Cisco Wireless Control System Configuration Guide

Software Release 5.1
July 2008

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

Customer Order Number:
Text Part Number: OL-15478-02

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

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

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

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

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

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

CONTENTS

Preface 17

Audience 17

Purpose 17

Organization 18

Conventions 19

Related Publications 19

Obtaining Documentation and Submitting a Service Request 19

CHAPTER 1 **Overview** 1-1

Overview of the Cisco Unified Wireless Network Solution 1-2

Overview of WCS 1-3

WCS Versions 1-4

WCS Base 1-4

WCS Base + Location 1-5

Relationship with Cisco Location Appliances 1-5

Comparison of WCS Base and WCS Location 1-6

Embedded Access Points 1-7

WCS User Interface 1-7

Cisco WCS Navigator 1-8

1-8

CHAPTER 2 **Getting Started** 2-1

Prerequisites 2-2

System Requirements 2-2

Installing WCS for Windows 2-4

Installing WCS for Linux 2-10

Starting WCS 2-12

Starting WCS on Windows 2-12

Starting WCS on Linux 2-12

Logging into the WCS User Interface 2-13

General Tab 2-15

Client Tab 2-15

Security Tab 2-16

Customizing Tabs on the WCS Home Page 2-18
Customizing Content on the WCS Home Page 2-19
Using the Cisco WCS User Interface 2-24
Menu Bar 2-25
Monitor Menu 2-25
Configure Menu 2-25
Administration Menu 2-26
Location Menu 2-26
Help Menu 2-26
Sidebar Area 2-26
Alarm Dashboard 2-27
Command Buttons 2-27
Main Data Page 2-27
Administrative Tools 2-28

CHAPTER 3 **Configuring Security Solutions** 3-1
Cisco Unified Wireless Network Solution Security 3-2
Layer 1 Solutions 3-2
Layer 2 Solutions 3-2
Layer 3 Solutions 3-2
Single Point of Configuration Policy Manager Solutions 3-3
Rogue Access Point Solutions 3-3
Rogue Access Point Challenges 3-3
Tagging and Containing Rogue Access Points 3-3
Rogue Management 3-3
Integrated Security Solutions 3-4
Using WCS to Convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 Mode 3-5
Configuring a Firewall for WCS 3-6
Access Point Authorization 3-6
Management Frame Protection (MFP) 3-7
Guidelines for Using MFP 3-8
Configuring Intrusion Detection Systems (IDS) 3-9
Viewing IDS Sensors 3-9
Configuring IDS Signatures 3-9
Uploading IDS Signatures 3-12
Downloading IDS Signatures 3-13
Enabling or Disabling IDS Signatures 3-14
Viewing IDS Signature Events 3-17
Enabling Web Login 3-17

Downloading Customized Web Authentication 3-18
Connecting to the Guest WLAN 3-21
Deleting a Guest User 3-21
Certificate Signing Request (CSR) Generation 3-22

CHAPTER 4 **Performing System Tasks** 4-1
Adding System Components to the WCS Database 4-2
Adding a Controller to the WCS Database 4-2
Adding a Location Appliance to the WCS Database 4-2
Additional Functionality with Location Appliance 4-3
Using WCS to Update System Software 4-4
Downloading Vendor Device Certificates 4-5
Downloading Vendor CA Certificates 4-5
Using WCS to Enable Long Preambles for SpectraLink NetLink Phones 4-6
Creating an RF Calibration Model 4-7

CHAPTER 5 **Adding and Using Maps** 5-1
Creating Maps 5-2
Adding a Campus 5-2
Adding Buildings 5-3
Adding a Building to a Campus Map 5-3
Adding a Standalone Building 5-4
Adding Outdoor Areas 5-6
Enabling Location Presence on a Location Server 5-7
Searching Maps 5-9
Finding Coverage Holes 5-10
Adding and Enhancing Floor Plans 5-10
Adding Floor Plans to a Campus Building 5-11
Adding Floor Plans to a Standalone Building 5-12
Using the Map Editor to Enhance Floor Plans 5-13
Using the Map Editor to Draw Polygon Areas 5-14
Using Planning Mode to Calculate Access Point Requirements 5-17
Adding Access Points 5-24
Placing Access Points 5-26
Creating a Network Design 5-28
Designing a Network 5-28
Changing Access Point Positions by Importing and Exporting a File 5-34
Using Chokepoints to Enhance Tag Location Reporting 5-35

Adding Chokepoints to the WCS Database and Map 5-35
Removing Chokepoints from the WCS Database and Map 5-42
Monitoring Chokepoints 5-43
Monitoring Maps 5-43
Monitoring Predicted Coverage 5-44
Access Point Layer 5-45
AP Mesh Info Layer 5-46
Clients Layer 5-47
802.11 Tags Layer 5-48
Rogue APs Layer 5-49
Rogue Clients Layer 5-50
Monitoring Channels on a Floor Map 5-51
Monitoring Transmit Power Levels on a Floor Map 5-51
Monitoring Coverage Holes on a Floor Map 5-52
Monitoring Clients on a Floor Map 5-53
Monitoring Outdoor Areas 5-54
Importing or Exporting WLSE Map Data 5-55
Creating and Applying Calibration Models 5-59
Analyzing Element Location Accuracy Using Testpoints 5-64
Assigning Testpoints to a Selected Area 5-65
Using the Accuracy Tool to Conduct Accuracy Testing 5-68
Using Scheduled Accuracy Testing to Verify Accuracy of Current Location 5-69
Using On-Demand Accuracy Testing to Test Location Accuracy 5-70

CHAPTER 6 **Monitoring Wireless Devices** 6-1
Monitoring Rogue Access Points, Adhocs, and Clients 6-2
Interpreting Security Summary Window 6-2
Security Index 6-3
Top Security Issues 6-3
Malicious Rogue Access Points 6-5
Adhocs Rogues 6-6
Unclassified Rogue Access Points 6-6
Friendly Rogue Access Points 6-6
Attacks Detected 6-7
Access Point Threats or Attacks 6-7
MFP Attacks 6-8
Client Security Events 6-8
Cisco Wired IPS Events 6-8
Monitoring Rogue Access Point 6-8

Monitoring Rogue Adhoc 6-10
Monitoring Rogue Clients 6-10
Monitoring Shunned Clients 6-11
Rogue Access Point Location, Tagging, and Containment 6-12
Detecting and Locating Rogue Access Points 6-13
Monitoring Clients 6-15
WLAN Client Troubleshooting 6-16
Configuring ACS View Server Credentials 6-31
Enabling Automatic Client Troubleshooting 6-31
Finding Clients 6-31
Receiving Radio Measurements 6-35
Monitoring Mesh Networks Using Maps 6-36
Monitoring Mesh Link Statistics Using Maps 6-36
Monitoring Mesh Access Points Using Maps 6-39
Monitoring Mesh Access Point Neighbors Using Maps 6-41
Monitoring Mesh Health 6-43
Mesh Statistics for an Access Point 6-47
Viewing the Mesh Network Hierarchy 6-52
Using Mesh Filters to Modify Map Display of Maps and Mesh Links 6-53
Monitoring Channel Width 6-55
Viewing Google Earth Maps 6-56
Google Earth Settings 6-57
Viewing Clients Identified as WGBs 6-58
Running a Link Test 6-59
Retrieving the Unique Device Identifier on Controllers and Access Points 6-61
Coverage Hole 6-64
Monitoring Pre-Coverage Holes 6-64
Viewing DHCP Statistics 6-66
RRM Dashboard 6-67
Channel Change Notifications 6-68
Transmission Power Change Notifications 6-69
RF Grouping Notifications 6-69
Viewing the RRM Dashboard 6-69

CHAPTER 7 **Managing WCS User Accounts** 7-1
Adding WCS User Accounts 7-2
Deleting WCS User Accounts 7-4
Changing Passwords 7-5

Monitoring Active Sessions 7-5
Viewing or Editing User Information 7-6
Viewing or Editing Group Information 7-7
Setting Lobby Ambassador Defaults 7-8
Editing the Default Lobby Ambassador Credentials 7-10
Viewing the Audit Trail 7-10
Enabling Audit Trails for Guest User Activities 7-12
Creating Guest User Accounts 7-12
Creating a Lobby Ambassador Account 7-13
Editing a Lobby Ambassador Account 7-14
Logging in to the WCS User Interface as a Lobby Ambassador 7-15
Managing WCS Guest User Accounts 7-15
Adding Guest User Accounts 7-16
Guest User Credentials 7-17
Viewing and Editing Guest Users 7-17
Deleting Guest User Templates 7-18
Scheduling WCS Guest User Accounts 7-19
Printing or E-mailing WCS Guest User Details 7-20
Logging the Lobby Ambassador Activities 7-20
Adding a New User 7-21
Add User Name, Password, and Groups 7-21
Assign a Virtual Domain 7-23
Virtual Domain RADIUS and TACACS+ Attributes 7-24
Understanding Virtual Domains as a User 7-25

CHAPTER 8 **Configuring Mobility Groups** 8-1
Overview of Mobility 8-2
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 8-11
Mobility Anchors 8-12
Configuring Mobility Anchors 8-13
Configuring Multiple Country Codes 8-15
Creating Config Groups 8-17

Adding New Group 8-18
Configuring Config Groups 8-19
Enabling a Background Audit 8-20
Adding or Removing Controllers from Config Group 8-20
Adding or Removing Templates from the Config Group 8-20
Applying or Scheduling Config Groups 8-21
Auditing Config Groups 8-22
Choosing Basic or Template-based Auditing 8-23
Viewing Configuration Audit Summary 8-24
Rebooting Config Groups 8-25
Reporting Config Groups 8-26
Downloading Software 8-26
Downloading IDS Signatures 8-27
Downloading Customized WebAuth 8-28

CHAPTER 9 **Configuring Access Points** 9-1
Setting AP Failover Priority 9-2
Configuring Global Credentials for Access Points 9-2
Autonomous to LWAPP Migration Support 9-4
Adding IOS Access Points to WCS 9-4
Adding IOS Access Points by Device Information 9-5
Adding Autonomous Access Points by CSV File 9-5
Viewing Autonomous Access Points in WCS 9-6
Work Group Bridge (WGB) Mode 9-6
Autonomous Access Point to LWAPP Access Point Migration 9-6
Adding/Modifying a Migration Template 9-7
Configuring Access Points 9-8
11n Antenna Selection 9-13
Configuring Access Point Radios for Location Optimized Monitor Mode 9-15
Scheduling Radio Status 9-15
Viewing Scheduled Tasks 9-16
Viewing Audit Status (for Access Points) 9-16
Searching Access Points 9-17
Viewing or Editing Rogue Access Point Rules 9-18
Configuring Spectrum Experts 9-18
Adding a Spectrum Expert 9-18
Monitoring Spectrum Experts 9-19
Spectrum Experts > Summary 9-19

Interferers > Summary 9-19
Spectrum Experts Details 9-20

CHAPTER 10 **Configuring Controllers and Switches** 10-1
Adding Controllers 10-2
Setting Multiple Country Codes 10-3
Searching Controllers 10-4
Managing User Authentication Order 10-5
Viewing Audit Status (for Controllers) 10-5
Viewing Latest Network Audit Report 10-8
Setting AP Failover Priority 10-8
Pinging a Network Device from a Controller 10-9
Enabling Load-Based CAC for Controllers 10-9
Enabling High Density 10-11
Requirements 10-11
Optimizing the Controller to Support High Density 10-12
Configuring 802.3 Bridging 10-14
Configuring an RRM Threshold Controller (for 802.11a/n or 802.11b/g/n) 10-14
Configuring 40-MHz Channel Bonding 10-15
Configuring EDCA Parameters for Individual Controller 10-16
Configuring SNMPv3 10-17
Viewing All Current Templates 10-17
Configuring NAC Out-of-Band Integration 10-18
Guidelines for Using NAC Out-of-Band Integration 10-19
Configuring NAC Out-of-Band Integration 10-20
Configuring Wired Guest Access 10-23
Creating an Ingress Interface 10-24
Creating an Egress Interface 10-25
Creating a Wired LAN for Guest Access 10-25
Using Switch Port Tracing 10-27
Removing Switches 10-29
Shutting Switch Port 10-29

CHAPTER 11 **Using Templates** 11-1
Adding Controller Templates 11-1
Configuring an NTP Server Template 11-3
Configuring General Templates 11-4

Configuring QoS Templates 11-6
Configuring a Traffic Stream Metrics QoS Template 11-8
Configuring WLAN Templates 11-9
Security 11-11
QoS 11-17
Advanced 11-17
Configuring H-REAP AP Groups 11-20
Configuring a File Encryption Template 11-22
Configuring a RADIUS Authentication Template 11-23
Configuring a RADIUS Accounting Template 11-25
Configuring a LDAP Server Template 11-26
Configuring a TACACS+ Server Template 11-27
Configuring a Local EAP General Template 11-28
Configuring a Local EAP Profile Template 11-30
Configuring an EAP-FAST Template 11-31
Configuring Network User Credential Retrieval Priority Templates 11-33
Configuring a Local Network Users Template 11-34
Configuring Guest User Templates 11-35
Configuring a User Login Policies Template 11-37
Configuring a MAC Filter Template 11-38
Configuring an Access Point or LBS Authorization 11-39
Configuring a Manually Disabled Client Template 11-39
Configuring a CPU Access Control List (ACL) Template 11-40
Configuring a Rogue Policies Template 11-41
Configuring a Rogue AP Rules Template 11-42
Configuring a Rogue AP Rule Groups Template 11-44
Configuring a Friendly Access Point Template 11-46
Configuring a Client Exclusion Policies Template 11-47
Configuring an Access Point Authentication and MFP Template 11-49
Configuring a Web Authentication Template 11-50
Downloading a Customized Web Authentication Page 11-52
Configuring Access Control List Templates 11-54
Configuring a Policy Name Template (for 802.11a/n or 802.11b/g/n) 11-55
Configuring High Density Templates 11-58
Configuring a Voice Parameter Template (for 802.11a/n or 802.11b/g/n) 11-60
Configuring a Video Parameter Template (for 802.11a/n or 802.11b/g/n) 11-61
Configuring EDCA Parameters through a Controller Template 11-62
Configuring a Roaming Parameters Template (for 802.11a/n or 802.11b/g/n) 11-63
Configuring an RRM Threshold Template (for 802.11a/n or 802.11b/g/n) 11-64
Configuring an RRM Interval Template (for 802.11a/n or 802.11b/g/n) 11-66

Configuring an 802.11h Template 11-66
Configuring a High Throughput Template (for 802.11a/n or 802.11b/g/n) 11-67
Configuring a Mesh Template 11-68
Configuring a TFTP Server Template 11-70
Configuring a Trap Receiver Template 11-70
Configuring a Trap Control Template 11-71
Configuring a Telnet SSH Template 11-73
Configuring a Legacy Syslog Template 11-74
Configuring a Multiple Syslog Template 11-75
Configuring a Local Management User Template 11-76
Configuring a User Authentication Priority Template 11-77
Applying Controller Templates 11-78
Adding Access Point Templates 11-78
Configuring Access Point Templates 11-79
Applying or Scheduling Templates 11-82
Configuring Scheduled Configuration Tasks 11-83
AP Template Tasks 11-83
Config Group Tasks 11-84
Configuring Radio Templates 11-86
Selecting Access Points 11-88
Applying the Report 11-88

CHAPTER 12 **Performing Maintenance Operations** 12-1
Checking the Status of WCS 12-2
Checking the Status of WCS on Windows 12-2
Checking the Status of WCS on Linux 12-2
Stopping WCS 12-3
Stopping WCS on Windows 12-3
Stopping WCS on Linux 12-3
Backing Up the WCS Database 12-4
Scheduling Automatic Backups 12-4
Performing a Manual Backup 12-5
Backing Up the WCS Database (for Windows) 12-5
Backing Up the WCS Database (for Linux) 12-5
Restoring the WCS Database 12-6
Restoring the WCS Database (for Windows) 12-6
Restoring the WCS Database (for Linux) 12-7
Importing the Location Appliance into WCS 12-8
Importing and Exporting Asset Information 12-11

Importing Asset Information 12-11
Exporting Asset Information 12-11
Auto-Synchronizing Location Appliances 12-12
Backing Up Location Appliance Data 12-13
Uninstalling WCS 12-15
Uninstalling WCS on Windows 12-15
Uninstalling WCS on Linux 12-15
Upgrading WCS 12-16
Using the Installer to Upgrade WCS for Windows 12-16
Using the Installer to Upgrade WCS for Linux 12-19
Manually Upgrading WCS on Windows 12-20
Manually Upgrading WCS on Linux 12-20
Upgrading the Network 12-21
Reinitializing the Database 12-21
Recovering the WCS Password 12-21

CHAPTER 13 **Configuring Hybrid REAP** 13-1
Overview of Hybrid REAP 13-2
Hybrid-REAP Authentication Process 13-2
Hybrid REAP Guidelines 13-4
Configuring Hybrid REAP 13-4
Configuring the Switch at the Remote Site 13-4
Configuring the Controller for Hybrid REAP 13-6
Configuring an Access Point for Hybrid REAP 13-9
Connecting Client Devices to the WLANs 13-11
Hybrid REAP Access Point Groups 13-12
Hybrid-REAP Groups and Backup RADIUS Servers 13-13
Hybrid-REAP Groups and Local Authentication 13-13
Configuring Hybrid-REAP Groups 13-13
Auditing an H-REAP Group 13-16

CHAPTER 14 **Alarms and Events** 14-1
Using the Alarm Dashboard 14-1
Alarm Acknowledgement 14-4
Monitoring Alarms 14-4
Using Edit View 14-5
Using Search 14-5
Monitoring Failed Objects 14-7

Monitoring Rogue Access Point Alarms 14-8
Monitoring Rogue Access Point Details 14-9
Monitoring Rogue Adhoc Alarms 14-10
Monitoring Rogue Adhoc Details 14-11
Detecting Access Points 14-12
Monitoring Events 14-13
Monitoring Rogue Clients 14-13
Monitoring E-mail Notifications 14-14
Monitoring Severity Configurations 14-14
Alarm and Event Dictionary 14-15
Notification Format 14-15
Traps Added in Release 2.0 14-15
Traps Added in Release 2.1 14-33
Traps Added in Release 2.2 14-37
Traps Added in Release 3.0 14-39
Traps Added in Release 3.1 14-41
Traps Added in Release 3.2 14-44
Traps Added In Release 4.0 14-45
Traps Added or Updated in Release 4.0.96.0 14-49
Traps Added or Updated in Release 4.1 14-51
Traps Added or Updated in Release 4.2 14-58
Traps Added or Updated in Release 5.0 14-62
Traps Added or Updated in Release 5.1 14-63
Unsupported Traps 14-63

CHAPTER 15 **Running Reports** 15-1
Choosing a Report 15-2
Enabling or Disabling a Schedule 15-2
Deleting a Report 15-3
Customizing a Report 15-3
Accessing the Schedule Panel 15-3
802.11n Scaling Reports 15-5
Client Count 15-5
Creating a New Client Count Report 15-6
Throughput 15-6
Creating a New Throughput Report 15-7
Access Point Reports 15-7
Viewing or Modifying Access Point Reports 15-8
Creating a New Access Point Report 15-8

Audit Reports 15-9
Viewing or Modifying Audit Reports 15-9
Creating a New Network Configuration Audit Report 15-10
Client Reports 15-10
Viewing or Modifying Client Reports 15-11
Creating a New Client Report 15-11
Compliance Reports 15-12
Viewing or Modifying Compliance Reports 15-12
Creating a New Compliance Report 15-13
Compliance Reports Results 15-13
Inventory Reports 15-14
Viewing or Modifying Inventory Reports 15-14
Creating a New Inventory Report 15-15
Mesh Reports 15-15
Viewing or Modifying Mesh Reports 15-16
Creating a New Mesh Report 15-16
Performance Reports 15-17
Viewing or Modifying Performance Reports 15-18
Creating a New Performance Report 15-18
Security Reports 15-18
Viewing or Modifying Security Reports 15-19
Creating a New Security Report 15-19

CHAPTER 16 **Administrative Tasks** 16-1
Running Background Tasks 16-2
Performing a Task 16-2
Configuration Sync 16-4
Importing Tasks Into ACS 16-5
Adding WCS to an ACS Server 16-5
Adding WCS as a TACACS+ Server 16-6
Adding WCS UserGroups into ACS for TACACS+ 16-7
Adding WCS to ACS server for Use with RADIUS 16-10
Adding WCS UserGroups into ACS for RADIUS 16-11
Adding WCS to a Non-Cisco ACS Server for Use with RADIUS 16-14
Setting AAA Mode 16-16
Auto Provisioning 16-17
Viewing Detailed Auto Provisioning Device Information 16-20
Editing a Current Auto Provisioning Filter 16-21

Deleting an Auto Provisioning Filter 16-21
Viewing Details of an Auto Provisioned Filter 16-22
Setting Auto Provisioning 16-22
Turning Password Rules On or Off 16-22
Configuring TACACS+ Servers 16-23
Configuring RADIUS Servers 16-24
Establishing Logging Options 16-26
Performing Data Management Tasks 16-27
Data Management 16-28
Report 16-29
Mail Server 16-29
Login Disclaimer 16-31
Alarms 16-31
Client 16-32
Severity Configurations 16-32
Notification Receiver 16-32
SNMP Settings 16-33
Audit 16-34
Auto Refresh 16-34
Setting User Preferences 16-35

CHAPTER 17 **Virtual Domains** 17-1
Creating a Virtual Domain 17-1
Understanding Virtual Domain Hierarchy 17-3
Modifying a Virtual Domain 17-6
Virtual Domain RADIUS and TACACS+ Attributes 17-7
Understanding Virtual Domains as a User 17-8

CHAPTER 18 **Google Earth Maps** 18-1
Creating an Outdoor Location Using Google Earth 18-1
Understanding Geographical Coordinates for Google Earth 18-1
Creating and Importing Coordinates in Google Earth (KML File) 18-2
Creating and Importing Coordinates as a CSV File 18-4
Importing a File into WCS 18-5
Viewing Google Earth Maps 18-6
Viewing Google Earth Map Details 18-6
Google Earth Settings 18-6

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

Troubleshooting Cisco Compatible Extensions Version 5 Client Devices A-2

Diagnostic Channel A-2

Configuring the Diagnostic Channel A-2

Web Auth Security on WLANs A-3

Debug Commands A-4

Debug Strategy A-4

Best Practices A-9

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

WCS Licenses B-2

Types of Licenses B-2

Licensing Enforcement B-3

Product Authorization Key Certificate B-3

Determining Which License To Use B-4

Installing a License B-4

Managing Licenses B-5

Adding a License B-5

Deleting a License B-6

Backup and Restore License B-6

Notices B-6

OpenSSL/Open SSL Project B-6

License Issues B-6

End User License Agreement B-8

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

Supported Hardware C-2

Supported 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 C-3

Configuring the Converted Appliance C-3

Licensing C-7

WLSE Upgrade License C-7

Preface

The preface provides an overview of the *Cisco Wireless Control System Configuration Guide, Release 5.1*, references related publications, and explains how to obtain other documentation and technical assistance, if necessary. It contains these sections:

- Audience, page xix
- Organization, page xx
- Conventions, page xxi
- Related Publications, page xxi
- Obtaining Documentation and Submitting a Service Request, page xxi

Audience

This guide describes the Cisco Wireless Control System (WCS). It is meant for networking professionals who use 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 document pertains specifically to WCS 5.1. Earlier versions of WCS software may look and operate somewhat differently.

