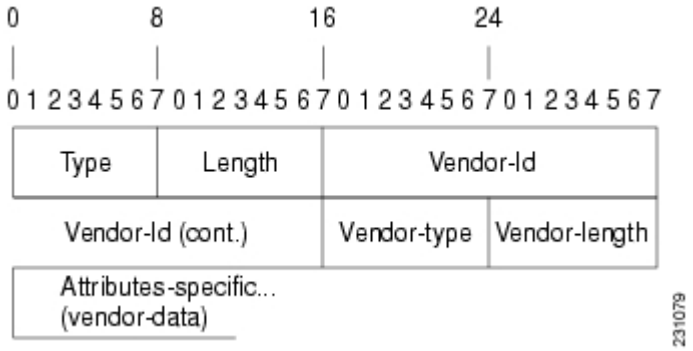
You can now associate ACS users with this ACS group.

Note To enable RADIUS in WCS, refer to the "Configuring RADIUS Servers" section on page 18-31. For information on configuring ACS view server credentials, refer to the "Configuring ACS View Server Credentials" section on page 6-2.

Adding WCS to a Non-Cisco ACS Server for Use with RADIUS

When you use a RADIUS server to log into WCS, the AAA server sends back an access=accept message with a usergroup and a list of available tasks, after the username and password were verified. The access=accept message comes back as a fragmented packet because of the large number of tasks in some user groups. You can look in the following file to see the tasks associated with a given user group: C:\Program Files\WCS5.0\webnms\webacs\WEB-INF\security\usergroup-map.xml. The tasks are passed back as a vendor specific attribute (VSA), and WCS requires authorization information using the VSA (IETF RADIUS attribute number 26). The VSA contains the WCS RADIUS task list information (refer to Figure 18-13).

Figure 18-13 Extracting Task List



The content of the VSA is as follows:

- Type = 26 (IETF VSA number)
- Vendor Id = 9 (Cisco vendor ID)
- Vendor Type = 1 (Custom attributes)
- Vendor Data = The WCS task information (for example Wireless-WCS: task0 = Users and Group)

Each line from the WCS RADIUS task list should be sent in its own RADIUS VSA.

In the data portion of the access=access packet, the truncated output sometimes shows only one role sent back for an Admin user group login. The tasks associated with the role start with task0 and increment with task1, task2, and so on. Table 18-2 defines what these attributes in the access=access packet example signify.

```
0000 06 6d 0e 59 07 3d 6a 24 02 47 07 35 d2 12 a4 eb .m.Y.=j$G.5...
0010 a2 5a fa 84 38 20 e4 e2 3a 3a bc e5 1a 20 00 00 .Z..8..:::..
0020 00 09 01 1a 57 69 72 65 6c 65 73 73 2d 57 43 53 ....Wireless-WCS
0030 3a 72 6f 6c 65 30 3d 41 64 6d 69 6e 1a 2b 00 00 :role0=Admin.+...
0040 00 09 01 25 57 69 72 65 6c 65 73 73 2d 57 43 53 ...%Wireless-WCS
0050 3a 74 61 73 6b 30 3d 55 73 65 72 73 20 61 6e 64 :task0=Users and
0060 20 47 72 6f 75 70 73 1a 27 00 00 00 09 01 21 57 Groups.”....!W
0070 69 72 65 6c 65 73 73 2d 57 43 53 3a 74 61 73 6b Wireless-WCS:task
0080 31 3d 41 75 64 69 74 20 54 72 61 69 6c 73 xx xx 1=Audit Trails.*
```

Table 18-2 Access=Access Packet Example

Attribute	Description
1a (26 in decimal)	Vendor attribute
2b (43 bytes in decimal)	Length as the total number of bytes to skip and still reach the next TLV (for task0, Users and Groups)
4-byte field	Vendor Cisco 09
01	Cisco AV pair - a TLV for WCS to read
25 (37 bytes in decimal)	Length
hex text string	Wireless-WCS:task0=Users and Groups
	The next TLV until the data portion is completely processed.
255.255.255.255	TLV: RADIUS type 8 (framed IP address)
Type 35 (0x19)	A class, which is a string
Type 80 (0x50)	Message authenticator

To troubleshoot, perform the following steps:

- Verify if the RADIUS packet is an access accept.
- Verify the task names for the user group in the access accept.
- Look at the different length fields in the RADIUS packet.

Setting AAA Mode

Follow these steps to choose a AAA mode.

Step 1 Choose **Administration > AAA**.

Step 2 Choose **AAA Mode** from the left sidebar menu. The AAA Mode Setting page appears (see Figure 18-14).

Figure 18-14 AAA Mode Settings Page

251750

Step 3 Choose which AAA mode you want to use. Only one can be selected at a time.

Any changes to local user accounts are effective only when you are configured for local mode (the default). If you use remote authentication, changes to the credentials are made on a remote server. The two remote authentication types are RADIUS and TACACS+. RADIUS requires separate credentials for different locations (East and West Coast). TACACS+ is an effective and secure management framework with a built-in failover mechanism.

Step 4 Select the **Enable Fallback to Local** check box if you want the administrator to use the local database when the external AAA server is down.

Note This option is unavailable if *Local* was selected as a AAA mode type.

Step 5 Click **OK**.

Auto Provisioning

Auto provisioning allows WCS to automatically configure a new or replace a current wireless LAN controller (WLC). The WCS 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 the Administration > AAA > Groups > *group name* > List of Tasks Permitted section of WCS. 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 WCS downloaded startup configuration file. If desired, you may 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 directlyenter the details in the application or import the details from a CSV file. The auto provisioning feature supports the 5500 and non-5500 series of controllers. The non-5500 series controllers have AP manager interface configuration information defined, whereas 5500 controllers do not have this information.

To access the Auto Provisioning feature, choose **Configure > Controller Auto Provisioning**.

- Auto Provisioning Device Management (Auto Provisioning Filter List)—Allows you to create and edit auto provisioning filters which define the list of allowable devices to be auto provisioned or auto monitored by WCS.
- Auto Provisioning Setting (Auto Provisioning Primary Search Key Setting)—Provides the ability to set the matching criteria search order.

Auto Provisioning Device Management (Auto Provisioning Filter List)

This feature allows you to create and edit auto provisioning filters which define the list of allowable devices to be auto provisioned or auto monitored by WCS.

Filter parameters include:

- Filter Name—Identifies the name of the filter.
- Filter Enable—Indicates whether or not the filter is enabled.

  Note Only enabled filters can participate in the Auto Provisioning process.

- Monitor Only—If selected, the WLC defined in this Filter is managed by WCS but not configured by WCS if the WLC contacts WCS during the auto provisioning process.
- Filter Mode—Indicates the search mode for this filter (Host Name, MAC Address, or Serial Number).
- Config Group Name—Indicates the Configuration Group name.

  Note All Config-Groups used by auto provision filters should not have any controller defined in them.

Select a Command Options for Auto Provisioning

The Select a command drop-down list has the following options:

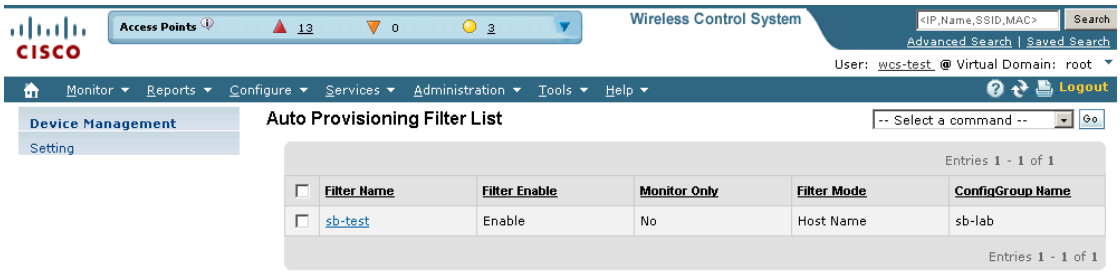
- Add Filter—Allows you to add an Auto Provisioning filter. See "Auto Provisioning Filters > New Filter" for more information.
- Delete Filter(s)—Allows you to delete the selected Auto Provisioning filter. See "Delete Filter(s)" for more information.
- List Filter(s) Device Info—Allows you to view details for the selected Auto Provisioning filter. See "List Filter(s) Device Info" for more information.
- List All Filter(s) Device Info—Allows you to view details for all of the Auto Provisioning filter. See "List All Filter(s) Device Info" for more information.

Auto Provisioning Filters > New Filter

To add an Auto Provisioning Filter, follow these steps:

Step 1 Choose **Configure > Auto Provisioning**. The Auto Provisioning Filter List page appears (see Figure 18-15).

Figure 18-15 Auto Provisioning Filter List



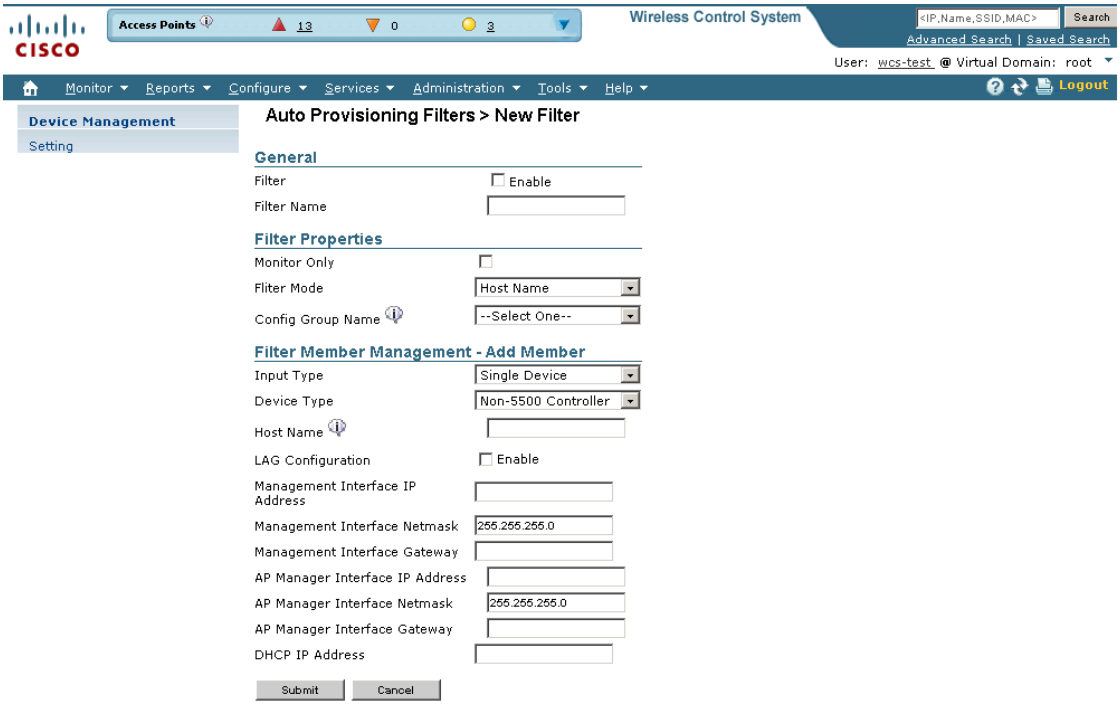
251758

Step 2 From the Select a command drop-down list, choose **Add Filter**.

Step 3 Click **Go**.

Step 4 Click **Go**. The Auto Provisioning Filters > New Filter page appears (see Figure 18-16).

Figure 18-16 Auto Provisioning Filters > New Filter



Step 5 Configure the following information:

- General
  - Enable Filter—Select check box to enable the new filter.

    Note Only enabled filters can participate in the Auto Provisioning process.

  - Filter Name—Enter a filter name.
- Filter Properties
  - Monitor Only—If selected, the WLC defined in this Filter is managed by WCS but not configured by WCS if the WLC contacts WCS during the auto provisioning process.
  - Filter Mode—From the drop-down list, choose **Host Name**, **MAC Address**, **Serial Number** to indicate the search mode for this filter.
  - Config Group Name—From the drop-down list, choose a config group name.
- Filter Member Management - Add Member
  - Input Type—From the drop-down list, choose **Single Device** or **CSV File**.

    If Single Device is selected, enter the host name, enable LAG configuration (if applicable), and enter the following: management interface IP Address, management interface netmask, management interface gateway, AP manager interface IP address, AP manager interface netmask, AP manager interface gateway, and DHCP IP address.

    If CSV File is selected, enter the CSV file or use the **Browse** button to navigate to the applicable CSV File.

Note You can choose the **Download a sample CSV File** link to download a sample CSV file to your computer and customize the various configurations.

Note Because MS-Excel can insert additional commas when you edit a CSV file, ensure that you edit the CSV file using a normal text editor application.

A CSV file contains the following sections:

**** The first part is the General Config section that contains parameters which are used to construct controller's startup config file.**
**** The first line in the CSV file must be keyword**
"!!deviceId, LAG, managementIP, managementVlanId, managementNetmask, managementGateway, apManagerIP, apManagerVlanId, apManagerNetmask, apManagerGateway, dhcpServerIP"

deviceId—it can be Host name, Mac address, or Serial number.
LAG—controller's LAG configuration (true/false).
managementIP—controller's Management interface IP address.
managementVlanId—controller's Management interface VLAN Id (0=untagged).
managementNetmask—controller's Management interface Network mask.
managementGateway—controller's Management interface Gateway IP.
apManagerIP—controller's AP Manager Interface IP address, optional for 5500 series controller.
apManagerVlanId—controller's AP Manager Interface VLAN Id (0=untagged), optional for 5500 series controller.
apManagerNetmask—controller's AP Manager Interface Netmask, optional for 5500 series controller.
apManagerGateway—controller's AP Manager Interface Gateway, optional for 5500 series controller.
dhcpServerIP—controller's DHCP IP address.

**** The second part is the Dynamic Interface section that contains dynamic interface parameters for a controller. This is an optional section.**
**** To configure a dynamic interface, the first eight parameters are mandatory and the last four parameters are optional.**
"!!deviceId, interfaceName, vlanId, quarantineVlanId, interfaceIP, interfaceNetmask, gateway, primaryPort, secondaryPort, primaryDHCP, secondaryDHCP, aclName"
deviceId—this deviceId must be defined previously in section 1.
interfaceName—name of the dynamic interface.
vlanId—vlan ID used by this interface.
quarantineVlanId—quarantine vlan ID used by this interface.
interfaceIP—IP address of the dynamic interface.
interfaceNetmask—Network Mask of the dynamic interface.
gateway—Gateway IP address of the dynamic interface.
primaryPort—physical primary port number used by the dynamic interface.
secondaryPort—physical secondary port number used by the dynamic interface, this is an optional parameter.
primaryDHCP—the IP address of the primary DHCP used by the dynamic interface, this is an optional parameter.
secondaryDHCP—IP address of the secondary DHCP used by the dynamic interface, this is an

optional parameter.

**** The third part is the Device Specific Config section, contains other device specific configuration parameters which are optional during auto provisioning.**
"!!deviceId, countryCode, mobilityGroupName, mobilityGroupMembers"
deviceId—this deviceId must be defined previously in section 1.
countryCode—country code for the controller, this is an optional parameter.
mobilityGroupName—default name of the mobility group this controller belongs to, this is an optional parameter. If this attribute is not specified then the existing default mobility group name will be used.
mobilityGroupMembers—IP addresses, Mac Addresses and mobility group name of the mobility group members of the controller, which are separated by semi colon, this is an optional parameter. Both IP address and Mac Address are required for a mobility group member, they are separated by forward slash. Mobility group name is an optional attribute in this field. If mobility group name is not present then the default mobility group name for this controller will be used.

- If you select the Single Device option, specify the following options:
  - Device Type—From the drop-down list, choose **5500 Controller** or **non-5500 Controller**.
  - Host Name
  - LAG Configuration: Enabled or Disabled.
  - Management Interface IP Address
  - Management Interface Netmask
  - Management Interface Gateway
  - AP Manager Interface IP Address
  - AP Manager Interface Netmask
  - AP Manager Interface Gateway
  - DHCP IP Address

Step 6 Click **Submit**.

Note You can specify the Dynamic Interface configuration and Device Specific configuration details only when you input a CSV file. These two configurations cannot be performed using the GUI.

Editing a Current Auto Provisioning Filter

To edit a current Auto Provisioning filter, follow these steps:

Step 1 Choose **Configure > Auto Provisioning**.

Step 2 Click the Filter Name of the filter you want to edit.

Step 3 Make the necessary changes to the current filter parameters.

Note To view detailed information for a filter member, click the **Device ID** of the member you want to view.
To delete a filter member. select the check box for the member you want to delete in the Filter Member Management - Delete Member section. When you click **Submit**, that member is deleted.

Step 4 Click **Submit**.

Delete Filter(s)

To delete an Auto Provisioning Filter, follow these steps:

Step 1 Choose **Configure > Auto Provisioning**.

Step 2 Select the check box of the filter you want to delete.

Step 3 From the Select a command drop-down list, choose **Delete Filter(s)**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

List Filter(s) Device Info

To view details for an individual Auto Provisioning Filter, follow these steps:

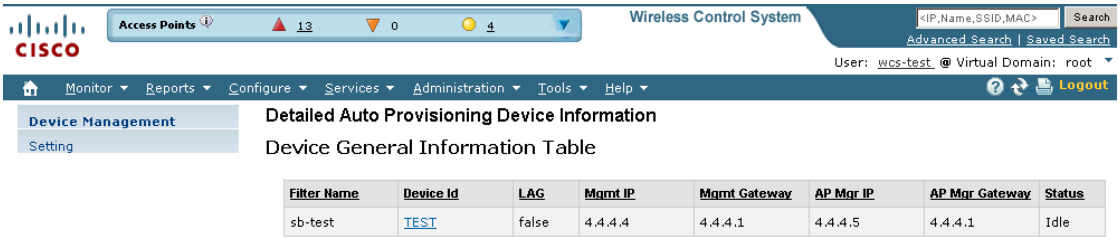
Step 1 Choose **Configure > Auto Provisioning**.

Step 2 Select the check box of the filter you want to view.

Step 3 From the Select a command drop-down list, choose **List Filter(s) Device Info**.

Step 4 Click **Go**. The Detailed Auto Provisioning Device Information page appears (see Figure 18-17).

Figure 18-17 Detailed Auto Provisioning Device Information



252000

The following information is provided for the selected filter:

- Filter Name—Indicates the filter name.
- Device ID—Indicates the device ID.
- LAG—Indicates the controller LAG status as true or false.
- Management IP—Indicates the management interface IP address of the controller.
- Management VlanId—Indicates the management VLAN Id of the controller.
- Management Netmask—Indicates the netmask mask of the management interface of the controller.
- Management Gateway—Indicates the netmask gateway of the management interface of the controller.
- AP Mgr IP—Indicates the IP address of the access point manager.
- AP Mgr Vlan Id—Indicates the VLAN identifier of the access point manager.
- AP Mgr Netmask—Indicates the netmask mask of the access point manager.
- AP Mgr Gateway—Indicates the gateway IP address of the access point manager.
- Status—Idle, Trap Received, Failed In Trap Processing, Failed In Applying Templates, Failed In Discovery Switch, Managed, Managed partially applied templates, or Unknown Error
- Country
- Mobility Grp—Indicates the name of the mobility group.
- Mobility Grp Members
- Timestamp—Indicates the date and time of the information.

List All Filter(s) Device Info

To view details for all Auto Provisioning Filters, follow these steps:

Step 1 Choose **Configure > Auto Provisioning**.

Step 2 From the Select a command drop-down list, choose **List All Filter(s) Device Info**.

Step 3 Click **Go**.

The following information is provided for the selected filter:

- Filter Name—Indicates the filter name.
- Device ID—Indicates the device ID.
- LAG—Indicates the controller LAG status as true or false.
- Management IP—Indicates the management interface IP address of the controller.
- Management VlanId—Indicates the management VLAN Id of the controller.
- Management Netmask—Indicates the netmask mask of the management interface of the controller.
- Management Gateway—Indicates the netmask gateway of the management interface of the controller.
- AP Mgr IP—Indicates the IP address of the access point manager.
- AP Mgr Vlan Id—Indicates the VLAN identifier of the access point manager.
- AP Mgr Netmask—Indicates the netmask mask of the access point manager.
- AP Mgr Gateway—Indicates the gateway IP address of the access point manager.
- Status—Idle, Trap Received, Failed In Trap Processing, Failed In Applying Templates, Failed In Discovery Switch, Managed, Managed partially applied templates, or Unknown Error
- Country
- Mobility Grp
- Mobility Grp Members
- Timestamp—Indicates the date and time of the information.

Export Filter(s)

To export an Auto Provisioning Filter, follow these steps:

Step 1 Choose **Configure > Auto Provisioning**.

Step 2 Select the check box of the filter(s) you want to export.

Step 3 From the Select a command drop-down list, choose **Export Filter(s) Config (CSV)**.

Step 4 Click **Go**.

Step 5 In the File Download dialog box that appears, click **Save** to save the file to a location on the computer.

Export All Filter(s)

To export all Auto Provisioning Filters, follow these steps:

Step 1 Choose **Configure > Auto Provisioning**.

Step 2 From the Select a command drop-down list, choose **Export All Filter(s) Config (CSV)**.

Step 3 Click **Go**.

Step 4 In the File Download dialog box that appears, click **Save** to save the file to a location on the computer.

Auto Provisioning Setting (Auto Provisioning Primary Search Key Setting)

The Primary Search Key Setting enables you to set the matching criteria search order.

To indicate the Search Key Order, follow these steps:

Step 1 Choose **Configure > Auto Provisioning**.

Step 2 From the left sidebar menu, choose **Auto Provisioning Setting**.

Step 3 Click to highlight the applicable search key.

Step 4 Use the **Move Up** or **Move Down** buttons to move the search key to a higher or lower priority.

Step 5 Click **Save** to confirm or **Cancel** to cancel the changes.

Turning Password Rules On or Off

You have the ability to customize the various password rules to meet your criteria. Follow these steps to customize the password rules.

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Local Password Policy**. The password rules are displayed individually, and each has a check box in front of it.

Step 3 Click the check boxes to enable the rules you want. The rules are as follows:

Note All rules are on by default.

- Password minimum length is 8 characters (the length configurable).
- Password cannot contain username or the reverse of the username.
- Password cannot be cisco or ocsic (Cisco reversed).
- Root password cannot be *public*.
- No character can be repeated more than three times consecutively in the password.
- Password must contain characters from three of the character classes: uppercase, lowercase, digits, and special characters.

Configuring TACACS+ Servers

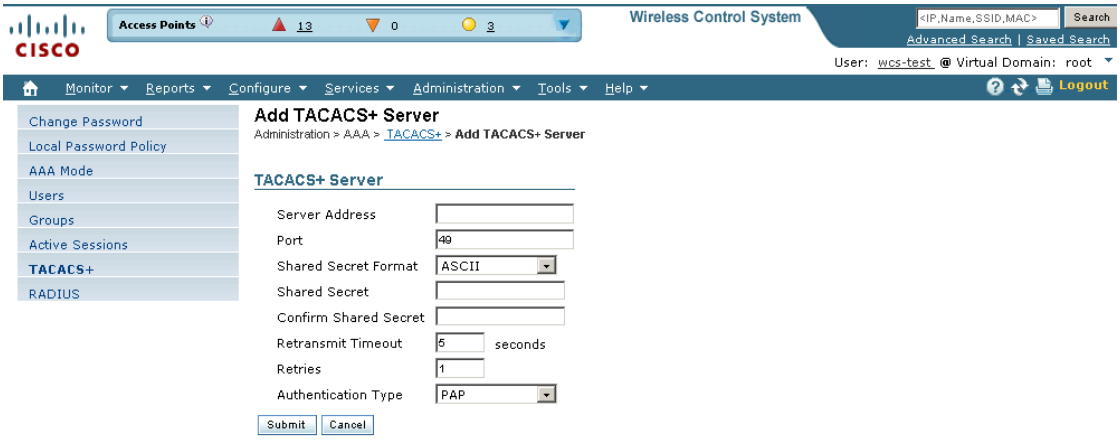
This section describes how to add and delete TACACS+ servers. TACACS+ servers provide an effective and secure management framework with built-in failover mechanisms. If you want to make configuration changes, you must be authenticated.

Note In order to activate TACACS+ servers, you must enable them as described in the "Importing Tasks Into ACS" section on page 18-8.

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **TACACS+**. The TACACS+ page appears (see Figure 18-18).

Figure 18-18 TACACS+ Page



Step 3 The TACACS+ page shows the TACACS+ server's IP address, port, retransmit rate, and authentication type (Password Authentication Protocol (PAP)) or Challenge Handshake Authentication Protocol (CHAP). The TACACS+ servers are tried based on how they were configured.

Note If you need to change the order of how TACACS+ servers are tried, delete any irrelevant TACACS+ servers and re-add the desired ones in the preferred order.

Step 4 Use the drop-down list in the upper right-hand corner to add or delete TACACS+ servers. You can click an IP address if you want to make changes to the information.

Step 5 The current server address and port are displayed. Use the drop-down list to choose either ASCII or hex shared secret format.

Step 6 Enter the TACACS+ shared secret used by your specified server.

Step 7 Re-enter the shared secret in the Confirm Shared Secret text box.

Step 8 Specify the time in seconds after which the TACACS+ authentication request times out and a retransmission is attempted by the controller.

Step 9 Specify the number of retries that will be attempted.

Step 10 In the Authentication Type drop-down list, choose a protocol: PAP or CHAP.

Step 11 Click **Submit**.

Note See the "Configuring ACS 5.x" section on page 18-76 for more information on Configuring ACS 5.x.

Configuring RADIUS Servers

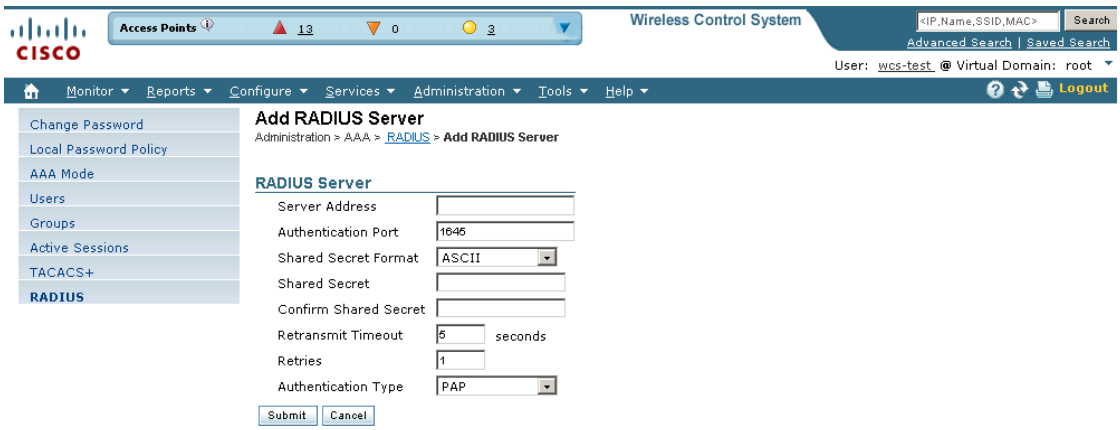
This section describes how to add and delete RADIUS servers. You must enable RADIUS servers and have a template set up for them in order to make configuration changes.

Note In order to activate RADIUS servers, you must enable them as described in the "Importing Tasks Into ACS" section on page 18-8.

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **RADIUS**. The RADIUS page appears (see Figure 18-19).

Figure 18-19 RADIUS Page



251754

Step 3 The RADIUS page shows the server address, authentication port, retransmit timeout value, and authentication type for each RADIUS server that is configured. The RADIUS servers are tried based on how they were configured.

Note If you need to change the order of how RADIUS servers are tried, delete any irrelevant RADIUS servers, and re-add the desired ones in the preferred order.

Step 4 Use the drop-down list in the upper right-hand corner to add or delete RADIUS servers. You can click an IP address if you want to make changes to the information.

Step 5 The current authentication port appears. Use the drop-down list to choose either ASCII or hex shared secret format.

Step 6 Enter the RADIUS shared secret used by your specified server.

Step 7 Re-enter the shared secret in the Confirm Shared Secret text box.

Step 8 Specify the time in seconds after which the RADIUS authentication request times out and a retransmission is attempted by the controller.

Step 9 Specify the number of retries that will be attempted.

Step 10 In the Authentication Type drop-down list, choose a protocol: PAP or CHAP.

Step 11 Click **Submit**.

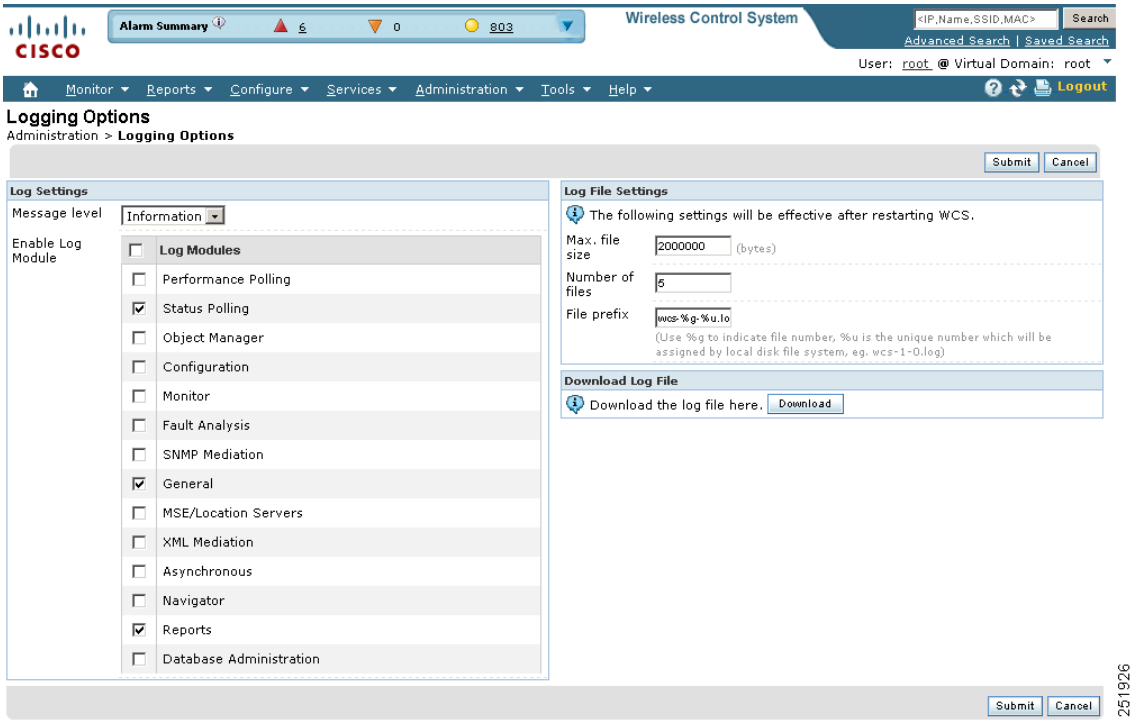
Establishing Logging Options

Use **Administration > Logging** to access the Administer Logging Options page. This logging function is related only to WCS logging and not syslog information. The logging for controller syslog information can be done on the Controller > Management > Syslog page.

Follow the steps below to enable e-mail logging. The settings you establish are stored and are used by the e-mail server.

Step 1 Choose A**dministration > Logging**. The Logging Options menu appears (see Figure 18-20).

Figure 18-20 Logging Options Page



Step 2 Choose a message level option of **Trace**, **Information**, or **Error**.

Step 3 Click the check boxes within the Enable Log Module portion of the page to enable various administration modules:

- Message Level—Select the minimum level of the messages that will be logged including **Error**, **Information**, or **Trace**.
- Enable Log Module—You can enable logging for the following administration modules:

- Status Polling—Used to log all background tasks.
- Object Manager—Captures logs related to managed devices and resource allocation.
- Configuration—Used to log controller configurations that you make from WCS.

Note To get complete controller configuration logs, also enable the General log module.

Note To get the configuration values that the WCS sends in logs to controllers, enable Trace Display Values (Administration > Settings > SNMP Settings > Trace Display Value).

- Monitor—Used for Alarms, Spectrum Intelligence, CCXV5, Clients/Tags, Client Radio Measurements, SSO, and Mesh.
- Fault Analysis—Used by the event and alert subsystem.
- SNMP Mediation—Captures logs for all SNMP communication between WCS and controllers.
- General—Contains logs that do not fall under other log module categories.

Note Cisco recommends that you enable this log module.

- MSE/Location Servers—Used for MSE-related operations such as adding or deleting an MSE and changing parameters on the MSE. It also enables logging for MSE synchronization including NW designs and controllers.
- XML Mediation—Used to enable trace for the communication between MSE/LOC 2700 and WCS.
- Asynchronous—Used for WCS notifications and for Simple Object Access Protocol (SOAP) messages that MSE generates.
- Navigator—Contains logs to debug issues when WCS does not respond to WCS Navigator's periodic polling through the Northbound Webservice API.
- Reports—Used to log messages related to creating, saving, scheduling, and running reports. This module also contains a list of scheduled and saved reports.
- Database Administration—Contains logs to debug important database-related operations in WCS.

Note Some functions should be used only for short periods of time during debugging so that the performance is not degraded. For example, trace mode and SNMP meditation should be enabled only during debugging because a lot of log information is generated.

Step 4 In the Log File Settings portion, enter the following settings. These settings will be effective after restarting WCS.

- Max. file size—Maximum number of MBs allowed per log file.
- Number of files—Maximum number of log files allowed.
- File prefix—Log file prefix, which can include the characters "%g" to sequentially number of files.

Step 5 Click the Download Log File section to download log files to the local machine.

Note The logs.zip filename includes a prefix with the host name, date, and time so that you can easily identify the stored log file. Included in the zip file is an html file that documents the log files.

Step 6 Click **Submit**.

Using Logging Options to Enhance Troubleshooting

The logging screen allows you to customize the amount of data WCS collects in order to debug an issue. For easily reproduced issues, follow these steps prior to contacting TAC. These steps may create a smoother troubleshooting session:

Step 1 Choose **Administration > Logging**.

Step 2 From the Message Level drop-down list, choose **Trace**.

Step 3 Select each check box to enable all log modules.

Step 4 Reproduce the current problem.

Step 5 Return to the Logging Options page.

Step 6 Click **Download** from the Download Log File section.

Step 7 After you have retrieved the logs, select **Information** from the Message Level drop-down list.

Note Leaving the Message Level at *Trace* can adversely affect performance over a long period of time.

Performing Data Management Tasks

Within the Settings page, you can indicates the data that you want to generate for reports and e-mails. Choose **Administration > Settings** in the left sidebar menu.

- See the "Alarms" section on page 18-35 to specify how to handle old alarms and how to display assigned and acknowledged alarms in the Alarm Summary page.
- See "Audit" section on page 18-37 to configure audit information.
- See the "Client" section on page 18-39 to enable client troubleshooting on a diagnostic channel.
- See the "CLI Session" section on page 18-41 to establish a telnet or SSH session.
- See the "Controller Upgrade Settings" section on page 18-41 for information on controller upgrade settings.
- See the "Data Management" section on page 18-42 to establish trends for hourly, daily, and weekly data periods.
- See the "Guest Account Settings" section on page 18-43 to designate where the scheduled reports will reside and for how long.
- See the "Login Disclaimer" section on page 18-44 to enter disclaimer information.
- See the "Mail Server Configuration" section on page 18-45 to set the primary and secondary SMTP server host and port.

- See the "Notification Receiver" section on page 18-47 to configure parameters for notification support of guest access functionality.
- See the "Server Settings" section on page 18-53 to turn FTP, TFTP, HTTP, or HTTPS on or off.
- See the "Severity Configurations" section on page 18-54 to configure the severity level for newly generated alarms.
- See the "SNMP Credentials" section on page 18-56 to specify which credentials to use for tracing the rogue access points.
- See the "SNMP Settings" section on page 18-58 to configure global SNMP settings from WCS.
- See the "Switch Port Trace" section on page 18-60 to identify the switch port to which a rogue access point is connected.