Organization

This guide contains the following chapters:

Chapter 1, "Overview," describes the Cisco Unified Wireless Network Solution and the Cisco Wireless Control System (WCS).

Chapter 2, "Getting Started," describes how to prepare WCS for operation.

Chapter 3, "Configuring Security Solutions," describes security solutions for wireless LANs.

Chapter 4, "Performing System Tasks," describes how to use WCS to add a controller and location appliance to the WCS database, update system software, enable long preambles for SpectraLink NetLink phones, and create an RF calibration model.

Chapter 5, "Adding and Using Maps," describes how to add maps to the Cisco WCS database and use them to monitor your wireless LAN.

Chapter 6, "Monitoring Wireless Devices," describes how to use WCS to monitor your wireless LANs.

Chapter 7, "Managing WCS User Accounts," describes how to add, delete, and change the passwords of WCS user accounts. It also describes creating a guest user account on WCS and how to configure it for limited activity.

Chapter 8, "Configuring Mobility Groups," provides an overview of mobility and mobility groups and describes how to configure them.

Chapter 9, "Configuring Access Points,"describes how to configure access points for specific tasks within the Cisco WCS database.

Chapter 10, "Configuring Controllers and Switches," describes how to configure controllers and switches in the Cisco WCS database.

Chapter 11, "Using Templates," describes how to set parameters for multiple devices without having to re-enter the common information.

Chapter 12, "Performing Maintenance Operations," describes how to check the status of, stop, uninstall, and upgrade WCS. It also provides instructions for backing up and restoring the WCS database.

Chapter 13, "Configuring Hybrid REAP," describes hybrid REAP and explains how to configure this feature on controllers and access points.

Chapter 14, "Alarms and Events," defines alarms and events and what constitutes each.

Chapter 15, "Running Reports,"describes the various reports that can be generated to run on an immediate and scheduled basis for use with diagnosing system and network health.

Chapter 16, "Administrative Tasks," describes certain administrative tasks you can perform with WCS.

Chapter 17, "Virtual Domains," describes how virtual domains are established so users can only view the devices and maps for which they are responsible. It describes various virtual domain tasks.

Chapter 18, "Google Earth Maps,"describes how to create an outdoor location, import a file, view Google Earth maps, and specify Google Earth settings.

Appendix A, "Troubleshooting and Best Practices," provides some troubleshooting and best practices tips for a few of the more complicated features.

Appendix B, "WCS and End User Licenses," provides the end user license and warranty that apply to WCS.

Appendix C, "Conversion of a WLSE Autonomous Deployment to a WCS Controller Deployment," describes how to convert a Cisco Wireless LAN Solution Engine (WLSE) network management appliance to a Cisco Wireless Control System (WCS) network management station.

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 this 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, refer to the following documents:

- *Wireless Control System Online Help*
- *Release Notes for Cisco Wireless Control System 5.1 for Windows or Linux*
- *Cisco Location Application Configuration Guide*
- *Release Notes for Cisco Location Appliance Software*

Click this link to browse to these documents:
http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.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 Wireless Control System (WCS). It contains these sections:

- Overview of the Cisco Unified Wireless Network Solution, page 1-1
- Overview of WCS, page 1-2
- WCS Versions, page 1-3
- Embedded Access Points, page 1-6
- WCS User Interface, page 1-6
- Cisco WCS Navigator, page 1-7

Overview of the Cisco Unified Wireless Network Solution

The Cisco Unified Wireless Network solution is designed to provide 802.11 wireless networking solutions for enterprises and service providers. It simplifies the deployment and management of large-scale wireless LANs and enables 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:

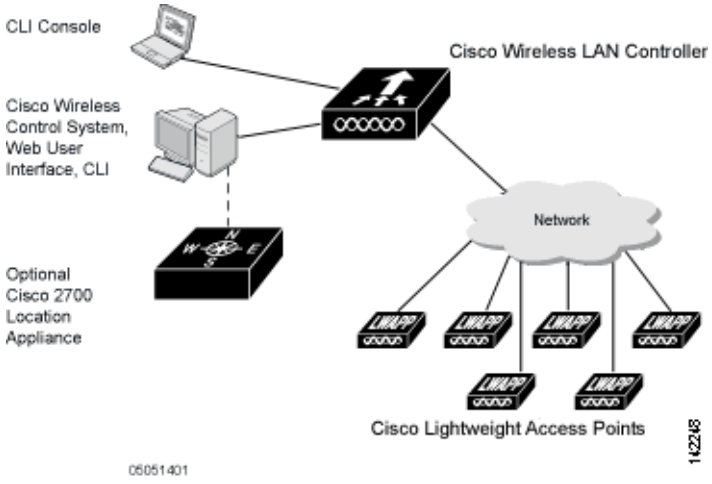
- An HTTPS full-featured web user interface hosted by Cisco controllers can be used to configure and monitor individual controllers.
- A full-featured command line interface (CLI) can be used to configure and monitor individual controllers.
- The Cisco Wireless Control System (WCS) can be used to configure 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 4 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 This document refers to controllers throughout. Unless specified otherwise, the descriptions herein apply 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, 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



Overview of WCS

The Cisco Wireless Control System (WCS) is a Cisco Unified Wireless Network Solution management tool that adds to the capabilities of the web user interface and command line interface (CLI), moving from individual controllers to a network of controllers. 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 and Red Hat Enterprise Linux ES 5.1. On both Windows and Linux, WCS can run as a normal application or as a service, which runs continuously and resumes running after a reboot.

The WCS user interface enables operators to control all permitted Cisco Unified Wireless Network Solution configuration, monitoring, and control functions through Internet Explorer 6.0 or later. Operator permissions are defined by the administrator using the WCS user interface Administration menu, which enables the administrator to manage user accounts and schedule periodic maintenance tasks.

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

WCS Versions

You can install WCS with one of two capabilities: WCS Base or WCS Location. Regardless of whether you choose WCS Base or WCS Location, a license is required.

WCS Base

The WCS Base supports wireless client data access, rogue access point, 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
- Rogue adhoc
- 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 tabular 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 hocs, 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 hocs to the nearest Cisco access point
  - Real-time and historical location of clients to the nearest Cisco access point

WCS Base + Location

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

- On-demand location of rogue access points and rogue ad hocs 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

Relationship with Cisco Location Appliances

When WCS Location is used, end users can also deploy Cisco 2700 Series Location Appliances. The location appliance enhances the high-accuracy built-in 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.

After a quick command line interface (CLI) configuration, the remaining location appliance configuration can be completed using the WCS user interface. After each location appliance is configured, it communicates directly with its associated controllers to collect operator-defined location data. The associated WCS server operators can then communicate with each location appliance to transfer and display selected data.

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.

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 (RFID) asset tags, rogue access points, rogue ad hocs, and rogue clients for each location appliance in the Cisco Unified Wireless Network Solution. Operators 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 whom you have specified 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 Oct 2005.

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

Comparison of WCS Base and WCS Location

Table 1-1 compares the 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 AP 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

Embedded Access Points

WCS software release 5.1 is supported for use with the AP801, the integrated access point in the Cisco 880 Series Integrated Services Routers (ISRs). This access point uses its own software image separate from the router and can operate as an autonomous access point that is configured and managed locally or as a centrally managed access point using LWAPP. The AP801 is preloaded with both an autonomous Cisco IOS release and an LWAPP recovery software image.

When you want to use the AP801, you must enable the LWAPP recovery image on the access point by entering this CLI command on the router in privileged EXEC mode: **service-module wlan-ap 0 bootimage unified**. 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 LWAPP software release from the controller, and acts as a lightweight access point.

Note To use the CLI commands mentioned above, the router must be running Cisco IOS Release 12.4(20)T or later.

In order to support LWAPP, the router must be running the Cisco Advanced IP Services IOS image. A license is required to upgrade to this image on the router. Refer to these URLS for licensing information:

http://cisco.com/en/US/docs/ios/csa/configuration/guide/csa_overview.html

http://cisco.com/en/US/docs/ios/csa/configuration/guide/csa_commands.html

The Cisco 880 Series ISRs with an LWAPP recovery image require DHCP to obtain an IP address on the access point. An IP address is needed to communicate with the controller and to download its image upon boot-up. 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 embedded-ap-pool
    network 60.0.0.0 255.255.255.0
    dns-server 171.70.168.183
    default-router 60.0.0.1
    option 43 hex f104.0a0a.0a0f /* single WLC IP address (10.10.10.15) in hex format */
```

The AP801 has a single 2.4-GHz 802.11g/b/n radio, which supports lower packet levels than the 802.11b/g/n 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's configuration.

Note For more information on the AP801, refer to the documentation for the 800 series routers at this URL:

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

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 Cisco recommends Internet Explorer 6.0 or later on a Windows workstation for full access to WCS functionality.

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 WCS for operation. It contains these sections:

- Prerequisites, page 2-1
- System Requirements, page 2-2
- Installing WCS for Windows, page 2-4
- Installing WCS for Linux, page 2-11
- Starting WCS, page 2-13
- Logging into the WCS User Interface, page 2-14
- Customizing Content on the WCS Home Page, page 2-20
- Using the Cisco WCS User Interface, page 2-22

Prerequisites

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

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

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

- Verified 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 Quad processor with 8-GB RAM.
- 80-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.

Standard Server

- Up to 2000 Cisco Aironet lightweight access points , 150 Cisco wireless LAN controllers, and 1000 autonomous access points.
- 3.2-GHz Intel Dual Core processor with 4-GB RAM.
- 40-GB minimum of 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 with 2-GB RAM.
- 30-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. Refer to Windows documentation for instructions on enabling this mode.

- Red Hat Linux Enterprise Server 5.0 or 5.1 32-bit operating system installations.

  Red Hat Linux Enterprise Server 5.0 or 5.1 64-bit operating system installations are not supported.

- Windows 2003 and Redhat Linux version support on VmWare ESX 3.0.1 version and above.

  VmWare must be installed on a system with these minimum requirements:
  Quad CPU running at 3.16 GHz, 8 GBs RAM, and a 200 GB hard drive.

  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 6.0/SP1 or Internet Explorer 7.0 with the Flash plugin. The Cisco WCS user interface has been tested and verified on a Windows workstation.

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 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.

Wireless LAN Controller Requirements

Cisco WCS 5.1.64.0 supports management of the following wireless LAN controllers:

- 4.2.61.0
- 4.2.99.0
- 4.2.112.0
- 4.2.130.0
- 5.0.148.0
- 5.1.151.0

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 RAM.
- 38-GB of free space on your hard drive.

WCS Navigator

- 20 WCSs

- 30K access points

Installing WCS for Windows

This section describes how to install Cisco WCS for Windows operating systems. Before installing Cisco WCS, refer to the "Prerequisites" section on page 2-1 and the "System Requirements" section on page 2-2. These sections give an overview of the system requirements and measures that you should take prior to the installation. 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. Refer to the "Upgrading WCS" section on page 12-15.

If installing WCS for Linux, see the "Installing WCS for Linux" section on page 2-11.

Guidelines Before Installing WCS

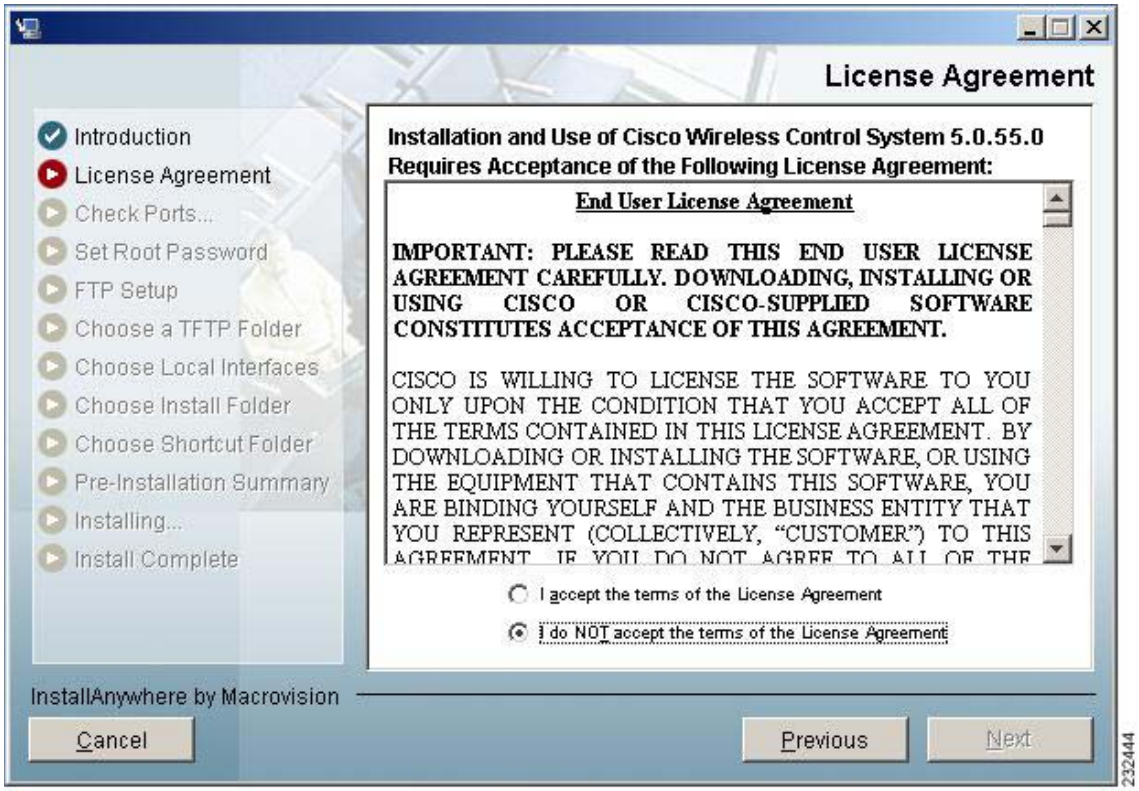
- You cannot install the WCS software if the username used to log into the server contains special characters such as exclamation marks (!). To ensure successful installation, log into the server using a username with no special characters before installing the software.
- Cisco WCS does not support 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 impact 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-K9-5.1.XX.Y.exe file where 5.1.XX.Y is the software build. If you received the installer from Cisco.com, double click the WCS-STANDARD-K9-5.1.XX.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 (see Figure 2-1). You must click the "I accept the terms of the License Agreement" option to continue.

Figure 2-1 License Agreement Window



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 12-15. For a first-time install, continue to Step 4.

Figure 2-2 Ineligible for Automated Upgrade

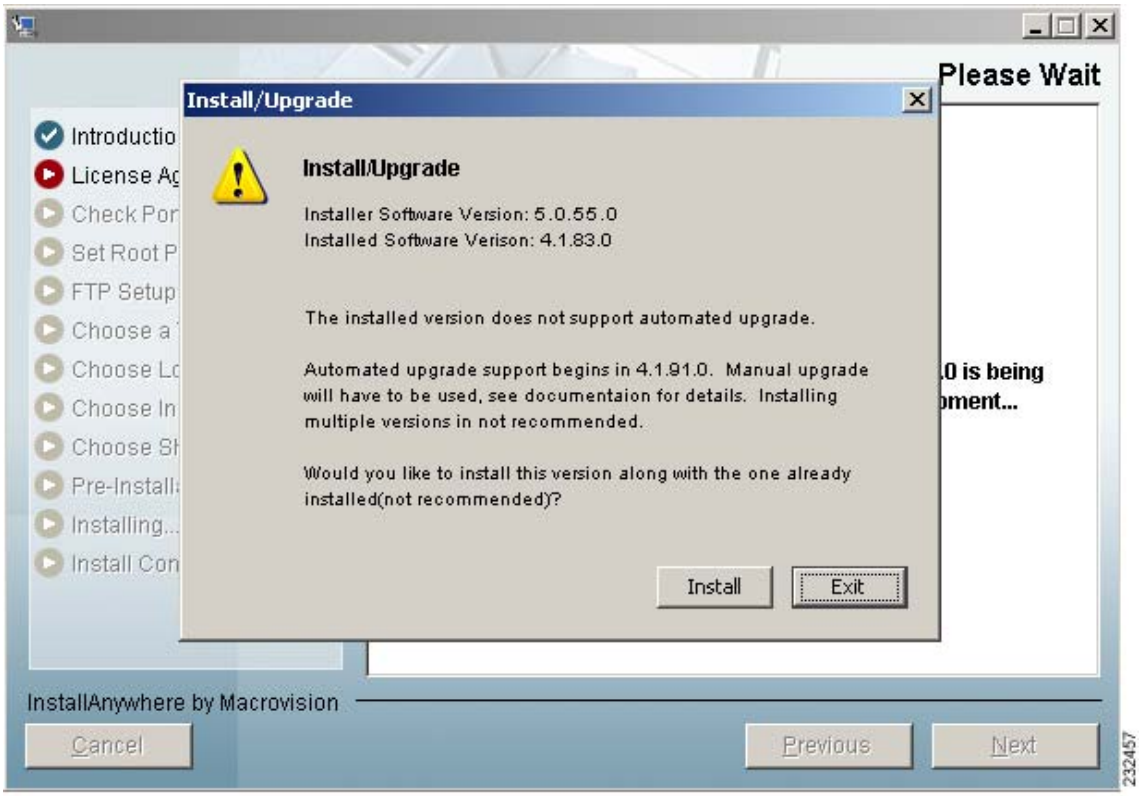
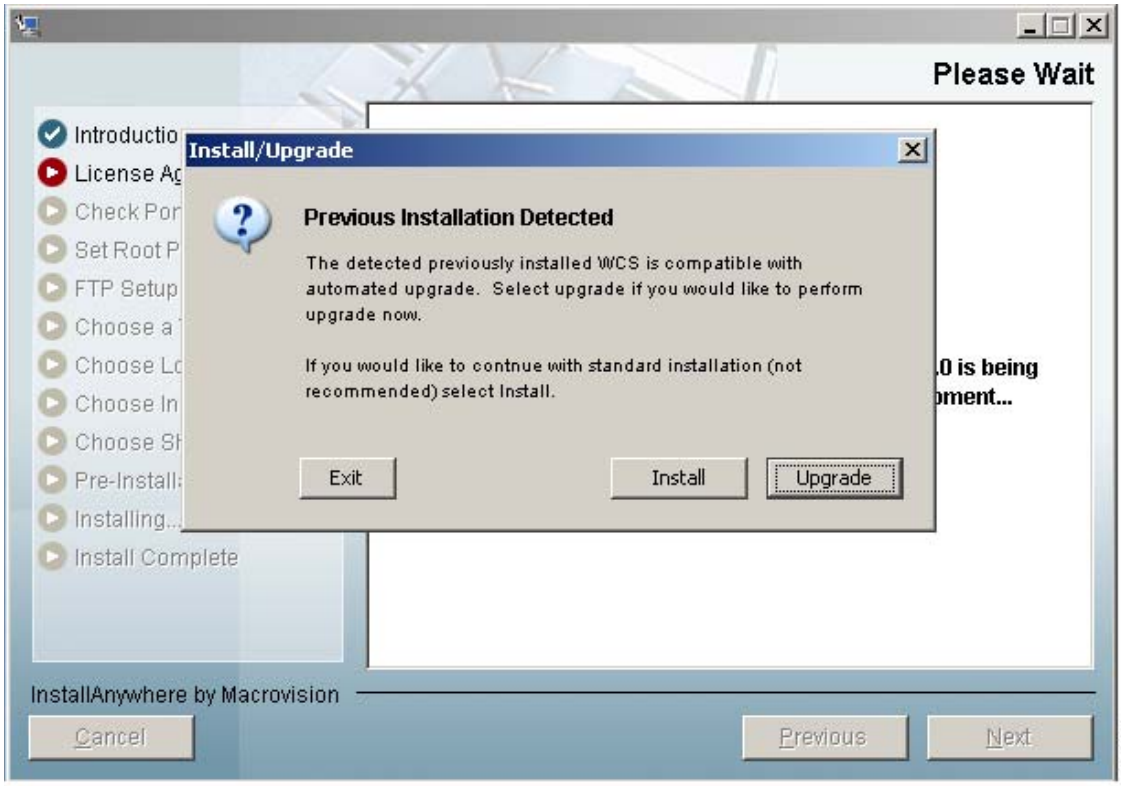
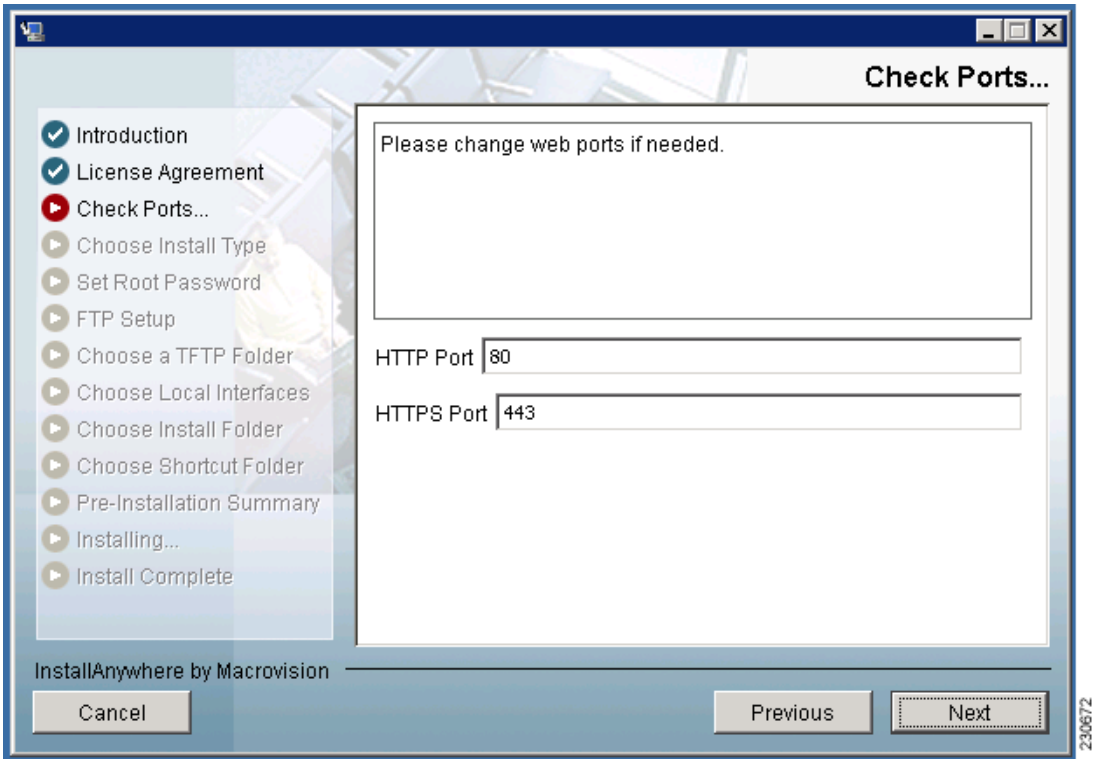


Figure 2-3 Previous Installation Detected



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 and click **Next** to open the Choose Install Type window. The default ports for HTTP and HTTPS are 80 and 443, respectively.

Figure 2-4 Check Ports Window



Step 5 Enter and re-enter the root password. The rules for a strong password are as follows:

- The minimum password length is 8.
- 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 repeated 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 6 Enter the root FTP password.

Step 7 From the FTP Server File window, choose a folder in which to store the FTP server files and click **Next** to bring up 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 Cisco WCS is uninstalled.

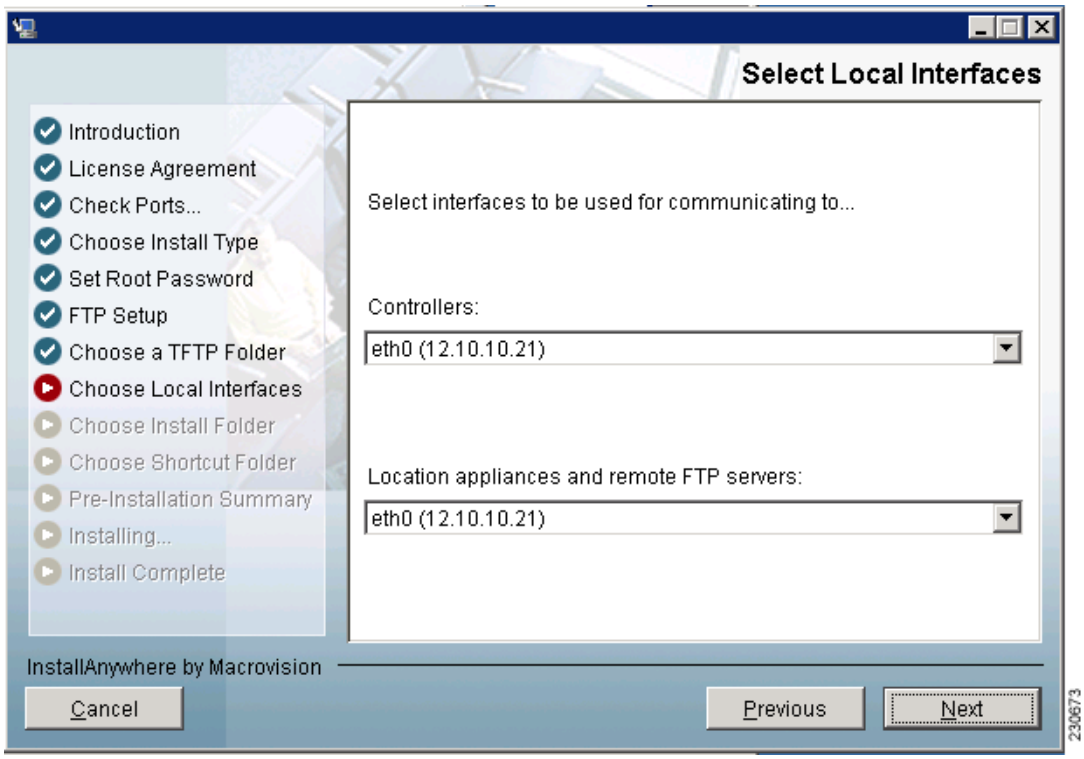
Step 8 From the TFTP Server File window, choose a folder in which to store the TFTP server files and click **Next**.

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 "Configuring WCS to Run as a Domain User" section on page 2-10) and then configure the TFTP root (see the "Configuring TFTP as a Network Drive" section on page 2-11).

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.

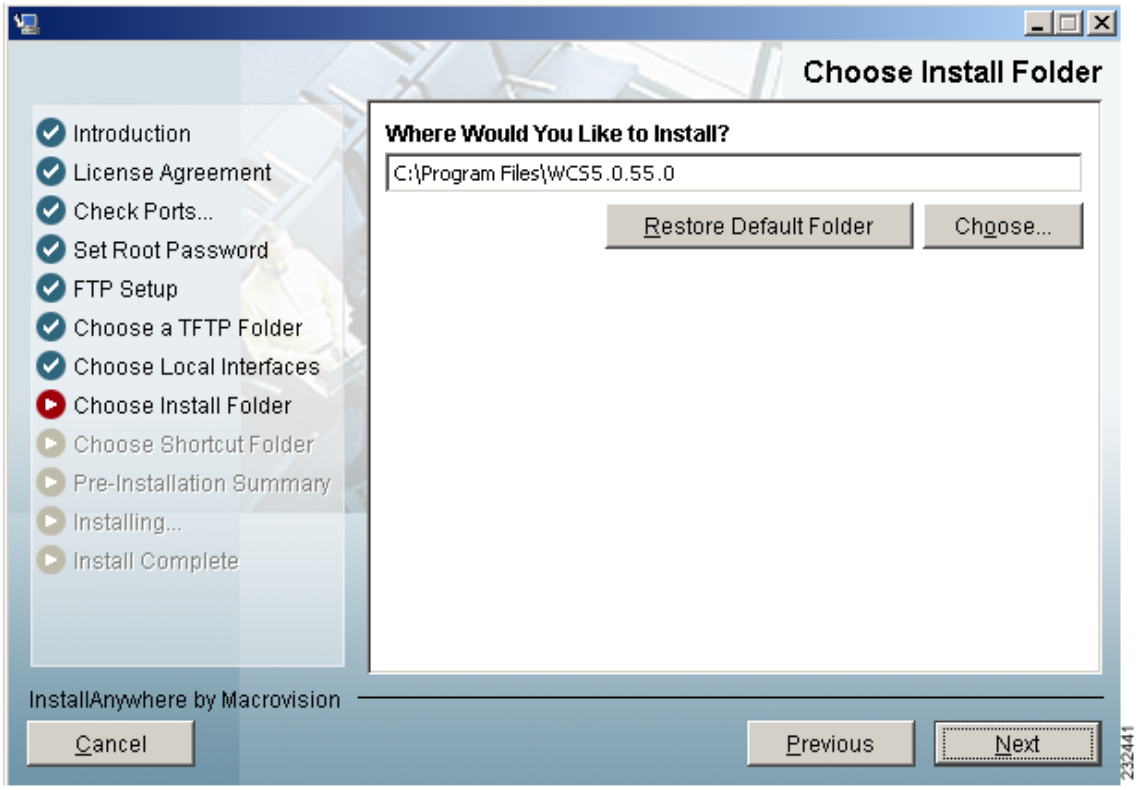
Step 9 If you are installing Cisco WCS on a multi-homed server (a server having multiple interfaces), the installer automatically detects the presence of multiple interfaces. The Select Local Interfaces window appears (see Figure 2-5). Choose the interfaces to be used by the server for communicating with controllers, location appliances and remote FTP servers, and clients. Click **Next**.

Figure 2-5 Select Local Interfaces Window



Step 10 Choose a folder in which to install the Cisco WCS at the Choose Install Folder window (see Figure 2-6). Click **Next** to continue.

Figure 2-6 Choose Install Folder



Step 11 Follow the prompts that appear on the screen to complete the installation. After the installation is complete, the Install Complete window appears. Click **Done** to complete the installation.

Note You can check the install log to determine if anything 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 WCS to Run as a Domain User

Follow these steps to configure WCS to run as a domain user.

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. Navigate to 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 2-4.

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. The same steps are repeated for each service.

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

a. Navigate to Administrative Tools > Services.

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

c. Choose 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. Navigate to Administrative Tools > Services.

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

c. Choose 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.

Configuring TFTP as a Network Drive

To configure TFTP as a network, you must have completed the steps in the "Configuring WCS to Run as a Domain User" section on page 2-10. 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.

Step 3 Restart WCS.

Installing WCS for Linux

You must have root privileges on Linux. This section describes how to install Cisco WCS for Linux operating systems.

Step 1 If not already done, log in as root. If you are using a graphical environment, 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-K9-5.1.XX.Y.bin where *5.1.xx.y* represents the current release number.

Step 4 Enter **./WCS-STANDARD-K9-5.1.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 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 12-15. For a first-time installation, continue to Step 6.

Step 6 The Check Ports prompt appears. 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.

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

- The minimum password length is 8.
- 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 repeated 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 8 Enter the root FTP password.

Step 9 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 10 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 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. Choose the interfaces to be used by the server for communicating with controllers, location appliances and remote FTP servers, and clients.

Step 12 Choose a folder in which to install the Cisco WCS.

Step 13 Follow the prompts that appear to complete the installation. After the installation is complete, the Install Complete statement appears.

Note You can check the install log to determine if anything 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.

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 "Checking the Status of WCS" section on page 12-1.

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 Windows Start menu, click **Programs > Wireless Control System> StartWCS**.
- From the command prompt, navigate to the WCS installation directory (C:\Program Files\WCS32\bin) and enter **WCS Admin start**.

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

Note If you are starting WCS after a restore 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. Refer to 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 2-14 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 /opt/WCS32 directory (or the directory chosen during installation) and enter **./StartWCS**.
- Navigate to the opt/WCS32/bin directory and enter **WCSAdmin start**.

The CLI displays messages indicate 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 2-14 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 6.0 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 you use a web browser other than Internet Explorer 6.0 on a 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 window, enter the root password which was created during installation.

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 allows 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.

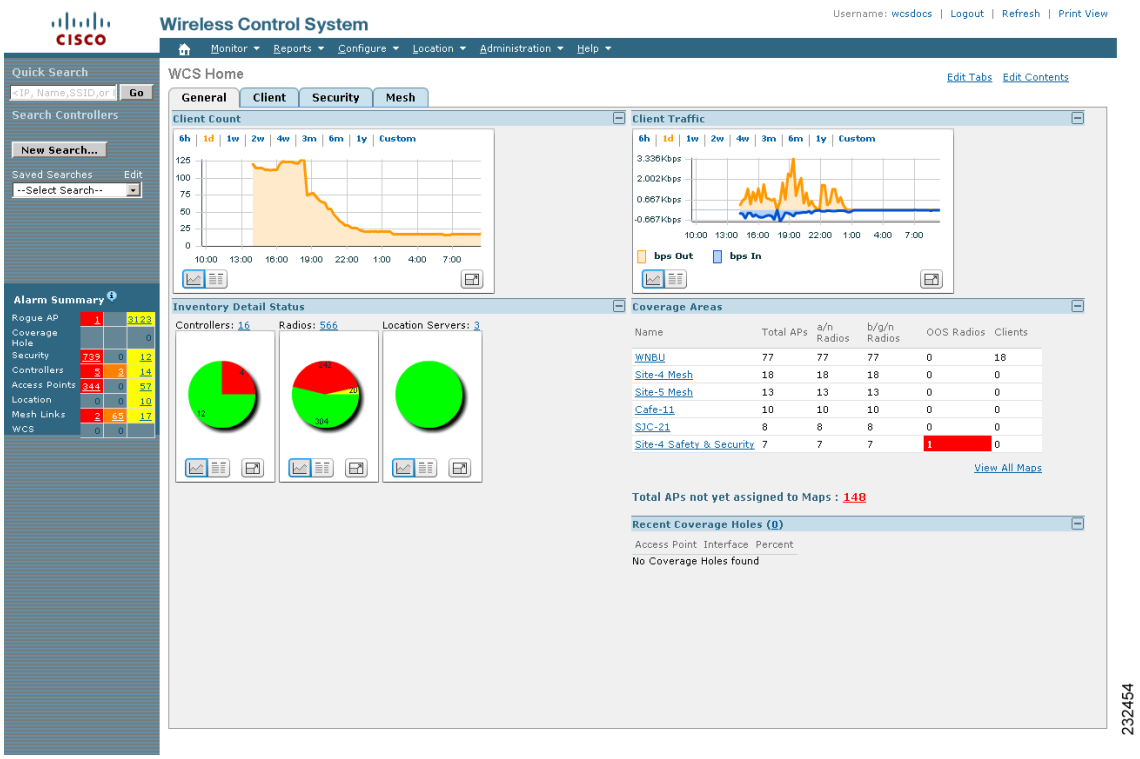
Note When an upgrade occurs, the user-defined tabs arranged by the previous user in the previous version is maintained. Therefore, the latest components may not show. Look at the Edit Componenets link to find what new components are added.