Alarms

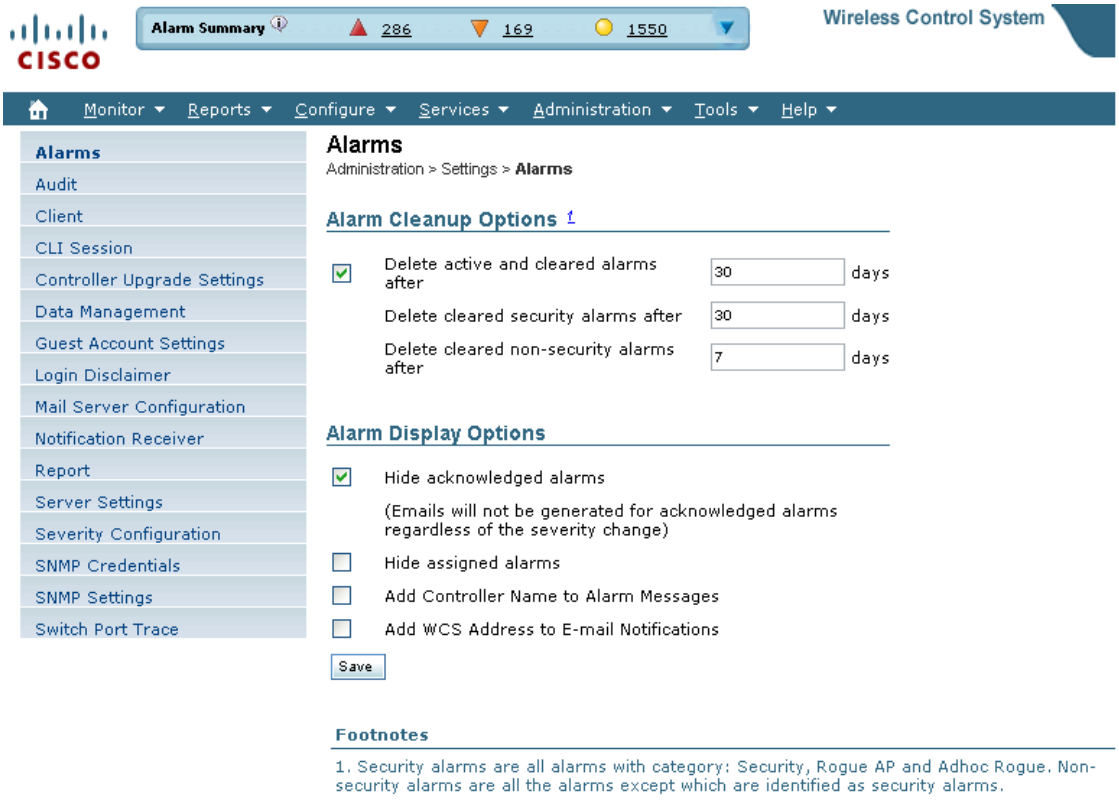
This Alarms page enables you to handle old alarms and display assigned and acknowledged alarms in the Alarm Summary page.

To open this page, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Alarms**. The Administration > Settings > Alarms page appears (see Figure 18-21).

Figure 18-21 Settings > Alarms Page



Step 3 Add or modify the following Alarms parameters:

- Alarm Cleanup Options
  - Delete active and cleared alarms after—Enter the number of days after which active and cleared alarms are deleted. This option can be disabled by clearing the check box.
  - Delete cleared security alarms after—Enter the number of days after which Security, Rogue AP, and Adhoc Rogue alarms are deleted.
  - Delete cleared non-security alarms after—Enter the number of days after which non-security alarms are deleted. Non-security alarms include all alarms that do not fall under the Security, Rogue AP, or Adhoc Rogue categories.

Note Data cleanup tasks run nightly to delete old alarms. In addition to the data cleanup task, WCS has an hourly task to check alarm table size. When the alarm table size exceeds 300 K, the task deletes the oldest cleared alarms until the alarm table size is within 300 K.

- Alarm Display Options

Note These preferences only apply to the Alarm Summary page. Quick searches or alarms for any entity display all alarms regardless of the acknowledged or assigned state.

- Hide acknowledged alarms—When the check box is selected, Acknowledged alarms do not appear on the Alarm Summary page. This option is enabled by default.

  Note E-mails are not generated for acknowledged alarms regardless of severity change.

- Hide assigned alarms—When the check box is selected, assigned alarms do not appear on the Alarm Summary page.
- Add controller name to alarm messages—Select the check box to add the name of the controller to alarm messages.
- Add WCS address to email notifications—Select the check box to add the WCS address to email notifications.

Step 4 Click **Save**.

Audit

You can choose between basic and template-based auditing. The default setting is Basic Audit.

- Basic Audit—Audits the configuration objects in the WCS database against current WLC device values. Prior to the 5.1.0.0 version of WCS, this was the only audit mode available.

  Note Configuration objects refer to the device configuration stored in the WCS database.

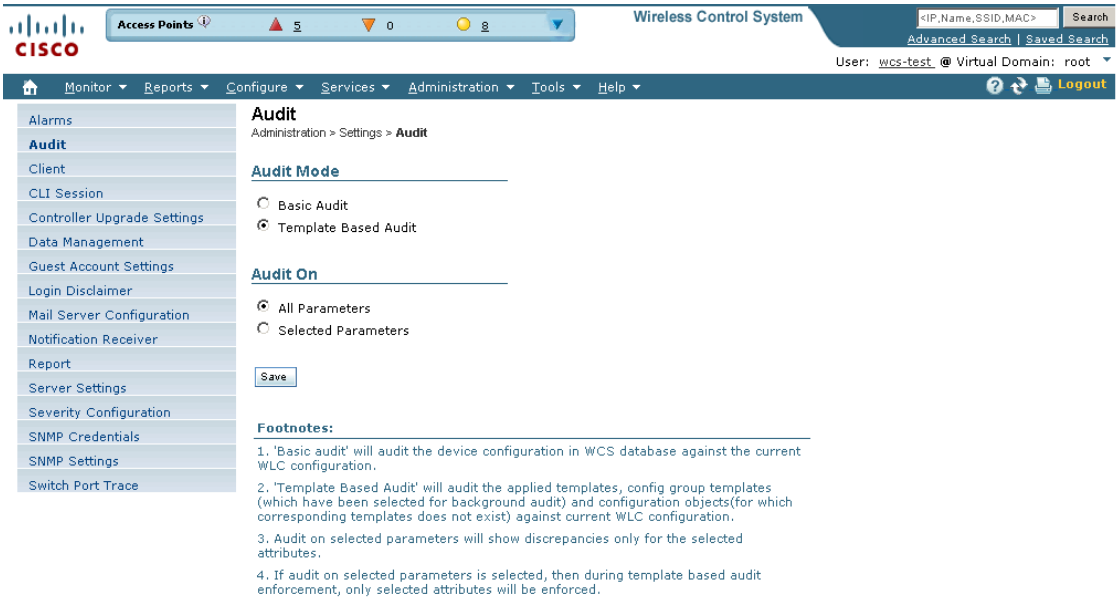
- Template-based Audit—Audits on the applied templates, config group templates (which have been selected for the background audit), and configuration audits (for which corresponding templates do not exist) against current WLC device values.

Follow these steps to indicate the type of audit you want to perform.

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Audit**. The Audit Setting page appears (see Figure 18-22).

Figure 18-22 Audit Settings Page



Step 3 Select the radio button for either Basic or Template-Based Audit. A basic audit audits the device configuration in the WCS database against the current WLC configuration. A template-based audit audits the applied templates, config group templates, and configuration objects (for which corresponding templates do not exist) against current WLC configuration.

Step 4 Choose if you want the audit to run on all parameters or only on selected parameters. If you select the Selected Parameters radio button, you can access the Configure Audit Parameters configuration page. (See the "Configuring Audit Parameters" section on page 18-38 below). The Select audit parameters URL appears.

The selected audit parameters are used during network and controller audits.

Step 5 Click **Save**.

Note These settings are in effect when the controller audit or network audit is performed.

Configuring Audit Parameters

To configure the audit parameters for a global audit, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Audit**.

Step 3 Select the **Selected Parameters** radio button to display the **Select Audit Parameters** link.

Step 4 Click **Save**.

Step 5 Click **Select Audit Parameters** to choose the required parameters for the audit in the Audit Configuration > Parameter Selection page.

Step 6 Select the parameters that you want audited from each of the tabs. The tabs include System, WLAN, Security, Wireless, and Selected Attributes.

Step 7 When all desired audit parameters are selected, click **Submit** to confirm the parameters or click **Cancel** to close the page without saving any audit parameters.

Once you click **Submit**, the selected audit parameters display under the Selected Attributes tab.

A current Controller Audit Report can be accessed from the Configure > Controllers page by selecting an object from the Audit Status column.

Note You can audit a controller by selecting **Audit Now** from the Select a command drop-down list in the Configure > Controllers page or by clicking **Audit Now** directly from the Controller Audit report. See the "Viewing Audit Status (for Controllers)" section on page 10-34.

Client

In the Administration > Settings > Client page, you can configure the following client processes to improve WCS performance and scalability.

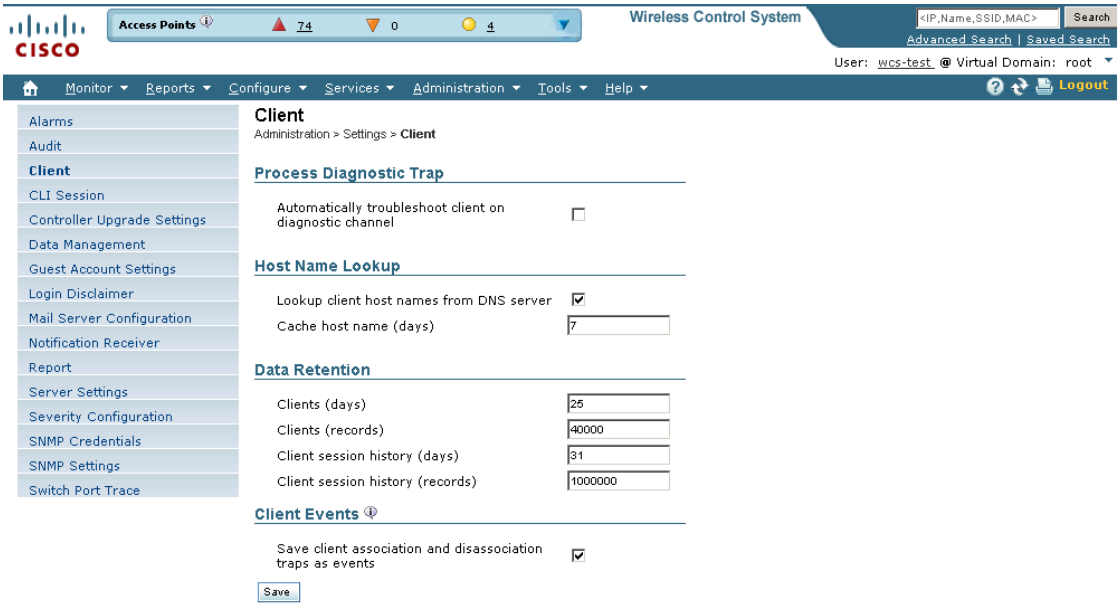
Note See the "Client Troubleshooting" section on page 11-11 for further information on client troubleshooting.

- Process Diagnostic Trap
- Host Name Lookup
- Data Retention
- Client Traps

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Client**. The Client page appears (see Figure 18-23).

Figure 18-23 Administration > Settings > Client Page



Step 1 Click if you want to enable automatic client troubleshooting on a diagnostic channel. Automatic client troubleshooting is available only for CCXV5 clients.

Note If the check box is selected, WCS processes the diagnostic association trap. If it is not selected, WCS raises the trap, but automated troubleshooting is not initiated.

Note While processing the diagnostic association trap, the WCS invokes a series of tests on the client. The client is updated on all completed tasks. The automated troubleshooting report is placed in dist/acs/win/webnms/logs. When the test is complete, the location of the log is updated in client details pages:V5 tab:Automated Troubleshooting Report section. An export button allows you to export the logs.

Step 2 Select the **Lookup client host names for DNS server** check box. DNS lookup can take a considerable amount of time. Therefore, you can enable or disable the DNS lookup for client host name. It is set to Disable by default. If you enable the check box, you need to enter the number of days that you want the host name to remain in the cache.

Step 3 In the Data Retention section, enter or edit the following data retention parameters. Client association history can take a lot of database and disk space. This can be an problem for database backup and restore functions. You can configure the retaining duration of a client association history to help manage this potential issue.

- Client (days)—Enter the number of days that you want WCS to retain the data. The default is 7days. The valid range is 1 to 365 days.
- Client (records)—Enter the number of client records that you want WCS to retain.
- Client session history (days)

- Client session history (records)

Step 4 In some deployments, WCS may receive large amounts of client association and disassociation traps. Saving these traps as events may cause a slight performance issue. In such cases, other events that may be useful may be aged out sooner than expected.

To ensure that WCS does not save client association and disassociation traps as events, clear the **Save client association and disassociation traps as events** check box.

Step 5 If you click the **Poll clients when client traps received** check box, WCS polls clients to quickly identify client sessions. In a busy network, you may want to disable polling while the client traps are received.

Step 6 Click **Save**.

CLI Session

Many WCS features such as autonomous access point and controller CLI templates, along with migration templates require executing CLI commands on the autonomous access point or controller. These CLI commands can be executed by establishing telnet or SSH sessions. The CLI session page allows you to select the session protocol. SSH is the default.

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **CLI Session**.

Step 3 The default controller session protocol SSH is selected. To instead choose Telnet, select that radio button.

Step 4 The default autonomous access point session protocol SSH is selected. To instead select Telnet, click that radio button.

Step 5 Click **Save**.

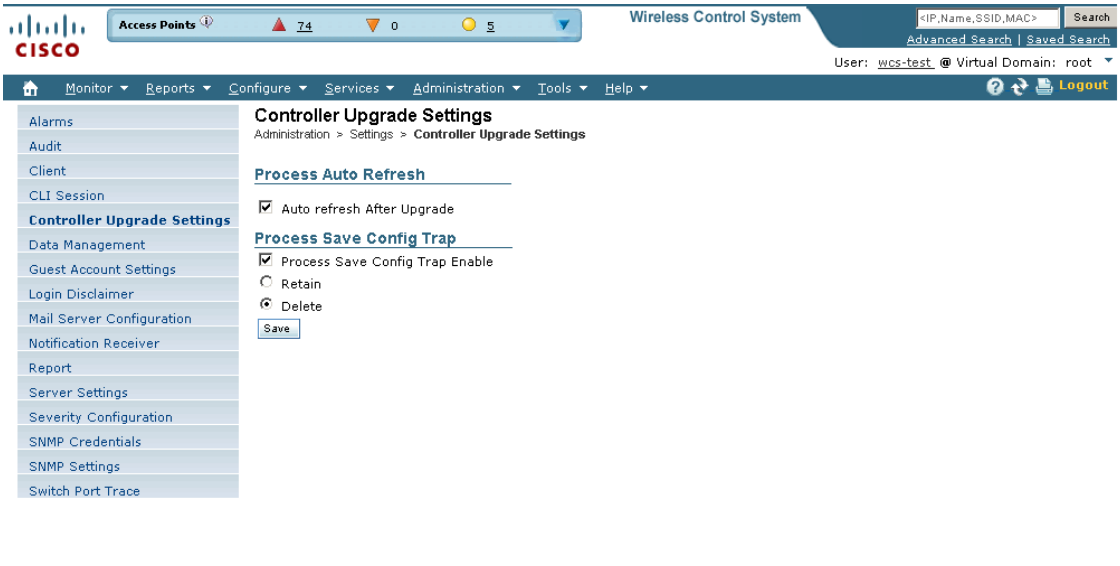
Controller Upgrade Settings

The Controller Upgrade Settings page allows you to auto-refresh after a controller upgrade. Follow these steps to perform an auto-refresh.

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Controller Upgrade Settings** (see Figure 18-24).

Figure 18-24 Controller Upgrade Settings



Step 3 Select the **Auto refresh After Upgrade** check box to automatically restore the configuration whenever there is a change in the WLC image.

Step 4 Determine the action WCS will take when a save config trap is received. When this option is enabled, you can choose to retain or delete the extra configurations present on the device but not on WCS. The setting is applied to all controllers managed by WCS. If you select the **Auto Refresh on Save Config Trap** check box on the Configure > Controllers > Properties > Settings page, it overrides this global setting.

Note It may take up to 3 minutes for the automatic refresh to occur.

Step 5 Click **Save**.

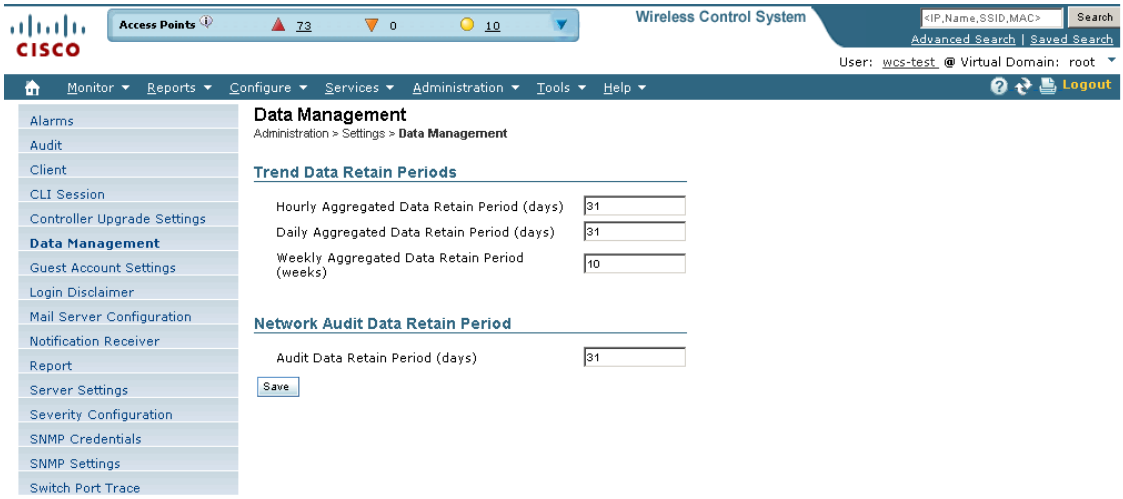
Data Management

Follow the steps below to set retention periods for aggregated data used in timed calculations and network audit calculations. You can configure retention periods on an hourly, daily, and weekly basis.

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Data Management**. The Data Management page appears (see Figure 18-25).

Figure 18-25 Data Management Page



251920

Step 3 Specify the number of days to keep the hourly data. The valid range is 1 to 31.

Step 4 Specify the number of days to keep the daily data. The valid range is 7 to 365.

Step 5 Specify the number of weeks to keep the weekly data. The valid range is 2 to 108.

Step 6 Specify the number of days to retain the audit data collected by the Network Audit background task before purging. The limit is 90 days, and the minimum cleanup interval is 7 days.

Note For the best interactive graph data views, change the default settings to the maximum possible: 90 days for daily aggregated data and 54 weeks for weekly aggregated data. You must also make the appropriate measures to increase RAM and CPU capacity to compensate for these adjustments.

Step 7 Click **Save**.

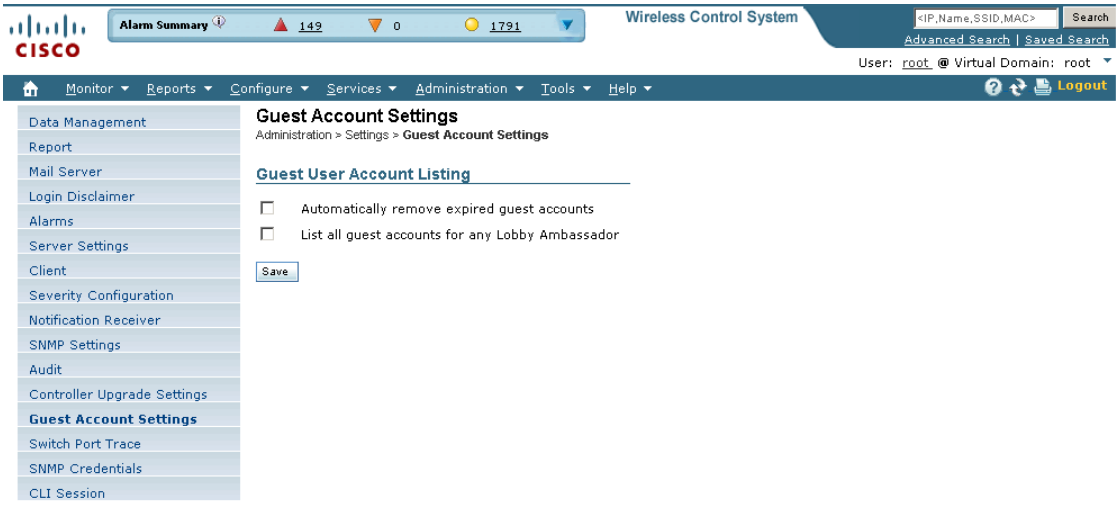
Guest Account Settings

The Guest Account Settings page allows you to globally remove all expired templates. Follow these steps to configure guest account settings.

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Guest Account Settings** (see Figure 18-26).

Figure 18-26 Guest Account Settings Page



251923

Step 3 When the **Automatically remove expired guest accounts option** is selected, the guest accounts whose lifetime has ended are not retained, and they are moved to the Expired state. Those accounts in the expired state are deleted from WCS.

Step 4 By default, WCS Lobby Ambassadors can access only the guest accounts that have been created by them. If you select the **List all guest accounts for any Lobby Ambassador** check box, the Lobby Ambassador can access all guest accounts irrespective of wh0 created them.

Step 5 Click **Save**.

Login Disclaimer

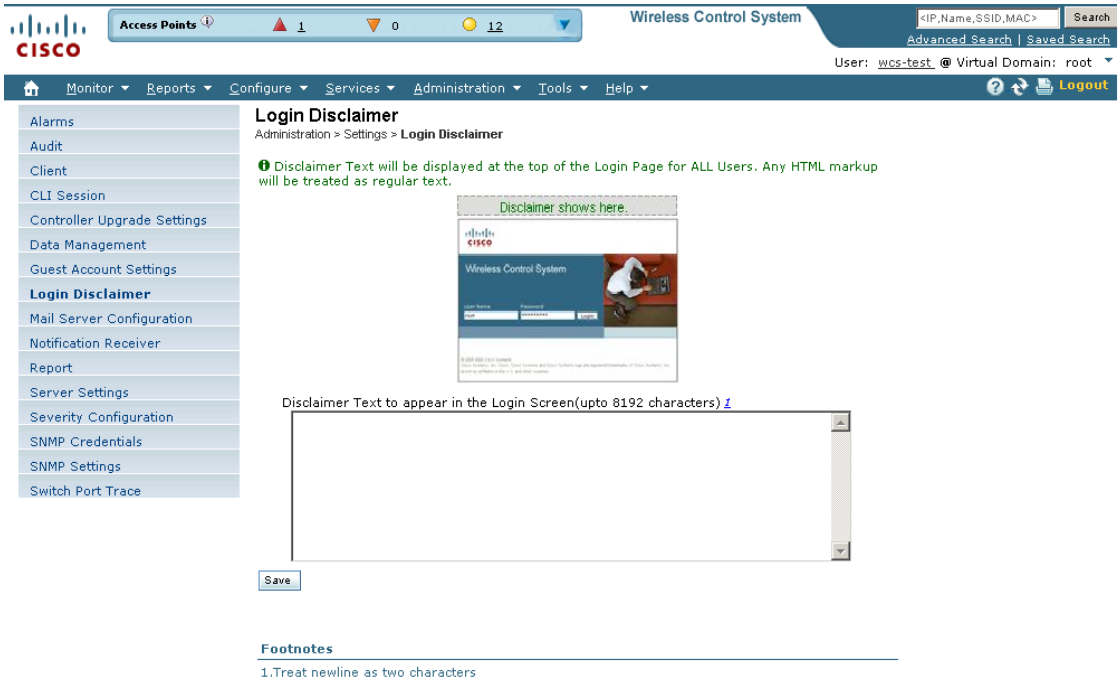
The Login Disclaimer page allows you to enter disclaimer text at the top of the Login page for all users.

To enter Login Disclaimer text, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Login Disclaimer**. The Login Disclaimer page appears (see Figure 18-27).

Figure 18-27 Login Disclaimer Page



Step 3 Enter your Login Disclaimer text in the available text box.

Step 4 Click **Save**.

Mail Server Configuration

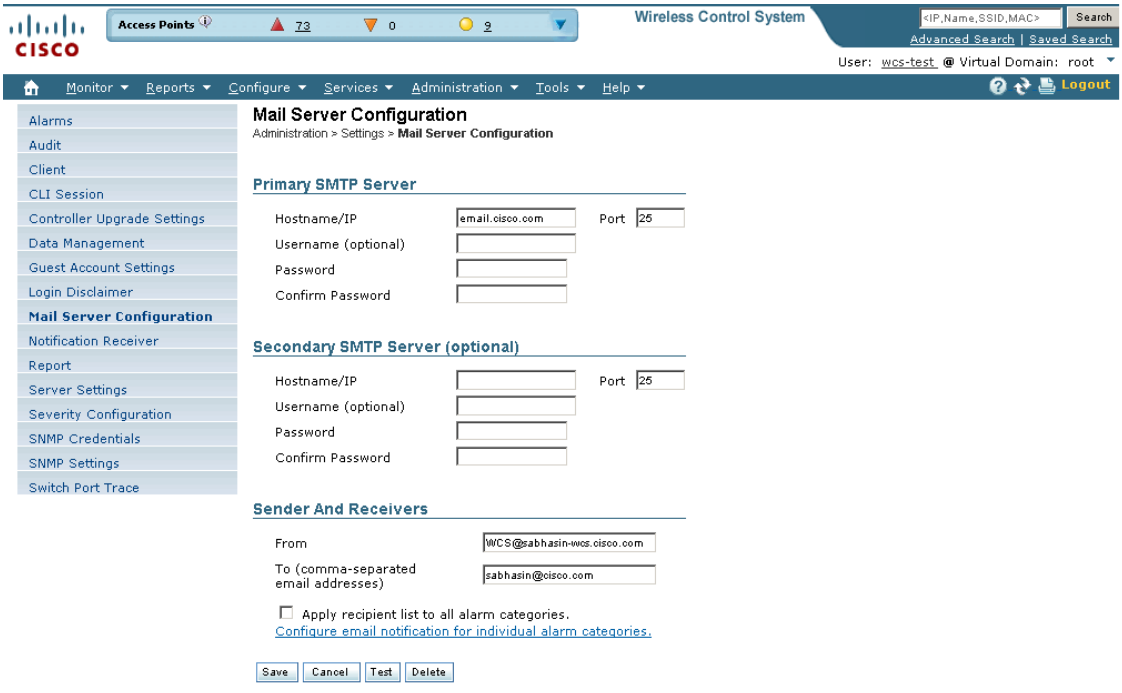
You can configure global e-mail parameters for sending e-mails from WCS reports, alarm notifications, and so on. This mail server page enables you to configure e-mail parameters in one place. The Mail Server page enables you to set the primary and secondary SMTP server host and port, the sender's e-mail address, and the recipient's e-mail addresses. Follow these steps to configure global e-mail parameters.

Note You must configure the global SMTP server before setting global e-mail parameters.

Step 1 Choose **Administration > Setting**.

Step 2 From the left sidebar menu, choose **Mail Server Configuration**. The page in Figure 18-28 appears.

Figure 18-28 Mail Server Configuration Page



Step 3 Enter the host name of the primary SMTP server.

Step 4 Provide a password for logging on to the SMTP server and confirm it.

Step 5 Provide the same information for the secondary SMTP server (only if a secondary mail server is available).

Step 6 The From text box in the Sender and Receivers portion of the page is populated with *WCS@<WCS server IP address>*. You can change it to a different sender.

Step 7 Enter the recipient's e-mail addresses in the To text box. The e-mail address you provide serves as the default value for other functional areas, such as alarms or reports. Multiple e-mail addresses can be added and should be separated by commas.

Note Global changes you make to the recipient e-mail addresses in Step 7 are disregarded if e-mail notifications were set.

You must indicate the primary SMTP mail server and fill the From address text boxes.

If you want all alarm categories applied to the provided recipient list, select the **Apply recipient list to all alarm categories** check box.

Step 8 If you click the "Configure email notification for individual alarm categories" link, you can specify the alarm categories and severity levels you want to enable. Email notifications are sent when an alarm occurs that matches categories and the severity levels you select.

Note You can set each alarm severity by clicking the alarm category, choosing Critical, Major, Minor, or Warning, and providing an email address.

Step 9 Click the **Test** button to send a test e-mail using the parameters you configured. The results of the test operation appear on the same screen. The test feature checks the connectivity to both primary and secondary mail servers by sending an e-mail with a "WCS test e-mail" subject line.

Step 10 If the test results were satisfactory, click **Save**.

Notification Receiver

The Notification Receiver page displays current notification receivers that support guest access. Alerts and events are sent as SNMPv2 notifications to configured notification receivers.

In this page, you can view current or add additional notification receivers.

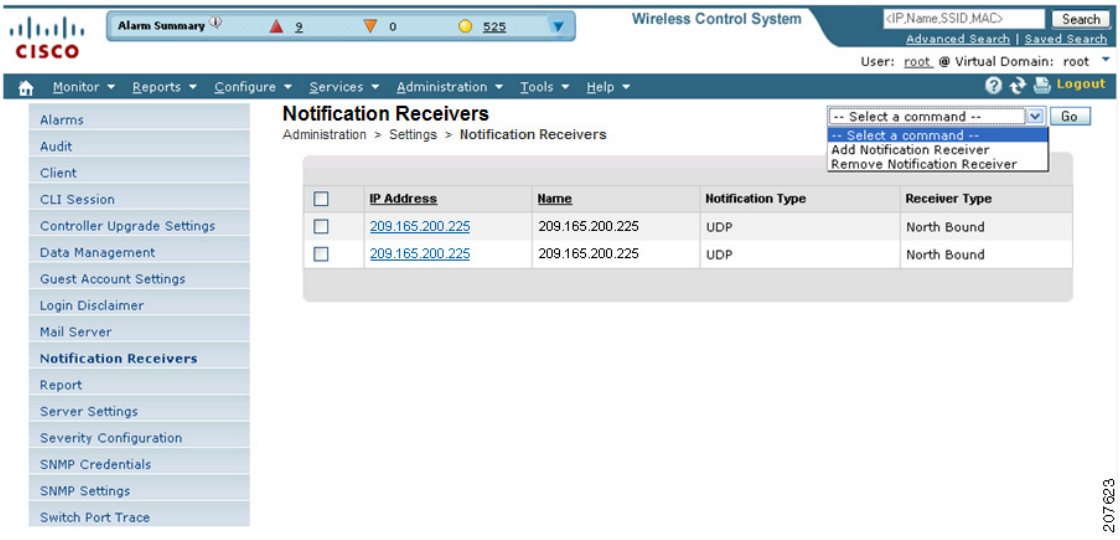
- Adding a Notification Receiver to WCS
- Removing a Notification Receiver

To access the Notification Receiver page, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Notification Receivers**. All currently configured servers appear in this page. If you want to add one, choose **Add Notification Receiver** from the Select a command drop-down list, and click **Go (see** Figure 18-29**)**.

Figure 18-29 Notification Receiver Page



Adding a Notification Receiver to WCS

Follow these steps to view current or add additional notification receivers:

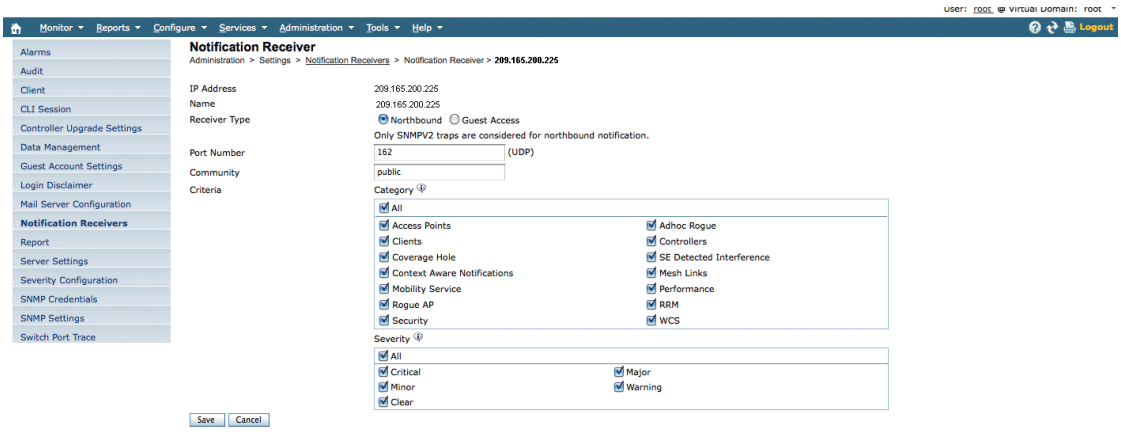
Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Notification Receivers**. All currently configured servers appear on this page.

Step 3 From the Select a command drop-down list, click **Add Notification Receiver**.

Step 4 Click **Go** (**see** Figure 18-29).

Figure 18-30 Notification Receiver Page



Step 5 Enter the server IP address and name.

Step 6 Choose the receiver type between basic North Bound and Guest Access.

The Notification Type automatically defaults to UDP.

Step 7 Enter the UDP parameters including Port Number and Community.

Note The receiver that you configure should be listening to UDP on the same port that is configured.

Step 8 If you have selected North Bound as the receiver type, specify the criteria and severity.

Note Alarms for only selected category will be processed.

Note Alarms with only selected severity matching the selected categories will be processed.

Step 9 Click **Save** to confirm the Notification Receiver information.

Note

- By default only INFO level events will be processed for selected Category.
- Only SNMPV2 traps will be considered for northbound notification.

Removing a Notification Receiver

To delete a notification receiver, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Notification Receivers**. All currently configured servers appear on this page.

Step 3 Select the check box(es) of the notification receiver(s) that you want to delete.

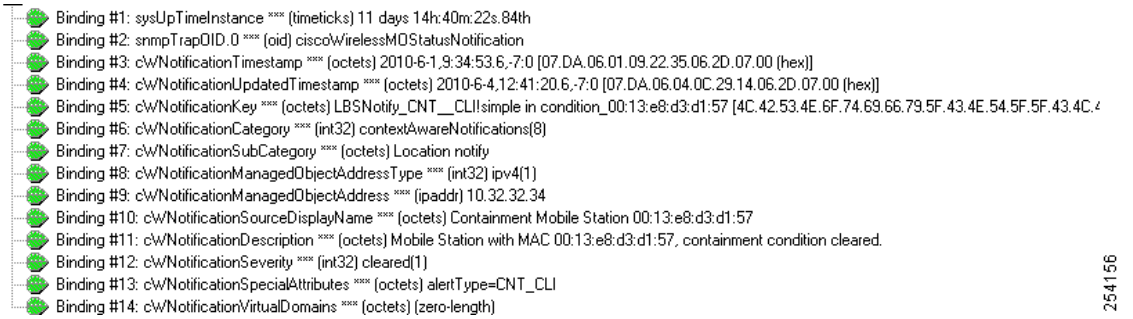
Step 4 From the Select a command drop-down list, click **Remove Notification Receiver**.

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the deletion.

The sample display from a northbound SNMP receiver that has received event traps from WCS is as follows:

Figure 18-31 Sample display from a northbound SNMP receiver



The sample output below shows the log file generated by WCS. This log file is located in the log file directory on the WCS server (/opt/WCS7.0.28.0/webnms/logs). The log output helps you troubleshoot when alarms are not being received by the northbound SNMP receiver.

```
06/04/10 08:30:58.559 INFO[com.cisco.wcslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]Adding into queue
06/04/10 08:30:58.560 INFO[com.cisco.wcslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]incrTotalNotifications2
06/04/10 08:30:58.560 INFO[com.cisco.wcslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]incrHandledInNotification2
06/04/10 08:30:58.560 INFO[com.cisco.wcslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]incrNonCongestedIn2
06/04/10 08:30:58.560 INFO[com.cisco.wcslogger.services] :
[NBNotificationService][addNBAlert]Added into queue
06/04/10 08:30:58.561 INFO[com.cisco.wcslogger.services] :
[NBNotificationService$NbOrderQueue][getNbAlarm]incrHandledOutNotification2
06/04/10 08:30:58.561 INFO[com.cisco.wcslogger.services] :
[NBNotificationService][startNotifier]Processing the
alertNoiseProfile_LradIf!00:17:df:a9:c8:30!0
06/04/10 08:30:58.561 INFO[com.cisco.wcslogger.notification] :
[NbAlertToNmsAlertCorrelator][formVarBindList]Generating the varbind list for NB
06/04/10 08:30:58.562 INFO[com.cisco.wcslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.2.1.1.3.0 variable value: 10 days, 20:22:17.26
06/04/10 08:30:58.562 INFO[com.cisco.wcslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.6.3.1.1.4.1.0 variable value:
1.3.6.1.4.1.9.9.199991.0.1
06/04/10 08:30:58.562 INFO[com.cisco.wcslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.2 variable value:
07:da:05:18:0c:30:0d:09:2d:07:00
06/04/10 08:30:58.563 INFO[com.cisco.wcslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.3 variable value:
07:da:06:04:08:1e:3a:04:2d:07:00
```

```
06/04/10 08:30:58.563 INFO[com.cisco.wcslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.4 variable value:
NoiseProfile_LradIf!00:17:df:a9:c8:30!0
06/04/10 08:30:58.563 INFO[com.cisco.wcslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.5 variable value: 2
06/04/10 08:30:58.563 INFO[com.cisco.wcslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.6 variable value: Radio
load threshold violation
06/04/10 08:30:58.563 INFO[com.cisco.wcslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.7 variable value: 1
06/04/10 08:30:58.564 INFO[com.cisco.wcslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.8 variable value:
172.19.29.112
06/04/10 08:30:58.564 INFO[com.cisco.wcslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.9 variable value: AP
1250-LWAP-ANGN-170-CMR, Interface 802.11b/g/n
06/04/10 08:30:58.564 INFO[com.cisco.wcslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.10 variable value:
Noise changed to acceptable level on '802.11b/g/n' interface of AP
'1250-LWAP-ANGN-170-CMR', connected to Controller '172.19.29.112'.
06/04/10 08:30:58.564 INFO[com.cisco.wcslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.11 variable value: 1
06/04/10 08:30:58.564 INFO[com.cisco.wcslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.12 variable value:
06/04/10 08:30:58.565 INFO[com.cisco.wcslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.14 variable value:
06/04/10 08:30:58.573 INFO[com.cisco.wcslogger.notification] : [NBUtil][sendTrap]OSS list
size with reachability status as up1
06/04/10 08:30:58.573 INFO[com.cisco.wcslogger.notification] : [NBUtil][sendTrap]Sending
UDP Notification for receiver:172.19.27.85 on port:162
```

MIB to WCS alert/event mapping

Table 18-3 summarizes the Cisco-WCS-Notification-MIB to WCS alert/event mapping.

Table 18-3 Cisco-WCS-Notification-MIB to WCS Alert/Event Mapping

Field Name and Object ID	Data Type	WCS Event/Alert field	Description
cWcsNotificationTimestamp	DateAndTime	createTime - NmsAlert eventTime - NmsEvent	Creation time for alarm/event.
cWcsNotificationUpdatedTimestamp	DateAndTime	modTime - NmsAlert	Modification time for Alarm. Events do not have modification time.
cWNotificationKey	SnmpAdminString	objectId - NmsEvent entityString- NmsAlert	Unique alarm/event ID in string form.

Table 18-3 Cisco-WCS-Notification-MIB to WCS Alert/Event Mapping (continued)

Field Name and Object ID	Data Type	WCS Event/Alert field	Description
cWcsNotificationSubCategory	OCTET STRING	Type field in alert and eventType in event.	This object represents the subcategory of the alert.
cWcsNotificationServerAddress	InetAddress	N/A	WCS IP address.
cWcsNotificationManagedObjectAddressType	InetAddressType	N/A	The type of Internet address by which the managed object is reachable. Possible values: 0 - unknown 1 - IPv4 2 - IPv6 3 - IPv4z 4 - IPv6z 16 - DNS Always set to "1" because WCS only supports ipv4 addresses.
cWcsNotificationManagedObjectAddress	InetAddress	getNode() value is used if present	getNode is populated for events and some alerts. If it is not null, then it will be used for this field.
cWcsNotificationSourceDisplayName	OCTET STRING	sourceDisplayName field in alert/event.	This object represents the display name of the source of the notification.
cWcsNotificationDescription	OCTET STRING	Text - NmsEvent Message - NmsAlert	Alarm description string.
cWcsNotificationSeverity	INTEGER	severity - NmsEvent, NmsAlert	Severity of the alert/event critical(1), major(2), minor(3), warning(4), clear(5), info(6), unknown(7).

Table 18-3 Cisco-WCS-Notification-MIB to WCS Alert/Event Mapping (continued)

Field Name and Object ID	Data Type	WCS Event/Alert field	Description
cWcsNotificationSpecialAttributes	OCTET STRING	All the attributes in alerts/events apart from the base alert/event class.	This object represents the specialized attributes in alerts like APAssociated, APDisassociated, RogueAPAlert, CoverageHoleAlert, etc. The string is formatted in 'property=value' pairs in CSV format.
cWNotificationVirtualDomains	OCTET STRING	N/A	Virtual Domain of the object that caused the alarm. This field is not populated for running release and this will be populated with empty string.

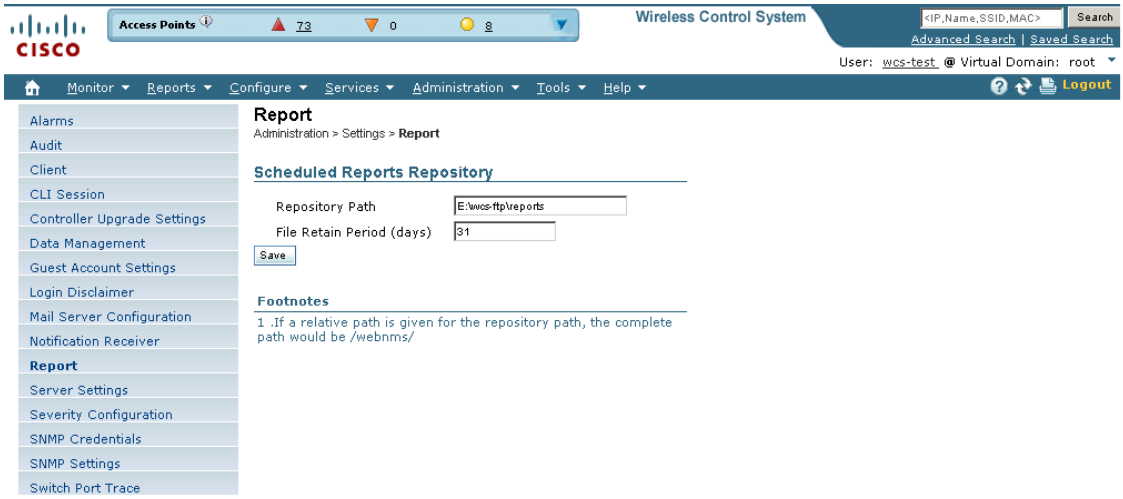
Report

Follow these steps to indicate where the scheduled reports will reside and for how many days:

Step 1 Choose **Administration > Setting**.

Step 2 From the left sidebar menu, choose **Report**. The Report page appears (see Figure 18-32).

Figure 18-32 Report Page



251932

Step 3 Enter the path for saving report data files on a local PC. You can edit the existing default path.

Step 4 Specify the number of days to retain report data files.

Step 5 Click **Save**.

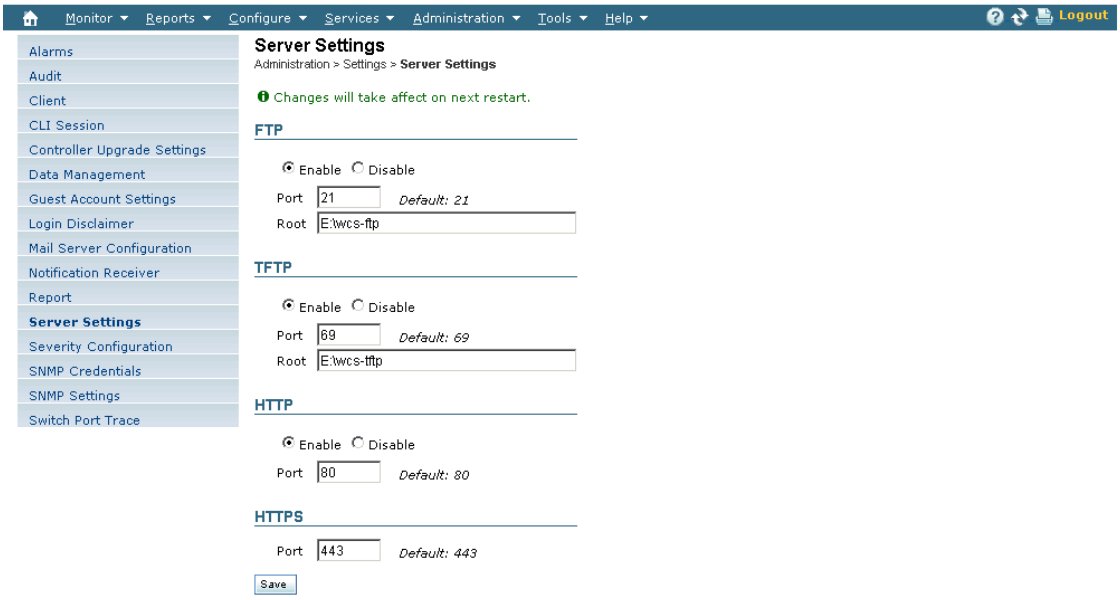
Server Settings

Follow these steps to turn TFTP, FTP, HTTP, or HTTPS on or off:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Server Setting**. The Server Setting page appears (see Figure 18-33).

Figure 18-33 Server Settings Page



Step 3 If you want to modify the FTP and TFTP directories or the HTTP and HTTPS ports that were established during installation, enter the port number (or port number and root where required) that you want to modify and click **Enable** or **Disable**.

The changes are reflected after a restart.

Severity Configurations

You can change the severity level for newly generated alarms.

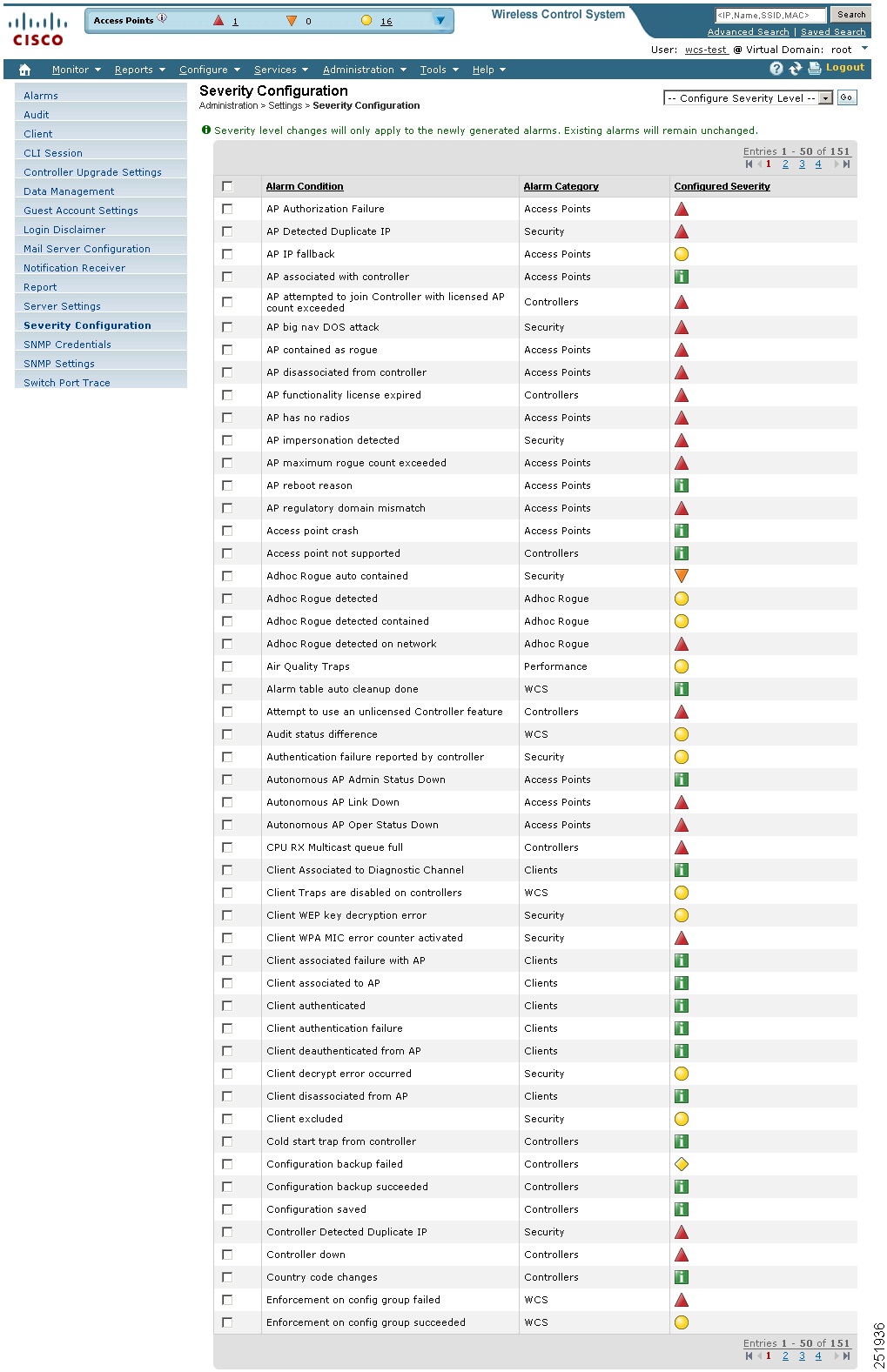
Note Existing alarms remain unchanged.

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. The Severity Configuration page appears (see Figure 18-34).

Figure 18-34 Severity Configuration Page



Step 3 Choose the check box of the alarm condition whose severity level you want to change.

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.

SNMP Credentials

The SNMP Credentials page allows you to specify credentials to use for tracing the rogue access points. Use this option when you cannot find a specific entry using a number-based entry. When a switch credential is not added to WCS, you can use SNMP credentials on this page to connect to the switch.

To configure SNMP credentials, follow these steps:

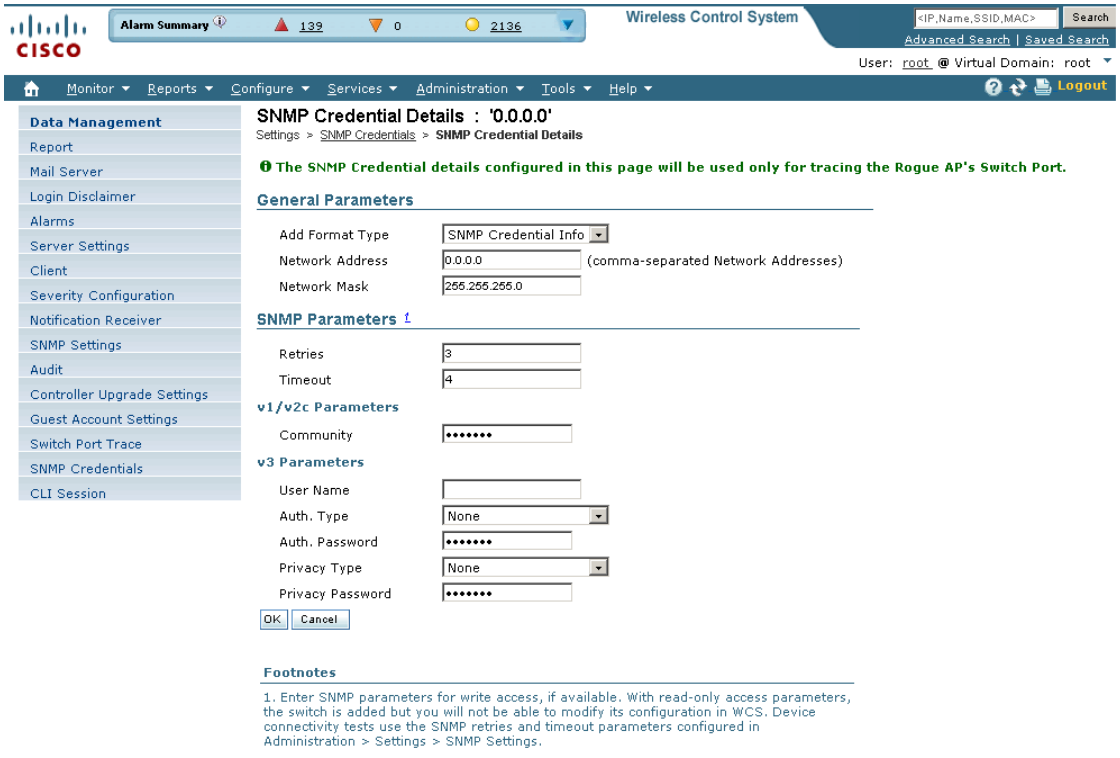
Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **SNMP Credentials**.

Step 3 Perform one of the following:

- To add a new SNMP entry, select **Add SNMP Entries** from the Select a command drop-down list, and click **Go**. The Credentials Details page appears.
- To modify an existing SNMP credential, click the **Network Address** link. The SNMP Credential Details page appears (see Figure 18-35). An SNMP credential is defined per network so only network addresses are allowed. 0.0.0.0 is the SNMP credential default and is used when no specific SNMP credential is defined. The default community string is *private* for both read and write. You should update the pre-populated SNMP credential with your own SNMP information.

Figure 18-35 SNMP Credential Details Page



Step 4 Choose one of the following:

If you want to add SNMP credentials or use commas to separate multiple SNMP credentials, leave the Add Format Type drop-down list at SNMP Credential Info.

If you want to add multiple SNMP credentials 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.

Step 5 If you chose SNMP Credential Info, enter the network address of the SNMP credential you want to add. If you want to add multiple SNMP credentials, use commas between network addresses. Make sure that SNMP credentials are correct so that switch port tracing executes as expected.

During SPT, if WCS finds switches and connects to them, WCS saves the switches internally. These switches are displayed in Configure > Ethernet Switches. When you update the SNMP credentials, the automatically added switches get deleted.

Step 6 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 IP address column is mandatory.

Sample File:

```
ip_address,snmpv1_community,snmpv2_community,snmpv3_user_name,snmpv3_auth_type,snmpv3_auth
_password,snmpv3_privacy_type,snmpv3_privacy_password,network_mask
209.165.200.224,private,private,user1,HMAC-MD5,12345,DES,12345,255.255.255.224
209.165.200.225,private,private,user1,HMAC-MD5,password3,DES,password4,255.255.255.224
209.165.200.226,private,private,user1,HMAC-MD5,12345,DES,12345,255.255.255.224
```

The CSV file can contain the following fields:

- ip_address: IP address

- network_mask: Network mask
- snmpv1_community: SNMP V1 community
- snmpv2_community: SNMP V2 community
- snmpv3_user_name: SNMP V3 user name
- snmpv3_auth_type: SNMP V3 authorization type. Can be None or HMAC-MD5 or HMAC-SHA
- snmpv3_auth_password: SNMP V3 authorization password
- snmpv3_privacy_type: SNMP V3 privacy type. Can be None or DES or CFB-AES-128
- snmpv3_privacy_password: SNMP V3 privacy password snmp_retries:SNMP retries
- snmp_timeout: SNMP timeout

Step 7 In the Retries parameter, enter the number of times an attempt is made to discover the switch.

Note Enter SNMP parameters for write access, if available. With read-only access parameters, the switch is added but you will not be able to modify its configuration in WCS. Device connectivity tests use the SNMP retries and timeout parameters configured in Administration > Settings > SNMP Settings.

Step 8 Enter the session timeout value in seconds. This value is the maximum amount of time allowed for a client before it must reauthenticate.

Step 9 If SNMP v1 or v2 with default community is configured, the network is open to easy attacks because default communities are well known. SNMP v1 or v2 with a non-default community is more secure than a default community, but SNMP v3 with Auth and Privacy type and no default user is the most secure SNMP connection.

Step 10 Click **OK**.

If WCS can use the SNMP credential listed to access the switch, the switch is added for later use and will appear on the Configure > Ethernet Switches page.

Note If you manually added switches through the Configure > Ethernet Switches page, switch port tracing will use the credentials from that page, not the ones listed on the SNMP Credentials page. If the manually added switch credentials have changed, you need to update them from the Configure > Ethernet page.

SNMP Settings

The SNMP Settings page allows you to configure global SNMP settings from WCS.

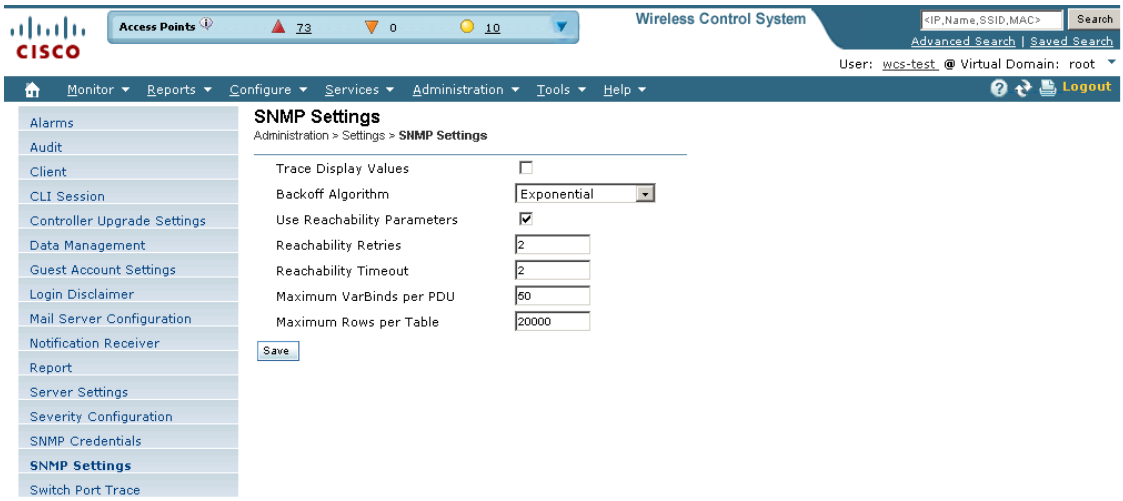
Note Any changes you make on this screen globally effect WCS. The changes are saved across restarts as well as across backups and restores.

Follow these steps to configure global SNMP settings:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **SNMP Settings**. The SNMP Settings page appears (see Figure 18-36).

Figure 18-36 SNMP Settings Page



251938

Step 3 If Trace Display Values is selected, mediation trace-level logging shows data values fetched from the controller using SNMP. If unselected, the values do not appear.

Note The default is unselected for security reasons.

Step 4 For the Backoff Algorithm, choose either **Exponential** or **Constant Timeout** from the drop-down list. If you choose Exponential (the default value), each SNMP try waits twice as long as the previous try, starting with the specified timeout for the first try. If you choose Constant Timeout, each SNMP try waits the same, specified amount of time.

Note Constant Timeout is useful on unreliable networks (such as satellite networks) where the desired number of retries is large. Because it does not double the timeout per try, it does not take as long to timeout with a high number of retries.

Step 5 Determine if you want to use reachability parameters. If selected, the WCS defaults to the global Reachability Retries and Timeout that you configure. If unselected, WCS always uses the timeout and retries specified per-controller or per-IOS access point. The default is selected.

Note Adjust this setting downward if switch port tracing is taking a long time to complete.

Step 6 For the Reachability Retries parameter, enter the number of global retries used for determining device reachability. The default number is 2. This parameter is only available if the Use Reachability Parameters check box is selected.

Note Adjust this setting downward if switch port tracing is taking a long time to complete.

Step 7 For the Reachability Timeout parameter, enter a global timeout used for determining device reachability. The default number is 2. This parameter is only available if the Use Reachability Parameters check box is selected.

Step 8 At the Maximum VarBinds per PDU parameter, enter a number to indicate the largest number of SNMP variable bindings allowed in a request or response PDU. The default is 100.

Note For customers who have issues with PDU fragmentation in their network, this number can be reduced to 50, which typically eliminates the fragmentation.

Step 9 Click **Save** to confirm these settings.

Switch Port Trace

The Switch Port Trace page allows you to run a trace on detected rogue access points on the wire.

To correctly trace and contain rogue access points, you must correctly provide the following information.

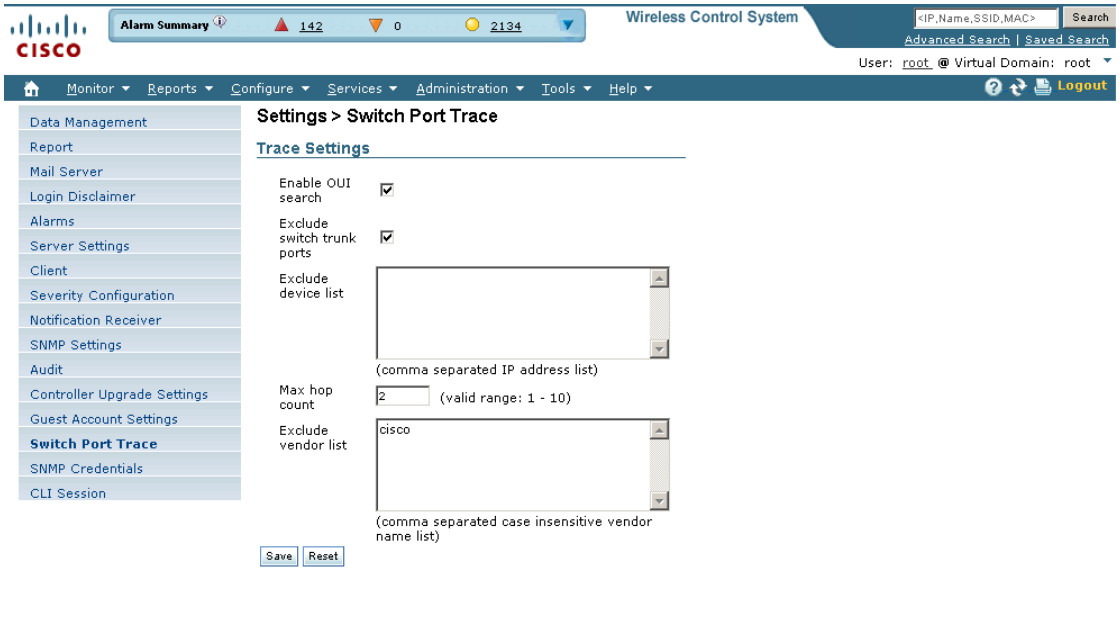
- Reporting APs—A rogue access point has to be reported by one or more managed access points.
- AP CDP Neighbor—Access point CDP neighbor information is required to determine the seed switches.
- Switch IP address and SNMP credentials—All switches to be traced must have a management IP address and SNMP management enabled. You can add network address based entries instead of only adding individual switches. The correct write community string must be specified to enable/disable switch ports. For tracing, read community strings are sufficient.
- Switch port configuration—Trunking switch ports must be correctly configured. Switch port security must be turned off.
- Only Cisco Ethernet switches are supported.
- Switch VLAN settings must be properly configured.
- CDP protocol must be enabled on all switches.
- An Ethernet connection must exist between the rogue access point and the Cisco switch.
- You should have some traffic between rogue access points and the Ethernet switch.
- The rogue access point must be connected to a switch within the max hop limit. The default hop count is 2, and the maximum is 10.
- If SNMPv3 is chosen, use the context option and create one for each VLAN, in addition to the one for the main group (which is required for non-VLAN-based MIBs).

Follow these steps to specify options for switch port tracing.

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Switch Port Trace** (see Figure 18-37).

Figure 18-37 Switch Port Trace Page



Step 3 Configure the following basic settings as needed:

- MAC address +1/-1 search—Select the check box to enable.

  This search involves the MAC address +1/-1 convention where the wired-side MAC address of the rogue access point is obtained by adding or subtracting the radio MAC address by one.

- Rogue client MAC address search—Select the check box to enable.

  When a rogue access point client exists, the MAC address of the client is added to the searchable MAC address list.

- Vendor (OUI) search—Select the check box to enable. OUI refers to Organizational Unique Identifier search which searches the first 3 bytes in a MAC address.

- Exclude switch trunk ports—Select the check box to exclude switch trunk ports from the switch port trace.

  Note When more than one port is traced for a given MAC address, additional checks are performed to improve accuracy. These checks include: trunk port, non-AP CDP neighbors present on the port, and whether or not the MAC address is the only one on this port.

- Exclude device list—Select the check box to exclude additional devices from the trace. Enter into the device list text box each device that you want to exclude from the switch port trace. Separate each device names with commas.

- Max hop count—Enter the maximum number of hops for this trace. Keep in mind that the greater the hop count, the longer the switch port trace will take to perform.

- Exclude vendor list—Enter in the vendor list text box any vendors that you want to exclude from the switch port trace. Separate vendor names with commas. The vendor list is not case sensitive.

Step 4 Configure the following advanced settings as needed:

- TraceRogueAP task max thread—Switch port tracing uses multiple threads to trace rogue access points. This field indicates the maximum number of rogue access points that can be traced on parallel threads.
- TraceRogueAP max queue size—Switch port tracing maintains a queue to trace rogue access points. Whenever you select a rogue access point for tracing, it is queued for processing. This field indicates the maximum number of entries that you can store in the queue.
- SwitchTask max thread—Switch port tracing uses multiple threads to query switch devices. This field indicates the maximum number of switch devices that you can query on parallel threads.

Note The default value for these parameters should be good for normal operations. These parameters directly impact the performance of switch port tracing and WCS. Unless required, Cisco does not recommend that you alter these parameters.

- Select CDP device capabilities—Select the check box to enable.

Note WCS uses CDP to discover neighbors during tracing. When the neighbors are verified, WCS uses the CDP capabilities field to determine whether or not the neighbor device is a valid switch. If the neighbor device is not a valid switch, it is not traced.

Step 5 Click **Save** to confirm changes made. Click **Reset** to return the page to the original settings. Click **Factory Reset** to return settings to the factory defaults.

High Availability

To ensure continued operation in case of failure, WCS now provides a high availability (or failover framework). When an active (primary) WCS fails, a secondary WCS takes over operations (in less than two minutes) for the failed primary WCS and continues to provide service. Upon failover, a peer of the failed primary WCS is activated on the secondary WCS using the local database and files, and the secondary WCS runs a fully functional WCS. While the secondary host is in failover mode, the database and file backups of other primary WCSs continue uninterrupted.

To activate and use high availability, you must buy a high availability license. The license is deployed on each primary WCS that is supported by a secondary WCS. After the license is validated, you must configure parameters on the WCS administration interface (see the "Configuring High Availability" section on page 18-64).

Failover Scenario

When a failure of a primary WCS is automatically detected, the following events take place:

Note One physical secondary WCS can back many primary WCSs.

1. The primary WCS is confirmed as non-functioning (hardware crash, network crash, or the like) by the health monitor on the secondary WCS.

2. If automatic failover has been enabled, WCS is started on the secondary as described in Step 3. If automatic failover is disabled, an email is sent to the administrator asking if they want to manually start failover.
3. The secondary WCS instance is started immediately (using the configuration already in place) and uses the corresponding database of the primary. After a successful failover, the client should point to the newly activated WCS (the secondary WCS). The secondary WCS updates all controllers with its own address as the trap destination.

   Note The redirecting of web traffic to the secondary WCS does not occur automatically. You must use your infrastructure tools to properly configure this redirection.

   MSEs that were served from the primary WCS are now served by the secondary WCS. Any Navigators in the network start monitoring the secondary WCS.
4. The result of the failover operation is indicated as an event in the Health Monitor UI, or a critical alarm is sent to the administrator and to other WCS instances.

Prerequisites and Limitations

Before initiating failover, you must consider the following prerequisites and limitations:

- You must have the extra hardware identical to the primary WCS to run a stand-by instance of WCS.
- This design is based on the software-based WCS and does not accommodate appliance-based WCS.
- The presence of Navigator is considered so that multi-WCS deployments are accommodated.
- A reliable high-speed wired network must exist between the primary WCS and its backup WCS.
- The primary and secondary WCS must be running the same WCS software release.
- WCS supports both Windows- or Linux-based platforms. However, for this failover design, all WCSs in the primary-secondary group must run on the same operating system (either Windows or Linux).
- Failover should be considered temporary. The failed primary WCS should be restored to normal as soon as possible, and failback will be re-initiated. The longer it takes to restore the failed primary WCS, the longer the other WCSs sharing that secondary WCS must run without failover support.
- The latest controller software must be used.
- The primary and secondary host are not required to share the same subnet. They can be geographically separated.
- If a secondary host fails for any reason, all the primary instances are affected, and they run in stand-alone mode without any failover support.
- The ports over which the primary and secondary WCSs communicate must be open (not blocked with network firewalls, application fireways, gateways, and so on). The tomcat port is configurable during installation, and its default port is 8082. You should reserve solid database ports from 1315 to 1319.
- Any access control lists imposed between the primary and secondary WCS must allow traffic to go between the primary and secondary WCSs.
- In a 2:1 high availability scenario, the secondary WCS must be a high-end PC with more memory than the two primary PCs.

Configuring High Availability

Note When database transaction logs grow to 1/3 of the database partition disk space, set the database to "Standalone" mode to prevent transaction logs from keep growing. But it requires a complete *netcopy* next time when the database synchronization occurs.

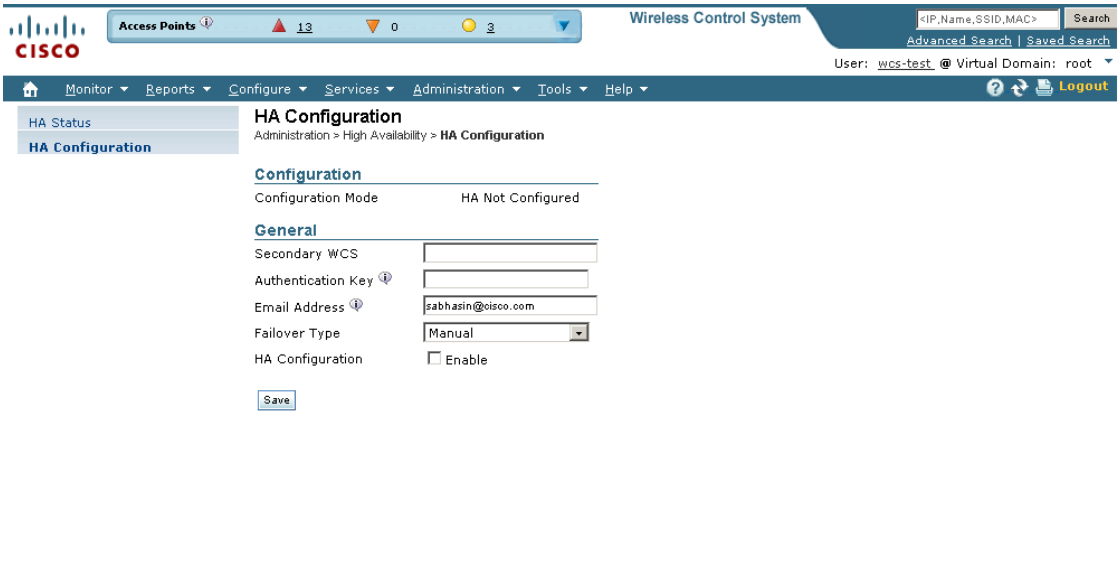
Follow these steps to configure high availability on the primary WCS. See the "Installing WCS for Windows" section on page 2-5 to see the installation steps.

Note Before you configure high availability, you must configure a mail server. See the "Mail Server Configuration" section on page 18-45 for steps on configuring a mail server.

Step 1 Choose **Administration > High Availability**.

Step 2 Choose **HA Configuration** from the left sidebar menu. The High Availability Configuration page appears (see Figure 18-38).

Figure 18-38 High Availability Configuration Page



The current status of high availability is shown in the upper portion of the page.

Step 3 Enter the IP address or hostname of the secondary WCS.

Step 4 Enter the authentication key specified during the installation of the secondary WCS.

Step 5 The default admin email address that you configured in Administration > Settings > Email Server is automatically supplied. You can make any necessary changes. Any changes you make to these email addresses must also be entered in the Secondary SMTP Server section of the Administration > Settings > Mail Server page.

Note You must enter an email address when configuring high availability. WCS tests the email server configuration, and if the test fails (because the mail server cannot connect), WCS does not allow the high availability configuration.

Step 6 Choose either a manual or automatic failover option. If you choose manual, you can trigger the failover operation with a button in the secondary HealthMonitor GUI or with the URL specified in the email which the administrator receives upon failure of the primary WCS. If you choose automatic, the secondary WCS initiates a failover on its own when a failure is detected on the primary.

Step 7 Click **Save Only** to retain the configuration but not enable high availability at the current time, or click **Save & Enable** to enable high availability.

At this point, the secondary is either reachable with the database, and files are synchronized between health monitors, or the secondary is unreachable, and an error is returned because secondary installation did not occur.

From the WCS GUI (Administration > High Availability) after high availability has been enabled, you can perform the following functions:

- Update—Use the Update function to make changes to the Report Repository path (Administration > Settings > Report) or FTP/TFTP root directory (Administration > Settings > Server Settings) and to appropriately synchronize the files.
- Disable—Use the Disable function to break the connection between the primary and secondary WCSs. The database and files stop synchronizing.
- Delete—Use the Delete operation to decommission the primary WCS from the secondary WCS.
- Cancel—User the Cancel operation to cancel any modifications you made to the high availability configuration. You are returned to the High Availability Status page after you choose Cancel.

Deploying High Availability

Follow these steps to deploy high availability on an existing WCS installation.

Step 1 Identify and prepare the hardware to run the secondary WCS.

Step 2 Ensure that network connectivity between the primary and secondary WCS is functioning, and all necessary ports are open.

Step 3 Install the secondary WCS with the same version of WCS that is installed on the primary. See the "Installing WCS for Windows" section on page 2-5.

Step 4 Start the secondary WCS as a standby server. In this mode, the WCS application does not start. At the same time, the Health Monitor is started on the secondary WCS.