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 2-7 shows a typical WCS Home page.

You should see 4 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 2-7 WCS Home



Note To exit the WCS user interface, close the browser window 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 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. • Location Servers—Lists the number of location servers that are managed in WCS. Graphically depicts reachable and unreachable location servers. Check the WCS logs to see if anything went wrong while manually adding the location servers to WCS. (The trace for location servers must be turned on.)
Coverage Areas	Displays a graphical representation of client count over time with the default option of one day. The time options vary from one day to one year. Custom dates can also be specified.
Client Count	Displays the total number of clients in WCS over the selected period of time.
Recent Coverage Holes	Displays the most five 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

This client tab assists in identifying, diagnosing, and resolving client issues. The following are factory default components for the Client tab:

Top APs By Client Count

Displays the five access points with the highest client count showing the following data:

- AP Name—This is the name assigned to the access point. Click an item in the list to see the details of that access point.
- Map Location —The name of the map where the client is located.
- a/n Clients—The number of 802.11a clients currently associated with the controller.
- b/g/n Clients—The number of 802.11b clients and 802.11g clients currently associated with the controller.
- Total Client—Total number of clients currently associated with the controller.

Most Recent Client Alarms

Displays the five most recent client alarms by default showing the following data:

- Client—IP address, MAC address, or user-defined name of client.
- Date/Time—Date and time of client notification.
- Event Type—Reason for client notification. For example, disassociated, WEP decrypt error, or authentication failure.

Click the number in parentheses to access the Alarms page.

Manually Disabled Clients

Provides a link to view a list of manually disabled clients. Click **Manually Disabled Clients** to access this page.

This page enables you to view manually disabled client template information.

- MAC Address—Client MAC address.
- Description—Optional user-defined description.

Client Traffic

A graphic shows the associated clients during a given time frame. The client traffic (bps Out and bps In) appears in time increments of six hours, one day, one week, two weeks, four weeks, three months, six months, one year, or a custom time frame.

Security Tab

If you click the Security tab from the WCS Home page, you see the following factory default components:

Table 2-2 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 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 Rogue Adhoc Alarm	Displays the five most recent rogue adhoc alarms. Click the number in parentheses to access the Alarms page. Click an item under MAC address to view adhoc details.
Most Recent Security Alarms	Displays the five most recent security alarms. Click the number in parentheses to access the Alarms page.

Table 2-2 Security Tab Components

Component	Description
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.
Adhoc Rogues	Displays adhoc rogues for the past hour, past 24 hours, and total active.
Security Index	Displays security index for WCS. Also lists which security issues are happening the most.

Mesh Tab

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

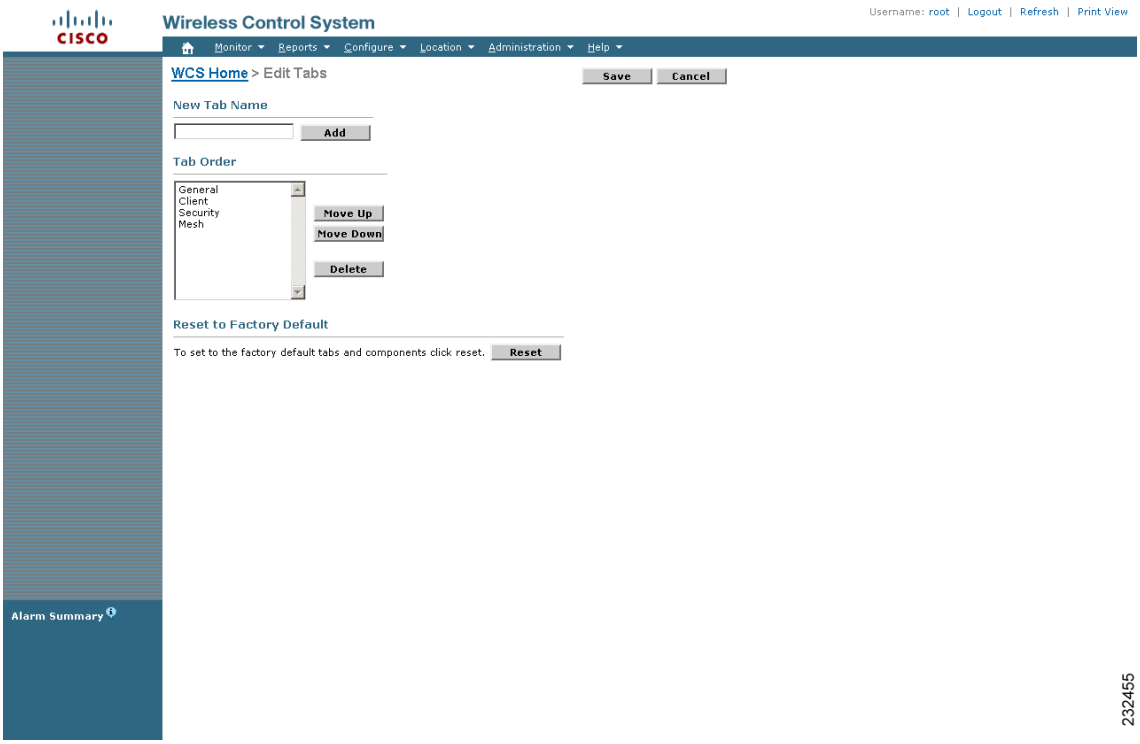
Table 2-3 Mesh Tab Components

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.

Customizing Tabs on the WCS Home Page

You can customize the home page from the default four tabs and personalize its look. When you click the Edit Tabs link on the WCS Home page, you move to a screen in which customization can begin (see Figure 2-8). Follow these steps to create a new tab.

Figure 2-8 WCS Home > Edit Tab



Step 1 Enter the name of the new tab you are creating and click **Add**. The tab name you add appears in the Tab Order window.

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 2 Click on the tab names in the Tab Order window 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 2-7, click **Reset**.

Customizing Content on the WCS Home Page

You can customize the home page components and personalize its look. When you click the Edit Contents link on the WCS Home page, you move to a screen in which customization can begin (see Figure 2-8). 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, Location > Location Servers, and Configure > Spectrum Experts.) These graphs

refresh automatically within a predetermined time based on the default polling cycles of dependent tasks. When a graph is time based, an additional link bar at the top of the graph window 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** to enlarge the graph in a separate window.

Note Hold your mouse over the applicable button for a tool tip identifying the View in Chart or View in GridClick the View in Chart button to view the data in a graph. Click the **View in Grid** button to view the data in a table.

There are several components listed in the Available Contents on the WCS Home > Edit Contents window. These options and their explanations are as follows:

- Client Security Component—This component displays client security details within the last 24 hours. The contents include excluded client events, WEP decrypt errors, WPA MIC errors, shunned clients, and IPSEC failures in the last hour, last 24 hours, and total.
- Controller CPU Utilization— This component displays in graphical form the average maximum and minimum CPU utilizations.
- Most Recent AP Alarms—This component displays the five most recent access point alarms by default. You can change the number of alarms to display. The All Alarm link goes to the alarm page in which all alarms are visible.
- Recent Alarms—This component displays the five most recent alarms by default. You can change the number of alarms to display. The All Alarm link goes to the alarm page in which all alarms are visible.
- Rogue AP Detail Summary—This component displays the five most recent rogue alarms. You can change the number of alarms to display. The summary provides the MAC address, SSID, type, state, and date and time stamp.
- Controller Memory Utilization—This component displays in graphical form the average maximum and minimum memory utilizations.
- Clients Detected by Location Server—This component shows the client count detected by the location server within the last 15 minutes. You can change the number of minutes to 30 or 60.

- Client Count—This component displays a graphical representation of the client count over time with the default option as one day. The time options vary from one day to one year, or you can enter custom dates.
- Inventory Status—The inventory status shows the following:
  - Controllers: Lists the number of controllers that are managed in WCS and graphically depicts the number of reachable and unreachable controllers.
  - Radios: Lists the number of radios managed in WCS and graphically depicts the number of radios in out-of-service (critical), minor, or ok conditions.
  - Location Servers: Lists the number of location servers that are managed in WCS and graphically depicts the number of reachable and unreachable location servers.
- Recent Coverage Holes—This component displays the most five recent coverage alarms. You can change the number of alarms to display.
- Client Traffic—This component displays in graphical form the average traffic in and out for all clients located in WCS.
- Coverage Areas—This component shows the different coverage areas on the map, lists the number of access points, radios, and clients within them, and provides a status. You can change the number of maps to display.
- Cisco Wired IPS Events—This component displays wired IPS events that have occurred.
- Unclassified Rogue APs—This component displays unclassified rogue access points that have accessed the network.
- Friendly Rogue APs—This component displays friendly rogue access points that have accessed the network.
- Adhoc Rogues—This component displays adhoc rogue that have accessed the network.

Follow these steps to create new content for the WCS home page.

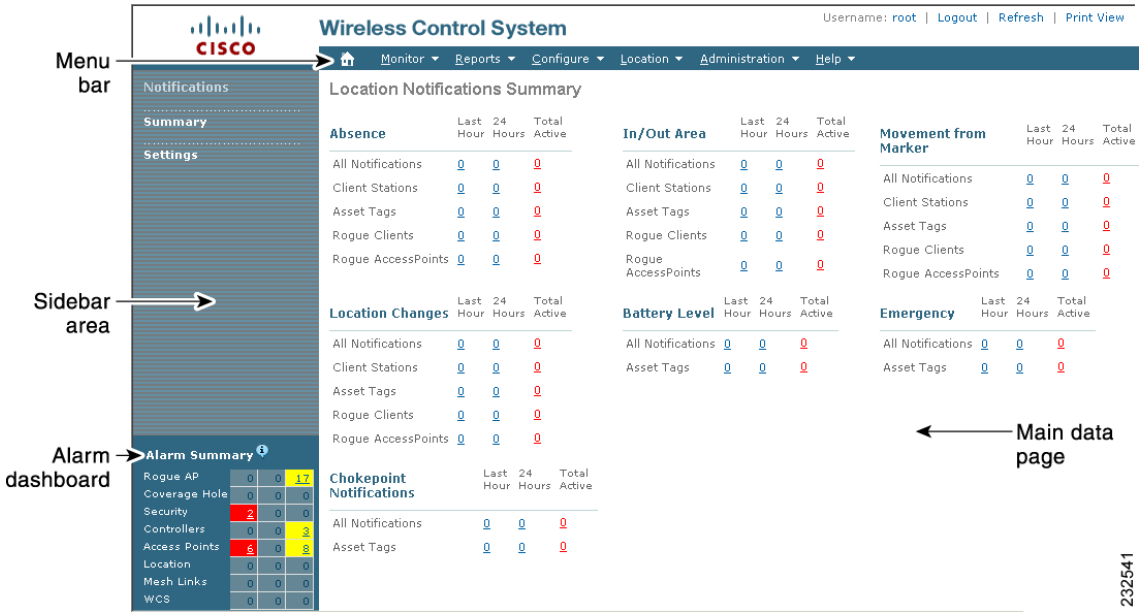
Step 1 The home page is divided into two parts. From the Available Contents window, highlight the desired component and choose to add it to the left column or right column. The component moves to the appropriate column.

Step 2 Click the component from the Left Column or Right Column window and designate to move it up, down, to the right, or to remove.

Using the Cisco WCS User Interface

A typical Cisco WCS user interface page consists of the areas illustrated in Figure 2-9.

Figure 2-9 WCS User Interface



The following sections describe the Cisco WCS user interface page areas and how to use them:

- Menu Bar, page 2-23
- Sidebar Area, page 2-24
- Alarm Dashboard, page 2-25
- Command Buttons, page 2-25
- Main Data Page, page 2-25
- Administrative Tools, page 2-26

Menu Bar

There are five menus on each window: **Monitor**, **Reports, Configure**, **Location**, **Administration**, and **Help**. When you move the mouse over any of the menus, a drop-down menu appears.

Note The Location menu is displayed only in Cisco WCS Location version.

Monitor Menu

The Monitor menu provides you with a top level description of the devices on your network. You can monitor your network, maps, various devices, security, alarms, events, or reports.

Configure Menu

The Configure menu allows you to configure templates, controllers, and access points on your network.

Administration Menu

The Administration menu allows you to schedule tasks like making a backup, checking a device status, auditing your network, synchronizing the location server, and so on. You can also choose Logging to enable various logging modules and specify restart requirements. You can also choose AAA for user administration such as changing passwords, establishing groups, setting application security settings, and so on.

Location Menu

The Location menu allows you to configure location appliances. A location appliance is a Cisco server that collects and stores up to 30 days of historical location data for up to 2,500 laptop clients, palmtop clients, VoIP telephone clients, active RFID (Radio Frequency Identifier) asset tags, rogue access points, and rogue access point clients.

Note The Location menu is displayed only in Cisco WCS location version.

For more information on location appliances, refer to the *Cisco 2700 Series Location Appliance Installation and Configuration Guide*.

Note Read/Write permissions are used by the location function of the location appliance. *Write* permissions allow a client application or location appliance operator to modify location data only (such as asset information), while *Read* permissions only allow a client to read location data.