Step 5 On every primary WCS that needs to use this secondary WCS, stop the WCS.

Step 6 On the primary host, install the new version of WCS and perform all necessary upgrade steps.

Step 7 Start the primary WCS (as a primary). See the "Starting WCS" section on page 2-16. The Health Monitor also starts.

Step 8 Configure the high availability parameters described in the "Configuring High Availability" section on page 18-64.

Step 9 Click **Activate** to activate high availability on the primary. WCS primary first copies its database to the secondary WCS and then connects to the secondary. The following files are copied over from the primary to the secondary WCS:

- DB password file
- all auto provisioning startup config files
- all domain maps
- all history reports which are generated by scheduled report tasks

High availability deployment is complete. Use https://<wcsip>:8082 to access the HealthMonitor UI. Within the HealthMonitor UI, use the root password to login.

To modify the health monitor authentication key, enter **hmadmin [-options] authKey [pass]**.

To view the current status of the health monitor, enter **hmadmin [-options] status**.

Adding a New Primary WCS

Follow these steps to add a new primary WCS to an existing setup. This new primary WCS uses the existing secondary as the failover server.

Step 1 Ensure that network connectivity between the new primary and secondary is functioning and that all necessary ports are open.

Step 2 Make sure that the same WCS release that is loaded on the other primary WCS and secondary WCS is loaded on the new primary WCS.

Step 3 Install the correct version of WCS on the primary WCS.

Step 4 Upgrade the primary WCS. The Health Monitor also starts.

Step 5 Follow the steps in the "Configuring High Availability" section on page 18-64.

Step 6 After the primary WCS connects to the secondary, the Health Monitor on the primary connects to the secondary Health Monitor. They mutually acknowledge each other and start the monitoring.

High availability deployment is now complete.

Removing a Primary WCS

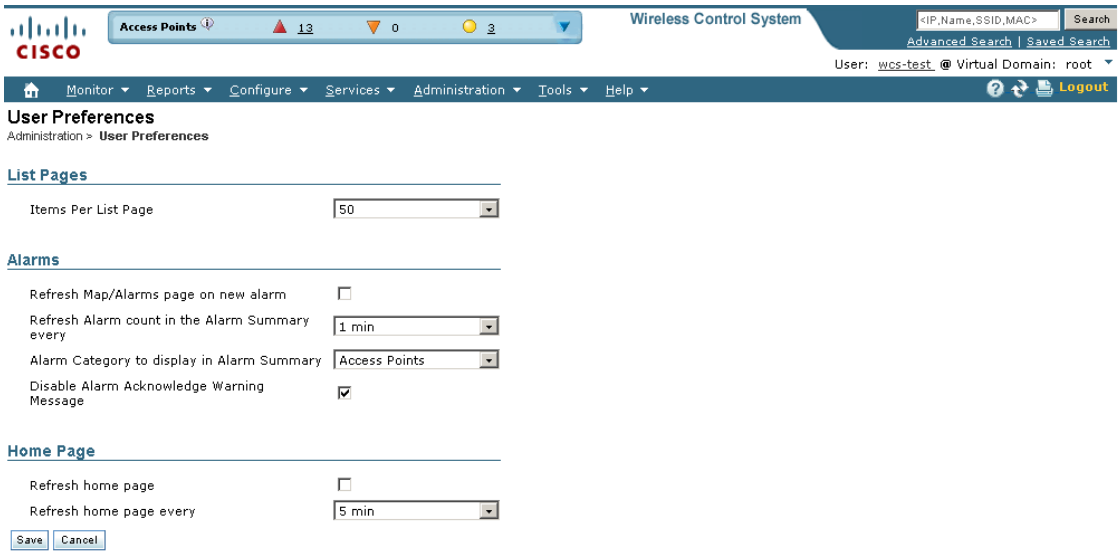
When a primary WCS instance is removed from a group, you must disable the peer database instance on the secondary WCS and remove the Health Monitor for that primary. (To remove the primary WCS from high availability, use the Remove button on the High Availability configuration page.) The secondary WCS disables the database instance and removes the uninstalled primary WCS from its Health Monitor.

Setting User Preferences

This page contains user-specific settings you may want to adjust.

Step 1 Choose **Administration > User Preferences**. The User Preferences Page appears (see Figure 18-39).

Figure 18-39 User Preferences Page



Step 2 Use the Items Per List Page drop-down list to configure the number of entries shown on a given list page (such as alarms, events, AP list, etc.).

Step 3 If you want the maps and alarms page to automatically refresh when a new alarm is raised by WCS, click the check box in the Alarms portion of the page.

Step 4 Use the drop-down list to indicate how often you want the alarm count refreshed in the Alarm summary page on the left panel. If you instead want to specify how often to reset, use the drop-down list to choose a time interval.

Step 5 Use the Alarm Category to display in Alarm Summary drop-down list to decide which alarm categories to display in the Alarm Summary page.

Step 6 If you do not want the alarm acknowledge warning message to appear, click the **Disable Alarm Acknowledge Warning Message** check box.

Step 7 Specify how often you want the home page refreshed by clicking the **Refresh home page** check box and choosing a time interval from the **Refresh home page every** drop-down list.

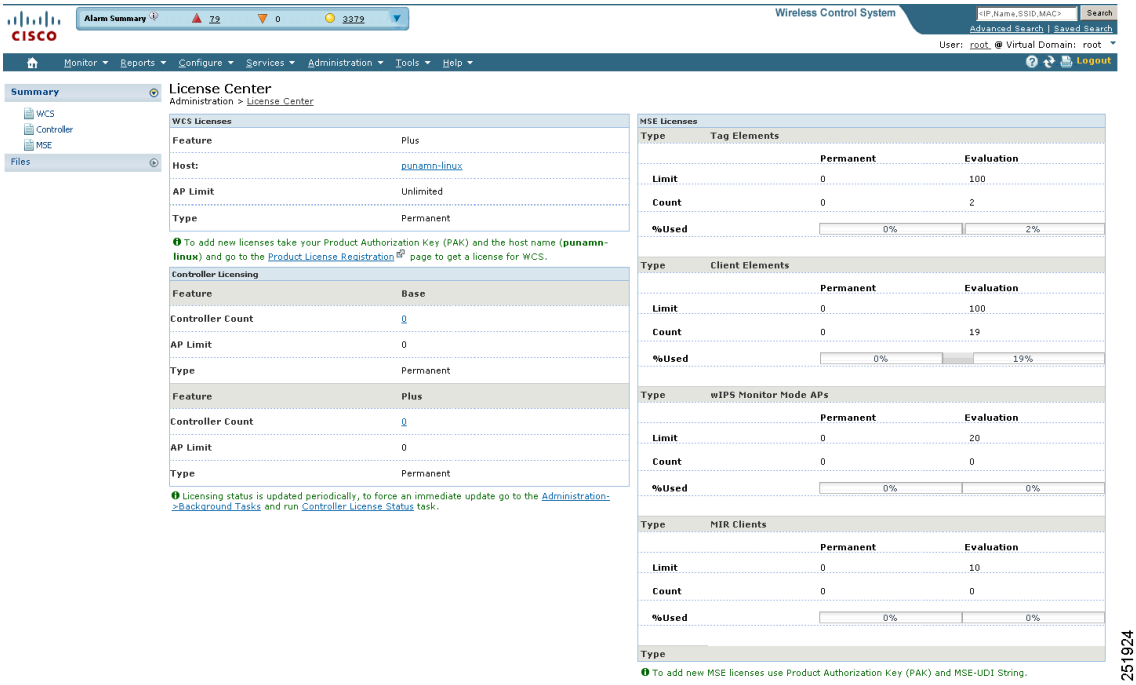
Step 8 Click **Save**.

Accessing the License Center

The License Center allows you to manage WCS, wireless LAN controllers, and MSE licenses. To view the License Center page, choose **Administration > License Center** (see Figure 18-40).

Note Although WCS and MSE licenses can be fully managed from the License Center, WLC licenses can only be viewed. You must use WLC or CLM to manage WLC licenses.

Figure 18-40 License Center



WCS License Information

The WCS Licenses portion of the License Center page displays the following:

- Feature—The type of license, either Base or PLUS. A *Base* license supports standard WCS capabilities, which includes wireless client data access, rogue access point containment functions, Cisco WLAN Solution monitoring and control, and client and rogue access point location to the nearest access point. Cisco WCS PLUS license supports Cisco WCS Base license features and the following capabilities: mobility services enablement and high availability.

Note To upgrade to a PLUS license, you must purchase upgrade licenses with the total count meeting or exceeding your Base license.

Note An older Cisco WCS Location license is forward-compatible and is equivalent to a PLUS license. When upgrading to this release, older Location licenses appear as PLUS licenses. Older Enterprise SKUs which generated Location licenses are also forward-compatible and become PLUS licenses when loaded. The process to provision a Cisco WCS PLUS license is the same as provisioning a current Cisco WCS license.

- Host—The WCS host name.

Note The host name provides a link to the WCS License Files section.

- AP Limit—The total number of licensed access points.
- AP Count—The current number of access points using licenses.

Note AP count includes both associated and unassociated access points. When you are near the AP limit, you can delete any unassociated access points to increase available license capacity. For a demo license, you can click the "If you do not have a Product Authorization Key (PAK), please click here for available licenses" link and choose **Wireless Control System Trial License**.

- % Used—The percentage of access points licensed across WCS. If the percentage drops to 75%, the value appears in red. At this level, a message also appears indicating that both associated and unassociated access points are part of the AP count.
- Type—Permanent if all licenses are permanent. If any licenses are evaluations (or demos), it shows the number of days remaining on the license that has the fewest number of days until expiration.

Note To add a new license for WCS, go to the Product License Registration link

(http://www.cisco.com/go/license/)

and provide your Product Authorization Key (PAK) and host name.

See the *Cisco Wireless Control System Licensing and Ordering Guide* at this location: http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd804b4646.html#wp9000156.

It covers selecting the correct SKU, ordering the SKU, installing the software, registering the PAK certificate, and installing the license file on the server.

See the "WCS Licenses" section on page B-1 for more information on licensing enforcement, PAK certificates, license types, and installing and managing WCS licenses.

Controller License Information

The Controller Licensing portion of the License Center page provides the following information for both WPLUS and Base licenses:

- Controller Count—The current number of licensed controllers.

Note Only 5500 series controllers are included in the count.

Note Clicking the number in this column is the same as choosing Summary > Controller from the left sidebar menu, except that it is sorted by the feature you click. This page provides a summary of active controllers.

- AP Limit—The total number of licensed access points.
- Type—The four different types of licenses are as follows:

Note For any controllers with a type other than Permanent, the least number of days left to expiration is shown.

- Permanent—Licenses are node-locked and have no usage period associated with them. They are issued by Cisco's licensing portal and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.
- Evaluation—Licenses are non-node-locked and are valid only for a limited period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node-locked, their usage is recorded on the device. The number of days remaining on the evaluation license that has the fewest number of days until expiration is shown.
- Extension—Licenses are node-locked and metered. They are issued by Cisco's licensing portal and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.
- Grace Period—Licenses are node-locked and metered. These licenses are issued by Cisco's licensing portal as part of the permission ticket to rehost a license. They are installed on the device as part of the rehost operation, and you must accept a EULA as part of the rehost operation.

If you need to revoke a license from one controller and install it on another, it is called *rehosting*. You might want to rehost a license in order to change the purpose of a controller. See Performing System Tasks of the *Cisco Wireless LAN Controller Configuration Guide* for information on rehosting a license.

Note The licensing status is updated periodically. To initiate an immediate update, go to Administration > Background Tasks and run the Controller License Status task.

If your network contains various Cisco licensed devices, you might want to consider using the Cisco License Manager (CLM) to manage all of the licenses using a single application. CLM is a secure client/server application that manages Cisco software licenses network wide. You can download the CLM software and access user documentation at this URL: http://www.cisco.com/go/clm. You can either register a PAK certificate with CLM or with the licensing portal found at http://www.cisco.com/go/license.

MSE License Information

The MSE Licenses portion of the License Center page provides the following information:

- Type—The four different types of licenses are as follows:
  - Permanent—Licenses are node-locked and have no usage period associated with them. They are issued by Cisco's licensing portal and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.
  - Evaluation—Licenses are non-node-locked and are valid only for a limited time period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node-locked, their usage is recorded on the device. The number of days remaining on the evaluation license which has the fewest number of days until expiration is shown.

  - Extension—Licenses are node-locked and metered. They are issued by Cisco's licensing portal and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.

- Tag Elements

Note In some cases, you may need to delete a license manually from an MSE before you can apply a tag license from the system manager. To get rid of a tag license, you must uninstall and reinstall MSE.

  - Limit—The total number of tag elements with licenses.
  - Count—The number of tag elements currently licensed across MSEs.
  - % Used—The percentage of tag elements licensed across MSEs.

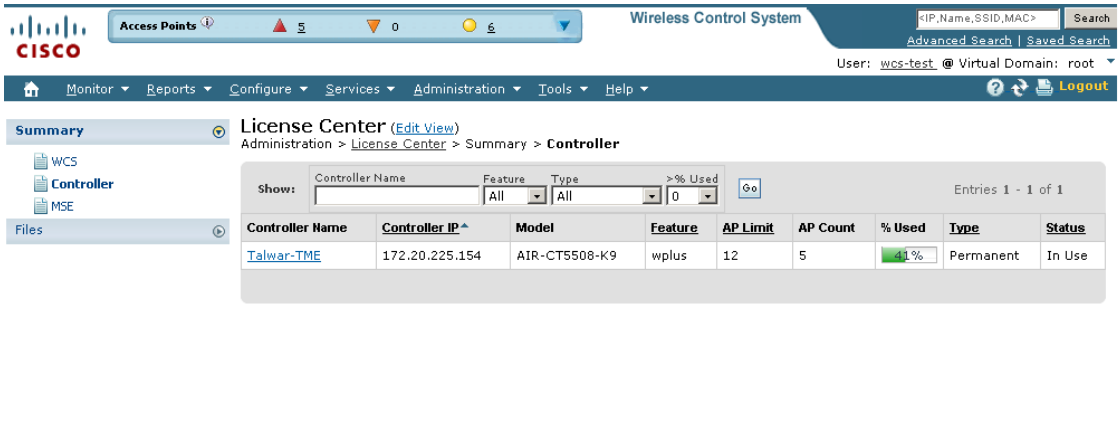
- Client Elements
  - Limit—The total number of client elements with licenses.
  - Count—The number of client elements currently licensed across MSEs.
  - % Used—The percentage of client elements licensed across MSEs.

- Monitor Mode APs
  - Limit—The total number of CAM access points licensed across MSEs.
  - Count—The number of CAM access points currently licensed across MSEs.
  - % Used—The percentage of CAM access points licensed across MSEs.

Controller

If you want to see more details about controller licensing, choose the **Summary > Controller** option from the left sidebar menu. The License Center page appears (see Figure 18-41). All currently active licenses on the controller are summarized.

Figure 18-41 License Center (Edit View) Page



251757

All licensed controllers and their information in the bulleted list below are displayed. If you want to change how the controller results are displayed, click **Edit View**. In the Edit View page, highlight **License Status**, and click **Hide** to remove the column from the display.

Above the Controller Summary list is a series of filters that allow you to filter the list by Controller Name, Feature, Type, or Greater Than Percent Used. For example, if you enter 50, the list shows any WLCs that have more than 50% of its licenses used.

Note You can also use the **Advanced Search** link to sort the list of controllers.

- Controller Name—Provides a link to the Files > Controller Files page.
- Controller IP—The IP address of the controller.
- Model—The controller model type.
- Feature—The type of license, either Base or WPLUS. The Base license supports the standard software set, and the WPLUS license supports the premium Wireless Plus (WPLUS) software set. The WPLUS software set provides the standard feature set as well as added functionality for OfficeExtend access points, CAPWAP data encryptions, and enterprise wireless mesh.
- AP Limit—The maximum capacity of access points allowed to join this controller.
- AP Count—The current number of access points using licenses.
- % Used—The percentage of licensed access points that are being used. If the percentage is greater than 75%, the bar appears red to indicate that the limit is being approached.
- Type—The four different types of licenses are as follows:

  Note For any controllers with a type other than Permanent, the least number of days left to expiration is shown.

  - Permanent—Licenses are node-locked and have no usage period associated with them. They are issued by Cisco's licensing portal and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.
  - Evaluation—Licenses are non-node-locked and are valid only for a limited time period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node-locked, their usage is recorded on the device. The number of days remaining on the evaluation license which has the fewest number of days until expiration is shown.
  - Extension—Licenses are node-locked and metered. They are issued by Cisco's licensing portal and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.

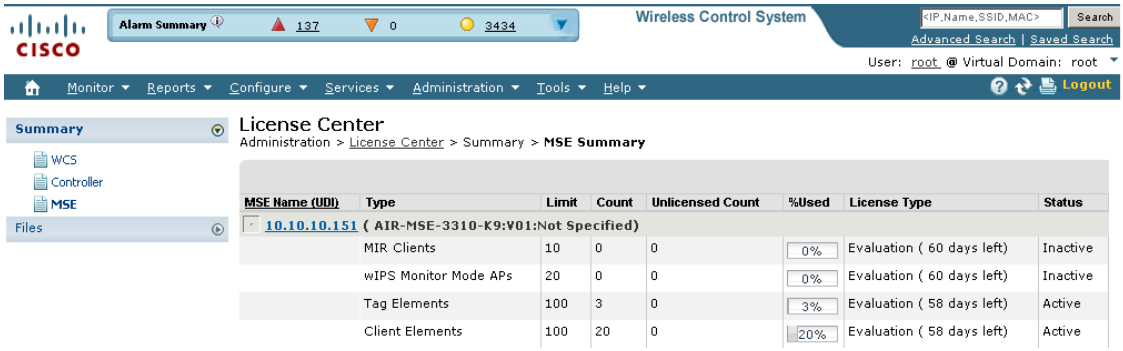
  Note If a license shows as expired, the controller does not stop functioning. Only upon a reboot will the controller with the expired license become inactive.

- Status—In Use, Not in Use, Inactive, or EULA Not Accepted.

MSE

If you want to see more details about MSE licensing, choose **Summary > MSE** from the left sidebar menu. The License Center page appears (see Figure 18-42).

Figure 18-42 License Center Page



251930

All licensed MSEs are listed in the following columns.

- MSE Name—Provides a link to the MSE license file list page.
- Type—Specifies the type of MSE.

Note Under wIPS Monitor Mode APs, an active link takes you to a list of licensed access points. You cannot access a list of licensed clients or tags.

- Limit—Displays the total number of client elements licensed across MSEs.
- Count—Displays the number of client elements that are currently licensed across MSEs.
- Unlicensed Count—Displays the number of client elements that are not licensed.
- % Used—Displays the percentage of clients used across all MSEs.
- License Type—The four different types of licenses are as follows:
  - Permanent—Licenses are node-locked and have no usage period associated with them. They are issued by Cisco's licensing portal and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.
  - Evaluation—Licenses are non-node-locked and are valid only for a limited time period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node-locked, their usage is recorded on the device. The number of days remaining on the evaluation license which has the fewest number of days until expiration is shown.

  - Extension—Licenses are node-locked and metered. They are issued by Cisco's licensing portal and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.

- Status
  - Active—License is installed and being used by a feature.
  - Inactive—License is installed but not being used by a feature.
  - Expired—License has expired.
  - Corrupted—License is corrupted.

Managing Individual Licenses

Managing Controller Licenses

Choose **Files > Controller Files** from the left sidebar menu to monitor the controller licenses.

Note WCS does not directly manage controller licenses. It simply monitors the licenses. You can manage the licenses using CLI, WebUI, or Cisco License Manager (CM) at:

www.cisco.com/go/license.

The page displays the following information:

- Controller Name
- Controller IP
- Feature—The feature options are wplus-ap-count, wplus, base-ap-count, and base. Two are active at any one time for an enable feature level of WPLUS or Base and the AP count (base-ap-count or wplus-ap-count), which determines the number of access points that the controller supports (12, 25, 50, 100, or 250). For every physical license installed, two license files show up in the controller as a feature level license and an ap-count license. For example, if you install a WPlus 500 license on the controller, you see a wplus or wplus-ap-count feature.

  Note You can have both a WPLUS and Base license, but only one can be active at a time.

- AP Limit—The number of access points that the controller supports.
- EULA Status—Whether the End User License Agreement has been accepted or not.
- Comments—Any user-entered comments about the license when it is installed.
- Type—Permanent, evaluation, or extension.

  Note For any controllers with a type other than Permanent, the number of days left to expiration is shown. A license is not in use does not incur the reduction in count until it is in use.

- Status —The status can be described as follows:
  - Inactive—The license level is being used, but this license is not in use.

- Not In Use—The license level is not being used, and this license is currently unrecognized.
- Expired in Use—The license is being used, but it is expired and will not be used upon next reboot.
- Expired Not in Use—The license has expired and can no longer be used.
- Count Consumed—The ap-count license is In Use.

All licensed controllers and their information are displayed. If you want to change how the controller results are displayed, click **Edit View**. In the Edit View page, use the **Show** and **Hide** buttons to determine how the columns appear.

Above the Controller Summary list is a series of filters that allow you to sort the list by Controller Name, Feature, or Type.

Managing WCS Licenses

Follow these steps to manage WCS licenses. For information on deciding on a license, types of licenses, installing a license, and backing up and restoring WCS licenses, refer to the "WCS Licenses" section on page B-1.

Step 1 Choose **Administration > License Center** to access the License Center page. It provides information about the WCS licenses, the controller license, and elements of MSE licenses.

For WCS licenses, the following is displayed:

- Feature
- Host name
- AP Limit
- AP Count (for specified number of access points)
- Capacity of licenses currently used
- Type

For controller licensing, the following is displayed:

- Feature
- Controller Count
- AP Limit
- Type

For tag elements, client elements, and wIPS Monitor Mode APs within MSE, the following is displayed:

- Limit
- Count
- % Used

Step 2 Choose **Files > WCS Files** from the left sidebar menu to see the following:

- Product Activation Key (PAK)
- the feature
- the access point limit
- type

You can click the check box of the desired license and either add or delete it.

Managing MSE Licenses

To manage MSE license, choose **Files > MSE Files** from the left sidebar menu. The page displays the MSE licenses found and includes the following information:

- MSE License File
- MSE Name
- Element Type
- Limit
- License Type

Note Evaluation extension and tag licenses are not displayed on this page.

With full WCS support, the complete functionality of CLM is embedded within WCS. You therefore have a single point of management for devices and their licenses.

If you need to search for a particular license file, you can choose an element type from the drop-down box, and click **Go**. For example, if you choose Client, and click Go, all license files with client licenses are returned.

Configuring ACS 5.x

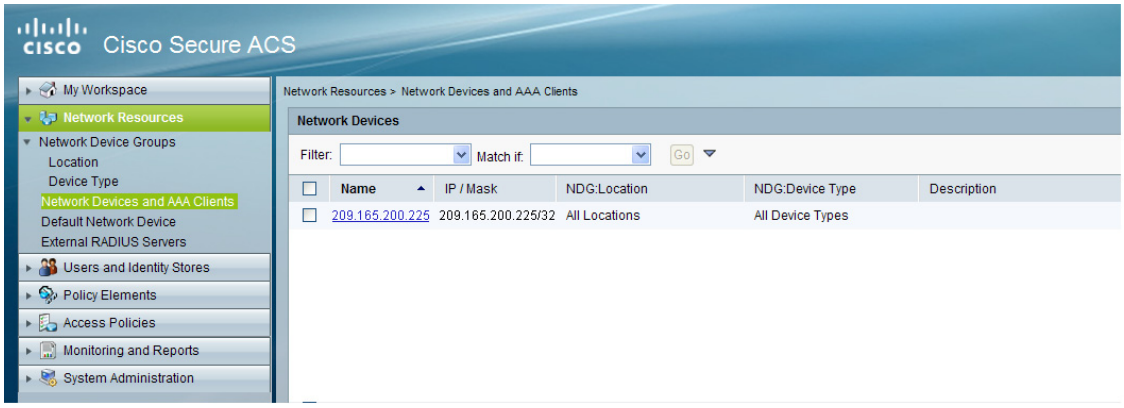
This section provides instructions for configuring ACS 5.x to work with WCS.

Creating Network Devices and AAA Clients

To create Network Devices and AAA Clients, perform the following steps:

Step 1 Choose **Network Resources > Network Devices and AAA Clients**.

Figure 18-43 Network Devices Page



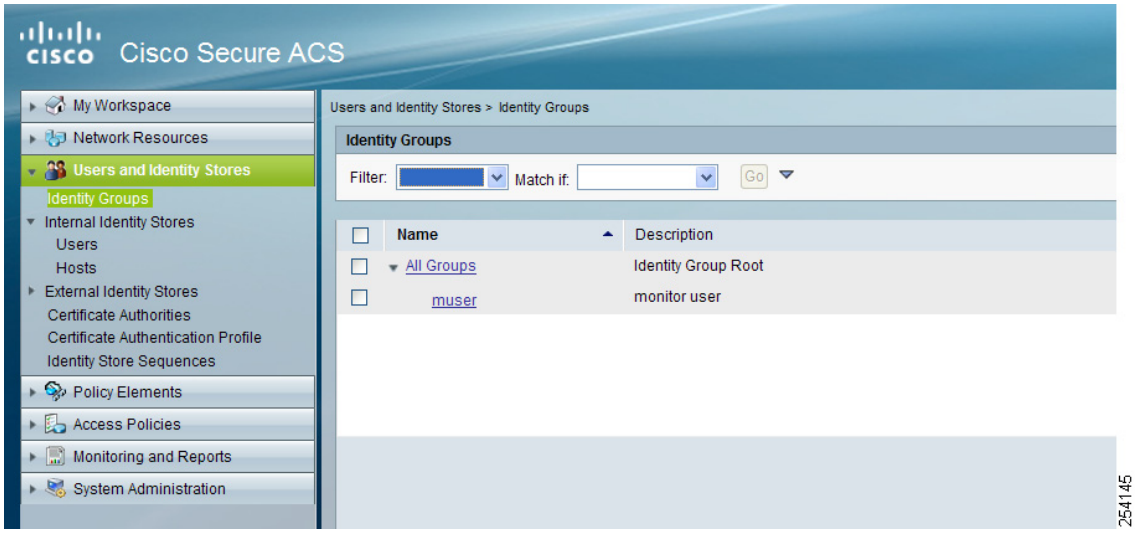
Step 2 Enter IP Address.

Adding Groups

To add groups, perform the following steps:

Step 1 Choose **Users and Identity Stores > Identity Groups.**

Figure 18-44 Identify Groups Page



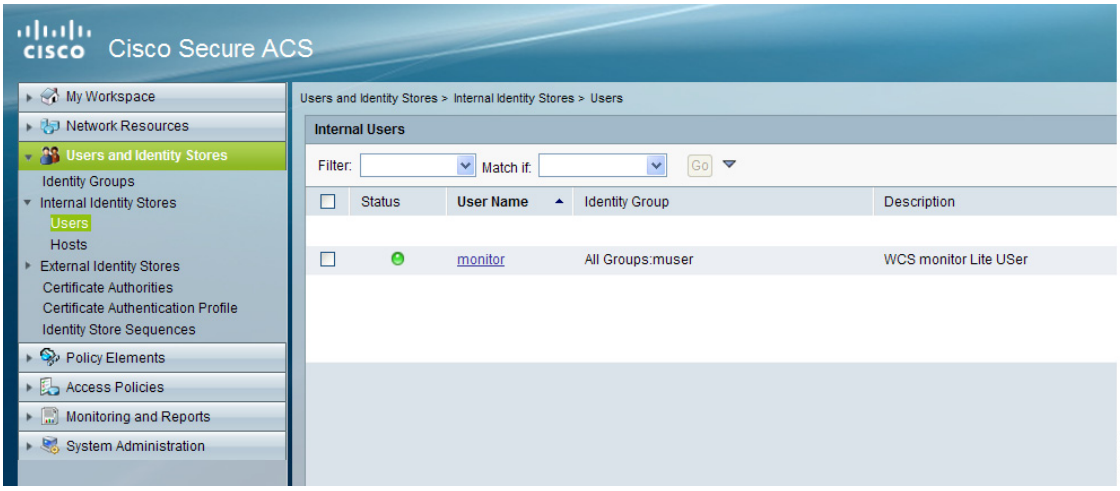
Step 2 Create a Group

Adding Users

To add users, perform the following steps:

Step 1 Choose **Users and Identity Stores > Internal Identity Stores > Users.**

Figure 18-45 Internal Users Page



Step 2 Add a user, and then map to group to that user.

Creating Policy Elements or Authorization Profiles

Creating Policy Elements or Authorization Profiles for RADIUS

To create policy elements or authorization profiles for RADIUS, perform the following steps:

Step 1 Choose **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**.

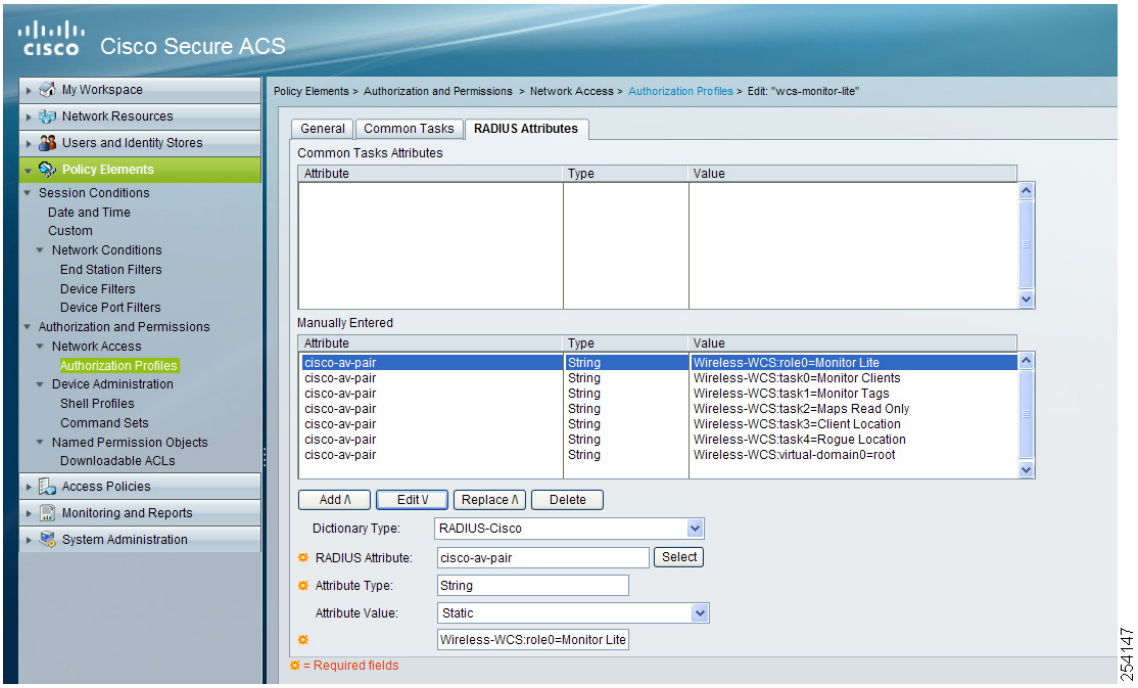
Step 2 Click **Create**.

Step 3 Enter Name and Description.

Step 4 Click the RADIUS Attributes tab.

Step 5 Add RADIUS Attributes one by one (see Figure 18-46).

Figure 18-46 Authorization Profiles Page



Step 6 Click **Submit**.

Creating Policy Elements or Authorization Profiles For TACACS

To create policy elements or authorization profiles for RADIUS, perform the following steps:

Step 1 Choose **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles.**

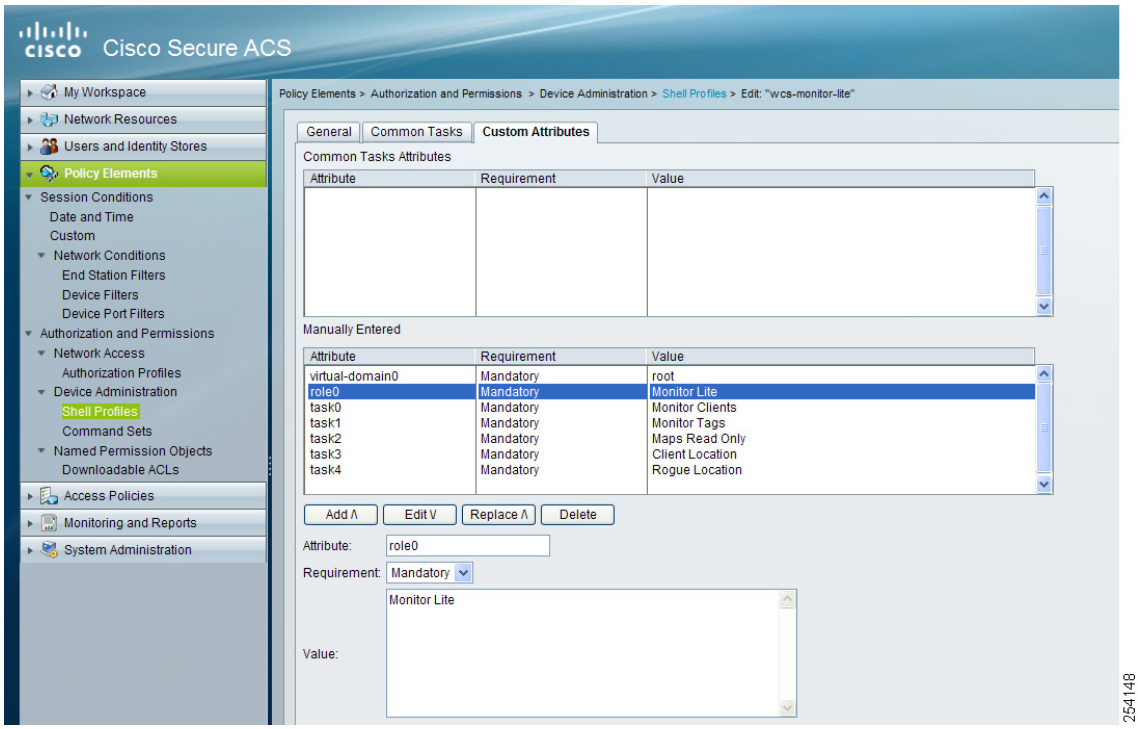
Step 2 Click **Create**.

Step 3 Enter Name and Description.

Step 4 Click the **Custom Attributes** tab.

Step 5 Add the TACACS Attributes one by one (see Figure 18-47).

Figure 18-47 Shell Profiles Page



Step 6 Click **Submit**.

Creating Authorization Rules

This section provides instructions for configuring authorization for RADIUS and TACACS.

Creating Service Selection Rules for RADIUS

To create service selection rules for RADIUS, perform the following steps:

Step 1 Choose **Access Policies > Access Services > Service Selection Rules**.

Step 2 Click **Create**.

Step 3 Select the protocol as Radius and service as Default Network Access (see Figure 18-48).

Figure 18-48 Service Selection Page

Step 4 Click **OK**.

Creating Service Selection Rules for TACACS

To create service selection rules for TACACS, perform the following steps:

Step 1 Choose **Access Policies > Access Services > Service Selection Rules**.

Step 2 Click **Create**.

Step 3 Select the protocol as TACACS and Service as Default Device Admin (see Figure 18-49).

Figure 18-49 Service Selection Page

Step 4 Click **OK**.

Configuring Access Services

This section provides instructions for configuring access services for RADIUS and TACACS.

Configuring Access Services for RADIUS

To configure access services for RADIUS, perform the following steps:

Step 1 Choose **Access Policies > Access Services > Default Network Access**.

Step 2 In the General tab, select the Policy Structure you want to use. By default all the three will be selected. Similarly, in Allowed Protocols, select the protocols you want to use.

Note You can retain the defaults for identity and group mapping.

Step 3 To create an authorization rule for RADIUS, choose **Access Policies > Access Services > Default Network Access > Authorization**.

Step 4 Click **Create**.

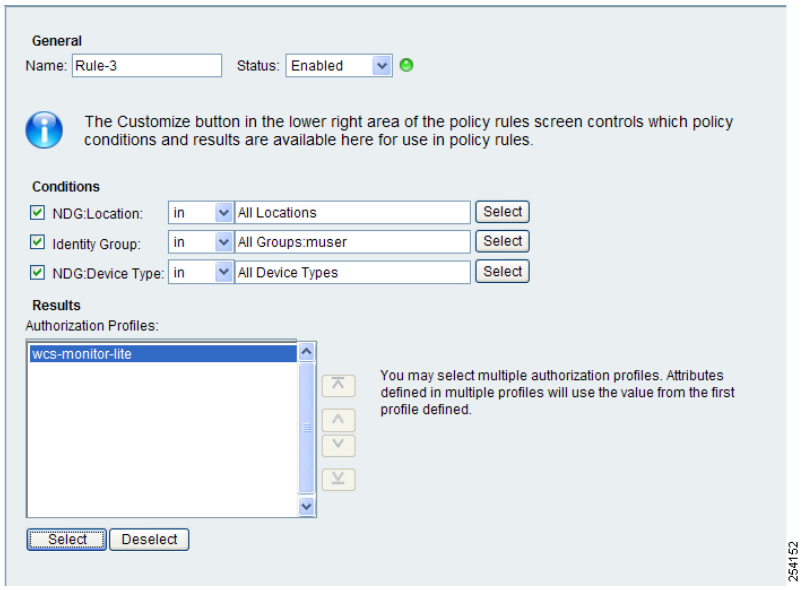
Step 5 In Location, select All Locations or you can create a rule based on the location.