Note Full permissions are required for administration. All functions under the Locate menu in Cisco WCS are administrative functions. An administrator must always have full permissions.

Help Menu

The Help menu allows you to access online help and check the version of Cisco WCS.

To check the version of WCS, click **About the Software**. The product name, version number, copyright statement, and Apache Software Foundation statement is displayed.

Sidebar Area

The sidebar area allows you to choose a new configuration panel 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 windows contain a group of menus in this area. Click the menu item to reveal a submenu and then click the item to chose it.

Alarm Dashboard

When Cisco WCS receives alarm messages from a controller, the Cisco WCS user interface displays an alarm indicator in the lower left corner in an alarm summary panel known as the alarm dashboard. The alarm dashboard only appears when the Macromedia flash is installed.

Alarms indicate the current fault or state of an element that needs attention. These are usually generated by one or more events. The alarm can be cleared, but the event remains. An example of an alarm is *AP down*, which means that the current status of the access point is down.

Alarms are color coded as follows:

- Clear = No alarm
- Red = Critical alarm
- Orange = Major alarm
- Yellow = Minor alarm

You can click any of the various types of alarms (such as rogues, coverage, security, controllers, access points, location, mesh links, and WCS) to display details.

Command Buttons

The Cisco WCS user interface uses a number of command buttons throughout its windows. 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 window and returns to the previous window
- 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

Main Data Page

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

- Text fields 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 fields 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 field until the **GO** button is selected.

Administrative Tools

This area provides shortcuts to administration functions (such as logged in as, logout, refresh, and help) that are used on a regular basis when configuring a controller through the web user interface.

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
- Using WCS to Convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 Mode, page 3-4
- Configuring a Firewall for WCS, page 3-5
- Access Point Authorization, page 3-6
- Management Frame Protection (MFP), page 3-6
- Configuring Intrusion Detection Systems (IDS), page 3-8
- Configuring IDS Signatures, page 3-8
- Enabling Web Login, page 3-16
- Certificate Signing Request (CSR) Generation, page 3-21

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 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).

Rogue Management

WCS rogue management includes rogue access points and rogue adhocs. You can click the **Security** tab from the WCS Home window to see the most recent rogue adhocs.

Most Recent Rogue Adhocs

The Most Recent Rogue Adhocs section displays the rogue adhoc MAC address, SSID, state, and date and time of initial detection.

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

Step 1 Click the **MAC Address** of a specific rogue adhoc to view its associated alarm details.

Step 2 To modify the alarm, choose one of the following commands from the Select a command drop-down menu and click **GO**.

- Assign to me—Assigns the selected alarm to the current user.
- Unassign—Unassigns the selected alarm.
- Delete—Deletes the selected alarm.
- Clear—Clears the selected alarm.
- Acknowledge—Allows you to designate the alarm as acknowledged.

  Note If you mark the alarm as acknowledged, it does not show in the Alarm Summary window.

- Unacknowledge—Changes the acknowledged alarm back to unacknowledged.
- Event History—Enables you to view events for the rogue adhoc alarm.

  Note Event History for this adhoc can also be accessed from the Most Recent Rogue Adhocs details page.

- Detecting APs—Enables you to view the access points that are currently detecting the rogue adhoc.
- Map (High Resolution)—Displays the current calculated rogue adhoc location on the Maps > *Building Name* > *Floor Name* page.
- Rogue Clients—Enables you to view the clients associated with this rogue adhoc.

- Set State to ‘Unknown - Alert’—Tags the rogue adhoc as the lowest threat, continues to monitor the rogue adhoc, and turns off containment.
- Set State to ‘Known - Internal’—Tags the rogue adhoc as internal, adds it to the known rogue adhoc list, and turns off containment.
- Set State to ‘Known - External’—Tags the rogue adhoc as external, adds it to the known rogue adhoc list, 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 deauthenticate and disassociate messages to the client devices that are associated to the rogue unit.

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 IOS-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 > Devices > 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 Authorization**.

Step 4 The AP Policies portion of the window 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 menu 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 Auth Entry** from the Select a command drop-down menu and click **GO**.

Step 6 From the drop-down menu, 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. Refer to the "Configuring an Access Point or LBS Authorization" section on page 11-39 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. Refer to the "Configuring WLAN Templates" section on page 11-9.

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.

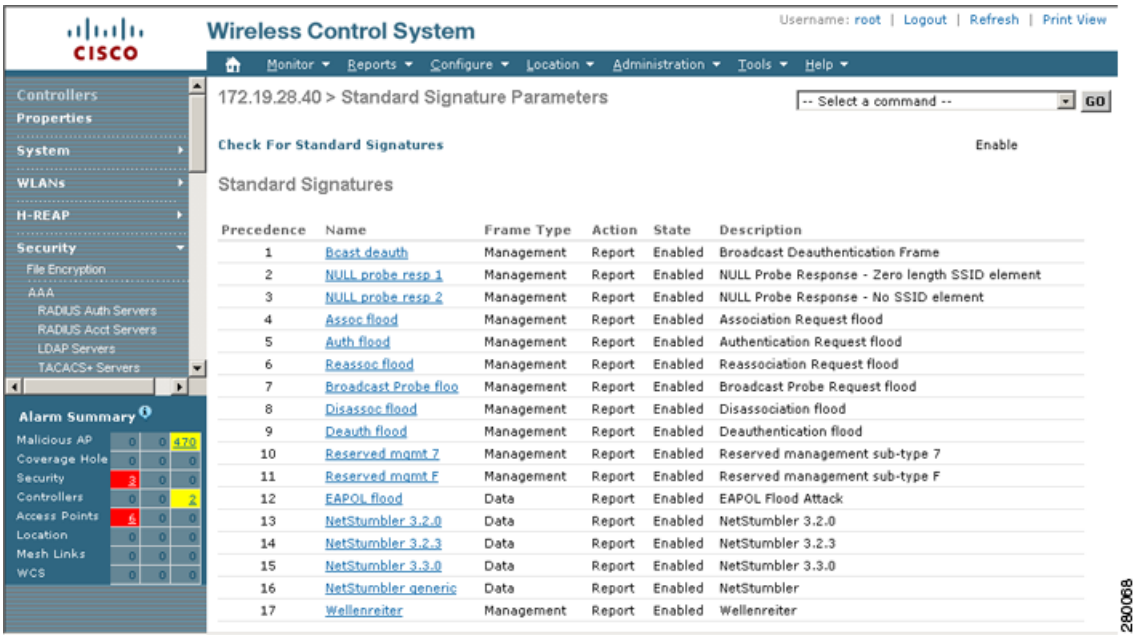
Step 3 From the left sidebar menu, choose **Security > IDS Sensor Lists**. The IDS Sensor window appears. This page lists all of the IDS sensors that have been configured for this controller.

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 3-1).

Figure 3-1 Standard Signature Window



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.

- 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.
- 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 3-1 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)

Follow these instructions to configure signatures:

- Uploading IDS Signatures, page 3-11
- Downloading IDS Signatures, page 3-12
- Enabling or Disabling IDS Signatures, page 3-13
- Viewing IDS Signature Events, page 3-16

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 3-12.

Step 2 Make sure you have a Trivial File Transfer Protocol (TFTP) server available for the signature download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port 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.

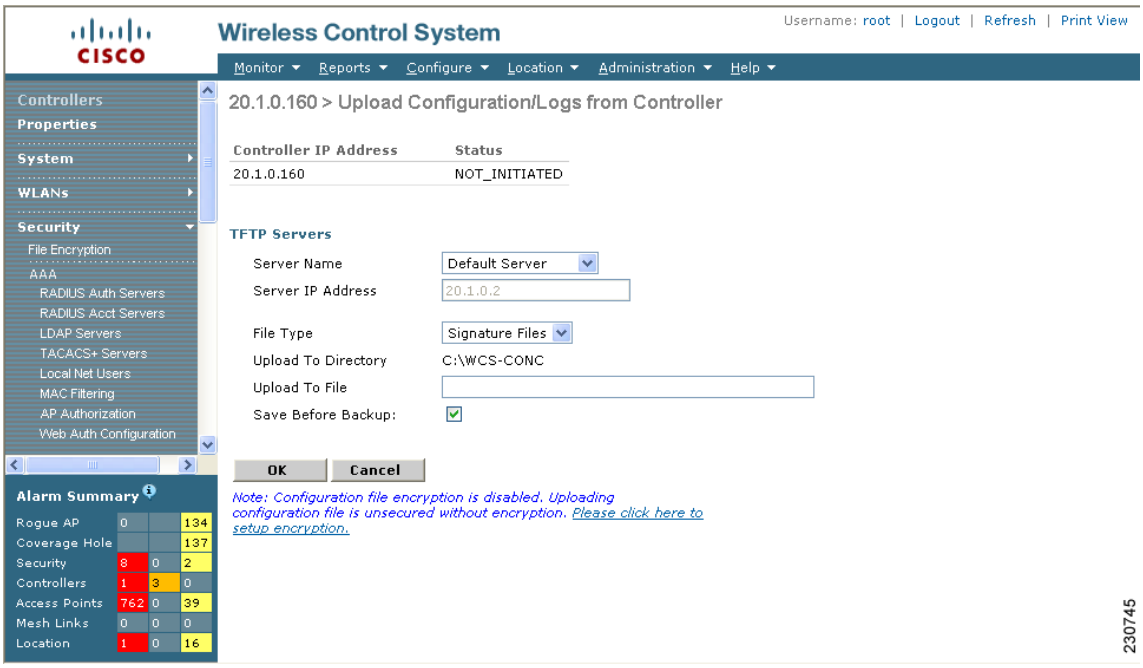
Step 3 Choose **Configure > Controllers**.

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 menu, choose **Upload Signature Files from Controller**. Figure 3-2 shows the window that appears.

Figure 3-2 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 menu.

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 menu, 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

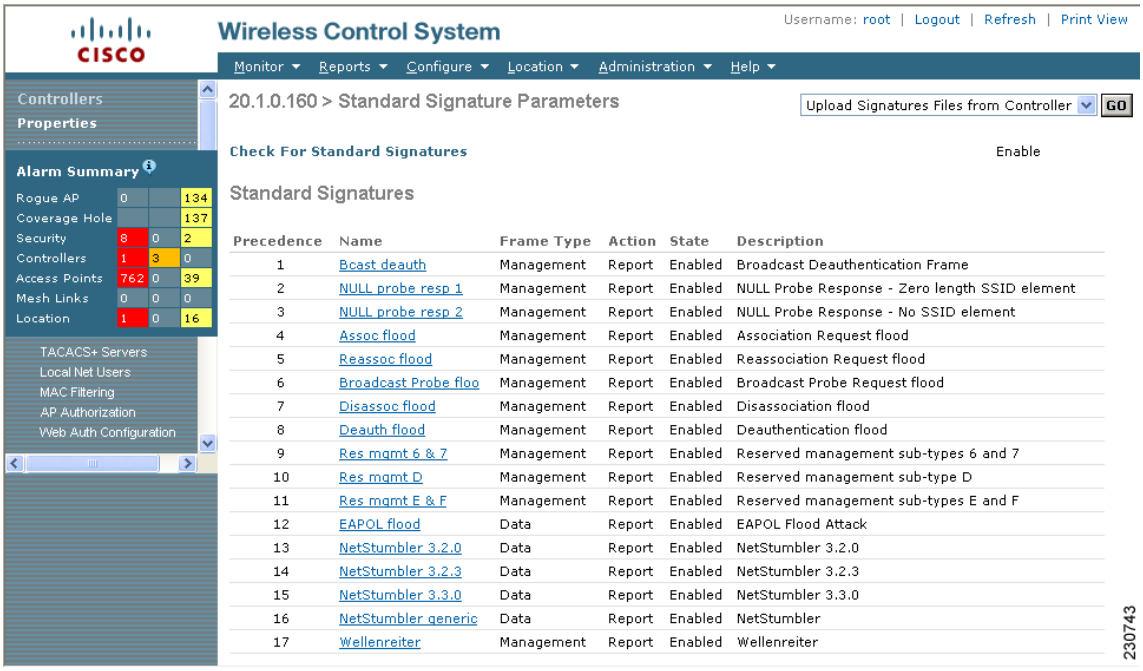
Follow these steps to enable or disable IDS signature.

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 3-3 shows a sample of the screen that appears.

Figure 3-3 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 3-4 shows a sample of a detailed signature screen.

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

- 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.

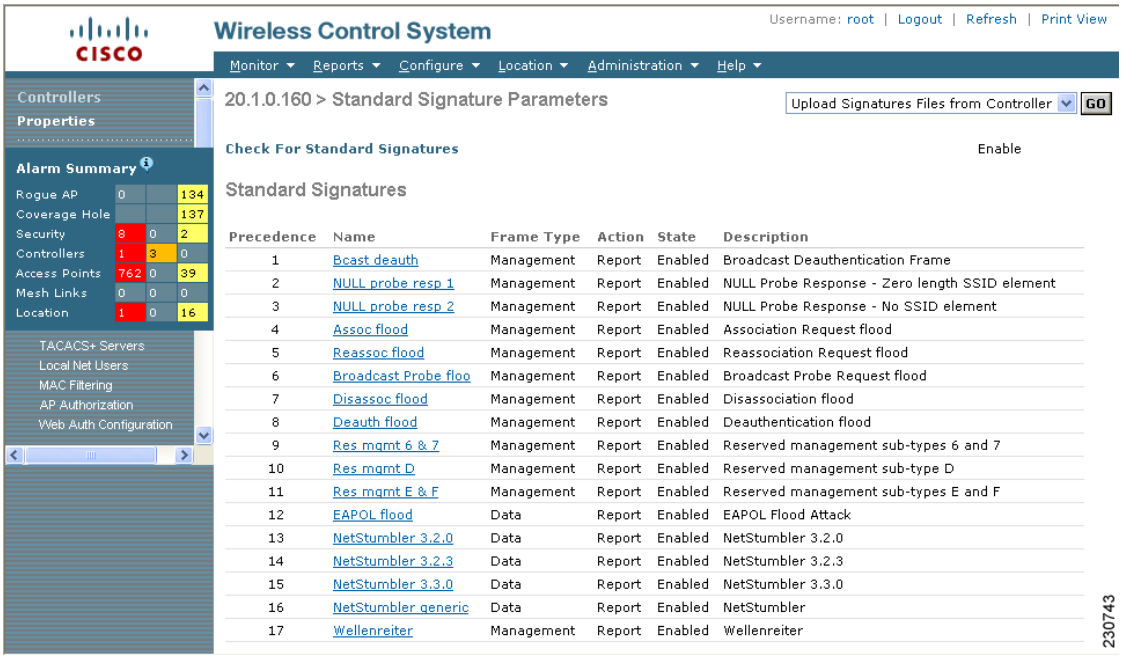
- Interval - Enter the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval. The range is 1 to 3600 seconds, and the default value is 1 second.
- Enable - Check this to enable this signature to detect security attacks or uncheck it to disable this signature.
- Signature Patterns - The pattern that is being used to detect a security attack.

Figure 3-4 Standard Signature

Step 5 In the Enable yes or no drop-down menu, 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 3-3) from the Select a command drop-down list and click **GO**. The Global Settings for Standard and Custom Signature window appears (see Figure 3-5).

Figure 3-5 Global Setting for Standard and Custom Signature



Step 7 Check the **Enable Check for All Standard and Custom Signatures** check box. This enables all signatures that were individually selected as enabled in Step 5. If this box remains unchecked, 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**.

Viewing IDS Signature Events

Follow these steps to see the number of attacks detected by the enabled signatures.

Step 1 Choose **Monitor > Events** or **Monitor > Alarms**.

Step 2 From the Event Category drop-down menu on the left sidebar menu, choose **Security** and click **Search**.

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 11-51 to create a template that replaces the Web authentication page provided on the controller.

Step 1 Choose **Configure > Controller.**

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 > Web Auth Configuration**.

Step 4 Choose the appropriate web authentication type from the drop-down menu. 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 3-17.
- 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 field is http://www.company.com, the user is directed to the company home page.

Step 5 Click 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 Provide the URL where the user is redirected after a successful authentication. For example, if the value entered for this field 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 on the preview image to download the sample login.html bundle file from the server. See Figure 3-6 for an example of the login.html file. The downloaded bundle is a .TAR file.

Figure 3-6 Login.html

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

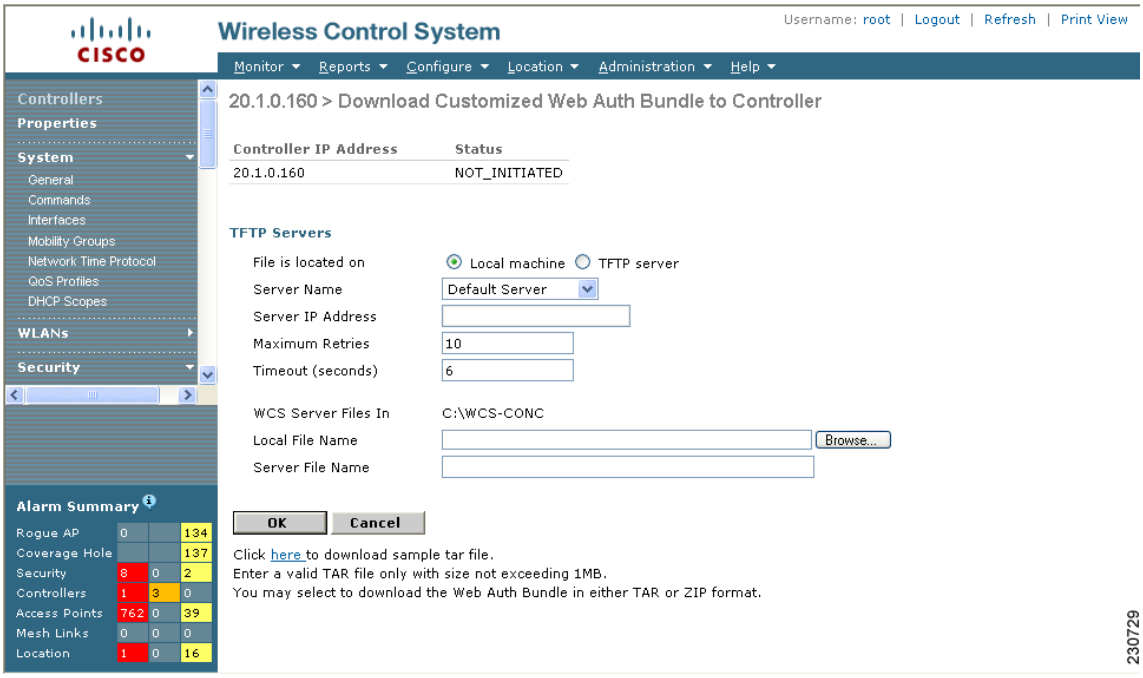
Note You can edit the text of the Submit button with any text or HTML editor to read "Accept terms and conditions and Submit."

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 window appears (see Figure 3-7).

Figure 3-7 Download Customized Web Auth Bundle to Controller



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 7-11 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 window, enter your username and password.

Note All entries are case sensitive.

The lobby ambassador has access to the templates only to add guest users.

Step 3 Click **Submit** to log into WCS. The WCS user interface is now active and available for use. The Guest Users Templates page is displayed. This page provides a summary of all created Guest User templates.

Note To exit the WCS user interface, close the browser window 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 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.

Deleting a Guest User

Follow these steps to delete all clients stations that are logged in and using the guest WLAN and its account's username.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > Guest Users**.

Step 3 Click the check box before the username you want to delete. WCS gives you a warning message before deletion.