Step 6 In Group, select the group that you created earlier.

Step 7 In Device Type, select All Device Types or you can create a rule based on the Device Type.

Step 8 In Authorization Profile, select the authorization profile created for RADIUS.

Figure 18-50 Authorization Page



Step 9 Click **OK**.

Step 10 Click **Save**.

Configuring Access Services for TACACS

To configure access services for TACACS, perform the following steps:

Step 1 Choose **Access Policies > Access Services > Default Device Admin**.

Step 2 In the General tab, select the Policy Structure you want to use. By default all the three will be selected. Similarly, in Allowed Protocols, select the protocols you want to use.

Note You can retain the defaults for identity and group mapping.

Step 3 To create an authorization rule for TACACS, choose **Access Policies > Access Services > Default Device Admin > Authorization**.

Step 4 Click **Create**.

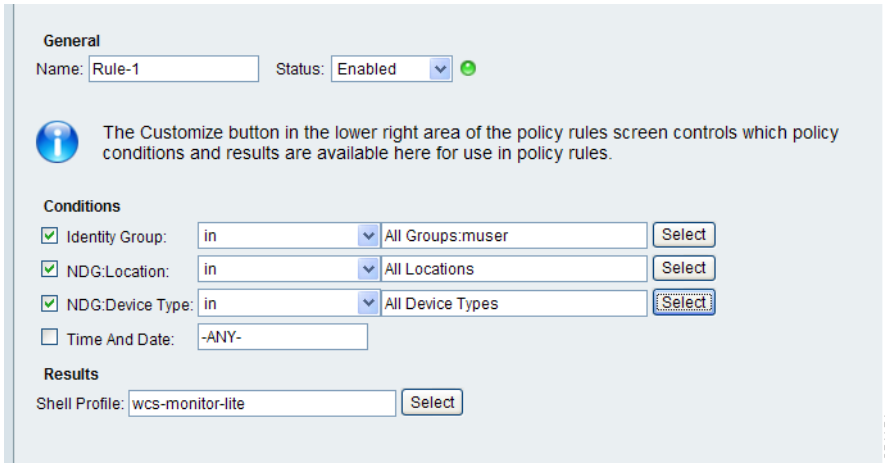
Step 5 In Location, select All Locations or you can create a rule based on the location.

Step 6 In Group, select the group that you created earlier.

Step 7 In Device Type, select All Device Types or you can create a rule based on the Device Type.

Step 8 In Shell Profile, select the shell profile created for TACACS.

Figure 18-51 Authorization Page



Step 9 Click **OK**.

Step 10 Click **Save**.

CHAPTER 19

Tools Menu

The Tools menu provides access to the Voice Audit, Location Accuracy Tool, Configuration Audit Summary, and Migration Analysis features of Cisco WCS.

Using Voice Audit

WCS provides an auditing mechanism to check the controller configuration and to ensure that any deviations from the deployment guidelines are highlighted as Audit Violation.

To access the Voice Audit feature, select **Tools > Voice Audit**.

The WCS Voice Audit has three tabs: Controllers, Rules, Reports.

Controller Tab

The Controllers tab allows you to choose the controller(s) on which to run the voice audit.

Note You can run the voice audit on a maximum of 50 controllers in a single operation.

To select the controller(s) for the voice audit, follow these steps:

Step 1 Choose **Tools > Voice Audit**.

Step 2 Click the **Controllers** tab.

Step 3 From the **Run audit on** drop-down list, select from **All Controllers**, a **Floor Area**, or a **Single Controller**.

- All Controllers—No additional Controller information necessary.
- A Floor Area—From the drop-down lists, select the applicable Campus, Building, Floor, and Controller.
- A Single Controller—Select the applicable controller from the drop-down list.

Step 4 Click the **Rules** tab to determine the rules for this voice audit. See Rules Tab for more information.

Rules Tab

The Rules tab allows you to indicate the applicable VoWLAN SSID and the applicable rules for this voice audit.

To indicate the rules for the voice audit, follow these steps:

Step 1 In the **Tools > Voice Audit** page, select the **Rules** tab.

Step 2 Type the applicable VoWLAN SSID in the **VoWLAN SSID** text box.

Step 3 From the **Rules List**, select the check boxes of the applicable rules for this voice audit (see Table 19-1).

Note The red circle indicates an invalid rule (due to insufficient data). The green circle indicates a valid rule.

Table 19-1 Rules List for Voice Audit

Rule	Rule Details
VoWLAN SSID	Description—Checks whether or not the VoWLAN SSID exists. Rule validity—User defined VoWLAN SSID.
CAC: 7920	Description—Checks whether or not 7920 AP CAC is enabled for VoWLAN. Rule validity—User defined VoWLAN SSID.
CAC: 7920 Clients	Description—Checks whether or not the 7920 Client CAC is disabled for VoWLAN. Rule validity—User defined VoWLAN SSID.
DHCP Assignment	Description—Checks whether or not DHCP assignment is disabled for VoWLAN. Rule validity—User defined VoWLAN SSID.
MFP Client	Description—Checks whether or not MFP Client protection is not set to **Required** for VoWLAN. Rule validity—User defined VoWLAN SSID.
Platinum QoS	Description—Checks whether or not QoS is set to Platinum (Voice) for VoWLAN. Rule validity—User defined VoWLAN SSID.
Non Platinum QoS	Description—Checks that QoS is not set to Platinum for non-VoWLAN. Rule validity—User defined VoWLAN SSID.
WMM	Description—Checks whether or not WMM is enabled for VoWLAN. Rule data—Select **Allowed** or **Required** from the drop-down list. Rule validity—User defined VoWLAN SSID.

Table 19-1 Rules List for Voice Audit

Rule	Rule Details
CCKM	Description—Checks whether or not CCKM is enabled for VoWLAN. Rule validity—User defined VoWLAN SSID.
ACM	Description—Checks whether or not Admission Control is enabled. Rule data—Select the check box for 802.11a/n ACM, 802.11b/g/n ACM, or both. Rule validity—At least one band must be selected.
DTPC	Description—Checks whether or not Dynamic Transmit Power Control is enabled. Rule data—Select the check box for 802.11a/n DTPC, 802.11b/g/n DTPC, or both. Rule validity—At least one band must be selected.
Expedited Bandwidth	Description—Checks whether or not Expedited Bandwidth is enabled. Rule data—Select the check box for 802.11a/n Expedited Bandwidth, 802.11b/g/n Expedited Bandwidth, or both. Rule validity—At least one band must be selected.
Load Based CAC	Description—Checks whether or not Load Based Admission Control (CAC) is enabled. Rule data—Select the check box for 802.11a/n Load Based CAC, 802.11b/g/n Load Based CAC, or both. Rule validity—At least one band must be selected.
CAC: Max Bandwidth	Description—Checks whether or not Maximum RF Bandwidth for Call Admission Control is configured properly. Rule data—Enter percentages in the text boxes for Maximum Allowed Bandwidth for 802.11a/n and 802.11b/g/n. Rule validity—Data for at least one band must be provided. Valid range is 0—100%.
CAC: Reserved Roaming Bandwidth	Description—Checks whether or not Reserved Roaming Bandwidth for Call Admission Control is configured properly. Rule data—Enter percentages in the text boxes for Maximum Reserved Roaming Bandwidth for 802.11a/n and 802.11b/g/n. Rule validity—Data for at least one band must be provided. Valid range is 0—100%.
Pico Cell mode	Description—Checks whether or not Pico Cell mode is disabled. Rule data—Select the check boxes for 802.11a/n Pico Cell mode, 802.11b/g/n Pico Cell mode, or both. Rule validity—At least one band must be selected.

Table 19-1 Rules List for Voice Audit

Rule	Rule Details
Beacon Period	Description—Checks whether or not Beacon Period is configured properly. Rule data—Enter the time (ms) in the text boxes for Beacon Period for 11a/n and 11b/g/n. Rule validity—Data for at least one band must be provided. Valid range is 20—1000. Enter 0 or keep it empty if a band should not be checked.
Short Preamble	Description—Checks whether or not Short Preamble is enabled for 11b/g.
Fragmentation Threshold	Description—Checks whether or not Fragmentation Threshold is configured properly. Rule data—Enter the threshold amount (bytes) in the text boxes for Fragmentation Threshold for 11a/n and 11b/g/n. Rule validity—Data for at least one band must be provided. Valid range is 256—2346. Enter 0 or keep it empty if a band should not be checked.
Data Rate	Description—Checks whether or not Data Rates are configured properly. Data Rate configuration for 11b/g—Select **Disabled**, **Supported**, or **Mandatory** for each Mbps category. Data Rate configuration for 11a—Select **Disabled**, **Supported**, or **Mandatory** for each Mbps category.
Aggressive Load Balancing	Description—Checks whether or not Aggressive Load Balancing is disable.
QoS Profile	Description—Checks that QoS Profiles are not altered from default values.
EAP Request Timeout	Description—Checks whether or not EAP Request Timeout is configured properly. Rule data—Enter the time limit (sec) for the EAP Request Timeout Rule validity—Data cannot be left blank or as zero. Valid range is 1—120.
ARP Unicast	Description—Checks whether or not ARP Unicast is disabled.

Note Use the **Reset** button to reset the rules to the default configuration.

Step 4 When the rules are configured for this voice audit, click **Save** to save the current configuration or **Save and Run** to save the configuration and run the report.

Step 5 Click the **Report** tab to view the Report results. See Reports Tab for more information.

Reports Tab

The Voice Audit Report provides a summary of the voice audit details and report results.

- Voice Audit Details
- Voice Audit Report Results

Voice Audit Details

The Voice Audit details provides the following information:

- Audit Status—Indicates whether or not the audit is complete.
- Start Time and End Times—Indicates the time at which the voice audit began and ended.
- # Total Devices—Indicates the number of devices involved in the voice audit.
- # Completed Devices—Indicates the number of devices the tool attempted to audit.

Note If a controller is unreachable, the audit skips it. The Voice Audit will not complete any rule checks for that controllers.

- # Rules—Indicates the number of rules selected for the voice audit.

Voice Audit Report Results

The Voice Audit Report results include the following information:

- IP Address—Indicates the IP Address for the controller involved in the voice audit.
- Rule—Indicates the rule that was applied for this controller.
- Result—Indicates the result (Skipped, Violation, Unreachable) of the applied rule.

Note If there is no mismatch between the current configuration and a rule value, no results are displayed for that rule.

- Details—Defines an explanation for the rule results.

Note If the applied rule results in a Violation, the Details link provides additional information including Name, the Device Value, and the Rule Value. Hold your mouse cursor over the link to view the additional details.

- Time—Provides a timestamp for the voice audit.

Verifying Location Accuracy

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.

You can analyze the location accuracy of non-rogue and rogue clients and asset tags by using the Accuracy Tool.

The Accuracy Tool enables you to run either a scheduled or on-demand location accuracy test. Both tests are configured and executed through a single page.

Using the Location Accuracy Tool to Test Location Accuracy

There are two ways to test location accuracy:

- Scheduled Accuracy Testing–Employed when clients and tags are already deployed and associated to the wireless LAN infrastructure. Scheduled tests can be configured and saved when clients and tags are already pre-positioned so that the test can be run on a regularly scheduled basis.
- On-Demand Accuracy Testing–Employed when elements are associated but not pre-positioned. On demand testing allows you to test the location accuracy of clients and tags at a number of different locations. It is generally used to test the location accuracy for a small number of clients and tags.

Both are configured and executed through a single page.

Note You must enable the **Advanced Debug** option in Cisco WCS to use the Scheduled and On-demand location accuracy testing features. The Location Accuracy Tool does not appear as an option under the Tools menu when the Advanced Debug option is not enabled.

To enable the advanced debug option in Cisco WCS, follow these steps:

Step 1 In Cisco WCS, choose **Monitor > Maps**.

Step 2 Select **Properties** from the Select a command drop-down list, and click **Go**.

Step 3 In the page that appears, select **Enabled** for the Advanced Debug Mode option. Click **OK**.

Note If Advanced Debug is already enabled, you do not need to do anything further. Click **Cancel**.

You can now run location accuracy tests on the mobility services engine using the Location Accuracy Tool.

Proceed to either the "Using Scheduled Accuracy Testing to Verify Accuracy of Current Location" or "Using On-Demand Location Accuracy Testing" section.

Using Scheduled Accuracy Testing to Verify Accuracy of Current Location

To configure a scheduled accuracy test, follow these steps:

Step 1 Choose **Tools > Location Accuracy Tool**.

Step 2 Choose **New Scheduled Accuracy Test** from the Select a command drop-down list.

Step 3 Enter a test name.

Step 4 Select an area type from the drop-down list.

Step 5 Campus is configured as Root Area by default. There is no need to change this setting.

Step 6 Choose the building from the drop-down list.

Step 7 Choose the floor from the drop-down list.

Step 8 Choose the begin and end time of the test by entering the days, hours, and minutes. Hours are represented using a 24-hour clock.

Note When entering the test start time, be sure to allow enough time prior to the test start to position testpoints on the map.

Step 9 Choose the destination point for the test results. You can have the report emailed to you or you can download the test results from the Accuracy Tests > Results page. Reports are in PDF format.

Note If you select the email option, a SMTP Mail Server must first be defined for the target email address. Choose **Administrator > Settings > Mail Server Configuration** to enter the appropriate information.

Step 10 Click **Position Testpoints**. The floor map appears with a list of all clients and tags on that floor with their MAC addresses.

Step 11 Click the check box next to each client and tag for which you want to check the location accuracy.

When you select the MAC address check box for a client or tag, two overlapping icons appear on the map for that element.

One icon represents the actual location and the other the reported location.

Note To enter a MAC address for a client or tag that is not listed, select the **Add New MAC** check box and enter the MAC address, and click **Go**. An icon for the element appears on the map. If the newly added element is on the mobility services engine but on a different floor, the icon appears in the left corner (0,0 position).

Step 12 If the actual location for an element is not the same as the reported location, drag the actual location icon for that element to the correct position on the map.

Note Only the actual location icon can be dragged.

Step 13 Click **Save** when all elements are positioned. A page appears confirming successful accuracy testing.

Step 14 Click **OK** to close the confirmation page. You are returned to the Accuracy Tests summary page.

Note The accuracy test status appears as Scheduled when the test is about to execute. A status of Running appears when the test is in progress and Idle when the test is complete. A Failure status appears when the test is not successful.

Step 15 To view the results of the location accuracy test, click **Test name** and then click **Download** on the page that appears.

The Scheduled Location Accuracy Report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges

- An error distance histogram
- A cumulative error distribution graph
- An error distance over time graph
- A summary by each MAC address whose location accuracy was tested noting its actual location, error distance and a map showing its spatial accuracy (actual vs. calculated location) and error distance over time for each MAC.

Using On-Demand Location Accuracy Testing

An on-demand accuracy test is run when elements are associated but not pre-positioned. On-demand testing allows you to test the location accuracy of clients and tags at a number of different locations. You generally use it to test the location accuracy for a small number of clients and tags.

To run an on-demand accuracy test, follow these steps:

Step 1 Choose **Tools > Location Accuracy Tool**.

Step 2 Choose **New On demand Accuracy Test** from the Select a command drop-down list.

Step 3 Enter a test name.

Step 4 Select the area type from the drop-down list.

Step 5 Campus is configured as root area by default. There is no need to change this setting.

Step 6 Choose the building from the drop-down list.

Step 7 Choose the floor from the drop-down list.

Step 8 View test results in the Accuracy Tests > Results page. Reports are in PDF format.

Step 9 Click **Position Testpoints**. The floor map appears with a red cross hair at the (0,0) coordinate.

Step 10 To test the location accuracy and RSSI of a location, select either client or tag from the drop-down list on the left. A list of all MAC addresses for the selected option (client or tag) appear in a drop-down list to its right.

Step 11 Select a MAC address from the drop-down list, move the red cross hair to a map location, and click the mouse to place it.

Step 12 Click **Start** to begin collecting accuracy data.

Step 13 Click **Stop** to finish collecting data. You should allow the test to run for at least two minutes before clicking Stop.

Step 14 Repeat Step 10 to Step 13 for each testpoint that you want to plot on the map.

Step 15 Click **Analyze** when you are finished mapping the testpoints.

Step 16 Click the **Results** tab on the page that appears.

The on-demand accuracy report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges
- An error distance histogram
- A cumulative error distribution graph

Step 17 To download accuracy test logs from the Accuracy Tests summary page:

a. Select the listed test check box and select either **Download Logs** or **Download Logs for Last Run** from the Select a command menu.

b. Click **Go**.

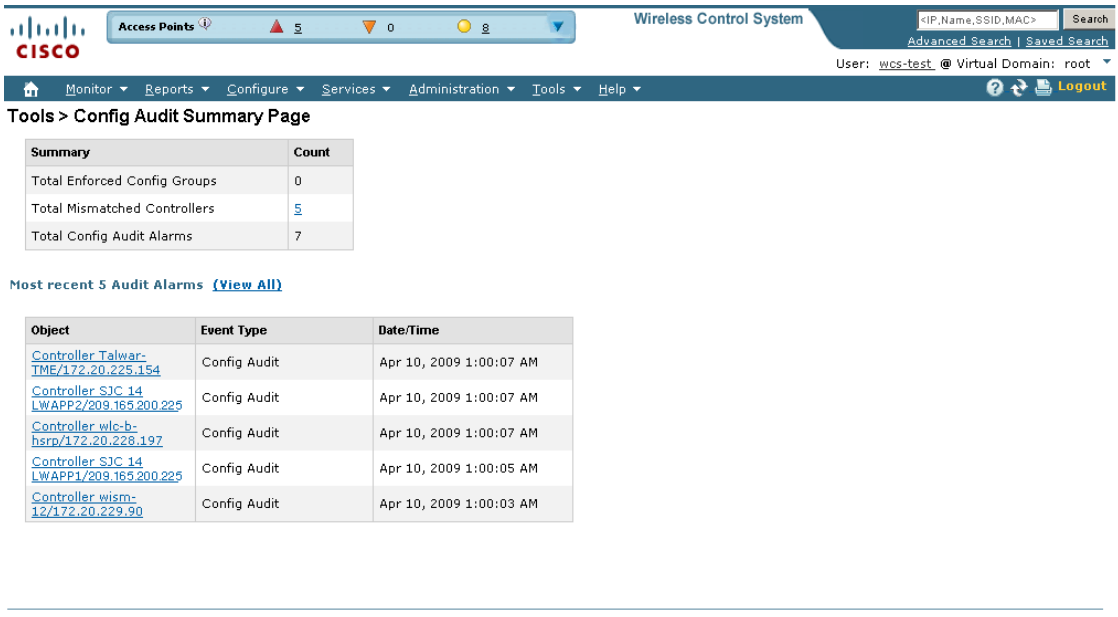
The Download Logs option downloads the logs for all accuracy tests for the selected test(s).

The Download Logs for Last Run option downloads logs for only the most recent test run for the selected test(s).

Viewing Configuration Audit Summary

Choose **Tools > Config Audit** to launch the Configuration Audit Summary page (see Figure 19-1).

Figure 19-1 Tools > Config Audit Summary Page



This page provides a summary of the following:

- Total Enforced Config Groups—Identifies the count of config group templates which are configured for Background Audit and enforcement enabled.

  Click the link to launch the Config Group page to view config groups with **Enforce Configuration** enabled.

- Total Mismatched Controllers—Identifies the number of mismatched controllers. Mismatched controllers indicate that there were configuration differences found between the WCS and the controller during the last audit.

  Click the link to launch the controller list sorted on the mismatched audit status column. Click an item in the Audit Status column to view the audit report for this controller.

- Total Config Audit Alarms—Identifies the number of alarms generated when audit discrepancies are enforced on config groups.

  Click the link to view all config audit alarm details.

  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 list of discrepancies for each controller.

- Most recent 5 audit alarms—Lists the most recent configuration audit alarms including the object name, event type, and date and time for the audit alarm.

  Click **<View All>** to view the applicable Alarm page which includes all configuration audit alarms.

Configuring Migration Analysis

Follow these steps to view the Migration Analysis Summary.

Note You can also access the migration analysis summary by choosing **Configure > Migration Templates** and selecting **View Migration Analysis Summary** from the Select a command drop-down list.

Step 1 Choose **Tools > Migration Analysis**.

The autonomous access points are eligible for migration only if all the criteria has 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—Conversion is supported only from 12.3(7)JA releases 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.

Upgrading Autonomous Access Points

You can choose to upgrade the autonomous access points manually or automatically. In the Migration Analysis page, you can select the access point with the software version listed as failed and choose **Upgrade Firmware** from the Select a command drop-down list. This process upgrades the autonomous firmware image of the Cisco IOS access point to a supported version.

WCS uses a Telnet-based connection to upgrade the access point firmware. If you choose the automatic option, the internal TFTP server is used with the default images present in WCS. The default images as per device type are as follows:

- ap801-k9w7-tar.124-10b.JA3.tar
- c1100-k9w7-tar.123-7.JA5.tar
- c1130-k9w7-tar.123-7.JA5.tar
- c1200-k9w7-tar.123-7.JA5.tar
- c1240-k9w7-tar.12307.JA5.tar
- c1250-k9w7-tar.124-10b.JA3.tar
- c1310-k9w7-tar.123-7.JA5.tar

If you choose the manual option, you are presented with an additional screen where TFTP server IP, file path, and file path name must be entered. The final page is the report page.

Viewing a Firmware Upgrade Report

Choose **View Firmware Upgrade Report** from the Select a command drop-down list to view a current report of the upgrade status for the selected access point.

The following information displays:

- AP Address—IP address of the access point.
- Status—Current status of the firmware upgrade.
- TimeStamp—Indicates the date and time of the upgrade.
- AP Logs

Click **OK** to return to the Migration Analysis Summary page.

See "Upgrading Autonomous Access Points" section on page 19-11 for more information.

Changing Station Role to Root Mode

Because a wired connection between the access point and controller is required to send the association request, the autonomous access point must be assigned the appropriate role. If the role shows as ineligible, you can choose **Change Station Role to Root Mode** from the Select a command drop-down list.

Viewing a Role Change Report

Because a wired connection between the access point and controller is required to send the association request, the autonomous access point must be assigned the appropriate role.

To view a report of these role changes, choose **View Role Change Report** from the Select a command drop-down list. The following information displays:

- AP Address—IP address of the access point.
- Status—Current status of the role change.
- TimeStamp—Indicates the date and time of the upgrade.
- AP Logs

Click **OK** to return to the Migration Analysis Summary page.

Running Migration Analysis

You can choose **Run Migration Analysis** from the Select a command drop-down list of the Migration Analysis Summary page. The resulting migration analysis summary shows the current status of different criteria. Initially, migration analysis is run automatically when the access point is discovered.

Viewing a Migration Analysis Report

You can choose **View Migration Analysis Report** from the Select a command drop-down list of the Migration Analysis Summary page to generate a report. The report includes the following:

- Access point address
- Status
- Timestamp
- Access point logs

CHAPTER 20

Virtual Domains

A Cisco WCS virtual domain consists of a set of devices and maps and restricts a user's view to information relevant to these devices and maps.

Through a virtual domain, an administrator can ensure that users are only able to view the devices and maps for which they are responsible. In addition, because of the virtual domain's filters, users are able to configure, view alarms, and generate reports for *only* their assigned part of the network.

The administrator specifies for each user a set of allowed virtual domains. Only one of these can be active for that user at login. The user can change the current virtual domain by selecting a different allowed virtual domain from the Virtual Domain drop-down list at the top of the screen. All reports, alarms, and other functionality are now filtered by that virtual domain.

Note The following cannot be partitioned in a virtual domain (and are only available from the root partition: Google Earth Maps, Auto Provisioning, Mobility Service Engines).

If there is only one virtual domain defined ("root") in the system AND the user does not have any virtual domains in the custom attributes fields in the TACACS+/RADIUS server, the user is assigned the "root" virtual domain by default.

If there is more than one virtual domain, and the user does not have any specified attributes, then the user is blocked from logging in.

The following tasks are associated with Virtual Domains:

- Creating a Virtual Domain
- Understanding Virtual Domain Hierarchy
- Modifying a Virtual Domain
- Understanding Virtual Domains as a User

Creating a Virtual Domain

Use the Administration > Virtual Domains page to create, edit, or delete virtual domains. Each virtual domain may contain a subset of the elements included with its parent virtual domain. You can assign additional maps, controllers, and access points to the new virtual domain. See "Modifying a Virtual Domain" for more information on managing virtual domains.

Note The maximum number of virtual domains that can be defined in WCS is 124.

- New—Click to create a new virtual domain. See "Creating a New Virtual Domain" for more information.
- Delete—Click to delete the selected virtual domain from the hierarchy.
- Export—Click to configure custom attributes for the selected virtual domain. See "Virtual Domain RADIUS and TACACS+ Attributes" for more information.

Creating a New Virtual Domain

Note See "Modifying a Virtual Domain" for more information.

Follow these steps to create a new virtual domain:

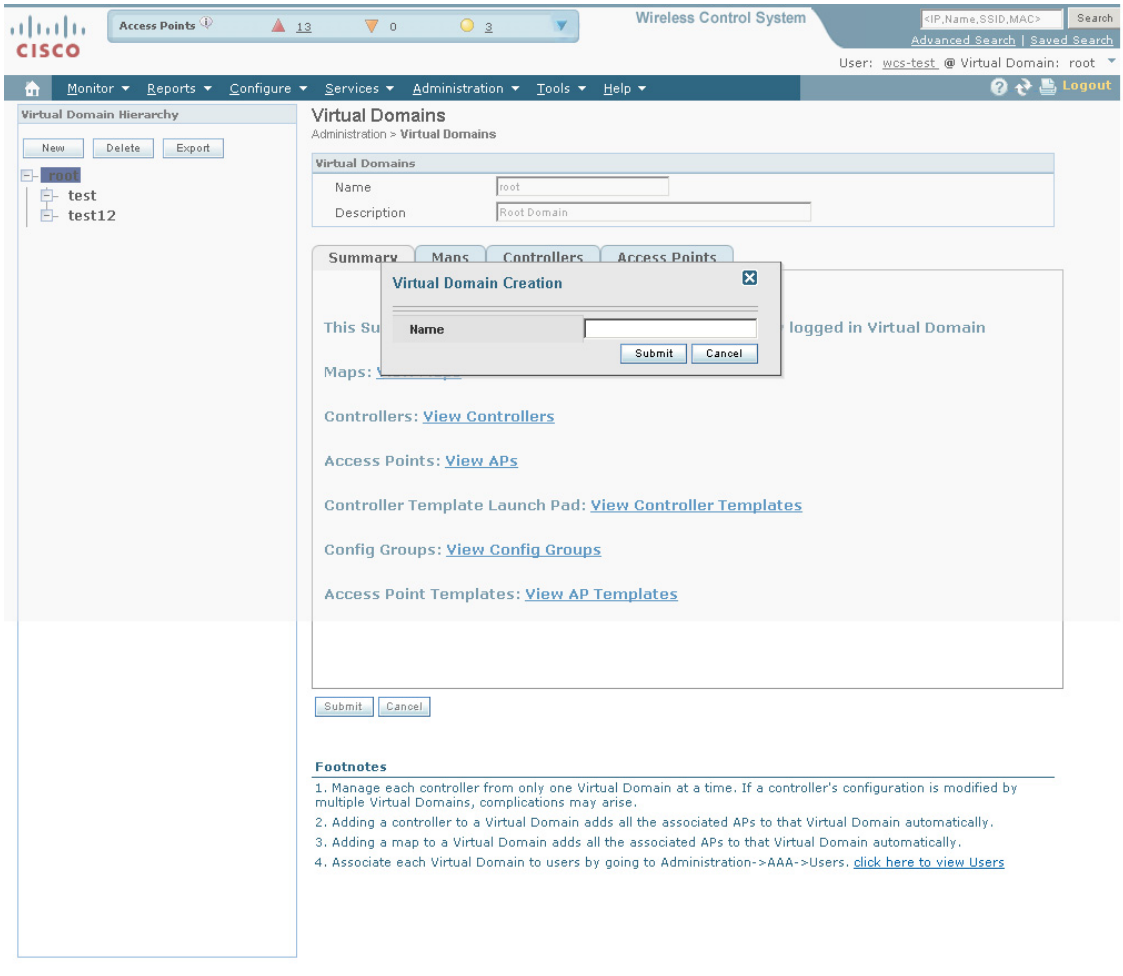
Step 1 Choose **Administration > Virtual Domains**.

Step 2 From the left Virtual Domain Hierarchy sidebar menu, select to highlight the virtual domain to which you want to add a sub (child) virtual domain.

Note The selected virtual domain becomes the parent virtual domain of the newly-created sub-virtual domain.

Step 3 Click **New** (see Figure 20-1).

Figure 20-1 Virtual Domains



Step 4 Enter the virtual domain name in the text box.

Step 5 Click **Submit** to create the virtual domain or **Cancel** to close the page with no changes.

Note Each virtual domain may contain a subset of the elements included with its parent virtual domain. When a user is assigned a virtual domain, that user may view the same maps, controllers, and access points that are assigned to its parent virtual domain.

Understanding Virtual Domain Hierarchy

Virtual domains are organized hierarchically. Sub-sets of an existing virtual domain contain the network elements that are contained in the parent virtual domain.

Note The default or "root" domain includes all virtual domains.

Because network elements are managed hierarchically some features and components such as report generation, searches, templates, config groups, and alarms are affected.

Note For instance, if you create a virtual domain with only access points and no controllers assigned, you lose some ability to choose controller-based features. For example, some options require you to navigate from the controller to the access point. Because controllers are not in the virtual domain, you are not able to generate the associated report.

Likewise, if you create a partition with only a few controllers and then go to Configure > Access Points and click an individual link in the AP Name column, the complete list of WCS-assigned controllers is displayed for Primary, Secondary, and Tertiary Controllers, rather than the limited number specified in the partition.

Note If a controller's configuration is modified by multiple Virtual Domains, complications may arise. To avoid this, manage each controller from only one Virtual Domain at a time.

See the following sections to better understand the effects of partitioning:

- Reports
- Search
- Alarms
- Templates
- Config Groups
- Maps
- Access Points
- Controllers
- Email Notification

Reports

Reports only include components assigned to the current virtual domain. For example, if you create a virtual domain with only access points and no controllers assigned, you lose some ability to choose controller-based features. For example, some report options require you to navigate from controller to access point. If you did not assign controllers when you created the virtual domain, you are not able to generate these kinds of reports.

Note Reports are only visible in the current virtual domain. The parent virtual domain cannot view the reports from its sub-virtual domain.

Client reports such as Client Count only include clients that belong to the current virtual domain.

Note If new clients are assigned to this partition by the administrator, the previous reports do not reflect these additions. Only new reports will reflect the new clients.

Search

Search results only include components that are assigned to the virtual domain in which the search is performed. Search results do not display floor areas when the campus is not assigned to the virtual domain.

Note The saved searches are only visible in the current virtual domain. The parent virtual domain cannot view these search results.

Note WCS does not partition network lists. If you search a controller by network list, all controllers will be returned.

Alarms

When a component is added to a virtual domain, no previous alarms for that component are visible to that virtual domain. Only newly-generated alarms are visible. For example, when a new controller is added to a virtual domain, any alarms generated for that controller prior to its addition do not appear in the current virtual domain.

Alarms are not deleted from a virtual domain when the associated controllers or access points are deleted from the same virtual domain.

Note In the Alarm Email Notifications parameter, only the root virtual domain can enable Location Notifications, Location Servers, and WCS email notifications.

Templates

When you create or discover a template in a virtual domain, it is only available in that virtual domain unless it is applied to a controller. If it is applied to a controller and that controller is assigned to a sub-virtual domain, the template stays with the controller in the new virtual domain.

Note If you create a sub virtual domain and then apply a template to both network elements in the virtual domain, WCS may incorrectly reflect the number of partitions to which the template was applied.

Config Groups

Config groups in a virtual domain can also be viewed by the parent virtual domain. A parent virtual domain can modify config groups for a sub (child) virtual domain. For example, the parent virtual domain can add or delete controllers from a sub virtual domain.

Maps

You can only view the maps that your administrator assigned to your current virtual domain.

- When a campus is assigned to a virtual domain, all buildings in that campus are automatically assigned to the same virtual domain.
- When a building is assigned to a virtual domain, it automatically includes all of the floors associated with that building.
- When a floor is assigned, it automatically includes all of the access points associated with that floor.

Note If only floors are assigned to a virtual domain, you lose some ability to choose map-based features. For example, some reports and searches require you to drill down from campus to building to floor. Since campus and buildings are not in the virtual domain, you are not able to generate these kinds of reports or searches.

Note Coverage areas shown in WCS are only applied to campus and buildings. In a floor-only virtual domain, WCS does not display coverage areas.

Note If a floor is directly assigned to a virtual domain, it cannot be deleted from the virtual domain which has the building to which the floor belongs.

Note Search results do not display floor areas when the campus is not assigned to the virtual domain.

Access Points

When a controller or map is assigned to a virtual domain, the access points associated with the controller or map are automatically assigned as well. Access points or controllers can also be assigned manually (separate from the controller or map) to a virtual domain.

Note If the controller is removed from the virtual domain, all of its associated access points are also removed. If an access point is manually assigned, it remains assigned even if its associated controller is removed from the current virtual domain.

Note If a manually-added access point is removed from a virtual domain but is still associated with a controller or map that is assigned to the same virtual domain, the access point remains visible in the virtual domain. Any alarms associated with this access point are not deleted with the deletion of the access point.

Note When maps are removed from a virtual domain, the access points on the maps can be removed from the virtual domain.

Note If you later move an access point to another partition, some events (such as generated alarms) may reside in the original partition location.

Controllers

Because network elements are managed hierarchically, controllers may be affected by partitioning. For instance, if you create a partition with only access points and no controllers assigned, all access points in the partition are not shown when you generate an access point report. Likewise, if you create a partition with only a few controllers and then go to Configure > Access Points and click an individual link in the AP Name column, the complete list of WCS-assigned controllers is displayed for Primary, Secondary, and Tertiary Controllers, rather than the limited number specified in the partition.

Email Notification

Email notification can be configured per virtual domain. An email is sent only when alarms occur in that virtual domain.

Modifying a Virtual Domain

Choose a Virtual Domain from the Virtual Domain Hierarchy on the left side to view or edit its assigned maps, controllers, and access points. The Summary page displays with links to view the current logged in virtual domain's available maps, controllers, and access points.

Note The following elements can be partitioned in a virtual domain: maps, controllers, access points, and templates.

The Maps, Controllers, and Access Points tabs are used to add or remove components assigned to this virtual domain.

To assign a map, controller, or access point to this domain, follow these steps:

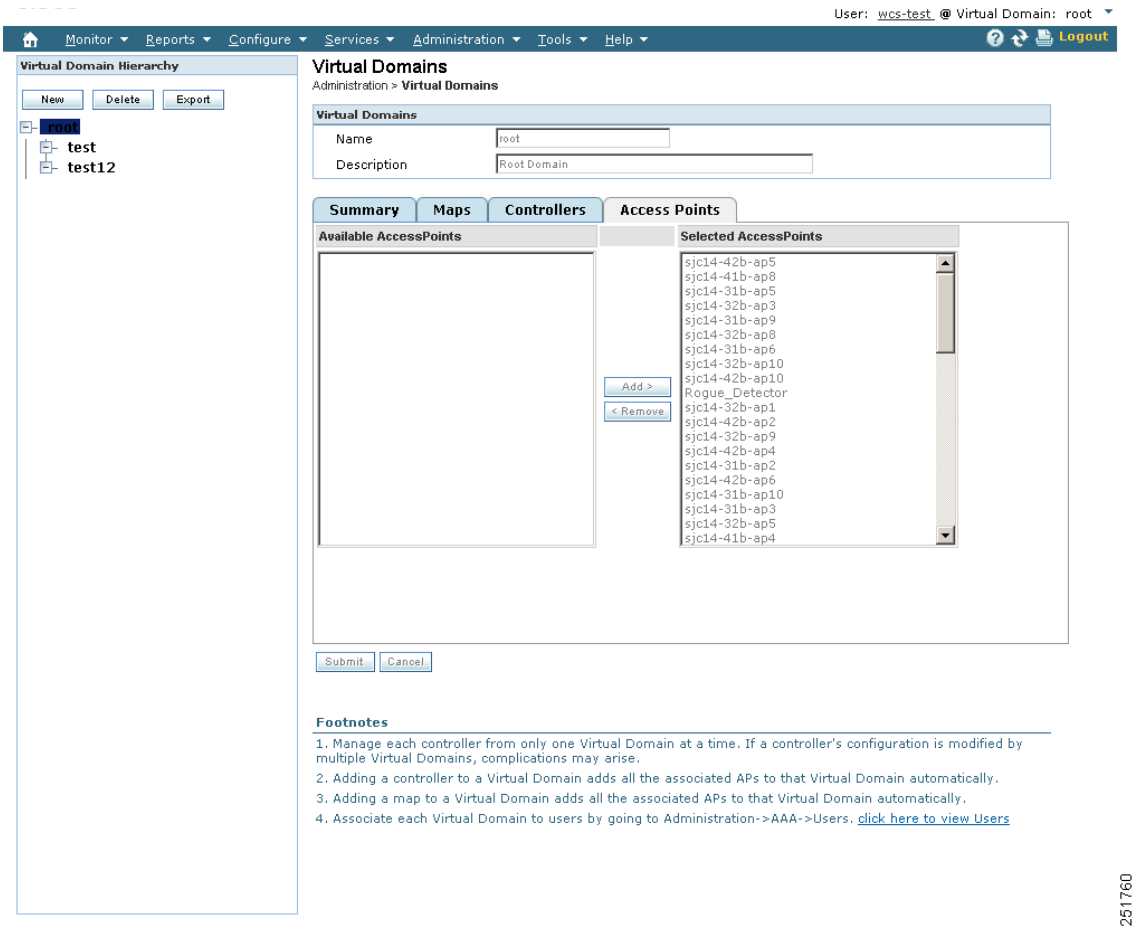
Step 1 Choose **Administration > Virtual Domains**.