Step 4 From the Select a command drop-down menu, choose **Delete Templates**. The window displays remove results if the deletion was successful.

Note The controller can also send notification when a guest account has expired by invoking a trap. WCS processes this trap and deletes the guest user account from the configuration of that controller.

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 WCS to perform system-level tasks. It contains these sections:

- Adding System Components to the WCS Database, page 4-1
- Using WCS to Update System Software, page 4-4
- Downloading Vendor Device Certificates, page 4-5
- Downloading Vendor CA Certificates, page 4-5
- Using WCS to Enable Long Preambles for SpectraLink NetLink Phones, page 4-6
- Creating an RF Calibration Model, page 4-7

Adding System Components to the WCS Database

This section describes how to add a controller and a location appliance to the WCS database.

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 menu, 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:

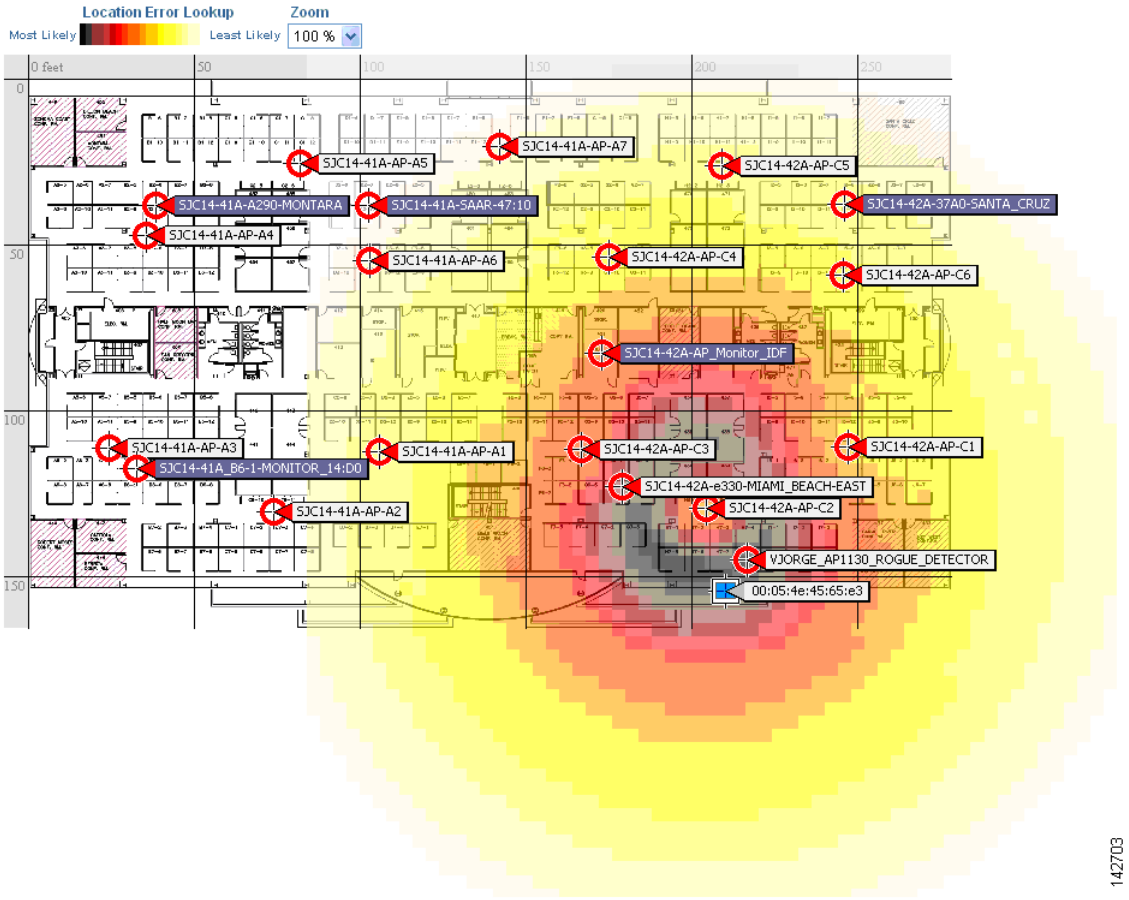
- The controller service port IP address might be set incorrectly. Check the service port setting on the controller.
- WCS might not have been able to contact the controller. Make sure that you can ping the controller from the WCS server.
- The SNMP settings on the controller might not match the SNMP 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.

Adding a Location Appliance to the WCS Database

To add a location appliance to the WCS database, follow the instructions in the *Cisco Location Appliance Configuration Guide*. It provides documentation on the Location > Location Server option within WCS and all of its capabilities (such as editing general properties, tracking, filtering, history, advanced, and NMSP parameters). WCS without the use of the location appliance supports on-demand or query-based location. This version visually displays a single device's location at a time, placing each single device on the floor map associated with the floor it is on. Location determination using this version of WCS with location is captured in Figure 4-1 where the blue icon is the only visual presented of a Wi-Fi client device.

Figure 4-1 Location Determination



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 RFID 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 **ping *ip-address*** 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 Check the check box of the desired controller, choose **Download Software** from the Select a Command drop-down menu, and click **GO**. WCS displays the Download Software to Controller page.

Step 4 If you use the built-in WCS TFTP server, check the **TFTP Server on WCS System** check box. If you use an external TFTP server, uncheck 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 > Controller**.

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 menu 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 Device Certificate** from the Upload/Download Commands drop-down menu and click **GO**.

Step 3 In the Certificate Password field, 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 in Step 10. If the certificate is on the local machine, you must specify the file path in the Local File Name parameter in Step 9 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 field, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 8 In the Timeout field, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

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

Step 10 In the Server File Name field, enter the name of the certificate.

Step 11 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 menu 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 menu 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 field, enter the maximum number of times that the TFTP server attempts to download the certificate.

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

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

Step 9 In the Server File Name field, enter the name of the certificate.

Step 10 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 menu, and **GO**.

Step 9 To reboot the controller, click **Reboot** from the Administrative Commands drop-down menu 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. It contains these sections:

- Creating Maps, page 5-1
- Placing Access Points, page 5-25
- Creating a Network Design, page 5-27
- Using Chokepoints to Enhance Tag Location Reporting, page 5-34
- Monitoring Maps, page 5-42
- Importing or Exporting WLSE Map Data, page 5-54
- Creating and Applying Calibration Models, page 5-57
- Analyzing Element Location Accuracy Using Testpoints, page 5-63
- Using the Accuracy Tool to Conduct Accuracy Testing, page 5-67

Creating Maps

With the Cisco WCS database, you can add maps and view your managed system on realistic campus, building, and floor map maps. Follow the instructions in the sections below to add a campus, buildings, outdoor areas, floor plans, and access points to maps in the Cisco WCS database:

- Adding a Campus, page 5-1
- Adding Buildings, page 5-2
- Adding Outdoor Areas, page 5-5
- Searching Maps, page 5-8

Adding a Campus

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 Click **Monitor** > **Maps** to display the Maps page.

Step 4 From the Select a command drop-down menu, 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 or CAD file containing the map of the campus and click **Open**.

Step 7 Check 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 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.

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 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 Click **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 menu, choose **New Building** and click **GO**.

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 an approximate building horizontal span and vertical span (width and depth on the map) in feet.

Tip The horizontal and vertical span should be larger than or the same size as any floors that you might add later.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.

e. Click **Place** to put the building on the campus map. WCS creates a building rectangle scaled to the size of the campus map.

f. Click on 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.

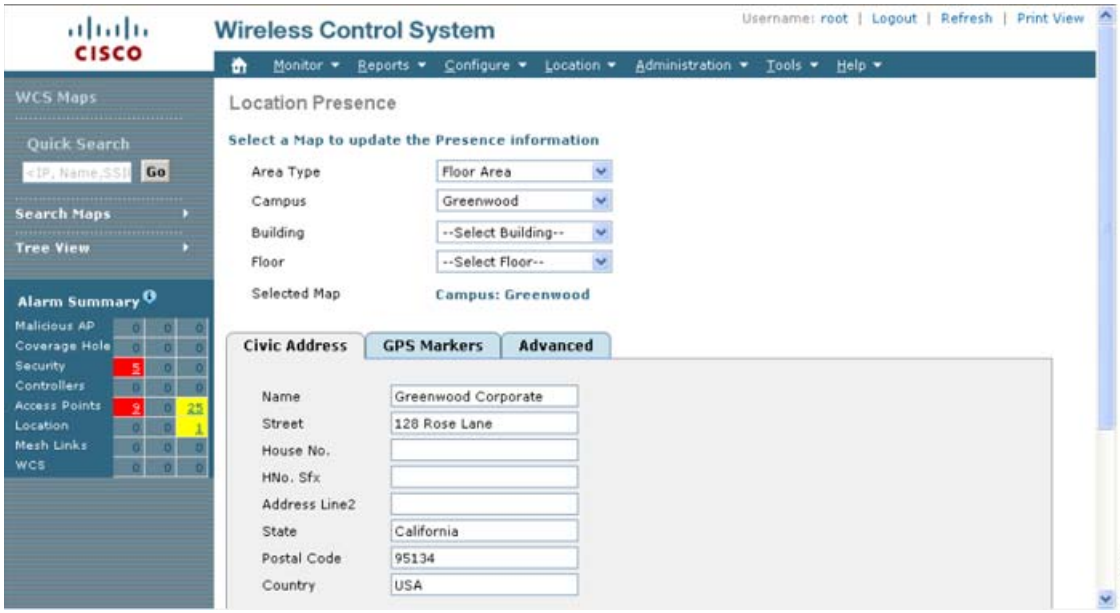
g. Click **Save** to save this building and its campus location to the database. WCS saves the building name in the building rectangle on the campus map.

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 menu. Click **GO**. The Location Presence window appears (see Figure 5-1).

Figure 5-1 Location Presence Window



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 (Administration > Location Presence).

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 checked. 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 Click **Monitor > Maps** to display the Maps page.

Step 2 From the Select a command drop-down menu, choose **New Building** and click **GO**.

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 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 **Edit Location Presence Info** from the Select a command drop-down menu. Click **GO**. The Location Presence window appears (see Figure 5-1).

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 (Administration > Location Presence).

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 checked. There is no need to alter this setting for standalone buildings.

Step 5 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 Click **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 menu, choose **New Outdoor Area** and click **GO**.

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

a. Enter the outdoor area name.

b. Enter the outdoor area contact name.

c. If desired, enter or browse to the filename of the outdoor area map.

d. Enter an approximate outdoor horizontal span and vertical span (width and depth on the map) in feet.

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 outdoor area change to match your actions.

e. 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.

f. Click on the outdoor area rectangle and drag it to the desired position on the campus map.

g. Click **Save** to save this outdoor area and its campus location to the database. WCS saves the outdoor area name in the outdoor area rectangle on the campus map.

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

Step 6 *(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 menu. Click **GO**. The Location Presence window appears (see Figure 5-1).

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 (Administration > Location Presence).

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 checked. There is no need to alter this setting for outdoor areas.

Step 7 Click **Save**.

Enabling Location Presence on a Location Server

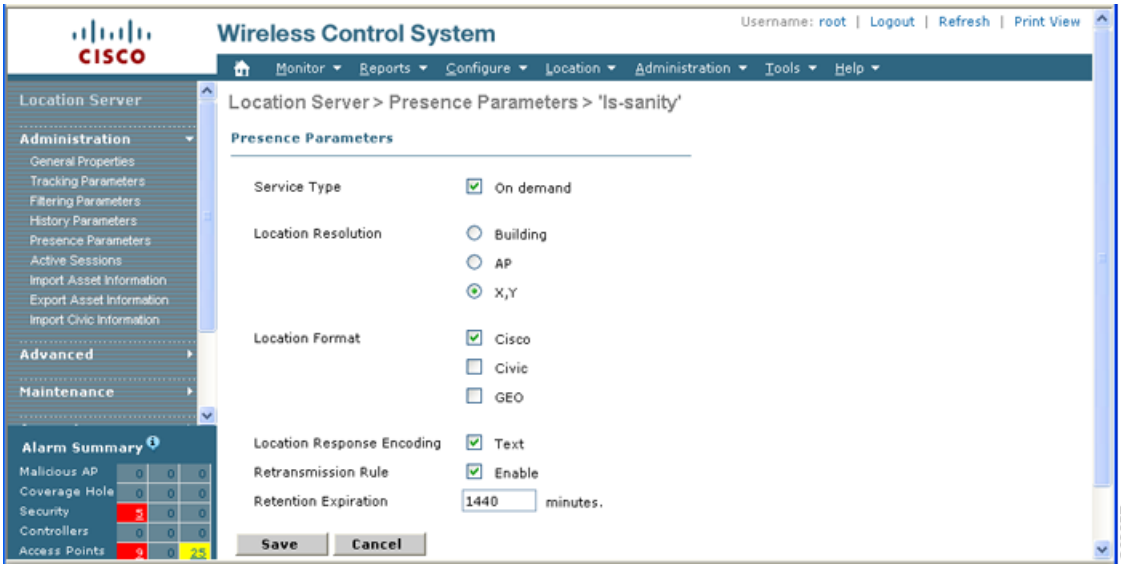
Follow these steps to enable and configure location presence on a location server. When enabled, the location server is capable of providing any requesting Cisco Compatible Extension v5 client with its location.

Note Before enabling this feature, synchronize the location server.

Step 1 Click **Mobility > Mobility Service Engines**. Choose the location server to which the campus or building is assigned.

Step 2 Choose **Presence Parameters** from the Administration menu (on the left sidebar menu). The Location Presence window appears (see Figure 5-2).

Figure 5-2 Location Server > Presence Parameters Window



Step 3 Check the **On Demand** check box to enable location presence for Cisco Compatible Extension v5 clients.

Step 4 Choose one of the Location Resolution options.

a. When *building* is selected, the location server can provide, to any requesting client, its location by building.

- For example, if a client requests its location and the client is located in Building A, the location server returns the client address as *Building A*.

b. When *ap* is selected, the location server can provide, to any requesting client, its location by its associated access point. The MAC address of the access point appears.

- For example, if a client requests its location and the client is associated with an access point with a MAC address of 3034:00hh:0adg, the location server returns the client address of *3034:00hh:0adg*.

c. When *X,Y* is selected, the location server can provide, to any requesting clients, 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 location server returns the client address of *50, 200*.

Step 5 Check any or all of the location formats.

a. Check the **Cisco** check box to provide location by campus, building, and floor with X and Y coordinates. This is the default setting.

b. Check the **Civic** check box to provide the name and address (street, city, state, postal code, country) of a campus, building, floor, or outdoor area. Expanded location details can also be entered in the Advanced panel.

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

Step 6 By default the Text check box for Location Response Encoding is checked. It indicates the format of the information when received by the client. There is no need to change this setting.