Step 2 From the left Virtual Domain Hierarchy sidebar menu, select to highlight the virtual domain that you want to view or edit.

Note Because all maps, controllers, and access points are included in the partition tree, you should expect it to take several minutes to load. This increases if you have a system with a significant number of controllers and access points.

Step 3 Choose the applicable Maps, Controllers, or Access Points tab (see Figure 20-2).

Figure 20-2 Virtual Domains Maps Tab



Step 4 In the Available (Maps, Controllers, or Access Points) column, click to highlight the new component(s) you want to assign to the virtual domain.

Step 5 Click **Add >** to move the component(s) to the Selected (Maps, Controllers, or Access Points) column.

Note To remove a component from the virtual domain, click to highlight the component in the Selected (Maps, Controllers, or Access Points) column and click **< Remove**. The component returns to the Available column.

Step 6 Click **Submit** to confirm the changes.

Virtual Domain RADIUS and TACACS+ Attributes

The Virtual Domain Custom Attributes page allows you to indicate the appropriate protocol-specific data for each virtual domain. The Export button on the Virtual Domain Hierarchy sidebar pre-formats the virtual domain's RADIUS and TACACS+ attributes. You can copy and paste these attributes into the ACS server. This allows you to copy only the applicable virtual domains into the ACS server screen and ensures that the users only have access to these virtual domains.

To apply the pre-formatted RADIUS and TACACS+ attributes to the ACS server, follow these steps:

Step 1 From the left Virtual Domain Hierarchy sidebar menu, select to highlight the virtual domain for which you want to apply the RADIUS and TACACS+ attributes.

Step 2 Click **Export**.

Step 3 Highlight the text inside of the RADIUS or TACACS+ Custom Attributes (depending on which one you are currently configuring), go to your browser's menu, and choose **Edit > Copy**.

Step 4 Log in to ACS.

Step 5 Go to User or Group Setup.

Note If you want to specify virtual domains on a per user basis, then you need to make sure you add ALL the custom attributes (for example, tasks, roles, virtual domains) information into the User custom attribute screen.

Step 6 For the applicable user or group, click **Edit Settings**.

Step 7 Use your browser's **Edit > Paste** feature to place the RADIUS or TACACS+ custom attributes into the applicable text box.

Step 8 Click the check boxes to enable these attributes.

Step 9 Click **Submit + Restart**.

Note For more information on adding RADIUS and TACACS+ attributes to the ACS server, see the "Adding WCS UserGroups into ACS for TACACS+" section on page 18-10 or the "Adding WCS UserGroups into ACS for RADIUS" section on page 18-14.

Understanding Virtual Domains as a User

When you log in, you can access any of the virtual domains that the administrator assigned to you.

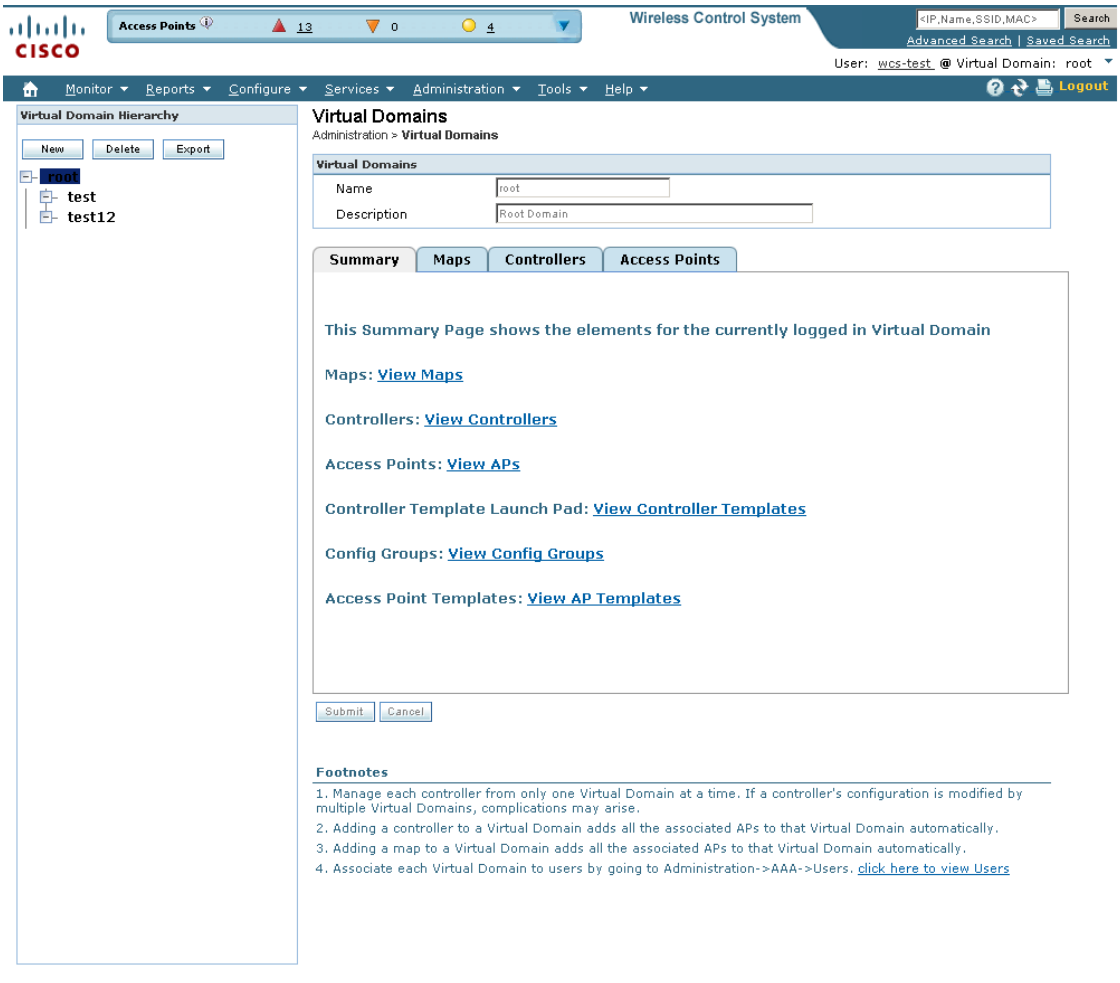
Only one virtual domain can be active at login. You can change the current virtual domain by using the Virtual Domain drop-down list at the top of the screen. Only virtual domains that have been assigned to you are available in the drop-down list.

When you select a different virtual domain from the drop-down list, all reports, alarms, and other functionality are filtered by the conditions of the new virtual domain.

Viewing Assigned Virtual Domain Components

To view all components (including maps, controllers, and access points) assigned to the current virtual domain, choose **Administration > Virtual Domains** (see Figure 20-3). Click a link in the Summary tab page to view the assigned components for your virtual domain.

Figure 20-3 Virtual Domains Summary Tab



Limited Menu Access

Non-root virtual domain users do not have access to the following WCS menus:

- Monitor > RRM
- Configure > Controller Auto- Provisioning
- Configure > ACS View Servers
- Services > Mobility Services
- Services > Synchronize Services
- Administration > Background Tasks

- Administration > Settings
- Administration > User Preferences
- Tools > Voice Audit
- Tools > Config Audit

CHAPTER 21

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
- Importing a File into WCS
- Viewing Google Earth Maps
- Adding Google Earth Location Launch Points to Access Point Pages

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

The following geographical information is required for each access point:

Note Before you can add coordinates for an access point, you must add the access point to a standard map. Positions will not show up on access points without heatmaps.

- 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. Default is 0.

  Coordinates in degrees, minutes, seconds, direction:

  - 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. 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 earth's surface 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. 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, select **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 parameter 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 parameter 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)—Parameter is ignored by WCS.
- Style, Color (optional)—Parameter is ignored by WCS.
- View—Allows you to configure the Latitude, Longitude, Range, Heading and Tilt coordinates. See the "Understanding Geographical Coordinates for Google Earth" section on page 21-1" 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, refer 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 WCS.

Creating and Importing Coordinates as a CSV File

To create a CSV file to import into WCS, follow these steps:

Step 1 Open a flat file and provide the necessary information as a comma-separated list. The Table 21-1 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 below, see the "Understanding Geographical Coordinates for Google Earth" section on page 21-1.

Table 21-1 Potential Fields for the CSV File

"FolderName"	"Value Optional"	Max Length: 32
"FolderState"	"Value Optional"	Permitted Values: true/false
"FolderLongitude"	"Value Optional"	Range: 0 to ±180

Table 21-1 Potential Fields for the CSV File (continued)

"FolderName"	"Value Optional"	Max Length: 32
"FolderLatitude"	"Value Optional"	Range: 0 to ±90
"FolderAltitude"	"Value Optional"	Range: 0 to 99999
"FolderRange"	"Value Optional"	Range: 0 to 99999
"FolderTilt"	"Value Optional"	Range: 0 to 90
"FolderHeading"	"Value Optional"	Range: 0 to ±180
"FolderGeoAddress"	"Value Optional"	Max Length: 128
"FolderGeoCity"	"Value Optional"	Max Length: 64
"FolderGeoState"	"Value Optional"	Max Length: 40
"FolderGeoZip"	"Value Optional"	Max Length: 12
"FolderGeoCountry"	"Value Optional"	Max Length: 64
"AP_Name"	"Value Required"	Max Length: 32
"AP_Longitude"	"Value Required"	Range: 0 to ±180
"AP_Latitude"	"Value Required"	Range: 0 to ±90

Step 2 Save the .csv file. The file is now ready to import into WCS.

Importing a File into WCS

To import a Google KML or a CSV into the Google Earth Maps feature of WCS, follow these steps:

Step 1 Log in to WCS.

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 WCS).
- Range validations are performed for tilt, heading, range, and other geographical coordinates fields.If longitude and latitudeare provided, range validations are performed; if not, the value is defaulted to 0.

Note In KML, the longitude and latitude ranges can only be entered in decimal format. In CSV, different formats are supported (refer to the CSV sample under Google Maps > Import CSV).

Note If the input file does not validate for completeness, an error page appears. The uploaded information cannot be saved until all errors are corrected.

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 WCS.

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 Google's website: http://earth.google.com.

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.

Step 2 Click **Cancel** to close the details page.

Adding Google Earth Location Launch Points to Access Point Pages

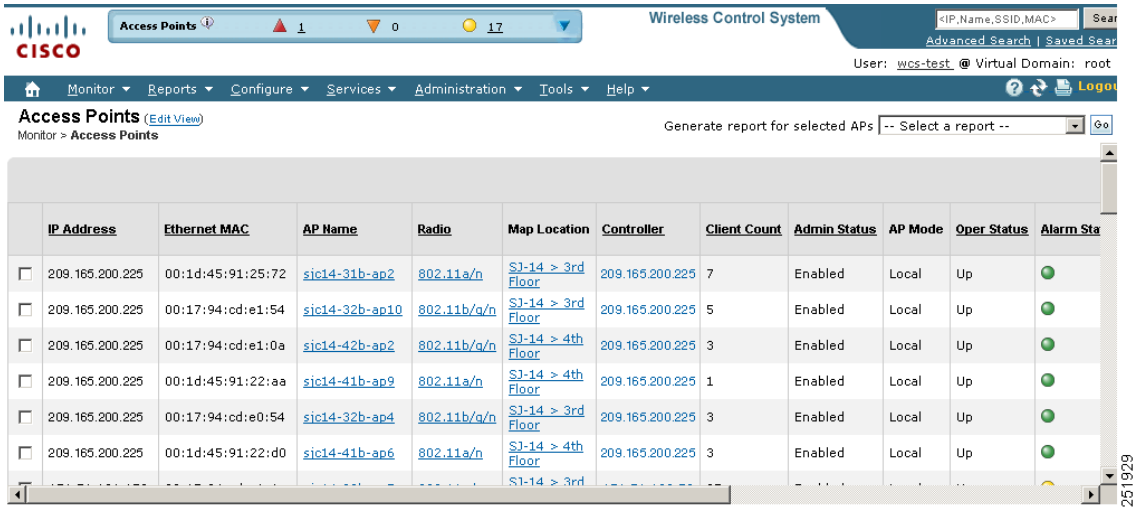
You can expand the number of Google Earth Location launch points within Cisco WCS by adding it to the Access Point summary and detail pages.

Follow these steps to add a Google Earth Location launch point to the Access Point summary and details page:

Step 1 Click **Monitor > Access Points** (see Figure 21-1).

Step 2 At Access Point summary page, click the **Edit View** link next to page heading.

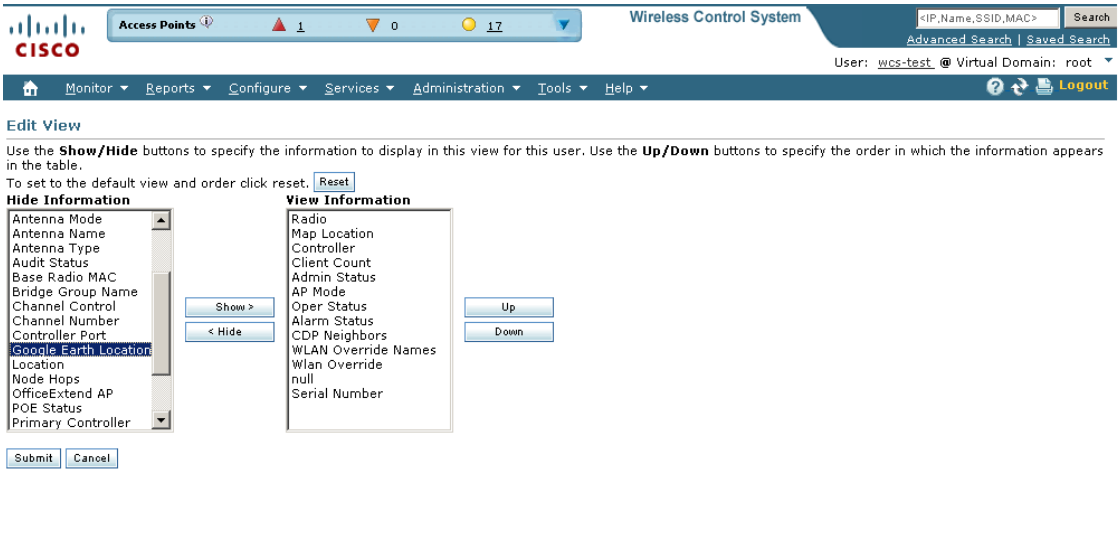
Figure 21-1 Monitor > Access Points Page



Step 3 In the Edit View page, highlight **Google Earth Location** in the left-hand column. Click **Show** (see Figure 21-2).

The Google Earth Location column heading moves into the View Information column.

Figure 21-2 Edit View Page



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 on 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. Choose 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 overlaid 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 WCS.

  – 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.

APPENDIX A

Troubleshooting and Best Practices

This appendix identifies and explains any additional troubleshooting or best practices you may find necessary as you implement a particular function.

This appendix includes the following sections:

- Troubleshooting Cisco Compatible Extensions Version 5 Client Devices, page A-1
- Web Auth Security on WLANs, page A-3

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 support 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.

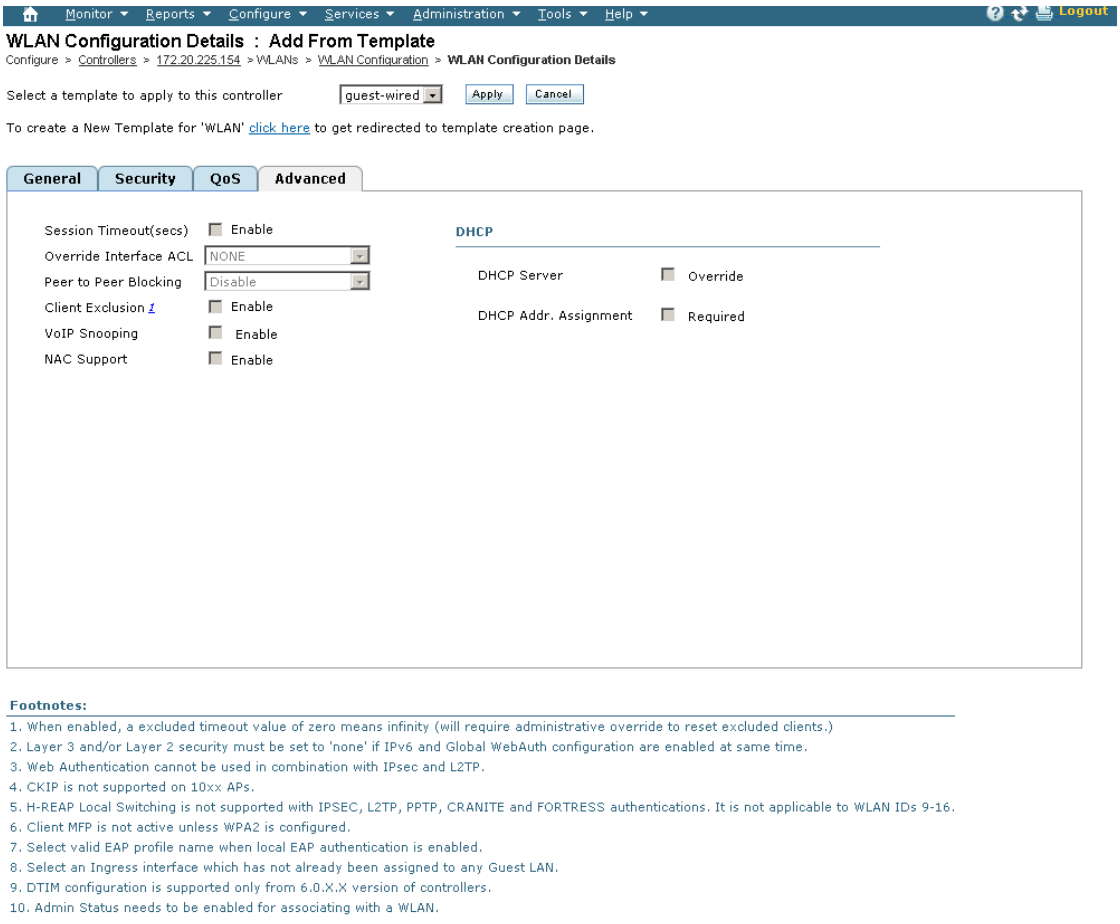
Step 3 Choose **WLAN> WLAN Configuration** from the left sidebar menu.

Step 4 Choose **Add a WLAN** from the Select a command drop-down menu to create a new or click the profile name of an existing.

Note Cisco recommends that you create a new WLAN on which to run the diagnostic tests.

Step 5 When the WLANs page appears, click the **Advanced** tab (see Figure A-1).

Figure A-1 WLANs 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 mobile client's radio.

Step 3 Enter the following debug commands via a serial console set for high speed (115200) or SSH session to the controller's management port:

```
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.

```
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
NPU Fast Fast Notified........................... Yes
Last Policy Manager State........................ WEBAUTH_REQD
Client Entry Create Time......................... 67733 seconds
Policy Type...................................... N/A
Encryption Cipher................................ None
Management Frame Protection...................... No
EAP Type......................................... Unknown
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: [0,0,0,0,0,0,0,0,0,0,0,0]
      ap:09:96:10(slot 1) .......................
antenna0: 48 seconds ago -45 dBm................. antenna1: 123 seconds ago -128 dBm
```

Step 5 Make sure the client's pemstate is WEBAUTH_REQD. Open the browser page on the client and look for the following messages:

```
Wed Mar  7 17:59:15 2007: ************* sshpmAddWebRedirectRules: POLICY SEMAPHORE LOCKED
*************
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: sshpmAddWebRedirectRules: using HTTP-S for web auth (addr:
10.50.234.15).
Wed Mar  7 17:59:15 2007: sshpmAddWebRedirectRules: inbound local http rule created for ms
10.50.234.3 local 1.1.1.1.
Wed Mar  7 17:59:15 2007: sshpmAddWebRedirectRules: inbound http redirect rule created.
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: sshpmAddWebRedirectRules: committing rules for ms 10.50.234.3
Wed Mar  7 17:59:15 2007: ************* sshpmPolicyCommitCallback: POLICY SEMAPHORE
UNLOCKED - [unconditionally] ************
```

```
Wed Mar  7 17:59:15 2007: sshpmPolicyCommitCallback: called; ContextPtr: 0x2c; Success: 1
Wed Mar  7 17:59:15 2007: ************* sshpmPolicyCommitCallback: POLICY SEMAPHORE
UNLOCKED - [unconditionally] ************
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=0xdfffffff,
prev_trd_index=0xdfffffff
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_mappings_cb: 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: SshPmAppgw/pm_appgw.c:507/ssh_appgw_tcp_listener_callback: New
initiator stream: src=10.50.234.1:61611, dst=10.76.108.121:2024
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 18:02:32 2007: SshAppgwHttp/appgw_http.c:531/ssh_appgw_http_conn_cb: New TCP
HTTP connection 10.50.234.3.1153 > 10.50.234.1.80
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:535/ssh_appgw_http_conn_cb: Responder
sees initiator as `10.50.234.15.1153'
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:539/ssh_appgw_http_conn_cb: Initiator
sees responder as `10.50.234.1.80'
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (i) reading_hdr 1 nmsgs 0
Wed Mar  7 18:02:32 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:136/ssh_appgw_http_st_wait_input: read
-1 bytes (offset 0 data 0)
Wed Mar  7 18:02:32 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 18:02:32 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:132/ssh_appgw_http_st_wait_input:
appgw_http.c.132: io->src is NULL
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:136/ssh_appgw_http_st_wait_input: read
-1 bytes (offset 0 data 0)
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (i) reading_hdr 1 nmsgs 0
Wed Mar  7 18:02:32 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
```

```
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:136/ssh_appgw_http_st_wait_input: read
-1 bytes (offset 0 data 0)
Wed Mar  7 18:02:32 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 18:02:32 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:36 2007: SshAppgwHttp/appgw_http.c:132/ssh_appgw_http_st_wait_input:
appgw_http.c.132: io->src is NULL
Wed Mar  7 18:02:36 2007: SshAppgwHttp/appgw_http.c:136/ssh_appgw_http_st_wait_input: read
-1 bytes (offset 0 data 0)
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (i) reading_hdr 1 nmsgs 0
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:136/ssh_appgw_http_st_wait_input: read
283 bytes (offset 0 data 0)
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 283
bytes:
Wed Mar  7 18:02:41 2007: 00000000: 4745 5420 2f20 4854 5450 2f31 2e31 0d0a  GET /
HTTP/1.1..
Wed Mar  7 18:02:41 2007: 00000010: 4163 6365 7074 3a20 696d 6167 652f 6769  Accept:
image/gi
Wed Mar  7 18:02:41 2007: 00000020: 662c 2069 6d61 6765 2f78 2d78 6269 746d  f,
image/x-xbitm
Wed Mar  7 18:02:41 2007: 00000030: 6170 2c20 696d 6167 652f 6a70 6567 2c20  ap,
image/jpeg,
Wed Mar  7 18:02:41 2007: 00000040: 696d 6167 652f 706a 7065 672c 2061 7070  image/pjpeg,
app
Wed Mar  7 18:02:41 2007: 00000050: 6c69 6361 7469 6f6e 2f78 2d73 686f 636b
lication/x-shock
Wed Mar  7 18:02:41 2007: 00000060: 7761 7665 2d66 6c61 7368 2c20 2a2f 2a0d  wave-flash,
*/*.
Wed Mar  7 18:02:41 2007: 00000070: 0a41 6363 6570 742d 4c61 6e67 7561 6765
.Accept-Language
Wed Mar  7 18:02:41 2007: 00000080: 3a20 656e 2d75 730d 0a41 6363 6570 742d  :
en-us..Accept-
Wed Mar  7 18:02:41 2007: 00000090: 456e 636f 6469 6e67 3a20 677a 6970 2c20  Encoding:
gzip,
Wed Mar  7 18:02:41 2007: 000000a0: 6465 666c 6174 650d 0a55 7365 722d 4167
deflate..User-Ag
Wed Mar  7 18:02:41 2007: 000000b0: 656e 743a 204d 6f7a 696c 6c61 2f34 2e30  ent:
Mozilla/4.0
Wed Mar  7 18:02:41 2007: 000000c0: 2028 636f 6d70 6174 6962 6c65 3b20 4d53   (compatible;
MS
Wed Mar  7 18:02:41 2007: 000000d0: 4945 2036 2e30 3b20 5769 6e64 6f77 7320  IE 6.0;
Windows
Wed Mar  7 18:02:41 2007: 000000e0: 4e54 2035 2e31 3b20 5356 3129 0d0a 486f  NT 5.1;
SV1)..Ho
Wed Mar  7 18:02:41 2007: 000000f0: 7374 3a20 3130 2e35 302e 3233 342e 310d  st:
10.50.234.1.
Wed Mar  7 18:02:41 2007: 00000100: 0a43 6f6e 6e65 6374 696f 6e3a 204b 6565  .Connection:
Kee
Wed Mar  7 18:02:41 2007: 00000110: 702d 416c 6976 650d 0a0d 0a              p-Alive....
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:985/ssh_appgw_parse_request_line: parsing request
line GET / HTTP/1.1
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:1018/ssh_appgw_parse_request_line: internal http
version 3
Wed Mar  7 18:02:41 2007: SshAppgwHttpState/appgw_http_state.c:1155/ssh_appgw_add_method:
caching method 2 for reply 0
Wed Mar  7 18:02:41 2007: SshAppgwHttpState/appgw_http_state.c:1604/ssh_appgw_check_msg:
examining request using service id 34
```