Step 7 Check the **Retransmission Rule Enable** check box to allow the receiving client to retransmit the received information to another party.

Step 8 Enter a **Retention Expiration** value in minutes. This determines how long the received information is stored by the client before it is overwritten. The default value is 24 hours (1440 minutes).

Step 9 Click **Save**.

Searching Maps

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

- **New Search** drop-down menu: Opens the Search Maps window. Use the Search Maps window to configure, run, and save searches.
- **Saved Searches** drop-down menu: Lists the saved custom searches. To open a saved search, choose it from the Saved Searches list.
- **Edit Link**: Opens the Edit Saved Searches window. You can delete saved searches in the Edit Saved Searches window.
- **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 window:

- Search for
- Map Name
- Search in
- Save Search
- Items per page

After you click **GO**, the map search results window appears:

Table 5-1 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.

Table 5-1 Map Search Results

Parameter	Options
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.
Clients	Displays the number of clients currently associated with the controller.
Status	A colored icon indicating the campus or building status (green for Up, yellow for Warning, or red for Down).

Finding Coverage Holes

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 WCS, enabling the IT manager to fill holes based on user demand. Follow these steps to find coverage holes on your wireless LAN.

Step 1 Click the **Coverage** indicator on the bottom left of the WCS user interface page (or click **Monitor > Alarms** and search for **Coverage** under Alarm Category) to display the Coverage Hole Alarms page.

Step 2 Click **Monitor > Maps** and search for access points by name (this search tool is case sensitive). WCS displays the Maps > Search Results page, which lists the floor or outdoor area where the access point is located.

Step 3 Click the floor or outdoor area link to display the related Maps > *Building Name* > *Floor Name* page.

Step 4 Look for areas of low signal strength near the access point that reported the coverage hole. These areas are the most likely locations of coverage holes. If areas of weak signal strength are detected, make sure that the floor plan map is accurate.

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.

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

Step 4 Click the desired campus. WCS displays the Maps > *Campus Name* page.

Step 5 Move 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.

Step 6 Click on the building name to display the Maps > *Campus Name* > *Building Name* page.

Step 7 From the Select a command drop-down menu, choose **New Floor Area** and click **GO**.

Step 8 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.

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

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

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. Either leave the **Maintain Aspect Ratio** check box checked to preserve the original image aspect ratio or uncheck 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 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 > *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 9 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 "Inspect VoWLAN Readiness" section on page 5-22 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.

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

Step 4 Click the desired building. WCS displays the Maps > *Building Name* page.

Step 5 From the Select a command drop-down menu, 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.

f. Check 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 checked to preserve the original image aspect ratio or uncheck 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 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 "Inspect VoWLAN Readiness" section on page 5-22 for instructions.

Using the Map Editor to Enhance Floor Plans

You can use the WCS map editor to define, draw, and enhance floor plan information. The map editor enables you to create obstacles so that they can be taken into consideration when computing RF prediction heat maps for access points. You can also add coverage areas for location appliances that locate clients and tags in that particular area. Follow these general guidelines to use the map editor.

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 menu, click **GO**, check 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 location appliance uses no more than 50 heavy walls in its calculations, and the location appliance 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 Click **Monitor > Maps** to display the Maps page.

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

Step 3 Click on a campus building.

Step 4 Click on 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 menu, 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 Choose the desired 802.11 standard from the Radio Type drop-down menu.

Step 9 Choose the antenna model from the Antenna drop-down menu.

Step 10 Determine the propogation pattern at the Antenna Mode drop-down menu.

Step 11 Make antenna adjustments by sliding the antenna orientation bar to the desired degree of direction.

Step 12 Choose the desired access point.

Step 13 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 In Cisco WCS, add the floor plan if it is not already represented in WCS (refer to the "Adding and Enhancing Floor Plans" section on page 5-9).

Step 2 Choose **Monitor > Maps**.

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

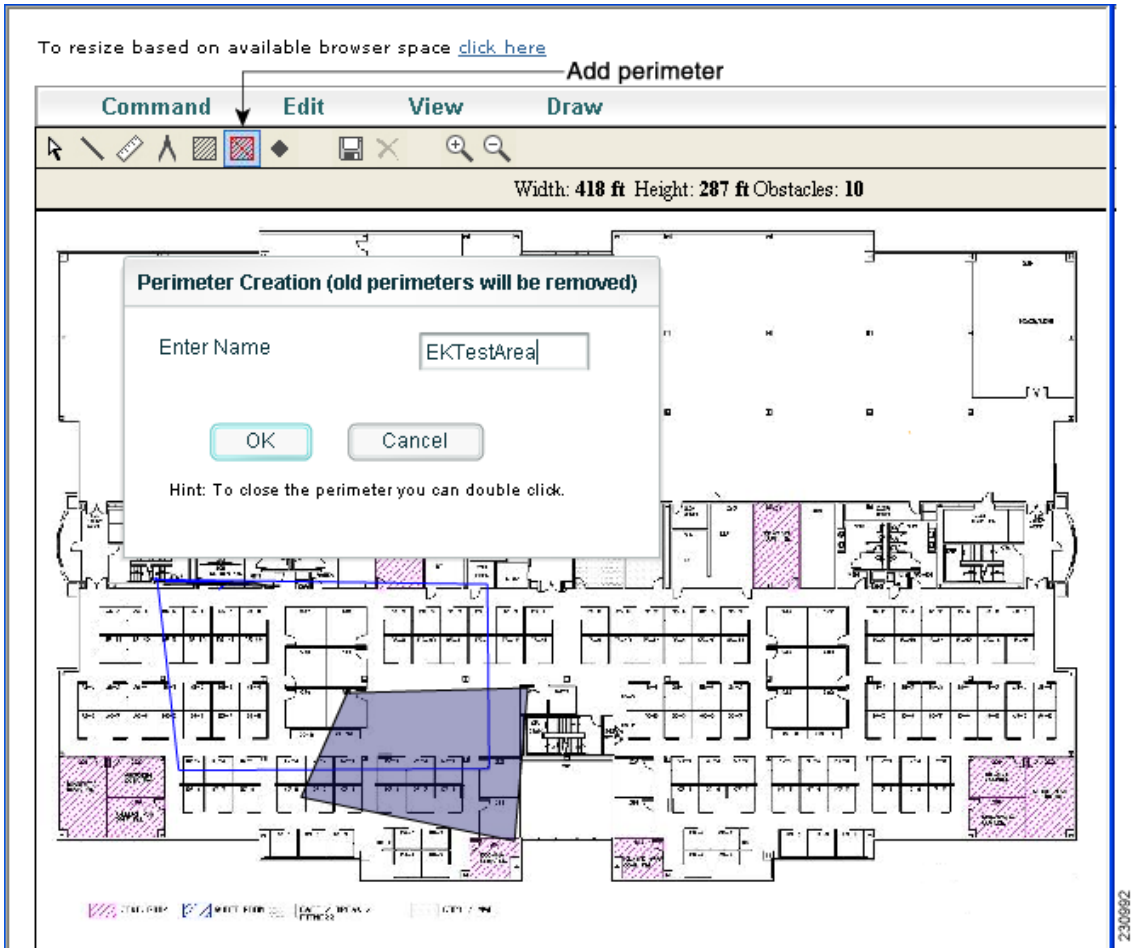
Step 4 From the Select a command drop-down menu, choose **Map Editor** and click **GO**.

Step 5 At the Map Editor screen, click the **Add Perimeter** icon on the tool bar (see Figure 5-3).

A pop-up window appears.

Note An example of a polygon-shaped area is seen in Figure 5-3.

Figure 5-3 Map Editor Page



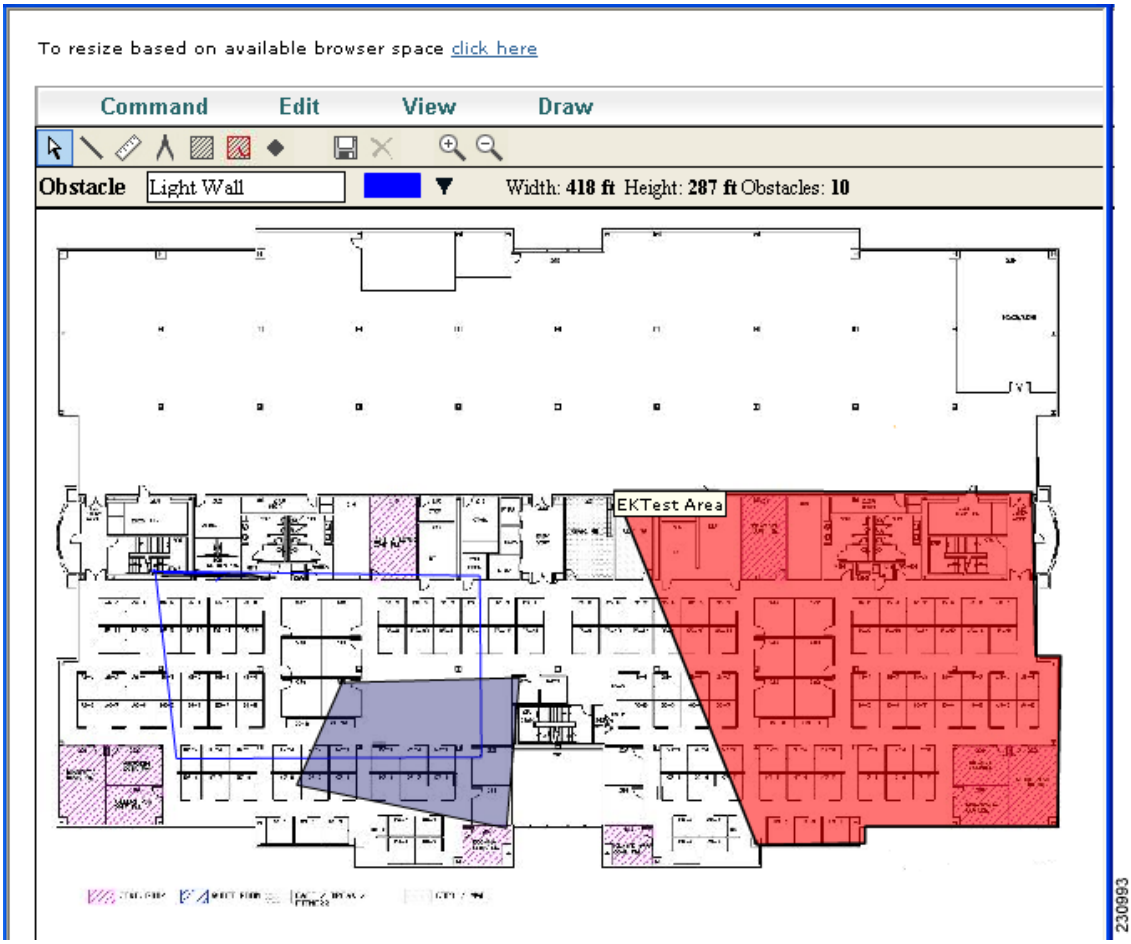
Step 6 Enter the name of the area that you are defining. Click **OK**.

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 5-4).
- The outlined area must be a closed object to highlight on the map.

Figure 5-4 Polygon Area



Step 8 Click the disk icon in the tool bar to save the newly drawn area.

Step 9 Choose **Command > Exit** to close the window. You are returned to the original floor plan.

Note When you return to the original floor plan view, after exiting the map editor, the newly drawn area is not seen; however, it appears in the Planning Model window when you add elements.

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

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

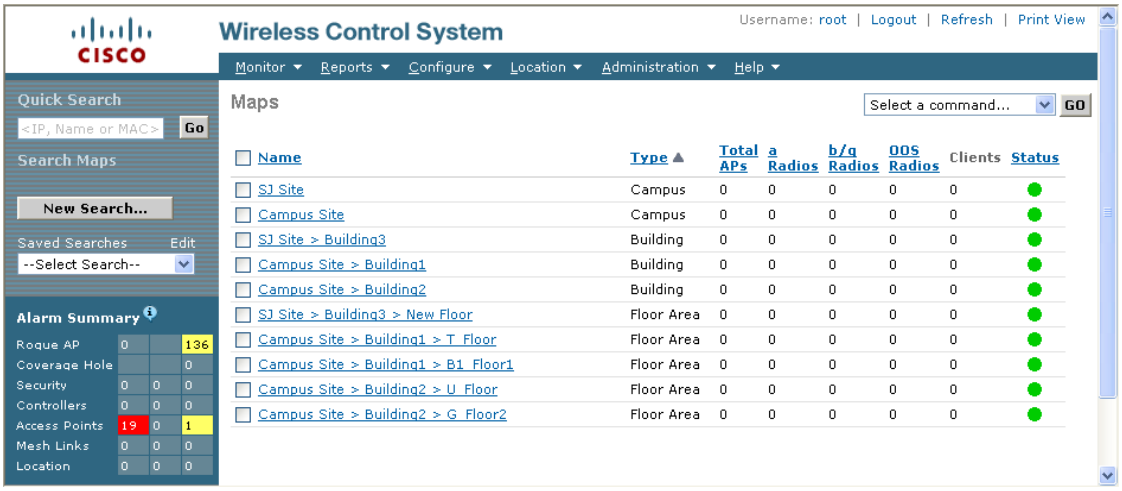
- location accuracy requirements
- number of active users
- number of users per square footage

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

Step 1 Choose **Monitor > Maps.**

The window appears (see Figure 5-5).

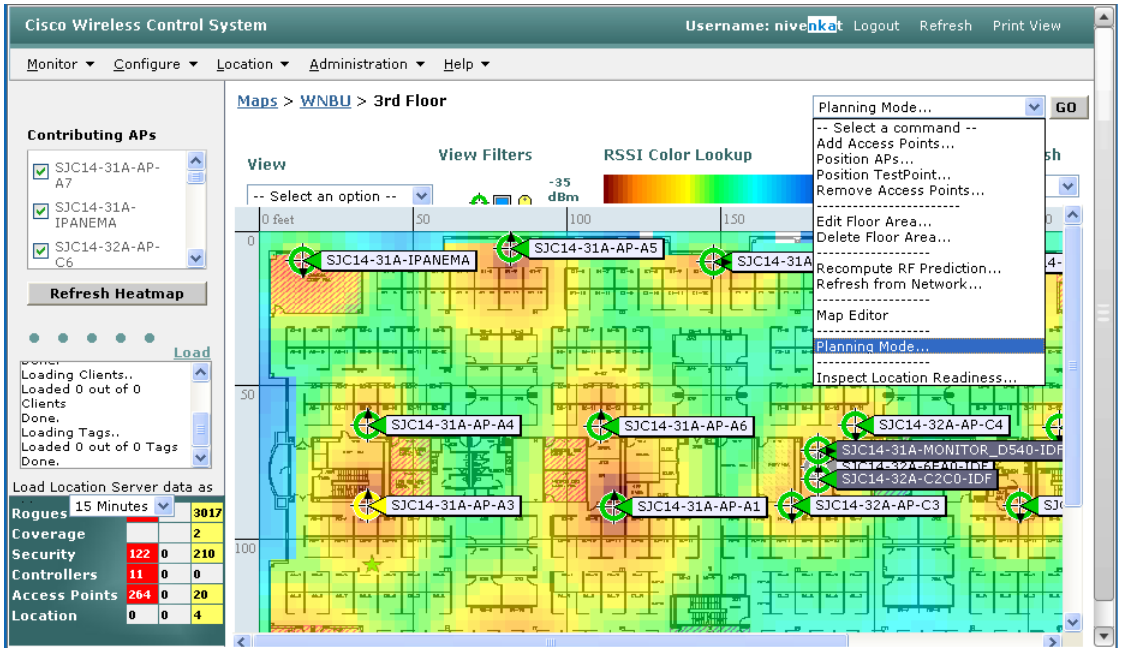
Figure 5-5 Monitor > Maps Page



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 5-6).

Figure 5-6 Selected Floor Area Showing Current Access Point Assignments



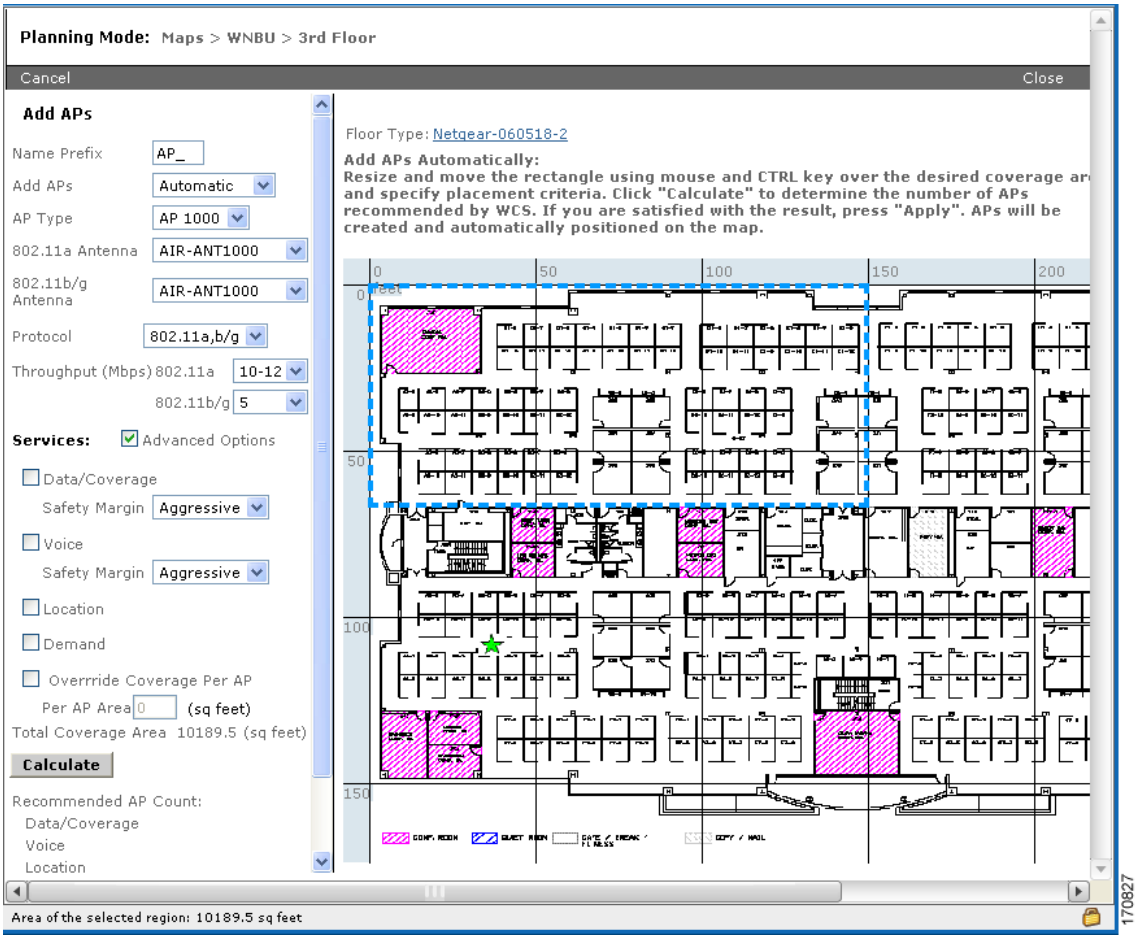
Step 3 Choose **Planning Mode** from the Select a command drop-down menu (top-right) and click **GO.** A blank floor map appears.

Step 4 Click **Add APs.**

Step 5 In the page that appears, drag the dashed-line rectangle over the map location for which you want to calculate the recommended access points (see Figure 5-7).

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 5-7 Add APs Page



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

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 Check the box(es) next to the **service(s)** that will be used on the floor. Options are Data/Coverage (default), Voice, and Location (Table 5-2).

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

Note If you check 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 service options (Table 5-3).

Table 5-2 Definition of Service Options

<table>
<tr><th>Service Options</th><th>Description</th></tr>
<tr><td>Data/Coverage</td><td>Select if data traffic is transmitted on the wireless LAN. The following densities are used depending on the band and data rates:
<table>
<tr><th>Band</th><th>Path Loss Model (dBm)</th><th>Date Rate (Mbps)</th><th>Area (Sq. ft.)</th></tr>
<tr><td>802.11a/n</td><td>–3.3</td><td>10-12</td><td>6000</td></tr>
<tr><td>802.11a/n</td><td>–3.3</td><td>15-18</td><td>4500</td></tr>
<tr><td>802.11a/n</td><td>–3.5</td><td>10-12</td><td>5000</td></tr>
<tr><td>802.11a/n</td><td>–3.5</td><td>15-18</td><td>3250</td></tr>
<tr><td>802.11b/g/n</td><td>–3.3</td><td>5</td><td>6500</td></tr>
<tr><td>802.11b/g/n</td><td>–3.3</td><td>6</td><td>4500</td></tr>
<tr><td>802.11b/g/n</td><td>–3.5</td><td>5</td><td>5500</td></tr>
<tr><td>802.11b/g/n</td><td>–3.5</td><td>6</td><td>3500</td></tr>
</table>
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>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/n)]
• Safe = Medium [–75 dBm (802.11a/b/g/n)]
• Very Safe = Maximum [(–72 dBm (802.11a/b/g/n)]
• 7920_enabled = [(–72 dBm (802.11a/n); –67 dBm (802.11b/g/n)]</td></tr>
<tr><td>Location</td><td>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 colocated 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 check the Location box, the calculation considers data/coverage, voice, and location in determining the optimum number of access points required.</td></tr>
</table>

Table 5-3 Definition of Advanced Options

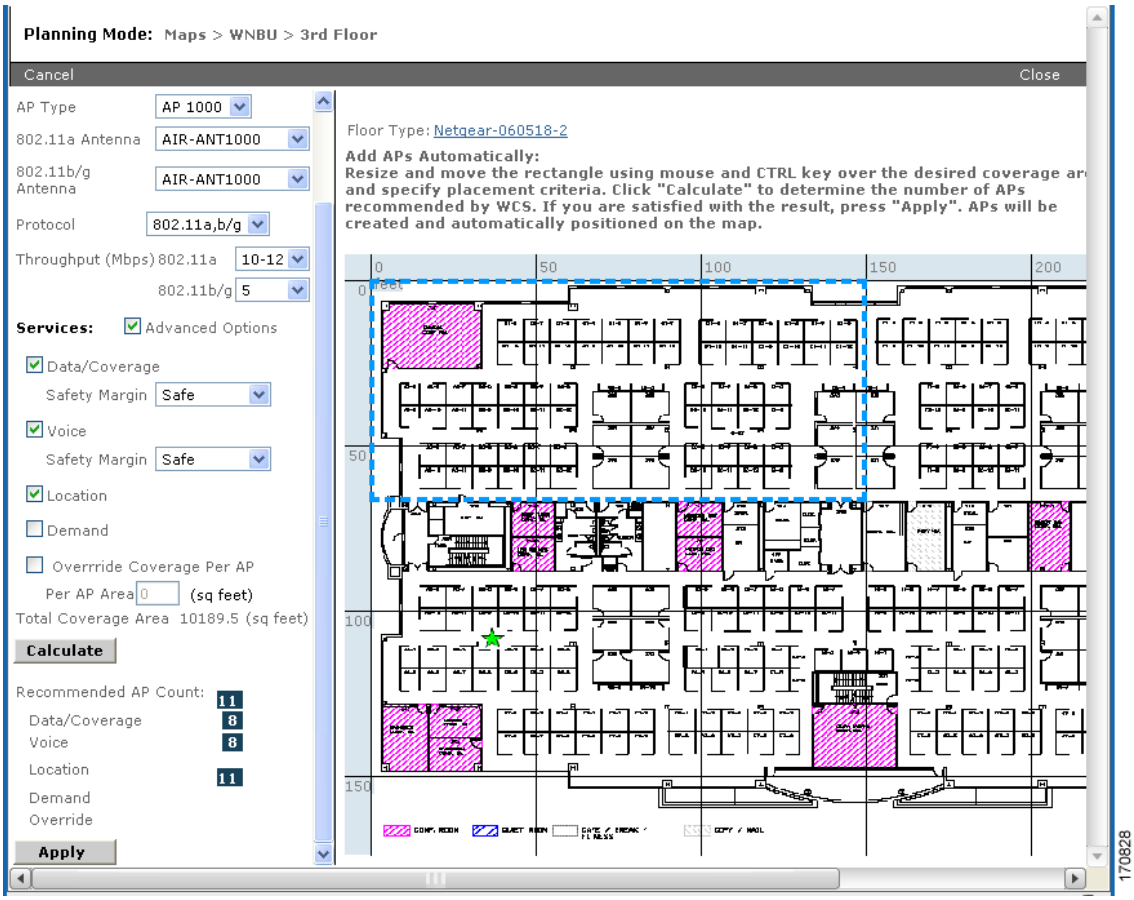
Advanced Options	Description
Demand	Select if you want to use the total number of users or user ratio per access point as a basis for the access point calculation.

Advanced 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 5-8).

Figure 5-8 Recommended Number of Access Points Given Selected Services and Parameters

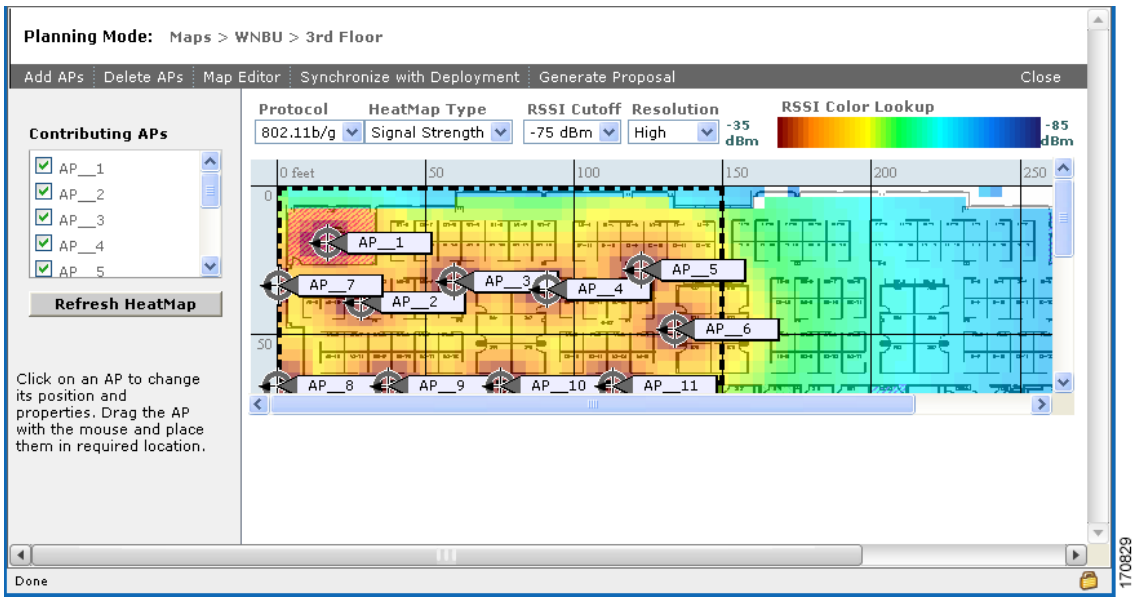


Note Recommended calculations assume the need for consistently strong signals unless adjusted downward by the **safety margin** advanced option. In some cases, the recommended number of access points is higher than what is required.

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.

Figure 5-9 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.

Inspect VoWLAN Location Readiness

The Inspect Location Readiness feature is a distance-based predictive tool that can point out problem areas with access point placement.

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 menu, click **Inspect Location Readiness**.

Inspect VoWLAN Readiness

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.

To access the VoWLAN Readiness Tool (VRT), 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 menu, click **Inspect VoWLAN Readiness**.

Step 4 Choose the applicable **Band**, **AP Transmit Power**, and **Client** parameters from the drop-down menus.

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 Click the desired floor plan or outdoor area map in the Coverage Areas component of the General tab. WCS displays the associated coverage area map.