```
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:594/ssh_appgw_http_get_dst_host: destination host:
10.50.234.1
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:1474/ssh_appgw_inject_reply: injecting 404 reply as
msg 0
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:284/ssh_appgw_http_st_write_data:
entering state st_write_data
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (i) reading_hdr 1 nmsgs 1
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:136/ssh_appgw_http_st_wait_input: read
-1 bytes (offset 0 data 0)
Wed Mar  7 18:02:41 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 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:1851/ssh_appgw_http_is_inject: next inject is msg# 0
current msg# 0
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:207/ssh_appgw_http_st_inject: entering
state st_inject (r): msgs 0
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:259/ssh_appgw_http_st_inject: closing
connection after inject
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:400/ssh_appgw_http_st_terminate:
entering state st_terminate (r): teardown 0 terminate i: 1 r: 1
Wed Mar  7 18:02:45 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (i) reading_hdr 1 nmsgs 1
Wed Mar  7 18:02:45 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:45 2007: SshAppgwHttp/appgw_http.c:400/ssh_appgw_http_st_terminate:
entering state st_terminate (i): teardown 0 terminate i: 1 r: 1
Wed Mar  7 18:02:45 2007:
SshAppgwHttp/appgw_http.c:732/ssh_appgw_http_connection_terminate: service HTTP-REDIR: TCP
HTTP connection 10.50.234.3.1153 > 10.50.234.1.80 terminated
Wed Mar  7 18:02:45 2007: SshPmStAppgw/pm_st_appgw.c:1094/ssh_pm_st_appgw_terminate:
terminating appgw instance
```

Step 6 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.

Step 7 Look at the client's entry 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.

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.

APPENDIX B

WCS and End-User Licenses

This appendix provides the end-user license and warranty that apply to the Cisco WCS. It contains these sections:

- WCS Licenses, page B-1
- Notices and Disclaimers, page B-5
- End-User License Agreement, page B-7

WCS Licenses

Before you purchase a Cisco Wireless Control System (WCS) license, decide whether if you will need a Base or PLUS license and how many access points will need to be supported and licensed.

The two types of licenses for Cisco WCS support different feature levels:

- **Cisco WCS Base supports standard WCS capabilities**, which includes wireless client data access, rogue access point containment functions, Cisco WLAN Solution monitoring and control, and client and rogue access point location to the nearest access point.
- **Cisco WCS PLUS license** supports Cisco WCS base license features and the following capabilities: mobility services enablement and high availability. An older Cisco WCS Location license is forward compatible and equivalent to a PLUS license. When upgrading to this release, older Location licenses will appear as PLUS licenses. Older Enterprise licenses are also forward compatible and become PLUS licenses when loaded. The process to provision a Cisco WCS PLUS license is the same as provisioning a current Cisco WCS license.

See the "Accessing the License Center" section on page 18-67 for information on managing WCS licenses on the GUI.

Types of Licenses

The licensing information for existing Cisco WCS deployments are being upgraded to support Cisco Unified Wireless Network Software Release 4.1.82.0. (While previous Cisco WCS SKUs will be available until September 2006, Cisco recommends that you purchase the new Cisco WCS SKUs outlined in the WCS Ordering Guide (http://www.cisco.com/en/US/products/ps6305/products_data_sheet0900aecd804b4646.html) for a more seamless migration to licensing. This chapter includes information on new or expansion Cisco WCS licenses, migrating from CiscoWorks Wireless LAN Solution Engine (WLSE) to Cisco WCS, upgrading to the Cisco WCS Location option, and deploying the free Cisco WCS demonstration license. The versions of Cisco Wireless Control System (WCS) licenses are as follows:

- WCS-ENT-PLUS-K9—Cisco WCS Enterprise PLUS License with Mobility Services Enablement, High availability, and Windows or Linux on multiple Cisco WCS servers.
- WCS-STANDARD-K9 — For customer buying new or expansion Cisco WCS licenses running Cisco Unified Wireless Network Software. It is available as Cisco WCS Base or Cisco WCS PLUS option in increments of 50, 100, or 500 lightweight access points.

Note When the number of access points exceeds the limit of those licensed, WCS generates an alarm. Also, when the user logs into WCS, they are alerted if the licensed access point count has been exceeded.

- WCS-WLSE-UPG-K9 — For CiscoWorks WLSE customers migrating from CiscoWorks WLSE (Model 1130) to Cisco WCS. See Appendix B for steps to migrate from CiscoWorks WLSE to the Cisco Unified Wireless Network architecture. It is available as a WCS-WLSE Base option or a WCS-WLSE PLUS option in increments of 50, 100, 500, or 1000 lightweight access points.

Note Dell platforms are not supported.

Note CiscoWorks WLSE Express (Model 1030) and CiscoWorks WLSE (Model 1105 or 1133) are NOT supported with this SKU. DO NOT install the CiscoWorks WLSE CDs on the CiscoWorks WLSE Express (Model 1030) appliance or CiscoWorks WLSE (Model 1105 or 1133) because this conversion does not work and is not supported by Cisco Systems.

- WCS-PLUS-UPG-K9 — For customers upgrading from their existing Cisco WCS Base licenses to equivalent Cisco WCS PLUS licenses. It is available as Cisco WCS PLUS in increments of 50, 100, or 500 lightweight access points.
- WCS-ADV-SI-SE-10—An incremental license that enables the integration of up to 10 Spectrum Experts. This license requires a valid Base or PLUS license.
- AIR-WCS-DEMO-K9 — For customers wishing to download the new full featured, PLUS Cisco WCS with Spectrum Integration demonstration license that supports ten access points for up to 30 days. Demo licenses are available at http://www.cisco.com/go/license.

Note The free 30-day trial license is NOT supported by the Cisco Technical Assistance Center (TAC).

Licensing Enforcement

Cisco Unified Wireless Network Releases enforces software based licensing. Customers are prompted to enter license files by all new Cisco WCS SKU families. Existing customers migrating to a later release are also impacted by licensing and should contact their Cisco Sales Representative or TAC to obtain Product Authorization Key (PAK) certificate if they have not already received PAK certificate from Cisco. For more information, refer to the WCS Ordering Guide (http://www.cisco.com/en/US/products/ps6305/products_data_sheet0900aecd804b4646.html).

All Cisco WCS licenses can be purchased or acquired directly from Cisco.com via the normal Cisco ordering processes. Cisco Unified Wireless Network Software Releases can be downloaded from Cisco.com or, for a nominal charge, a CD (WCS-CD-K9) can be purchased from the WCS-STANDARD-K9 or WCS-PLUS-UPG-K9 SKU families. The WCS-CD-K9 contains one software

image of Cisco WCS version 4.0 on a CD. Customers can select the appropriate Cisco WCS installer to designate whether they would like to install a Windows or Linux version. The Cisco WCS Base or PLUS features and access point quantity are activated after installation by inserting the license file that is tied to the original purchased Cisco WCS SKU. This CD is shipped via U.S. mail to the purchaser's address.

For the WCS-WLSE-UPG-K9 SKU family, two CDs are automatically shipped with any order in this specific SKU family. These CDs are special purpose CDs that are used specifically to convert the Cisco Works WLSE platform to Cisco WCS.

The Cisco WCS free demonstration license, AIR-WCS-DEMO-K9 is only available as a software download from Cisco.com. Within the 30 day trial period, this free license can be upgraded to one of the non-expiring Cisco WCS SKUs by applying license files generated through the purchase of one of the non-expiring Cisco WCS SKU families.

Product Authorization Key Certificate

All Cisco WCS SKUs require a PAK certificate to register the Cisco WCS license. The PAK is a paper certificate sent via U.S. mail from Cisco Systems upon purchase of the Cisco WCS license. The PAK certificate allows customers to receive a Cisco WCS license. It is used to register the Cisco WCS and generate license files. All customers must go to the PAK registration site listed on their PAK certificate to complete their Cisco WCS registration. The PAK certificate provides clear instructions on how to complete the Cisco WCS licensing process.

Note All customers that purchase Cisco WCS from Cisco.com via download or CD must activate their Cisco WCS license by registering at the PAK site. Customers receive the PAK via U.S. mail. Cisco WCS will not be activated until the PAK registration process is completed.

Determining Which License To Use

You should select the correct license based on your deployment situation, the number of access points to be supported, and Cisco WCS options (base or location). All SKUs within a SKU family can be combined with equivalent option levels such as Base to Base or PLUS to PLUS. Unequal option levels (Base and PLUS) cannot be mixed. Only one type of license can be used on the WCS at one time. For example, if your computer has a PLUS license, you cannot add a Base license. You can add to the current license by purchasing a license to increase the access point count. For example, if you have a PLUS license with an access point count of 50 and in a year you need to add more access points, you can buy another PLUS license with an access point count of 100, apply it to the WCS, and have a WCS with PLUS license for 150 access points. You can add a license to increase the number of access points in increments of 50, 100, 500, 1000, or 2500.

Note If you have a Base license and want to upgrade to a PLUS, you will need to purchase a PLUS upgrade license. You need to purchase a PLUS upgrade license equivalent to the total number of access points with a Base license. For example, if you have three Base licenses with support for 50, 100, and 200 access points (for a total of 350 access points), you must purchase enough upgrade licenses with support for 350 access points.

Installing a License

You need to have the Wireless Control System license key file to install your license. The key file is distributed to you in an e-mail from Cisco Systems. This file activates the features that you have purchased for your Cisco Wireless Control System (WCS). Do not edit the contents of the .lic file in any way or you will render the file useless.

Note If you upgrade to a WCS version without a license, you receive a critical alarm once a day and a notification regarding lack of a license each time you log in to WCS. Without a license, you have access to all WCS functionality except adding new controllers.

Cisco strongly recommends that you print the e-mail, save the attachment to a removable media, and store both in a safe place for future use, if needed by either yourself or anyone in your organization.

Before you proceed, make sure that the WCS server software has been installed and configured on the server.

To install the WCS license, follow these steps:

Step 1 Save the license file (.lic) to a temporary directory on your hard drive.

Step 2 Open a supported browser.

Step 3 In the Location or Address text box, enter the following URL, replacing IP address or host name of the WCS server: https://<IP address>.

Step 4 Log in to the WCS server as system administrator. User names and passwords are case-sensitive.

Step 5 Choose **Administration > License Center**.

Step 6 Choose **Files > WCS** from the left sidebar menu.

Step 7 Click **Add**. The Add a License File page appears.

Step 8 In the Add a License File page, click **Browse** to navigate to the location where you saved the .lic file.

Step 9 Click **Upload**.

The WCS server imports the license.

During the upload the following items are checked:

- Validity of the license file.
- Matching host names on the license and WCS system.
- The license file being installed must have a PLUS Feature. For example, Base or PLUS.
- The PLUS Feature (Base or PLUS) of the file being installed must match that of the system.

If you encounter a problem with the license file, please contact the Cisco Licensing team at 800-553-2447 or licensing@cisco.com.

Backup and Restore License

The license files are saved as part of the backup and restore process, so upgrading WCS will not require reentering of the license files. However, the restore must be on a system with the same host name for the restored licenses to work. If you have installed an upgraded license on your system, you must reinstall

the original license, followed by the upgrade license. For example, if you have upgraded a license from Base license to PLUS license, during the reinstall, you need to first install the Base license, then install the PLUS license. To backup the WCS database, refer to the "Backing Up the WCS Database" section on page 14-3.

Notices and Disclaimers

This chapter/appendix contains notices and disclaimers that pertain to Cisco WCS/Cisco WLAN Controller/whatever other product.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, for example, both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS"' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO

EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Disclaimers

All third party trademarks are the property of their respective owners.

End-User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND, OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

The following terms of this End User License Agreement ("Agreement") govern Customer's access and use of the Software, except to the extent (a) there is a separate signed agreement between Customer and Cisco governing Customer's use of the Software or (b) the Software includes a separate "click-accept" license agreement as part of the installation and/or download process. To the extent of a conflict between the provisions of the foregoing documents, the order of precedence shall be (1) the signed agreement, (2) the click-accept agreement, and (3) this End User License Agreement.

License. Conditioned upon compliance with the terms and conditions of this Agreement, Cisco Systems, Inc. or its subsidiary licensing the Software instead of Cisco Systems, Inc. ("Cisco"), grants to Customer a nonexclusive and nontransferable license to use for Customer's internal business purposes the Software

and the Documentation for which Customer has paid the required license fees. "Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) specifically pertaining to the Software and made available by Cisco with the Software in any manner (including on CD-Rom, or on-line).

Customer's license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or such number and types of agent(s), concurrent users, sessions, IP addresses, port(s), seat(s), server(s), site(s), features and feature sets as are set forth in the applicable Purchase Order which has been accepted by Cisco and for which Customer has paid to Cisco the required license fee.

Unless otherwise expressly provided in the Documentation, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable documentation permits installation on non-Cisco equipment) for communication with Cisco equipment owned or leased by Customer and used for Customer's internal business purposes. NOTE: For evaluation or beta copies for which Cisco does not charge a license fee, the above requirement to pay license fees does not apply.

General Limitations. This is a license, not a transfer of title, to the Software and Documentation, and Cisco retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of Cisco, its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Accordingly, except as otherwise expressly provided under this Agreement, Customer shall have no right, and Customer specifically agrees not to:

(i)transfer, assign or sublicense its license rights to any other person or entity, or use the Software on unauthorized or secondhand Cisco equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense or use shall be void;

(ii)make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;

(iii)reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction;

(iv)use or permit the Software to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of Cisco; or

(v)disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of Cisco. Customer shall implement reasonable security measures to protect such trade secrets.

To the extent required by law, and at Customer's written request, Cisco shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of Cisco's applicable fee, if any. Customer shall observe

strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Cisco makes such information available.

Software, Upgrades and Additional Copies. For purposes of this Agreement, "Software" shall include (and the terms and conditions of this Agreement shall apply to) computer programs, including firmware, as provided to Customer by Cisco or an authorized Cisco reseller, and any upgrades, updates, bug fixes or modified versions thereto (collectively, "Upgrades") or backup copies of the Software licensed or provided to Customer by Cisco or an authorized Cisco reseller. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE OR ADDITIONAL COPIES; (2) USE OF UPGRADES IS LIMITED TO CISCO EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in this Agreement, Customer shall not make any copies or duplicates of any Software without the prior written permission of Cisco.

Term and Termination. This Agreement and the license granted herein shall remain effective until terminated. Customer may terminate this Agreement and the license at any time by destroying all copies of Software and any Documentation. Customer's rights under this Agreement will terminate immediately without notice from Cisco if Customer fails to comply with any provision of this Agreement. Upon termination, Customer shall destroy all copies of Software and Documentation in its possession or control. All confidentiality obligations of Customer and all limitations of liability and disclaimers and restrictions of warranty shall survive termination of this Agreement. In addition, the provisions of the sections titled "U.S. Government End User Purchasers" and "General Terms Applicable to the Limited Warranty Statement and End User License" shall survive termination of this Agreement.

Customer Records. Customer grants to Cisco and its independent accountants the right to examine Customer's books, records and accounts during Customer's normal business hours to verify compliance with this Agreement. In the event such audit discloses non-compliance with this Agreement, Customer shall promptly pay to Cisco the appropriate license fees, plus the reasonable cost of conducting the audit.

Export. Software and Documentation, including technical data, may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software and Documentation.

U.S. Government End User Purchasers. The Software and Documentation qualify as "commercial items," as that term is defined at Federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms

are used in FAR 12.212. Consistent with FAR 12.212 and DoD FAR Supp. 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which this End User License Agreement may be incorporated, Customer may provide to Government end user or, if this Agreement is direct, Government end user will acquire, the Software and Documentation with only those rights set forth in this End User License Agreement. Use of either the Software or Documentation or both constitutes agreement by the Government that the Software and Documentation are "commercial computer software" and "commercial computer software documentation," and constitutes acceptance of the rights and restrictions herein.

Limited Warranty

Subject to the limitations and conditions set forth herein, Cisco warrants that commencing from the date of shipment to Customer (but in case of resale by an authorized Cisco reseller, commencing not more than ninety (90) days after original shipment by Cisco), and continuing for a period of the longer of (a) ninety (90) days or (b) the warranty period (if any) expressly set forth as applicable specifically to software in the warranty card accompanying the product of which the Software is a part (the "Product") (if any): (a) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (b) the Software substantially conforms to the Documentation. The date of shipment of a Product by Cisco is set forth on the packaging material in which the Product is shipped. Except for the foregoing, the Software is provided AS IS. This limited warranty extends only to the Customer who is the original licensee. Customer's sole and exclusive remedy and the entire liability of Cisco and its suppliers and licensors under this limited warranty will be (i) replacement of defective media and/or (ii) at Cisco's option, repair, replacement, or refund of the purchase price of the Software, in both cases subject to the condition that any error or defect constituting a breach of this limited warranty is reported to Cisco or the party supplying the Software to Customer, if different than Cisco, within the warranty period. Cisco or the party supplying the Software to Customer may, at its option, require return of the Software as a condition to the remedy. In no event does Cisco warrant that the Software is error free or that Customer will be able to operate the Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Cisco does not warrant that the Software or any equipment, system or network on which the Software is used will be free of vulnerability to intrusion or attack.

Restrictions. This warranty does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Cisco or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Cisco, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; or (d) is licensed, for beta, evaluation, testing or demonstration purposes for which Cisco does not charge a purchase price or license fee.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY CISCO, ITS SUPPLIERS AND LICENSORS. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY. THIS WARRANTY GIVES CUSTOMER SPECIFIC LEGAL RIGHTS, AND CUSTOMER MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

General Terms Applicable to the Limited Warranty Statement and End User License Agreement

Disclaimer of Liabilities. REGARDLESS WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Cisco's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim or if the Software is part of another Product, the price paid for such other Product. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Customer agrees that the limitations of liability and disclaimers set forth herein will apply regardless of whether Customer has accepted the Software or any other product or service delivered by Cisco. Customer acknowledges and agrees that Cisco has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

The validity, interpretation, and performance of this Warranty and End User License shall be controlled by and construed under the laws of the State of California, United States of America, as if performed wholly within the state and without giving effect to the principles of conflict of laws, and the State and federal courts of California shall have jurisdiction over any claim arising under this Agreement. The parties specifically disclaim the UN Convention on Contracts for the International Sale of Goods. Notwithstanding the foregoing, either party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such party's intellectual property or proprietary rights. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement shall remain in full force and effect. Except as expressly provided herein, this Agreement constitutes the entire agreement between the parties with respect to the license of the Software and Documentation and supersedes any conflicting or additional terms contained in any purchase order or elsewhere, all of which terms are excluded. This Agreement has been written in the English language, and the parties agree that the English version will govern.

Supplemental License Agreement

Cisco Wireless Control System (WCS)

IMPORTANT-READ CAREFULLY

You have agreed to the Cisco System, Inc. End User License Agreement (“EULA”) that governs your access and use of the Cisco Wireless Control System ("WCS"). This supplemental license agreement (this "supplement") contains additional terms and conditions.

Capitalized terms used and but not defined in this supplement have the meanings as defined in the EULA. To the extent of a conflict between the provisions of this supplement and the EULA, this supplement takes precedence.

By installing, downloading, accessing or otherwise using the Software, Customer agrees to be bound by the terms of this supplement. If Customer does not agree to the terms of this supplement, Customer may not install, download, or otherwise use the Software.

Restrictions on Managed Access Point and Devices

Customer may not use the Software unless:

- Customer obtains a WCS limited license by placing a Purchase Order for a WCS license for a specific number of access points, having the Purchase Order accepted by Cisco, and paying to Cisco the required license fee; or
- Customer obtains a WCS demonstration license by registering and downloading the Software for demonstration purposes in accordance with the Cisco Data Sheet for the Cisco Wireless Control System (the "WCS Data Sheet").

If Customer obtains a WCS limited license, Customer may not use the Software to manage more access points than those identified in the Software's Cisco SKU or the product description on Customer's accepted, paid Purchase Order plus those identified in the Software's Cisco SKUs or the product descriptions on Customer's prior accepted, paid Purchase Orders.

If Customer obtains a WCS demonstration license, Customer may not use the Software to manage more than the number of access points identified for the Cisco WCS demonstration license in the WCS Data Sheet.

Customer may use the Software only to manage those devices identified as managed devices in the product specifications section of WCS Data Sheet.

Server Restrictions

Customer may install and run the Software on multiple servers if the Software's Cisco SKU or product description on Customer's accepted, paid Purchase Order identifies the product as an enterprise or "ent" license. Otherwise, Customer may install and run the Software on only a single server.

Third-Party Proprietary Software

The Software includes proprietary software and technology from Cisco's suppliers. Some suppliers are intended third-party beneficiaries of the EULA and this supplement. Third-party-beneficiary suppliers include: (a) Hifn, Inc.; (b) Wind River Systems, Inc. and its suppliers; and (c) any other supplier Cisco identifies as a third-party beneficiary in the Documentation or additional supplements. These suppliers may enforce, and are express beneficiaries of, the EULA and this supplement. However, they are not in any contractual relationship with Customer.

The limited warranty in the EULA is made only by Cisco and is disclaimed by all Cisco suppliers. Cisco and any Cisco supplier may obtain injunctive relief if Customer's use of the Software is in violation of any license restrictions.

Open-Source Software

The Software includes certain open-source software. Despite anything to the contrary in the EULA or this supplement, the open-source software is governed by the terms and conditions of the applicable open-source license. The open-source software, the applicable open-source licenses and other open-source notices may be identified in the Documentation or in a README file accompanying the Software. Customer agrees to comply with all such licenses and other notices.

Other Terms and Conditions

The terms of the EULA and this supplement may be enforced by license registration and other software tools.

APPENDIX C

Conversion of a WLSE Autonomous Deployment to a WCS Controller Deployment

This chapter describes how to convert a Cisco Wireless LAN Solution Engine (WLSE) network management appliance to a Cisco Wireless Control System (WCS) network management station. After converting a WLSE appliance to WCS, you must re-create configuration templates and manually add access points (or import them). For information on how to migrate the data, refer to the "Importing or Exporting WLSE Map Data" section on page 5-79.

After WLSE is converted to WCS, it can no longer be used as a WLSE or converted back into a WLSE. This is a one-way conversion only.

- WLSE Autonomous: A WLSE network management appliance is deployed with autonomous access points from the Aironet products. Some access points act as domain controllers (WDS) for sets of access points in a SWAN architecture, and the access points communicate over the wired network using the WLCCP protocol.

  The WLSE network management station is a Cisco appliance with the WLSE software installed.

- WCS Controller: A WCS network management station is deployed on customer selected hardware running Red Hat Enterprise Linux. The network management station manages controller switches that control access points. The controllers communicate over the wired network with access points using the LWAPP protocol.

  - WCS maintains the Cisco wireless LAN solution configuration, which includes controllers, access points, and location appliances.
  - It enables Cisco WCS system administrators to assign logins, passwords, and privileges for all Cisco WCS operators and to set times for periodic system tasks.
  - It allows Cisco WCS operators to use a web browser on any connected workstation to access Cisco WCS configuration, monitoring, and administrative functions. The Cisco WCS operators can also add, change, and delete Wireless LAN Solution components and configurations in the Cisco WCS database, depending on privilege level.

This chapter contains these sections:

- Supported Hardware, page C-2
- Installation and Configuration, page C-2
- Minor Upgrades to WCS, page C-3
- Licensing, page C-7

Supported Hardware

Cisco WLSE Management Stations

The conversion from WLSE management station to WCS management station is supported on the Cisco 1130-19 and 1133 hardware platforms.

Note The conversion from WLSE management station to WCS management station is not supported on the Cisco WLSE 1030 Express platform.

Autonomous Access Points Convertible to LWAPP

The following autonomous AP models can be converted to a WCS controller deployment:

- Cisco Aironet 1230AG Series Access Point (AP 1232AG)
- Cisco Aironet 1200 Series Access Point (AP 1200)
- Cisco Aironet 1130AG Series Access Point (AP 1131AG)

Installation and Configuration

To convert a WLSE network management appliance to a WCS network management station, you need three CDs:

- A conversion CD for the Wireless Control System version 4.0 release. This CD installs the WCS software and Red Hat Enterprise Linux 3 on the WLSE network management appliance.
- An upgrade CD to upgrade the WCS network management station to Red Hat Enterprise Linux 4. It is necessary to complete the installation of WCS software and Red Hat Enterprise Linux 3 prior to performing the Red Hat Enterprise Linux 4 upgrade due to the partitioning of the WLSE network station.

Note After you have converted the WLSE network management appliance to a WCS network management station, it is irreversible and you cannot convert back to a WLSE network management appliance.

- An upgrade CD to upgrade the WCS network management station to Red Hat Enterprise Linux 5. It is necessary to complete the installation of WCS software and Red Hat Enterprise Linux 4 prior to performing the Red Hat Enterprise Linux 5 upgrade due to the partitioning of the WLSE network station.

Installing Cisco WCS

Follow these steps to install the Cisco WCS software. You need to have physical access to the WLSE network management appliance. Console access is necessary to the WLSE appliance because the setup and install scripts require console interaction. The complete installation process takes approximately 45 seconds.

Note Before installing the WCS software, backup any data on your WLSE appliance that you would like for record keeping. To backup the data, refer to *Backing Up and Restoring Data* in the *User Guide for the CiscoWorks WLSE and WLSE Express*.

Step 1 Insert the installation CD with the WCS software and the Red Hat Linux Enterprise 3 software into the CD drive of the WLSE network management appliance.

Step 2 Using the command line interface (CLI) prompt, log in the WLSE as **administrator**.

Step 3 Enter the **reload** command to reboot. The WLSE reboots, loads, and then installs from the CD. After the install, the CD automatically ejects and reboots again.

Step 4 Log in using **root** as the username and **setup** as the password. You are guided through the WCS wizard setup scripts as you would in a regular WCS install. Answer the prompts with the applicable values for your network setup. See "Installing WCS for Linux" procedure on page 2-11 if you need further assistance.

Note If you cannot execute the installation file, enter the **chmod +x WCS-install-file.bin** command.

Step 5 When you are prompted to reboot, type **Y** or **Yes**. After the reboot continue to Upgrading to Red Hat Enterprise Linux 4 or 5.

Upgrading to Red Hat Enterprise Linux 4 or 5

Follow these steps to upgrade the WLSE network management station to Red Hat Enterprise Linux 4 or 5.

Note Before upgrading the Red Hat Enterprise Linux, you should have already converted WLSE to the Cisco WCS software and Red Hat Linux Enterprise 3 software.

Step 1 Insert the upgrade CD with the Red Hat Enterprise Linux upgrade software (either version 4 or 5 as needed) into the CD drive of the WLSE network management appliance.

Step 2 Log in using **root** as the username and the password you were supplied in the wizard.

Step 3 Enter the **reboot** command to reboot the WLSE network management appliance.

Minor Upgrades to WCS

If you need to perform a minor upgrade that does not require an upgrade of Red Hat, you can download the upgrade from cisco.com and burn a CD yourself. If you burn a CD yourself, you cannot access the CD drive from the Linux CLI so you must mount the CD drive using mount /dev/cdrom /media.

Configuring the Converted Appliance

If you have installed Red Hat Linux 3 with the CD and performed the upgrade to 4.0, you are ready to configure the appliance. After the Linux installation, the machine reboots. You must have a connection to the appliance console, and then you are prompted to log in. After you log in, you are presented with the following prompts over the console connection.

Caution After WLSE is converted to WCS, it can no longer be used as a WLSE or converted back into a WLSE. This is a one-way conversion only.

Note The WCS server will not start until you have configured the appliance.

```
localhost.localdomain login:
```

Enter the login **root**.

```
Password:
```

Enter the **setup** password.

```
Setup parameters via Setup Wizard (yes/no) [yes]:
```

Enter **yes** if you want to use the setup wizard or **No** if you want to manually set the parameters. Only experienced Linux system administrators should opt to configure the system using the setup script. The option in square brackets is the default. You can press **Enter** to choose that default.

```
Current hostname=[localhost]
Configure hostname?  (Y)es/(S)kip/(U)se default [Yes]:
```

The host name is a unique name that can identify the device on the network.

```
Enter a host name [localhost]:
```

The host name should start with a letter, end with a letter or number, and contain only letters, numbers, and dashes.

```
Current domain=[localdomain]
Configure domain name? (Y)es/(S)kip/(U)se default [Yes]:
```

A domain name specifies the network domain this device belongs to.

```
Enter a domain name [localdomain]:
```

The domain name should start with a letter, end with a valid domain name suffix (such as .com), and contain only letters, numbers, dashes, and dots.

```
Configure root password? (Y)es/(S)kip/(U)se default [Yes]:
```

Press **Enter** to choose Yes.

```
Enter root password:
Confirm root password:
```

Enter a password for the superuser and confirm it by typing it again. Your typing is not visible.

```
Remote root login is currently disabled.
Configure remote root access? (Y)es/(S)kip/(U)se default [Yes]:
```

To enable root login over secure shell for this machine, choose **Yes**. This allows a **root** login both from the console and using SSH. Otherwise, choose **Skip**. If you choose to leave remote root login disabled, then a *root* login can only occur from the console.

```
Enable remote root login (yes/no) [no]
```

Choose **yes** to allow remote login through SSH in addition to console login. Choose **no** to allow root login only from the console.

```
Current IP address=[]
Current eth0 netmask=[]
Current gateway address=[]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Yes]:
```

Choose **Yes** to begin setup for the main ethernet interface. A network administrator can provide the information for the following prompts.

```
Enter eth0 IP address:
```

Enter an IP address for the main ethernet interface of this machine.

```
Enter network mask [255.255.0.0]:
```

Enter the network mask for the IP address you provided.

```
Enter default gateway address:
```

Provide the default gateway that must be reachable from the main Ethernet interface.

```
The second ethernet interface is currently disabled for this machine.
Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Yes]:
```

Choose **Yes** if you want to provide information for a second Ethernet interface. If you choose to configure eth1, you must manually edit the WCS property file (/opt/WCS4.0/webnms/classes/com/aes/common/net/LocalHostUtils.properties) to specify which of the eth1 or eth0 are used to communicate with controllers and which are used to communicate with location servers. (Changing the ManagementInterface= line to either ManagementInterface=eth0 or ManagementInterface=eth1 specifies the controller interface. Changing the PeerServerInterface= line to either PeerServerInterface=eth0 or PeerServerInterface=eth1 specifies the location server interface. This can be skipped, and the next prompt you would see would be DNS.

```
Enter eth1 IP address [none]:
```

Enter an IP address for the second Ethernet interface on this machine.

Because you entered an IP address for the second interface of this machine, you are given the opportunity to define up to two static routing entries for that interface. Each entry requires a network address, network mask, and a gateway address.

```
Enter network mask [255.0.0.0]:
```

Enter the network mask for the IP address you specified.

```
Enter network [none]:
```

Enter the network address.

```
Enter network mask [255.0.0.0]:
```

Enter the network mask for the IP address you provided.

```
Enter gateway address:
```

Enter a gateway address for the network and network mask you provided.

```
Domain Name Service (DNS) Setup
DNS is currently enabled.
No DNS servers currently defined
Configure DNS related parameters? (Y)es/(S)kip/(U)se default [Yes]:
```

You can enter up to three DNSs, but you can also leave it disabled. No servers have been defined.

```
Enable DNS (yes/no) [yes]:
```

Choose **Yes** to enable DNS.

```
Enter primary DNS server IP address:
```

Enter the IP address for this DNS server.

```
Enter backup DNS server IP address (or none) [none]:
```

Enter the backup IP address. If you enter a second DNS server, you are prompted for an optional third server.

```
Configure timezone? (Y)es/(S)kip/(U)se default [Yes]:
```

Choose **Yes** to configure the timezone.

```
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
 5) Asia
 6) Atlantic Ocean
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
11) UTC - I want to use Coordinated Universal Time.
12) Return to previous setup step (^).
```

You need to select a location so that time zone rules can be set correctly. Choose the number for the appropriate continent or ocean.

```
Please select a country.
```

You are given a choice of countries based on the continent or ocean you selected. Choose the appropriate number.

```
Please select one of the following time zone regions.
```

Enter the number for the desired time zone region based on the country you selected.

The timezone information you chose is given.

```
Is the above information OK?
1) Yes
2) No
```

Choose **Yes** to verify if the information is correct. If No, you will be taken through the series of prompts again.

```
NTP is currently disabled.
Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Yes]:
```

If you choose to enable network time protocol (NTP), the system is configured from the NTP servers you select. If you choose Skip, you are prompted to enter the current date and time.

```
Enable NTP (yes/no) [no]:
```

If you choose Yes, you will be required to enter an NTP server name or address.

```
Enter NTP server name or address:
Enter another NTP server IP address (or none) [none]:
```

All of your selections are shown. You are then asked to verify all the setup information you provided. You can enter Yes to proceed with the configuration, No to make more changes, or ^ to go back to the previous step.

```
Is the above information correct (yes, no, or ^):
```

If yes, the configuration information will be applied. Cisco recommends that you reboot the system when prompted to ensure that changes occur. The WCS server starts automatically after the reboot.

The next time you log in using *root*, you will only get the Linux shell prompt and not the setup script. You can rerun the setup script at any time to change settings by logging in using *root* and running /opt/setup-appliance/setup.sh.

Licensing

You will need a license to access the complete WCS user interface on the WLSE network management appliance. A discounted WCS WLSE Upgrade License is available for these appliances. When you purchase the license, you receive the WCS-WLSEU-K9-4.1.xx.0.iso conversion file you need and the WCS-WLSEU-K9-4.0.xx.0.upgrade.iso upgrade file you need.

Note In the filename *xx* represents the version number.

WLSE Upgrade License

The WLSE Upgrade license can only be used on a converted WLSE appliance. It cannot be transferred to a different machine at a later time.

The WLSE Upgrade license must be specific to the hostname of the network station that you are converting from WLSE to WCS. The installation and startup will proceed without the license but you cannot access the WCS user interface without the license.

To install the license, refer to the Appendix B, “WCS and End User Licenses.”

INDEX

Numerics

40 MHz channel bonding 10-42
802.11a/n Parameters
  High Throughput 10-41
802.11a policy name 12-83
802.11 association diagnostic test 11-20
802.11b/g/n DTIM period 12-31
802.11b/g RRM interval template 12-93, 12-95
802.11b/g RRM threshold templates 12-91
802.11b/g voice templates 12-86
802.11 counters report 17-87
802.11h template 12-94
  configuring 12-94
802.11n summary reports 17-82
802.11 security trap 12-103
802.11 tags
  filtering 5-59
802.1n scaling reports 17-3
802.1X authentication diagnostic test 11-20
802.1X supplicant credentials 12-9
802.3 bridging
  configuring 10-37
880 series ISRs 1-6

A

AAA override 12-27
AAA servers 12-26
AAA traps 12-103
absolute 21-2
Access 9-25
access control list template 12-74
access control list templates 12-69
access mode 9-6
access point
  configuring 12-59
  configuring for hybrid REAP 15-9
  credentials 9-2
  friendly 12-81
access point/radio templates 12-113
access point authentication and MFP templates 12-63
access point authorization template 12-59
access point configuration
  importing 9-25
access point floor settings
  filtering 5-55
access point heatmap
  filtering 5-33
access point icon 5-61
access point icons 5-62
access point load
  avoiding 12-85
Access point placement 5-49
access point placement 5-49
access point positions
  changing with import or export of file 5-53, 5-78
access points
  adding 5-44
  configuring 9-17
  configuring for LOMM 9-33
  converting to LWAPP C-2
  detecting 16-21
  embedded 1-6
  positioning 5-53
  searching 2-35, 9-35

selecting 12-132
access points, adding to maps 5-44 to 5-49
access point security statistics
for mesh 6-15
access point templates
adding 12-113
access point threats 3-8
access point threats or attacks 3-8
access point traps 12-103
acknowledged alarms
hiding 16-16
acknowledging alarms 16-16
ACL
template 12-69
ACL IP group details 12-70
ACL template 12-74
configuring 12-74
ACS server
adding WCS to 18-8
ACS View Server credentials 6-2
ACS view server tab 11-18
active interferer count per channel 9-39
active interferers 9-38
active interferers count chart 9-39
active sessions
monitoring 7-4
adaptive scan threshold 12-91
adaptive wIPS alarm report 17-103
adaptive wIPS top 10 APs report 17-105
add config groups 8-20
add group members 8-10
adding access point templates 12-113
adding a mobility services engine 13-2
adding a spectrum expert 9-37
adding autonomous access points
by CSV file 9-10
by device information 9-10
adding autonomous access points to WCS 9-10
adding a WLAN 10-23
adding controllers 10-2
adding event groups 13-10
adding IOS access points 9-10
by device information 9-10
adding launch points
for Google Earth 21-7
adding SNMP entries 18-56
adding templates from config group 8-23
adding WCS as TACACS+ server 18-9
adding WCS to ACS server
for use with RADIUS 18-13
adding WCS to an ACS server 18-8
adding WCS to a non-Cisco ACS server 18-17
adding WCS usergroups
into ACS for RADIUS 18-14
into ACS for TACACS+ 18-10
adhoc rogue events report 17-107
adhoc rogues 2-26, 3-6
adhoc rogues report 17-109
adjusted link metric 6-5
administration menu 2-29
advanced debug 19-6
advanced options 5-39
advanced search 2-32, 16-12
Advanced tab
on WLAN template 12-29
age out dual band 10-33
age out suppression 10-33
aggregated historical data 18-7
aggressive load balancing 10-30
Aironet IE 10-21, 12-30
alarm 16-1
alarm cleanup options 18-36
alarm counts
for access points 16-4
for controllers 16-4
for coverage hole 16-4
for malicious APs 16-4
for mesh links 16-4

for mobility 16-4
for security 16-4
for unclassified APs 16-4
for WCS failures 16-4
alarm dashboard 16-1
alarm details
viewing 16-9
alarm display options 18-36
alarm indicator 16-1
alarms 16-1
acknowledging 16-16
assigning 3-21
clearing 3-21
config audit 19-10
deleting 3-21
monitoring 16-5
rogue access point 16-11
rogue adhoc 16-19
searching 2-34
unassigning 3-21
alarm severity
configuring 16-14
alarm summary 2-30
alarm trigger threshold 12-64
alarm warning 16-16
all groups window 18-11
allow AAA override 10-20
alternate parent report 17-69
altitude 21-2
altitude mode 21-2
anonymous provision 12-51
anonymous provisioning 12-51
AP attack details 2-21
AP authentication
template 12-63
AP authorization
template 12-59
AP-detected interferers
searching 2-39
AP failover priority
setting 9-1, 10-38
AP join taken time 11-7
AP load
avoiding 12-85
AP manager IP 9-16
AP mesh info
filtering 5-35
AP mode 12-114
AP parameters tab 12-113
applying CLI commands 12-109
applying config groups 8-23
applying controller templates 12-112
AP policies 3-36
AP policies template 12-77
AP primary discovery timeout 10-39
AP profile status report 17-49
APs not assigned to maps 2-20
AP status report
viewing for scheduled task 12-121
AP template task history
viewing 12-122
AP template tasks 12-121
AP threats and attacks 11-7
AP timers
configuring 10-12
AP up time 6-11
AP uptime 2-26
asset matching criteria 13-12
assigned virtual domain components 20-10
assigning location presence 5-7
assigning virtual domains 7-16
association request failures 6-18
association request success 6-18
association request timeouts 6-18
asynchronous 18-33
attacks
access points 3-8
attacks detected 3-9

audit 18-37
AUDIT_STATUS_DIFFERENCE 16-77
auditing config groups 8-24
auditing H-REAP groups 15-16
audit report 18-37
  for alarms 16-10
audit reports
  configuring 9-35, 10-34
audit status 6-14
  viewing 10-34
  viewing for access points 9-35
  viewing for controllers 10-34
audit trail
  viewing 7-9
authentication order
  managing 10-34
authentication priority 10-34
  template 12-108
authentication process
  Hybrid REAP 15-2
authentication request failures 6-18
authentication request success 6-18
authentication request timeout 6-18
auto key generation 12-36
automated upgrade 14-9
automatic backups, scheduling 14-3, 18-1
automatic client exclusion 12-30
automatic client troubleshooting 11-10, 18-39, 18-40
automatic database synchronization 13-6
autonomous access points
  adding 9-10
  adding by CSV file 9-10
  downloading images 9-12
  upgrading 9-14
  viewing 9-12
autonomous AP images
  downloading 9-25
autonomous to lightweight migration 9-9
autonomous to LWAPP migration support 9-9
auto provisioning 18-19
auto provisioning filter
  editing 18-24
auto refresh 5-71, 5-72, 18-41
avoid access point load 12-85
avoid Cisco AP load 12-85
avoid foreign AP interference 12-85
avoid non-802.11 noise 12-85

B

background scanning 10-65
  on mesh configuration 12-99
  on templates 12-99
background scanning in mesh networks
  described 10-64 to 10-65
  scenarios 10-64 to 10-65
Background Scan parameter 10-66
background tasks
  running 18-1
backhaul interface 6-16
backing up the WCS database
  on Linux 14-5
  on Windows 14-4
backup and restore license B-4
band selection 10-31
bandwidth
  making expedited 12-87
battery level
  condition type 13-12
best practices A-1
bridge group 12-118
bridge group name 6-16
Bridging link information 6-5, 6-21
bridging link information 6-5, 6-21
bridging mesh statistics 6-16
broadcast deauthentication frame signatures 3-39
bronze 12-29
bronze queue 6-18

buildings
adding to a campus map 5-5
adding to WCS database 5-9
busiest APs report 17-51
busiest client report 17-22

C

CAC
enabling 10-39
CA certificates 4-4
CAD files 5-5
calculating access point requirements 5-37
calibrating client 12-111
call admission control 12-86
campus map, adding to WCS database 5-4
CAS 13-1
cascade reboot 8-25
category
for alarms 16-7
CDP 12-116
certificate signing request 3-49
change order buttons 17-7
changing access point positions 5-78
by importing or exporting a file 5-78
changing station role
root mode 9-15
channel bonding
configuring 10-42
channel change AP 6-40
channel change notifications 6-37
channel width
monitoring 6-23
checking the status of WCS
on Linux 14-2
on Windows 14-1
child-to-parent ping test 11-9
chokepoint
condition type 13-12
chokepoint icon 5-62
chokepoints
positioning 5-53
CIDR notation 12-70
Cisco Aironet 1510 Access Points
in Mesh network 10-64
Cisco AP load
avoiding 12-85
Cisco Discovery Protocol 9-22, 12-116
Cisco WCS base B-1
Cisco wired IPS events 2-26
Cisco Wireless LAN Solution
overview 1-1 to 1-2
security solutions 3-1 to 3-34
civic address 5-8
CKIP 10-18
clamped to ground 21-2
classification rule 12-77
clear config 9-25
CLI
template 12-108
CLI commands
applying to template 12-109
client
calibrating 12-111
managing 11-1
client alarm summary 11-5
client association failure 11-5
client authentication failure 11-5
client authentication provision 12-51
client authentication type distribution 11-6
client count 2-20, 11-3
client count report 17-24
client detail page 11-8
client details
retrieving from access point page 11-11
client devices
connecting to WLANs 15-12
client distribution 11-2

client elements 18-71
client excluded 11-5
client exclusion 10-21, 12-30
  happening automatically 12-30
client exclusion policies 12-61
  template 12-61
client exclusion policies template 12-61
client floor
  filtering 5-57
client icon 5-61
client MFP 3-36
client protocol distribution 11-3
client related traps 12-102
client reports 17-21
clients
  searching 2-37
clients detected by location server 2-26
client security events 2-26
client sessions report 17-26
client summary report 17-29
client tab 2-20, 11-1
client tab dashboard 11-11
client traffic 11-6
client troubleshooting
  automatic 18-39
  enabling 11-10
client WEP key decryption error 11-5
client WPA MIC error counter activated 11-5
CLI sessions 18-43, 18-60
color coding
  of obstacles 5-32
command buttons 2-30
compliance reports 17-41
component options icon 2-29
components
  of virtual domain 20-10
condition type
  for event definitions 13-11
config audit 19-9
config audit alarms 19-10
config group
  adding controllers 8-22
  adding templates 8-23
  configuring 8-21
  downloading IDS signatures 8-27
  downloading sw to controllers 8-26
  removing controllers 8-22
  removing templates 8-23
config group audits 8-24
config groups
  applying 8-23
  auditing 8-24
  creating 8-19
  downloading customized webauth 8-27
  rebooting 8-25
  reporting 8-26
config group task
  deleting 12-124
config group task history
  viewing 12-124
config group tasks 12-123
configuration audit report 17-41
configuration audit summary 19-9
configuration mismatch 6-39
configuration sync 18-5, 18-6
Configure Controllers
  802.11a/n Parameters
    High Throughput 10-41
configure menu 2-29
configuring 40 MHz channel bonding 10-42
configuring 802.3 bridging 10-38
configuring access points 9-17
configuring a client exclusion policy template 12-79
configuring a CPU ACL template 12-74
configuring a high throughput template 12-95
configuring alarm severity 16-14, 16-86
configuring a local EAP general template 12-46
configuring a local EAP profile template 12-47

configuring a manually disabled client template 12-60
configuring a mesh template 12-95, 12-98
configuring an 802.11h template 12-94
configuring an access point 12-59
configuring an access point for hybrid REAP 15-9
configuring an EAP-FAST template 12-49
configuring an RRM interval template 12-93
configuring an RRM threshold template 12-91
configuring a policy name template 12-83
configuring AP timers 10-12
configuring a roaming parameters template 12-88
configuring a TACACS+ server template 12-41
configuring a trusted AP policies template 12-77
configuring audit reports 10-34
configuring a user authentication priority template 12-108
configuring a user login policies template 12-56
configuring a video parameter template 12-87
configuring a voice parameter template 12-86
configuring config group 8-20
configuring controller WLANs 10-13
configuring DHCP proxy 10-10
configuring EDCA parameters
for individual controllers 10-44
through a template 12-88
configuring firewall for WCS 3-35
configuring global credentials 9-2
configuring global email parameters 18-46
configuring high availability 18-64
configuring H-REAP AP groups 12-32
configuring Hybrid REAP 13-1, 15-1
configuring hybrid REAP access point groups 15-12
configuring Hybrid-REAP groups 15-14
Configuring IDS 3-38
Configuring IDS signatures 3-38
configuring IDS signatures 3-38
configuring IGMP snooping 10-12
configuring intrusion detection systems 3-38
configuring LDAP bind requests 10-12
configuring multiple country codes 8-16
configuring NAC out-of-band 10-45
configuring radio templates 12-130
configuring RADIUS servers 18-31
configuring scheduled configuration tasks 12-121
configuring search results 2-44
configuring SNMPv3 10-44
configuring spectrum experts 9-37
configuring template
ACL 12-60
for rogue AP rule groups 12-79
configuring templates
802.11b/g RRM interval 12-93
802.11b/g RRM threshold 12-87
802.11b/g voice 12-86
access point/radio 12-113
access point authentication and MFP 12-77
access point authorization 12-59
file encryption 12-36
guest users 12-54
known rogue access point 12-94
local management user 12-106
MAC filter 12-57
QoS 12-13
RADIUS accounting 12-40
RADIUS authentication 12-37
syslog 12-105
Telnet SSH 12-104
traffic stream metrics QoS 12-16
trap control 12-101
WLAN 12-18
configuring the controller for hybrid REAP 15-5
configuring the switch
for hybrid REAP 15-4
configuring wired guest access 10-51
connecting client devices
to WLANs 15-12
Connecting to the Guest WLAN 3-49
Containment 6-1
containment

of rogue access point 16-21
of rogue access points 6-1
content
customizing 2-24
context aware configuring 13-14
context aware planning 13-14
context-aware software 13-1
controller
configuring for hybrid REAP 15-5
controller CPU utilization 2-26
controller details 9-16
controller license information 18-69
controller licenses
managing 18-74
searching 2-43
controller license status 18-6
controller memory utilization 2-26
controllers
adding 10-2
adding to WCS database 4-1
pinging network devices 10-39
searching 2-36, 10-33
specified 1-1
controller status report
viewing 12-123
controller template launch pad 12-1
controller templates
applying 12-112
controller upgrade settings 18-41, 18-43, 18-60
controller values
refreshing 10-36
controller WLANs
configuring 10-13
converting WLSE autonomous to WCS controller C-1
country codes
multiple 8-16, 10-29
setting 10-29
coverage hole 6-32, 6-39
coverage hole reports 17-89
coverage holes 2-20
CPU access control
template 12-74
Cranite 10-16
Creating a network design 5-51
creating a network design 5-51
creating a virtual domain 20-1
Creating guest user accounts 7-10
creating guest user accounts 7-10
creating placemarks 21-3
creating virtual domains 20-1
CSR 3-49
CSV file 9-10
method for adding autonomous access points 9-10
sample 10-3
CSV files 21-4
current AP template task
deleting 12-122
disabling 12-122
enabling 12-122
modifying 12-121
current config group task
disabling 12-123
enabling 12-123
modifying 12-123
currently logged guest users 2-28
current templates
viewing 10-45
customized web auth 10-56
customized webauth
downloading 8-27
Customized Web authentication 3-47
customized web authentication
downloading 12-67
customize report 17-7
customizing content on WCS Home page 2-24
customizing tabs on WCS Home page 2-23
Custom signature 3-44

D

dashboard
RRM 6-36
database synchronization
automatic 13-6
data collection
for RFID tag 12-111
data management tasks
performing 18-34
data retention 18-40
debug commands A-4
debug strategy A-4
default lobby ambassdor credentials
editing 7-9, 7-14
deleting a current AP template task 12-122
deleting a current config group task 12-124
deleting a license B-4
deleting a mobility services engine 13-4
deleting a WLAN 10-24
deleting controller templates 12-113
deleting event groups 13-11
deleting guest user templates 7-12
deleting WCS user accounts 7-4
designing a network 5-73
destination type
for report 17-4
detecting access points 16-21
detecting rogue access points 6-2
device certificates 4-3
device information 9-10
method for adding autonomous access points 9-10
device reports 17-48
DHCP diagnostic test 11-20
DHCP proxy
configuring 10-10
DHCP server
overriding 12-31
DHCP statistics 6-34
diagnostic channel A-1
diagnostic test
802.11 association 11-20
802.1X authentication 11-20
DHCP 11-20
DNS ping 11-20
DNS resolution 11-20
IP connectivity 11-20
profile redirect 11-20
disabled clients
template 12-60
disabling a current config group task 12-123
disabling current AP template task 12-122
disabling IDS signatures 3-43
discovering templates
from controllers 10-9
Distance
condition type 13-12
DNS ping diagnostic test 11-20
DNS resoltion diagnostic test 11-20
downloading a customized web authentication page 12-67
downloading autonomous AP images 9-25
downloading customized webauth 8-27
Downloading customized web authentication 3-47
Downloading IDS signatures 3-42
downloading IDS signatures 3-42
from your config group 8-27
downloading images
to autonomous access points 9-12
downloading sw to controllers
after adding config group 8-26
downloading vendor CA certificates 4-4
downloading vendor device certificates 4-3
downstream delay 12-17
downstream packet loss rate 12-17
drawing polygon areas
using map editor 5-30
DTIM 12-84
dynamic interface 12-11

E

EAP-FAST
  template 12-50
EAP-FAST template 12-49
EAPOL flood signature 3-40
EDCA parameter
  template 12-88
EDCA parameters
  configuring for individual controllers 10-44
  configuring through a template 12-88
edit content 2-25
edit contents 2-25
editing map properties 5-13
editing saved reports 17-12
editing scheduled run details 17-10
Editing signature parameters 3-46
editing the default lobby ambassador credentials 7-9, 7-14
edit link 5-21
edit links
  home page 2-23
edit location presence information 5-7
Edit View
  general 2-44
edit view
  for alarms 16-8
egress interface 10-16
email
  configuring parameters 18-45
email notifications
  monitoring 16-23
embedded access points 1-6
emergency
  condition type 13-12
enable background audit 8-20
enable enforcement 8-20
enable log module 18-32
enabling a current config group task 12-123
enabling audit trails
  for guest user activities 7-10
enabling current AP template task 12-122
enabling IDS signatures 3-43
enabling load-based CAC 10-37
Enabling Web login 3-46
enabling Web login 3-46
end user license agreement B-7 to B-12
establishing logging options 18-32
Ethernet bridging 9-3
Ethernet VLAN tagging guidelines 9-5
evaluation license
  for controller 18-70
  for MSE 18-70
event groups 13-10
event history 11-17, 16-10
event notification 1-5
Events 16-1
events 16-1
  monitoring 16-22
  searching 2-38
exclude device list 18-61
excluded packets 6-17
exclude switch trunk ports 18-61
exclude vendor list 18-61
executive summary report 17-84
expedited 12-87
expedited bandwidth 12-87
exporting a file 5-53
  to change access point position 5-53, 5-78
export task list 18-11
extend to ground 21-2
extension license
  for controller 18-70
  for MSE 18-71
external antennas 12-132
external web auth 10-56
extracting task list 18-17

F

Failover 18-62
failover mechanism 18-62
failover scenario 18-62
failure source
  for alarms 16-7
fast heartbeat interval 10-13
feature
  of WCS license 18-68
feature license B-2
file encryption template 12-36
filter
  editing current auto provisioning 18-24
filtering
  using to modify maps 6-21
filtering 802.11 floor settings 5-59
filtering client floor settings 5-57
filtering floor setting
  for access points 5-55
filtering floor settings
  for AP mesh info 5-35
filtering rogue adhoc settings 5-60
filtering rogue AP settings 5-59
filtering rogue client floors 5-60
filtering saved reports 17-11
filtering scheduled run results 17-10
firewall, configuring for WCS 3-35
floor area map 5-54
Floor Areas
  edit 5-72
floor component details 5-61
floor plans
  adding to a campus building 5-22 to 5-27
  adding to a standalone building 5-27 to 5-29
floor settings 5-54
foreign access point interference
  avoiding 12-85
foreign AP interference
  avoiding 12-85
Frame type 3-44
friendly access point template 12-81
friendly AP
  template 12-81
friendly rogue 12-77
friendly rogue access points 3-7
friendly rogue APs 2-26
FTP
  turning on and off 18-54

G

general tab
  home page 2-19
general templates
  configuring 12-4
generating migration analysis report 9-15
geographical coordinates 21-1
global credentials
  configuring 9-2
Global settings
  for standard and custom signatures 3-46
gold 12-29
gold queue 6-17
Google Earth
  adding launch points 21-7
Google Earth coordinates 21-2
Google Earth maps 21-1
  viewing 6-26
Google KML or CSV
  importing into WCS 21-5
GPS markers 5-8
grace period license
  for controller 18-70
groups
  for hybrid-REAP 15-14
  for rogue access point rules 12-79
group setup window on ACS server 18-12

GUEST_USER_ADDED 16-74
GUEST_USER_AUTHENTICATED 16-75
guest account settings 18-43
guest accounts status report 17-62
guest association report 17-64
guest count report 17-65
guest reports 17-62
guest user
  template 12-54
guest user account
  scheduling 7-12
Guest user accounts
  creating 7-10
guest user accounts
  creating 7-10
  managing 7-12
guest user details
  emailing 7-14
  print 7-14
guest user monitoring 6-36
guest user reports 17-120
guest users
  currently logged 2-28
guest user sessions report 17-66
guest user templates 12-54
Guest WLAN
  connecting 3-49
guidelines
  for Ethernet VLAN tagging 9-5
  for NAC out-of-band integration 10-46
guidelines for using the map editor 5-29

H

heater status 6-11
heat map
  described 5-48
help menu 2-30
hide acknowledged alarms 16-16
hierarchy
  of mesh network 6-19
Hierarchy of Mesh parent to child 6-22
hierarchy of mesh parent to child 6-22
High Throughput
  802.11a/n 10-41
high throughput
  template 12-95
high throughput template
  configuring 12-95
historical data 18-7
historical report type 17-1
Home page
  customizing content 2-24
  customizing tabs 2-23
H-REAP AP groups
  configuring 12-34
  configuring template 12-34
H-REAP configuration 12-117
H-REAP configuration tab 12-35
H-REAP groups
  auditing 15-16
H-REAP local switching 10-20
HTTP
  turning on and off 18-54
Hybrid REAP
  configuring 9-1, 10-1, 15-1
hybrid REAP access point groups 15-12
hybrid-REAP groups 15-13
Hybrid REAP local switching 12-30
hysteresis 12-91

I

identical audit status 6-14
IDS 3-38
  configuring 3-38
IDS sensors 3-38
IDS signatures 3-38

disabling 3-43
downloading 3-42
downloading from config group 8-27
enabling 3-43
uploading 3-41
IGMP snooping
configuring 10-12
images
downloading to autonomous access points 9-12
importing access point configuration 9-25
importing a file 5-53
to change access point position 5-53, 5-78
importing coordinates
as CSV file 21-4
into Google Earth 21-2
importing Google KML or CSV into WCS 21-5
In/Out
condition type 13-12
information elements
Aironet 12-30
infrastructure MFP 3-36
ingress interface 10-16
inspect location readiness 5-43
installer
using to upgrade 14-10
installing a license B-4
installing WCS
for WLSE conversion C-2
insufficient memory 6-17
integrating NAC out-of-band 10-45
interferers
summary 9-38
internal antennas 12-132
internal web auth 10-56
inter-subnet roaming 8-4
Intrusion Detection Systems 3-38
intrusion detection systems 3-38
invalid association request 6-19
invalid reassociation request 6-19
inventory detail status 2-20
inventory reports 17-41, 17-55
inventory status 2-27
IOS access points
adding 9-10
adding by device information 9-10
IOSAP_DOWN 16-76
IOSAP_LINK_DOWN 16-75
IOSAP_LINK_UP 16-75
IOSAP_UP 16-76
IP connectivity diagnostic test 11-20

K

KEK
key encryption key 12-39
key wrap 12-39
KML file 21-2

L

LAG advantages 12-8
LAG mode 12-6
latest network audit report 10-37
latitude 21-2
launch pad
for controller templates 12-1
Layer 1 security solutions 3-2
Layer 2 12-20
Layer 2 security solutions 3-2
Layer 3 12-24
Layer 3 security solutions 3-2
Layer 3 to Layer 2 mode, converting Cisco Wireless LAN Solution 3-34
LBS authorization 12-59
template 12-59
LDAP 10-28
LDAP bind requests
configuring 10-28

LDAP servers 10-20
template 12-43
LEAP authentication
requirements 8-8
legacy beam forming 12-132
legacy syslog
template 12-105
legacy syslog template 12-105
license
backup and restore B-4
license agreement B-7 to B-12
license installation B-4
license management 18-75
licenses B-1
license status 18-6
license types B-1
licensing 18-67
on WLSE network management C-4
limitations for high reliability 18-63
link aggregation 12-8
link aggregation (LAG)
guidelines 15-4
link latency 12-117
link metric
adjusted 6-5
unadjusted 6-5
link SNR 6-5
link stats report 17-70
Link test
running 11-9
link test
running 11-9
Link test result 11-10
load 5-72
load balancing 10-30
load-based AC 12-87
load-based CAC 12-87
enabling 10-39
Lobby ambassador 7-10
lobby ambassador defaults
setting 7-7
local authentication
for hybrid-REAP groups 15-14
local EAP authorization 10-20
Local EAP check box 12-27
local EAP general
template 12-46
local EAP general template 12-46
local EAP profile template 12-47
local management users
template 12-107
local management user template 12-107, 12-108
local net users
template 12-53
local net users template 10-28, 12-52
local password policy 18-29
local switching
Hybrid REAP 12-30
location
of rogue access point 16-21
of rogue access points 6-1
location appliance
importing 13-4
location appliance functionality 4-2
location appliance importing 13-4
location appliances
auto-synchronizing 13-6
relationship with WCS Location 1-4
location change
condition type 13-12
location configuration
template 12-110
location menu 2-29
location optimized monitor mode 9-20
location presence
assigning 5-7
location readiness
inspecting 5-43

location upgrade B-2
log analysis 11-16
logging 18-4
logging into the WCS user interface 2-18 to 2-19
logging options 18-32
logging the lobby ambassador activities 7-9
login.html 3-47
login disclaimer 18-44
login policies
  template 12-56
log message levels 18-32
log modules
  enabling 18-32
LOMM 9-20
  configuring access point radios 9-33
longitude 21-3
long preambles, enabling for SpectraLink NetLink phones 4-5
lookup client
  for DNS server 18-40
LWAPP migration 9-9
LWAPP uptime 2-27

M

MAC filtering 12-23
  template 12-57
MAC filter template 12-57
MAC frequency 3-45
MAC information 3-45
MACK
  message authenticator code keys 12-39
mail
  transport type 13-13
mail server configuration 18-45
maintaining WCS 14-1 to 14-14
malformed neighbor packets 6-17
malicious rogue 12-77
malicious rogue access points 3-5
managed network
  security index 3-5
management frame flood signatures 3-40
Management Frame Protection 3-36
management frame protection 10-22, 12-63
management interface 12-7
management queue 6-18
managing a virtual domain 20-7
managing clients 11-1
managing controller licenses 18-74
managing current reports 17-8
managing guest user accounts 7-12
managing licenses 18-75
managing MSE licenses 18-76
managing multiple WCSs 1-9
managing saved reports 17-11
managing user authentication order 10-34
managing virtual domains 20-7
managing WLAN schedules 10-25
mandatory data rates 12-85
manually disabled client
  template for 12-60
manually disabled clients 2-20
Map Editor
  general notes and guidelines 5-29
map editor
  general notes 5-29
  guidelines 5-29
  guidelines for using 5-29
  using 5-29
  using to draw polygon areas 5-30
map editor functions 5-29
map properties
  editing 5-13
Maps
  properties 5-13
maps
  monitoring 5-2 to 5-3
  searching 2-41, 5-21

using to monitor link stats 6-3
using to monitor mesh AP neighbors 6-8
map size 5-70
map view
updating 6-22
menu bar 2-29
mesh access point neighbors
monitoring 6-8
mesh access points
monitoring 6-6
mesh alarms
most recent 2-22
mesh configuration
template 12-98
mesh health 6-11
monitoring 6-11
mesh link statistics 6-3
monitoring 6-3
mesh neighbors 6-9
mesh network
monitoring using maps 6-3
mesh network hierarchy 6-19
mesh networks
background scanning 10-64
monitoring 6-3
mesh parent changing AP 2-27
mesh parent-child hierarchical view 5-35
mesh reports 17-68
mesh security statistics
for an AP 6-11
mesh statistics
for an access point 6-15
mesh tab
home page 2-22
mesh template
configuring 12-98
Mesh tree
viewing 6-19
mesh tree
viewing 6-19
message integrity check information element 12-63
metric collection 12-87
metrics
in QoS 12-16
MFP 3-36, 10-22
for clients 3-37
MFP attacks 3-8
MFP client protection 12-31
MFP signature generation 12-31
MFP templates 12-63
MIC IE 12-63
migration analysis
running 9-15
migration analysis report
generating 9-15
migration analysis summary
viewing 9-14
migration template 9-13
minimum RSSI 12-91
mirror mode 9-21
mismatched audit status 6-14
missing
condition type 13-11
mobile announce messages 8-8
mobility 8-1
mobility anchors 8-13, 10-26
mobility groups 8-7
prerequisites 8-8 to 8-9
mobility groups, configuring 8-8
mobility scalability 8-12
mobility services 13-1
mobility services engine
adding to WCS 13-2
deleting from WCS 13-4
keeping synchronized 13-4
modifying a current AP template task 12-121
modifying a current config group task 12-123
modifying a migration template 9-15

modifying map displays 6-21
using filters 6-21
Monitor Alarms
Rogue 3-18
monitoring active sessions 7-5
monitoring channel width 6-23
monitoring email notifications 16-23
monitoring events 16-22
monitoring guest users 6-36
monitoring mesh access point neighbors 6-8
using maps 6-8
monitoring mesh health 6-11, 6-23
monitoring mesh link statistics
using maps 6-3
monitoring mesh networks
using maps 6-3
monitoring neighboring channels 10-64
monitoring pre-coverage holes 6-32
monitoring rogue access point alarms 16-10
monitoring rogue access point details 16-14
monitoring rogue alarm events 16-22
monitoring security configurations 16-23, 18-54
monitoring spectrum experts 9-38
monitor menu 2-29
monitor mode
location optimized 9-20
monitor mode APs 18-71
most recent AP alarms 2-27
most recent audit alarms 19-10
most recent client alarms 11-6
most recent mesh alarms 2-22
most recent rogue adhocs 3-6
most recent security alarms 2-21, 2-27
MSE
synchronizing with WCS 13-4
MSE authorization
template 12-59
MSE license information 18-70
MSE licenses
managing 18-76
MSE synchronization status 13-9
multicast mobility mode 8-12
multiple country codes
configuring 8-16
setting 10-29
multiple syslog
template 12-106
multiple syslog template 12-106

N

N+1 redundancy 8-5
NAC out-of-band
configuring 10-45
NAC support 10-22
NAT 8-11
Navigator 1-9
netmask 12-70
NetStumbler signature 3-40
network address translation 8-11
network audit report
viewing latest 10-37
network design 5-73
network designs 13-4
network protection 3-38
Network Summary page 2-19
network summary reports 17-82
network users priority
template 12-51
network utilization reports 17-91
new rogue access points report 17-111
new rogue AP count report 17-113
new search 5-21
node hop count
worst 2-22
node hops 6-17
nodes report 17-72
noise

avoiding non-802.11 types 12-85
avoid non-802.11 12-85
non-802.11 noise
avoiding 12-85
non-aggregated historical data 18-8
non-Cisco ACS server
for use with RADIUS 18-17
normal mode
for Ethernet port 9-6
notification receiver 18-47
notifications
of channel change 6-37
of RF grouping 6-38
of transmission power change 6-38
NTP server template 12-8, 12-10
null probe response signatures 3-40

O

OfficeExtend 12-117
onstacle color coding 5-32
OUI search 18-61
outdoor areas, adding to a campus map 5-19 to 5-21
outdoor location
creating with Google Earth 21-1
out-of-sync 13-8
out of sync alerts 13-6
overview
Cisco Wireless LAN Solution 1-1 to 1-2
WCS 1-2

P

packet error rate
worse 2-22
packet error rate link color 6-21
packet error statistics report 17-75
packet jitter 12-16
packet latency 12-16
packet loss 12-16
packet loss rate 12-17
packet queue statistics report 17-77
packet stats report 17-73
parent changes 6-17
parent-to-child ping test 11-9
parent TSF 6-3
Passive Client 10-22
passthrough 12-25
password rules
turning on or off 18-29
PCI report 17-43
PEAP 12-49
peer-to-peer blocking 12-30
guidelines 10-46
percent time at maximum power 6-40
performance reports 17-86
performing data management tasks 18-34
permanent license
for controller 18-70
for MSE 18-70
pinging network devices from a controller 10-39
placemarks
creating 21-3
placement of access points 5-49
Planning Mode 5-35
planning mode 5-38
to calculate access point requirements 5-37
planning mode, calculating access point requirements 5-37
platinum 12-29
platinum queue 6-17
PLR 12-17
POE status 6-14
policy manager solutions 3-2
policy name template
configuring 12-83
polygon areas

drawing with map editor 5-30
poor neighbor SNR 6-17
positioning access points 5-53
positioning chokepoints 5-53
positioning Wi-Fi TDOA receivers 5-53
power injector setting 12-116
power injector settings 9-23
power-over-ethernet status 6-14
pre-coverage holes
monitoring 6-32
predictive tool
distance based 5-43
Prerequisites 2-1
prerequisites for high reliability 18-63
print guest user details 7-14
probe cycle count 10-32
profile redirect diagnostic test 11-20
protection type 12-64

Q

QoS 12-28
QoS profiles
configuring 10-66
QoS templates 12-13
quarantine 10-48
queues
silver, gold, platinum, bronze, management 6-17
quick search 2-32
Quiet time 3-45

R

radio measurements
receiving 6-2
radio resource management 12-85
Radio Resource Management statistics 6-37
radio status
scheduling 9-34
radio templates
configuring 12-130
RADIUS accounting servers
template 12-40
RADIUS accounting template 12-40
RADIUS and TACACS+ attributes
for virtual domain 7-18, 20-9
virtual domains 7-18, 20-9
RADIUS authentication template 12-37, 12-38
RADIUS fallback
template 12-42
RADIUS fallback mode 12-42
RADIUS servers 10-20
configuring 18-31
reachability status 9-37
reassociation request failures 6-18
reassociation request success 6-19
reassociation request timeouts 6-18
reauthentication request failures 6-19
reauthentication request success 6-19
reauthentication request timeout 6-19
rebooting config groups 8-25
receiving radio measurements 6-2
recent adhoc rogue alarms 3-9
recent alarms 2-27
recent coverage holes 2-20
recent rogue adhoc alarm 2-21
recent rogue alarms 2-27
recent rogue AP alarms 2-21, 3-9
recovering the WCS password 14-16
recurrence
for report 17-4
refresh browser 5-73
refresh component icon 2-29
refresh controller values 10-36
refresh from network 5-71, 5-73
refresh options 5-72
relative to ground 21-2

removing controllers from config group 8-22
removing switches 10-60
removing templates from config group 8-23
report
running new 17-2
report launch pad 17-2
reports
running 17-1
scheduled runs 17-9
reset AP now 9-25
restore WCS values 10-36
restoring WCS database
in high availability environment 14-8
restoring WCS database on Linux 14-7
retain WCS value 8-25
Retrieving UDI 6-29
RF calibration model, creating 4-6
RF grouping notifications 6-38
RFID data collection 12-111
RF profile traps 12-103
RF update traps 12-103
roaming 8-1
roaming parameter
template 12-90
roaming parameters template
configuring 12-90
roaming time 12-16, 12-17
rogue access point alarms 16-10
monitoring 16-10
rogue access point containment 16-21
rogue access point details 16-14
rogue access point events report 17-115
rogue access point location 6-1, 16-21
rogue access point rule groups 12-79
rogue access point rules
configuring a template 12-77
viewing or editing 9-36
rogue access points
friendly 3-7
malicious 3-5
monitoring 3-9
solutions for 3-2
unclassified 3-7
rogue access points report 17-117
rogue access point tagging 16-21
rogue adhoc alarm 2-21
rogue adhoc alarms
monitoring 16-19
rogue adhoc floors
filtering 5-60
rogue adhoc icon 5-62
rogue adhocs
most recent 3-6
rogue alarm events
monitoring 16-22
rogue AP alarms 2-21
rogue AP detail summary 2-27
rogue AP floors
filtering 5-59
rogue AP icon 5-62
rogue AP rule groups
template 12-79
rogue AP rules
template 12-77
rogue client floors
filtering 5-60
rogue client icon 5-62
rogue clients
searching 2-41
rogue detector 9-20
rogue location discovery protocol 12-76
rogue policies
template 12-76
template for 12-75
role criteria 9-14
root access points (RAPs)
selecting 9-9
root mode

changing from station role 9-15
routing state 6-16
RRM 12-85
RRM dashboard 6-36
RRM DCA 10-42
RRM intervals 12-93, 12-94, 12-95
template 12-93
RRM interval template
configuring 12-93, 12-95
RRM threshold
template 12-91
RRM thresholds 12-91
RRM threshold template
configuring 12-91
RSSI legend 5-71
rules
for rogue access point 12-77
viewing or editing for rogue access points 9-36
Running a link test 6-28
running a link test 11-9
running a new report 17-2
running a saved report 17-12
running background tasks 18-1
running migration analysis 9-15
running report 17-1
RX neighbor requests 6-17
RX neighbor responses 6-17

S

sample CSV file 10-3
saved report
running 17-12
saved reports
editing 17-12
filtering 17-11
managing 17-11
saved searches 2-43, 5-21
scalability parameters 8-12
scan cycle period threshold 10-33
scan threshold 12-91
scheduled configuration tasks
configuring 12-121
Schedule details 9-17
scheduled run details
editing 17-10
scheduled run results 17-9
filtering 17-10
scheduled tasks
viewing 9-34
schedules
managing for WLANs 10-25
scheduling guest user account 7-12
scheduling radio status 9-34
search alarm parameters 2-34
search feature 2-31
using for troubleshooting 11-12
searching access points 2-35
searching AP-detected interferers 2-40
searching clients 2-37
searching controller licenses 2-43
searching controllers 2-36, 10-33
searching events 2-39
searching maps 2-41
searching rogue clients 2-41
searching SE-detected interferers 2-39
searching shunned clients 2-42
searching tags 2-42
searching Wi-Fi TDOA receivers 2-40
search results
configuring 2-44
secondary WCS operation 18-62
security alarms
most recent 2-21
security color range 3-5
security configurations
monitoring 16-23, 18-54
security index 3-5

security mesh statistics 6-18
security reports 17-102
security solutions 3-1 to 3-34
security statistics
for mesh 6-15
security summary 17-119
security tab
home page 2-20
interpreting 3-4
security thermometer 3-5
SE-detected interferers
searching 2-39
selecting access points 12-132
sending mobile announce messages 8-8
sensors
viewing IDS types 3-38
set sorting buttons 17-7
setting AP failover 9-1
setting AP failover priority 10-37
setting multiple country codes 10-29
shunned clients
searching 2-41
shutting switch port 10-61
sidebar area 2-30
signature attacks summary 2-21
silver 12-29
silver queue 6-17
sniffer 12-115
sniffer mode 9-20
SNMP
transport type 13-13
SNMP authentication 12-102
SNMP credentials 18-56
SNMP mediation 18-33
SNMPv3
configuring 10-44
SNR definition 6-21
SNR down 6-5
SNR link
worst 2-22
SNR UP 6-5
SNR up 6-5
SOAP 13-13
software
downloading config groups to controllers 8-26
software, updating 4-2
SpectraLink NetLink phones, enabling long preambles 4-5
spectrum expert
adding 9-37
spectrum expert details 9-39
spectrum experts
configuring 9-37
monitoring 9-38
summary 9-38
Standard signature 3-44
standard signatures 3-39
starting WCS
on Linux 2-17
on Windows 2-16
static WEP 10-16
Static WEP-802.1X 10-17
station role
changing to root mode 9-15
statistics
DHCP 6-34
status, checking 14-1
status schedules
managing for WLANs 10-25
stopping WCS
on Linux 14-3
on Windows 14-2
stranded APs report 17-79
strongest AP RSSI 16-11
supplicant credentials
for AP 802.1X 12-9
supported Cisco WLSE management stations C-2
supported data rates 12-85

switch
configuring for hybrid REAP 15-4
switches
removing 10-61
switch port
shutting 10-61
switch port trace 18-60
switch port tracing
using 10-57
symmetric mobility tunneling 12-7
symmetric tunneling 8-5
synchornization
of configuration 18-5, 18-6
synchronization 13-6
viewing information from 13-9
synchronization history 13-9
synchronizing mobility services engines 13-4
synchronizing WCS and MSE 13-4
syslog
transport type 13-13
syslog templates 12-105, 12-106
System requirements 2-2

T

TACACS+ server
configuring a template for 12-45
template 12-45
TACACS+ servers
configuring 18-29
tag elements 18-71
tagged packets 9-8
tagging
of rogue access point 16-21
of rogue access points 6-1
tag icon 5-61
tags
searching 2-42
Target 6-3
target TSF 6-3
tasks
importing into ACS 18-8
Telnet SSH
template 12-101
Telnet SSH templates 12-104
temperature 6-11
template
configuring for rogue AP rules 12-77
template for configuring network user credentials 12-51
template launch pad
for controllers 12-1
templates
applied to controllers 10-10
discovering from controllers 10-9
using 12-1
test analysis tab 11-20
TFTP
turning on and off 18-54
TFTP details 9-16
TFTP server 3-41
thermometer color range 3-5
threats
access points 3-8
throughput report 17-33
tilt 21-2
tools menu 2-29
top APs by client count 11-3
total APs not assigned to maps 2-20
total interferer count 9-39
total mismatched controllers 19-10
trace 18-34
trace switch port 10-57
traffic indicator message 12-84
traffic stream metrics 12-87
traffic stream metrics QoS status 12-17
traffic stream metrics QoS template 12-16
traffic stream metrics report 17-93
transition time 12-91

transmission power change notifications 6-38
transport types 13-13
trap
  802.11 security 12-103
trap control
  template 12-101
trap control templates 12-101
trap receiver
  template 12-100
trap receiver template 12-100
traps
  AAA 12-103
  access point 12-103
  client related 12-102
  RF profile 12-103
  RF update 12-103
  unsupported 16-85
traps added in 2.1 16-47
traps added in 2.2 16-51
traps added in 3.0 16-54
traps added in 3.1 16-56
traps added in 3.2 16-59
traps added in 4.0 16-60
traps added in 4.0.96.0 16-65
traps added in 4.1 16-67, 16-74
traps added in release 6.0 16-82
traps added in release 7.0 16-86
trend report type 17-1
troubleshooting A-1
  using logging options 18-34
troubleshooting voice RF coverage 5-44
trunk mode 9-6
trusted AP policies
  template for 12-77
trusted AP policies template 12-77
tunneling 8-5
TX neighbor requests 6-17
TX neighbor responses 6-17
Tx power and channel report 17-96
type
  of WCS license 18-69

U

UDI
  retrieving on controllers and access points 6-29
unadjusted link metric 6-5
unclassified rogue 12-77
unclassified rogue access points 3-7
unclassified rogue APs 2-27
understanding virtual domains 7-18, 20-9
uninstalling WCS
  on Linux 14-9
  on Windows 14-8
unique clients report 17-37
unique device identifier 6-29
unknown association requests 6-19
unknown reassociation request 6-19
untagged packets 9-8
Update map view 6-22
update map view 6-22
updating system software 4-2
upgrade settings
  for controller 18-41
upgrading autonomous access points 9-14
upgrading the network 14-15
upgrading to Linux 4
  during WLSE conversion C-3
upgrading WCS
  in high availability environment 14-15
  on Linux 14-14
  on Windows 14-14
Uploading IDS signatures 3-41
uploading IDS signatures 3-41
upstream delay 12-17
upstream packet loss rate 12-17
uptime reports 17-58
User accounts

for guest 7-10
user accounts
for guest 7-10
user authentication order
managing 10-34
user authentication priority template
configuring 12-108
user credential retrieval priority 12-51
user details
emailing 7-14
printing 7-14
User Interface 2-28
user login policies
configuring a template 12-56
template 12-56
user preferences 18-66
using chokepoints 5-78
using Edit View
for alarms 16-8
using filtering 6-5, 6-21
using logging
for troubleshooting 18-34
using maps
to monitor mesh AP neighbors 6-8
to monitor mesh link statistics 6-3
using maps to monitor mesh networks 6-3
using planning mode 5-30
using search 16-8
using template
ACL 12-74
for friendly access point 12-81
using templates 12-1
802.11a policy name 12-83
802.11b/g RRM interval 12-93, 12-95
802.11b/g RRM threshold 12-91
802.11b/g voice 12-86
access point/radio 12-113
access point authentication & MFP 12-63
access point authorization 12-59
file encryption 12-36
for legacy syslog 12-105
for multiple syslog 12-106
guest users 12-54
local management user 12-107, 12-108
local net users 10-28, 12-52
MAC filter 12-57
NTP server 12-8, 12-10
QoS 12-13
RADIUS accounting 12-40
RADIUS authentication 12-37
syslog 12-105, 12-106
Telnet SSH 12-104
traffic stream metrics QoS 12-16
trap control 12-101
trap receiver 12-100
web authentication 12-64
WLAN 12-18
using the installer to upgrade 14-10
utilization reports 17-60

V

V5 client statistics 17-40
vendor CA certificates
downloading 4-4
vendor device certificates
downloading 4-3
vendor search 18-61
video parameter
template 12-87
video parameter template
configuring 12-87
video parameter templates
configuring 12-87
View 2-29
view audit reports 10-35
view history 11-4
view in chart icon 2-29

viewing alarm details 16-9
viewing all current templates 10-45
viewing an AP template task history 12-122
viewing AP status report
for scheduled task 12-121
viewing audit status 10-34
for access points 9-35
viewing autonomous access points 9-12
viewing clients
identified as WGBs 6-28
viewing controller status report
for the scheduled task 12-123
viewing DHCP statistics 6-34
viewing Google Earth maps 6-23, 21-6
Viewing Mesh tree 6-12
viewing mesh tree 6-15
view in grid icon 2-29
Viewing shunned clients 3-38
viewing shunned clients 3-38
viewing synchronization history 13-9
viewing synchronization info 13-9
viewing the audit trail 7-9
viewing the migration analysis 9-14
viewing the RRM dashboard 6-38
view list 11-13
virtual domain
managing 20-7
virtual domain hierarchy 20-3
virtual domains 20-1
assigning 7-16
attributes 7-18, 20-9
creating 20-1
hierarchy 20-3
managing 20-7
understanding 7-18, 20-9
VLAN tagging 9-3
Voice-over-Internet Protocol
snooping 10-21
voice parameter template
configuring 12-86
voice RF coverage
troubleshooting 5-44
voice statistics 17-100
VoIP calls graph 17-97
VoIP calls table 17-99
VoIP snooping 10-21

W

WCS
checking status
on Linux 14-2
on Windows 14-1
installing 2-5
maintaining 14-1 to 14-14
overview 1-2
servers supported 1-2
starting
on Linux 2-17
on Windows 2-16
stopping
on Linux 14-3
on Windows 14-2
uninstalling
on Linux 14-9
on Windows 14-8
upgrading
on Linux 14-14
on Windows 14-14
versions 1-3 to 1-6
WCS_EMAIL_FAILURE 16-76
WCS-ADV-SI-SE-10 B-2
WCS Base, described 1-3, 1-6
WCS controller deployment
from WLSE autonomous C-1
WCS database
backing up
on Linux 14-5

on Windows 14-4
restoring
on Linux 14-7
on Windows 14-5
restoring in high availability environment 14-8
scheduling automatic backups 14-3, 18-1
WCS guest operations report 17-67
WCS home 2-18
WCS Home page
customizing content 2-24
customizing tabs 2-23
WCS licenses B-1
WCS Location
described 1-4 to 1-6
relationship with Cisco location appliances 1-4
WCS Navigator 1-9
WCS on WLSE
licensing C-7
WCS password
recovering 14-16
WCS user accounts
adding 7-1
changing passwords 7-4
deleting 7-4
WCS user interface 7-11
described 1-3, 1-9
logging into 2-18 to 2-19
WCS values
restoring 10-36
web authentication
template 12-64
web authentication template 12-64
web authentication type 12-66
Web authentication types 3-47
web auth security A-3
web auth types 10-56
web login
enabling 3-46
web policy 10-19
Wellenreiter signature 3-41
WGB 9-12
WGBs
viewing those clients 6-28
Wi-Fi TDOA receiver icon 5-62
Wi-Fi TDOA receivers
positiioning 5-53
searching 2-40
wIPS 13-1
planning and configuring 13-16
wired guest access
configuring 10-51
Wireless Control System (WCS)
See WCS
WLAN
adding 10-23
deleting 10-24
WLAN AP groups 12-32
WLAN Configuration 12-124
WLAN details
viewing 10-14
WLANs
configuring 10-13
web auth security A-3
WLAN status schedules
managing 10-25
WLAN templates 12-18
WLSE autonomous deployment conversion C-1
WLSE management stations C-2
WLSE upgrade B-2
WLSE upgrade license C-7
WMM parameters 10-20
WMM policy 12-29
work group bridge mode 9-12
worst node hop count 2-22
worst node hops report 17-80
worst packet error rate 2-22
worst SNR link 2-22
WPA+WPA2 10-18

X

XML mediation 18-33

Z

zoom in or out 5-70