Step 2 From the Select a command drop-down menu, choose **Add Access Points** and click **GO**.

Step 3 On the Add Access Points page, choose the access points to add to the map.

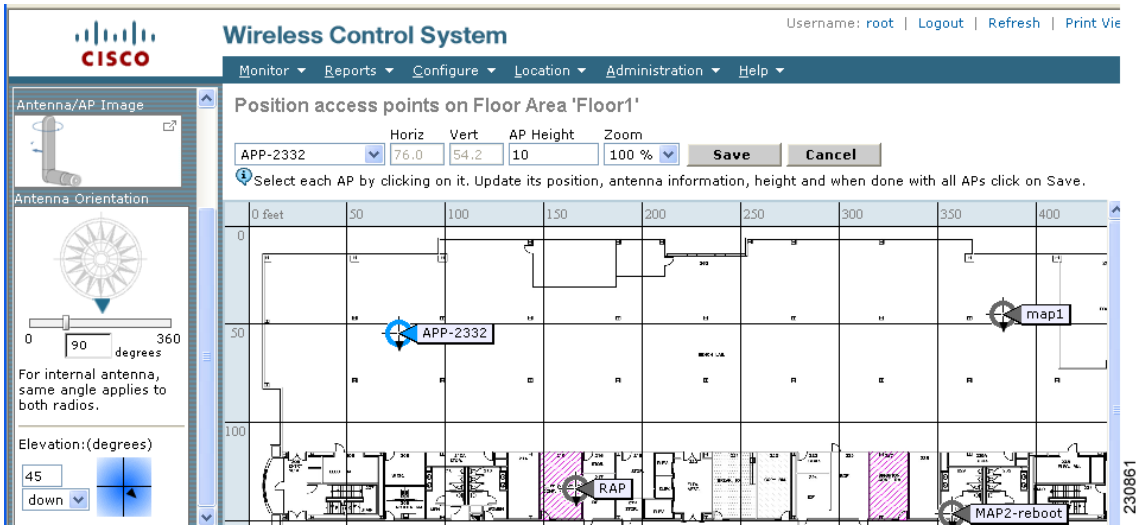
Step 4 Click **OK** to add the access points to the map and display the Position Access Points map.

Note The access point icons appear in the upper left area of the map.

Step 5 Click and drag the icons to indicate their physical locations.

Step 6 Click each icon and choose the antenna orientation in the sidebar (see Figure 5-10).

Figure 5-10 Antenna Sidebar



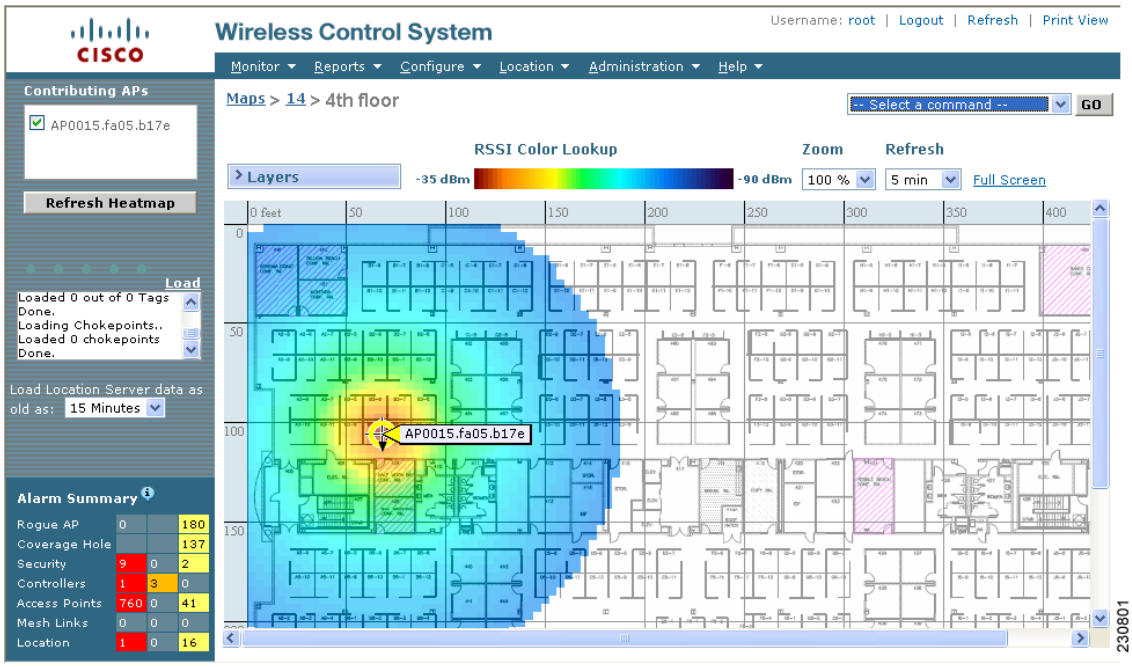
Note

- 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.
- 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.
- Refer to http://www.cisco.com/en/US/products/hw/wireless/ps469/tsd_products_support_series_home.html for further information about antenna elevation and azimuth patterns.

Step 7 Click **Save** to store the access point locations and orientations. 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 5-11 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 5-11 RF Prediction Heat Map



Placing Access Points

To determine the optimum 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.

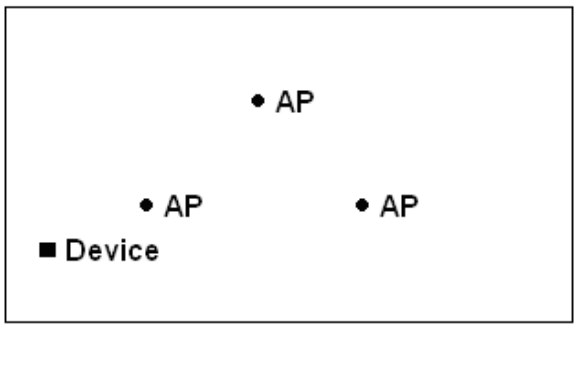
Note Devices must be detected at signals greater than –75 dBm for the controllers to forward information to the location appliance. No fewer than three access points should be able to detect any device at signals below –75 dBm.

Guidelines for Placing Access Points

Follow these rules for placing access points accurately:

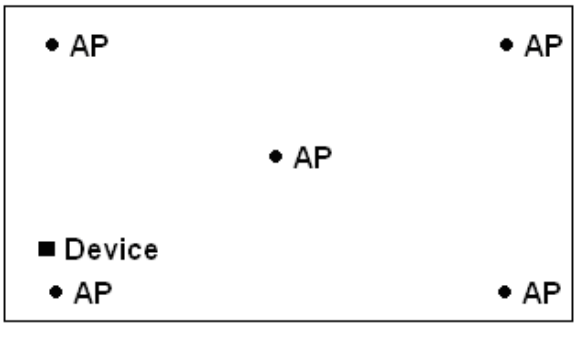
1. Place access points along the periphery of coverage areas in order to keep devices close to the exterior of rooms and buildings (see Figure 5-12). Access points placed in the center of these coverage areas provide good data on devices that would otherwise appear equidistant from all other access points.

Figure 5-12 Access Points Clustered Together



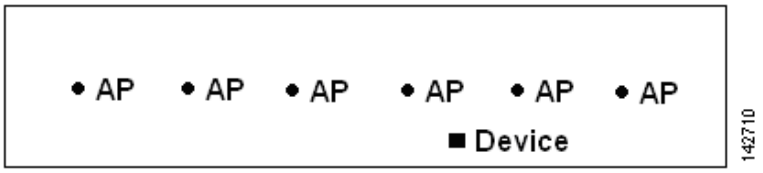
2. By increasing overall access point density and moving access points towards the perimeter of the coverage area, location accuracy is greatly improved (see Figure 5-13).

Figure 5-13 Improved Location Accuracy by Increasing Density



3. In long and narrow coverage areas, avoid placing access points in a straight line (see Figure 5-14). Stagger them so that each access point is more likely to provide a unique snapshot of a device's location.

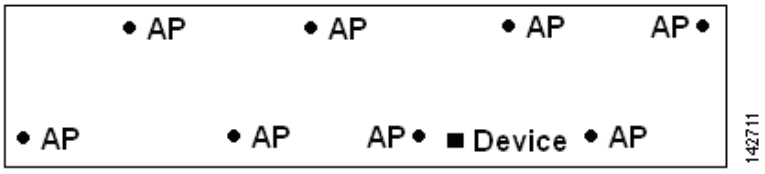
Figure 5-14 Refrain From Straight Line Placement



Although the design in Figure 5-14 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.

4. 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 5-15).

Figure 5-15 Improved Location Accuracy by Staggering Around Perimeter

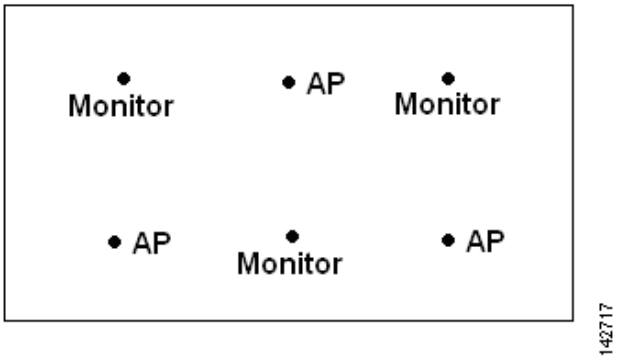


5. Designing a location-aware wireless LAN, while planning for voice as well, is better done with a few things in mind. Most current wireless handsets support only 802.11b/n, which offers only three non-overlapping channels. Therefore, wireless LANs designed for telephony tend to be less dense than those 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 5-16).

Figure 5-16 Less Dense Wireless LAN Installations



6. 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%).

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 location appliance are explained in the "Importing the Location Appliance into WCS" section on page 12-7.

Designing a Network

Follow these steps to design a network.

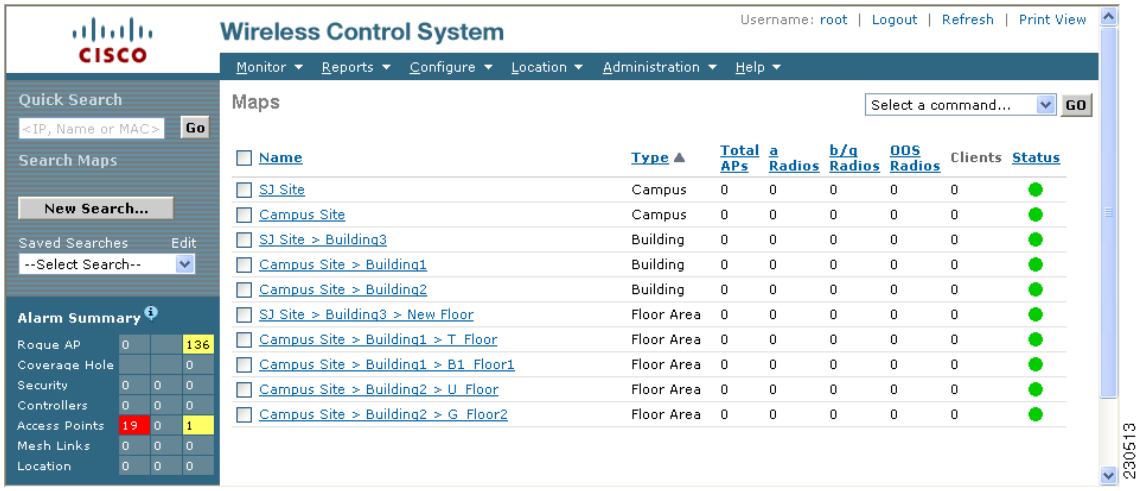
Step 1 Open the WCS web interface and log in.

Note To create or edit a network design, you must log into WCS and have SuperUser, Admin, or ConfigManager access privileges.

Step 2 Click the **Monitor** tab and choose the **Maps** subtab (see Figure 5-17).

Step 3 From the drop-down menu 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 13.

Figure 5-17 Creating a New Network Design



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.

Step 6 Check 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.

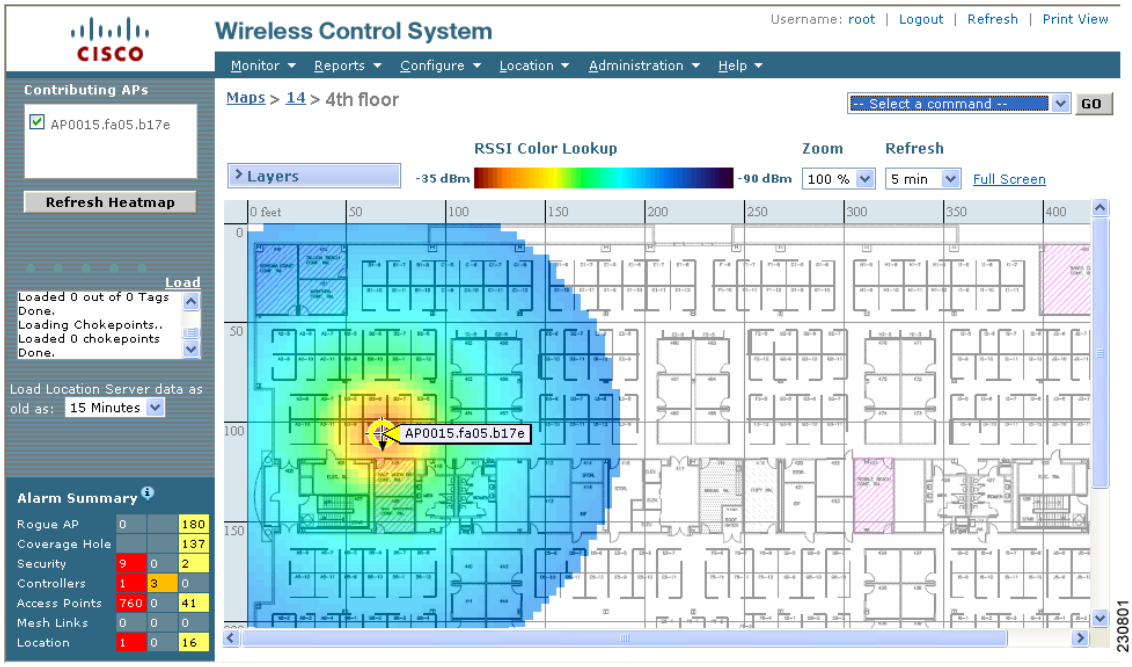
You should uncheck the Maintain Aspect Ratio check box if you want to override this automatic adjustment. You could then adjust both span values to match the real world campus dimensions.

Step 7 Click **OK**.

Step 8 On the Monitor > Maps subtab, click the hyperlink associated with the above-made campus map. A window showing the new campus image is displayed.

Step 9 From the drop-down menu on the upper right of the window, select **New Building** and click **GO** (see Figure 5-18).

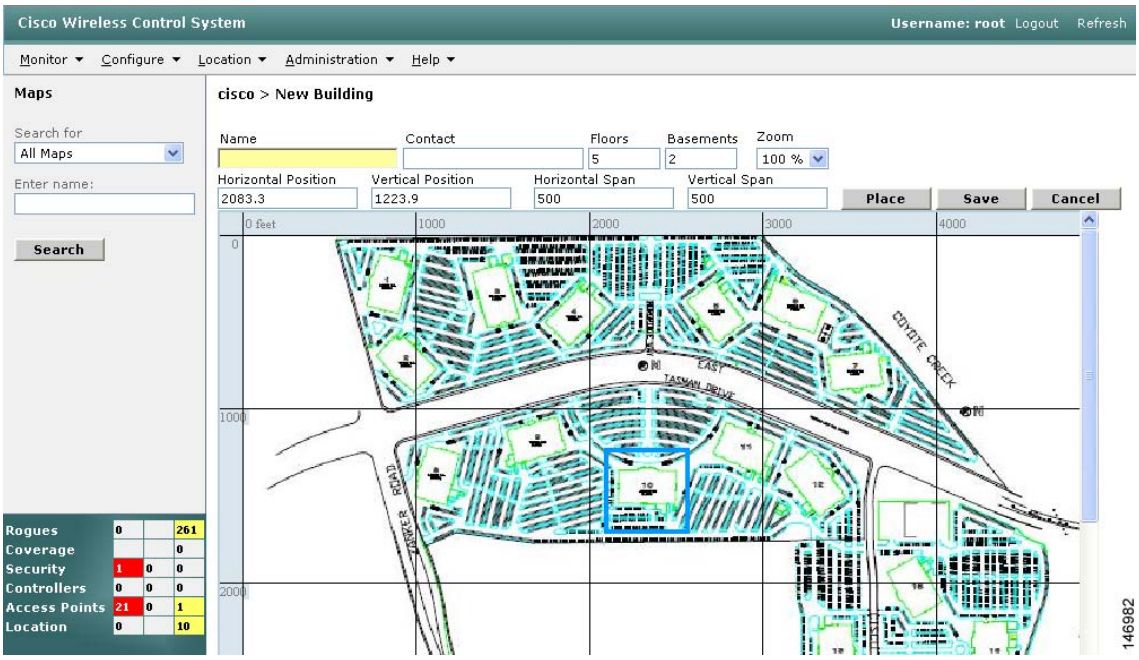
Figure 5-18 New Building



Step 10 Enter the name of the building, the contact person, and the number of floors and basements in the building.

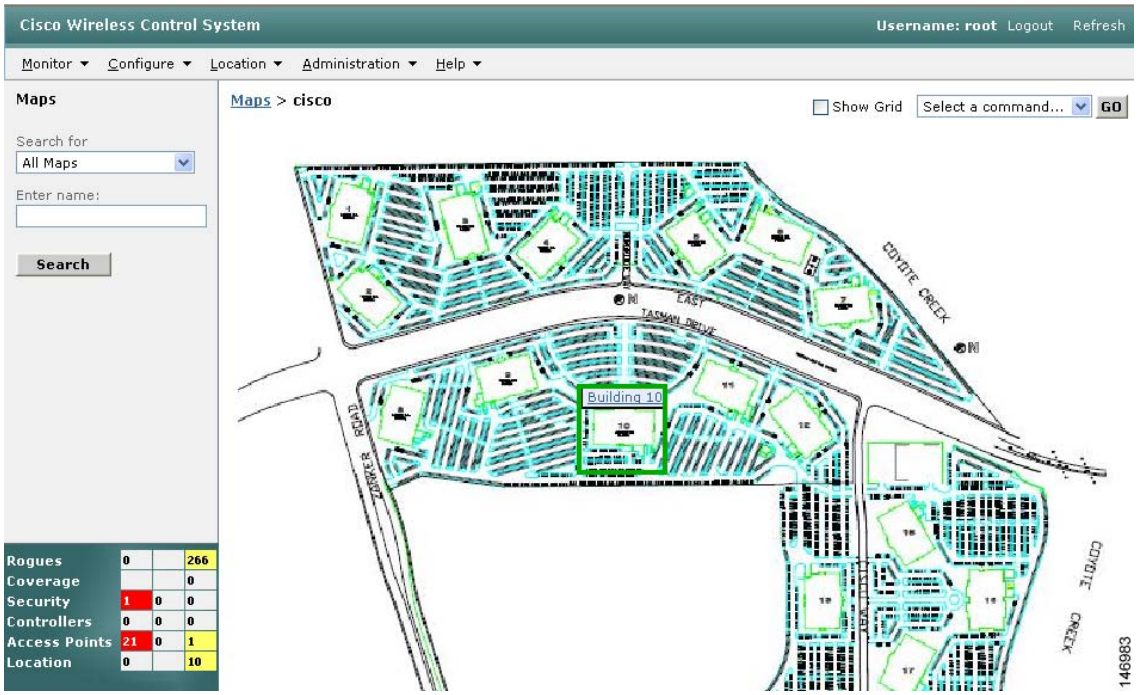
Step 11 Indicate which building on the campus map is the correct building by clicking the blue box in the upper left of the campus image and dragging it to the intended location (see Figure 5-19). To resize the blue box, hold down the **Ctrl** key and click and drag to adjust its horizontal size. You 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 5-19 Repositioning Building Highlighted in Blue



Step 12 WCS is then returned to the campus image with the newly created building highlighted in a green box. Click the **green box** (see Figure 5-20).

Figure 5-20 Newly Created Building Highlighted in Green



Step 13 To create a building without a campus, choose **New Building** and click **GO**.

Step 14 Enter the building's name, contact information, number of floors and basements, and dimension information. Click **Save**. WCS is returned to the Monitor > Maps window.

Step 15 Click the hyperlink associated with the newly created building.

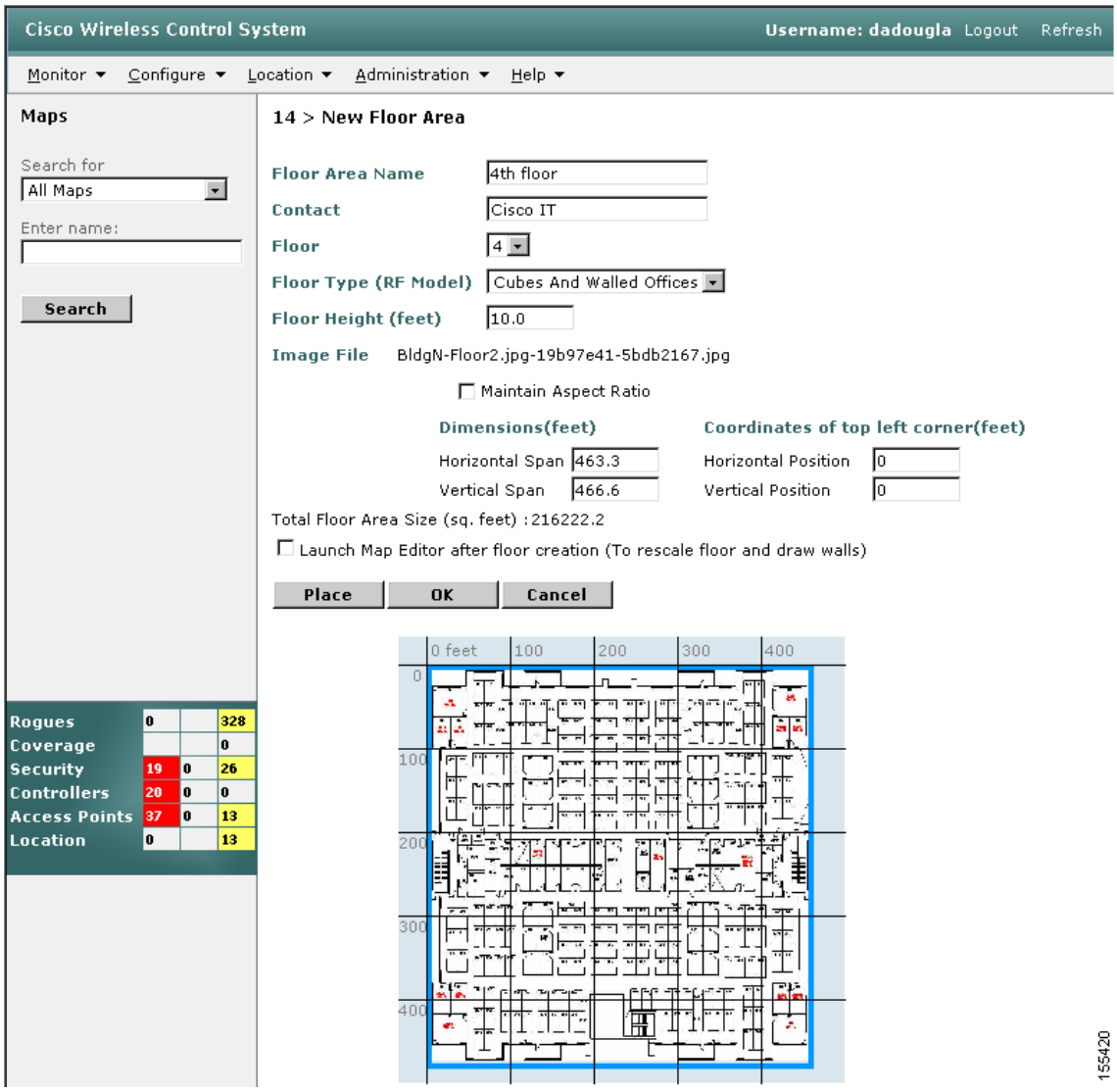
Step 16 On the Monitor > Maps > [Campus Name] > [Building Name] window, go to the drop-down menu and choose **New Floor Area**. Click **GO**.

Step 17 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 "Creating and Applying Calibration Models" section on page 5-57.

Step 18 If the floor area is a different dimension than the building, adjust floor dimensions by either making numerical changes to the text fields under the Dimensions heading or by holding the **Ctrl** key and clicking and dragging the blue box around the floor image. If the floor's location is offset from the upper left corner of the building, change the placement of the floor within the building by either clicking and dragging the blue box to the desired location or by altering the numerical values under the **Coordinates of top left corner** heading (see Figure 5-21). After making changes to any numerical values, click **Place**.

Figure 5-21 Repositioning Using Numerical Value Fields



Step 19 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 to Enhance Floor Plans" section on page 5-12.

Step 20 At the new floor's image window (Monitor > Maps > [CampusName] > [BuildingName] > [FloorName]), go to the drop-down menu on the upper right and choose **Add Access Points**. Click **GO**.

Step 21 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. Check the box to the left of the Name column to select all access points. Click **OK**.

Step 22 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 on 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 23 To adjust the directional arrow, choose the appropriate orientation in the Antenna Angle drop-down menu. 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 24 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 menu, choose **Properties**.

Step 3 At the Unit of Dimension drop-down menu, choose feet or meters.

Step 4 The **Advanced Debug** option must be enabled on both the location appliance and WCS so the location accuracy testpoint is correct.

Step 5 In the Import/Export AP Placement portion of the window, 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. (Refer to the "Inspect VoWLAN Readiness" section on page 5-22.)

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 6 Click **Import**. The RF calculation takes approximately two seconds per access point.

Using Chokepoints to Enhance Tag Location Reporting

Installation of chokepoints provides enhanced location information for RFID tags. When an active Cisco Compatible Extensions version 1 compliant RFID tag enters the range of a chokepoint, it is stimulated by the chokepoint. The MAC address of this chokepoint is then included in the next beacon sent by the stimulated tag. All access points that detect this tag beacon then forward the information to the controller and location appliance.

Using chokepoints in conjunction with active compatible extensions compliant tags provides immediate location information on a tag and its asset. When a Cisco Compatible Extension's tag moves out of the range of a chokepoint, its subsequent beacon frames do not contain any identifying chokepoint information. Location determination of the tag defaults to the standard calculation methods based on RSSIs reported by the access point associated with the tag.

Adding Chokepoints to the WCS Database and Map

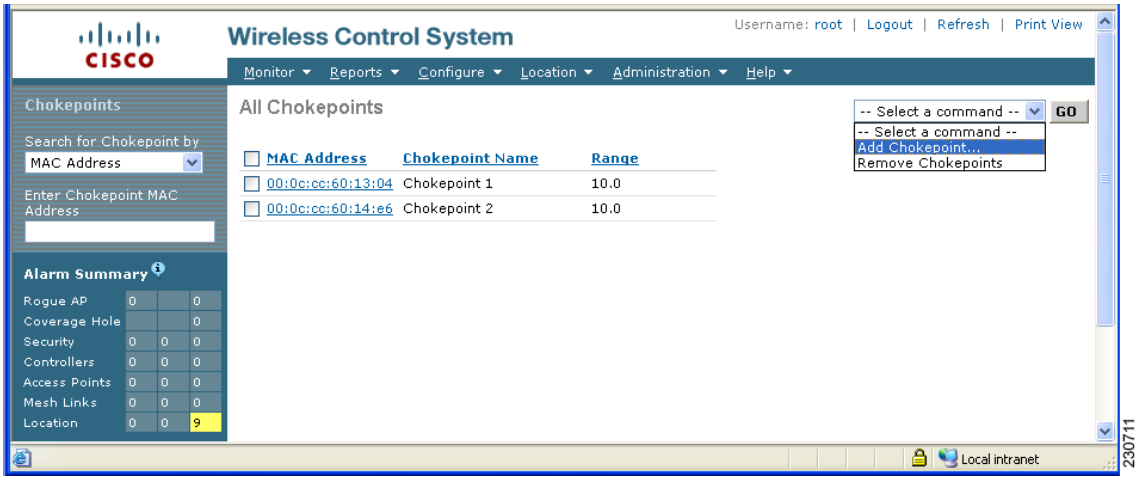
Chokepoints are installed and configured as recommended by the Chokepoint vendor. After the chokepoint installation is complete and operational, the chokepoint is added to WCS and placed on floor maps. They are forwarded to the location server during synchronization.

Follow these steps to add a chokepoint to the WCS database and appropriate map:

Step 1 Choose **Configure > Chokepoints** from the main menu.

The All Chokepoints summary window appears (see Figure 5-22).

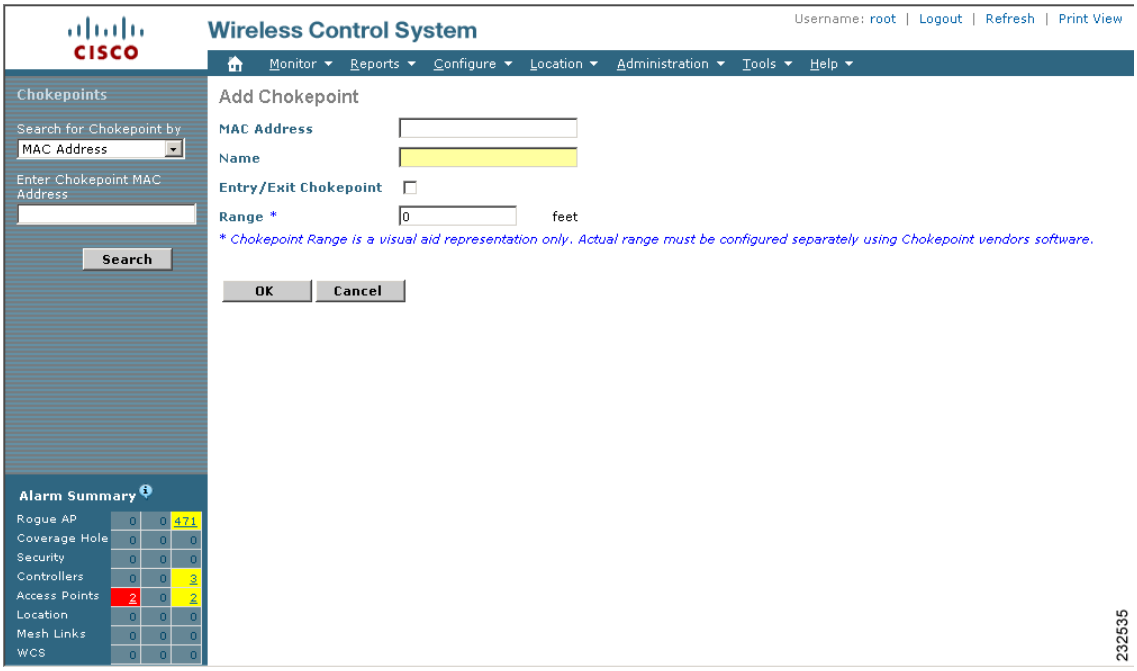
Figure 5-22 Configure > Chokepoints



Step 2 Select **Add Chokepoints** from the Select a command menu (Figure 5-22). Click **GO.**

The Add Chokepoint entry window appears (see Figure 5-23).

Figure 5-23 Add Chokepoint Configuration Page



Step 3 Enter the MAC address, name, and coverage range for the chokepoint.

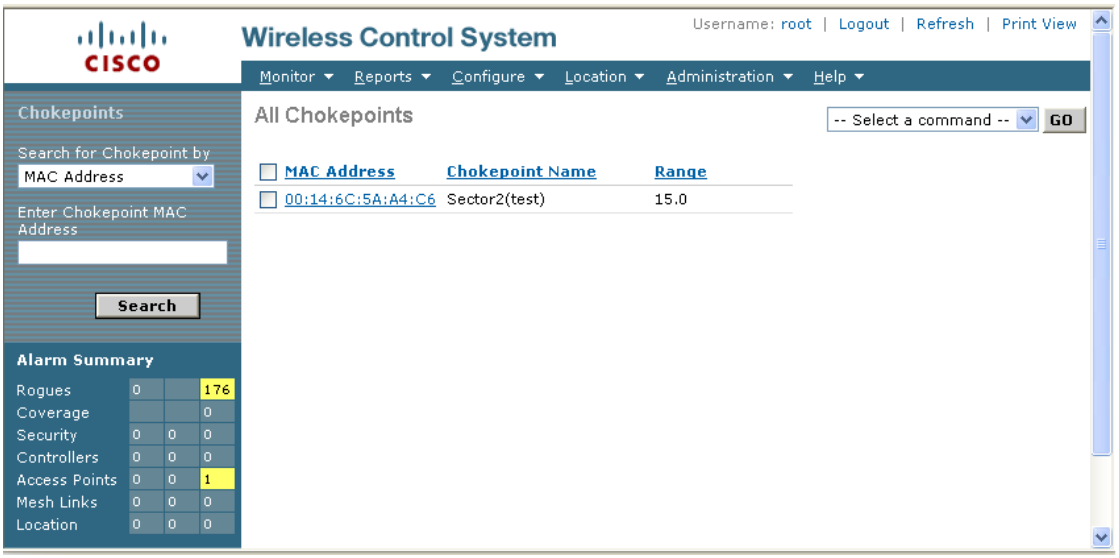
Note The chokepoint range is product-specific and is supplied by the chokepoint vendor.

Step 4 Specify whether the chokepoint is an entry or exit chokepoint.

Step 5 Click **OK** to save the chokepoint entry to the database.

The All Chokepoints summary page appears with the new chokepoint entry listed (Figure 5-24).

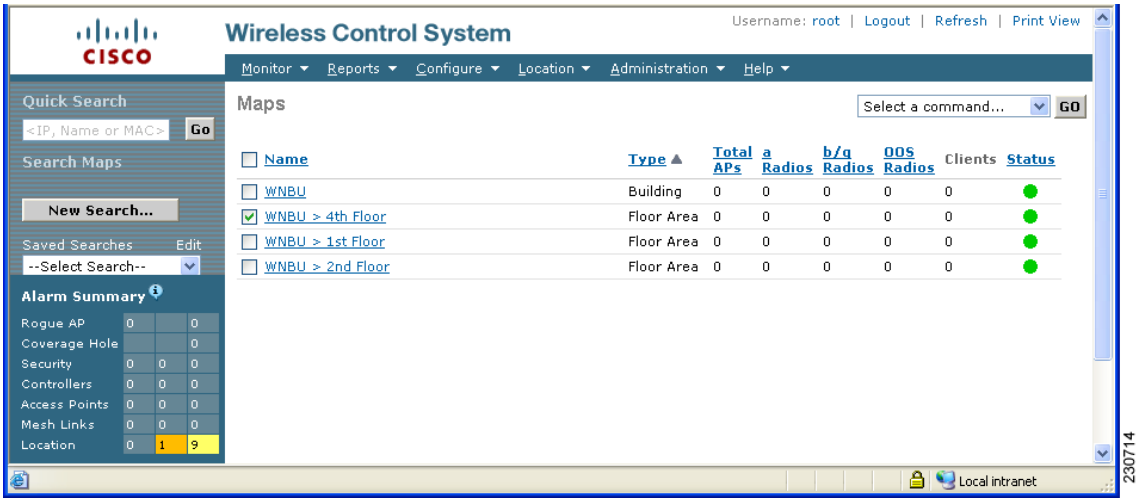
Figure 5-24 All Chokepoints Summary Page



Note After the chokepoint is added to the database, place it on the appropriate WCS floor map.

Step 6 To add the chokepoint to a map, choose **Monitor > Maps** (Figure 5-25).

Figure 5-25 Monitor > Maps



Step 7 On the Maps page, choose the link that corresponds to the floor location of the chokepoint. The floor map appears (Figure 5-26).

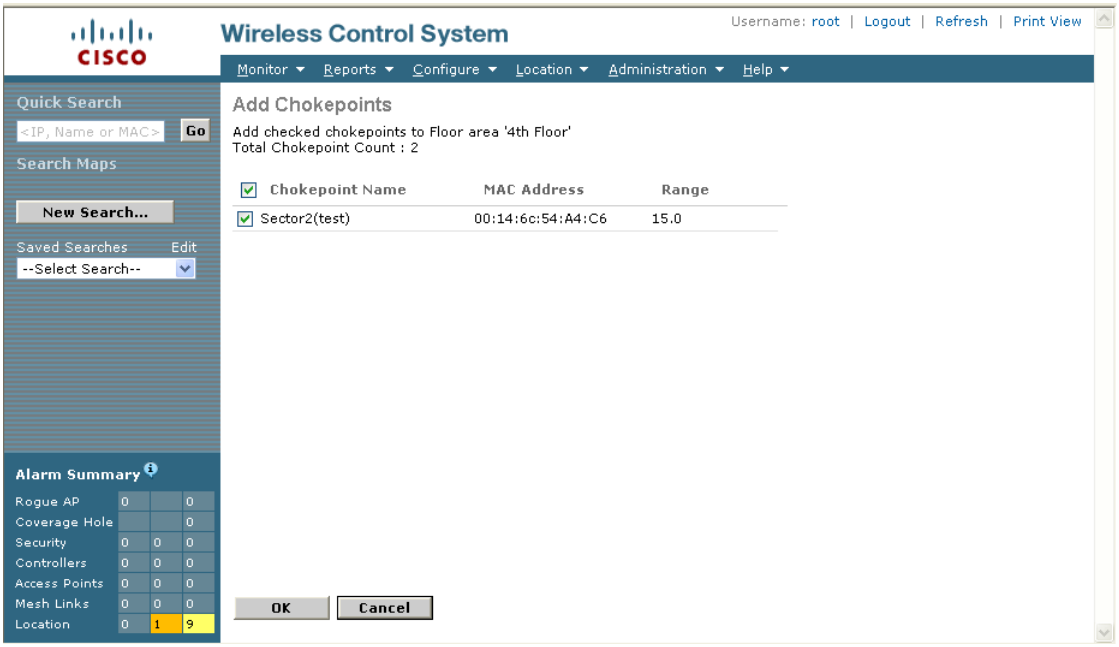
Figure 5-26 Selected Floor Map

Step 8 Select **Add Chokepoints** from the Select a command menu. Click **GO**.

The Add Chokepoints summary page appears (see Figure 5-27).

Note The Add Chokepoints summary page lists all recently added chokepoints that are in the database but not yet mapped.

Figure 5-27 Add Chokepoints Summary Page



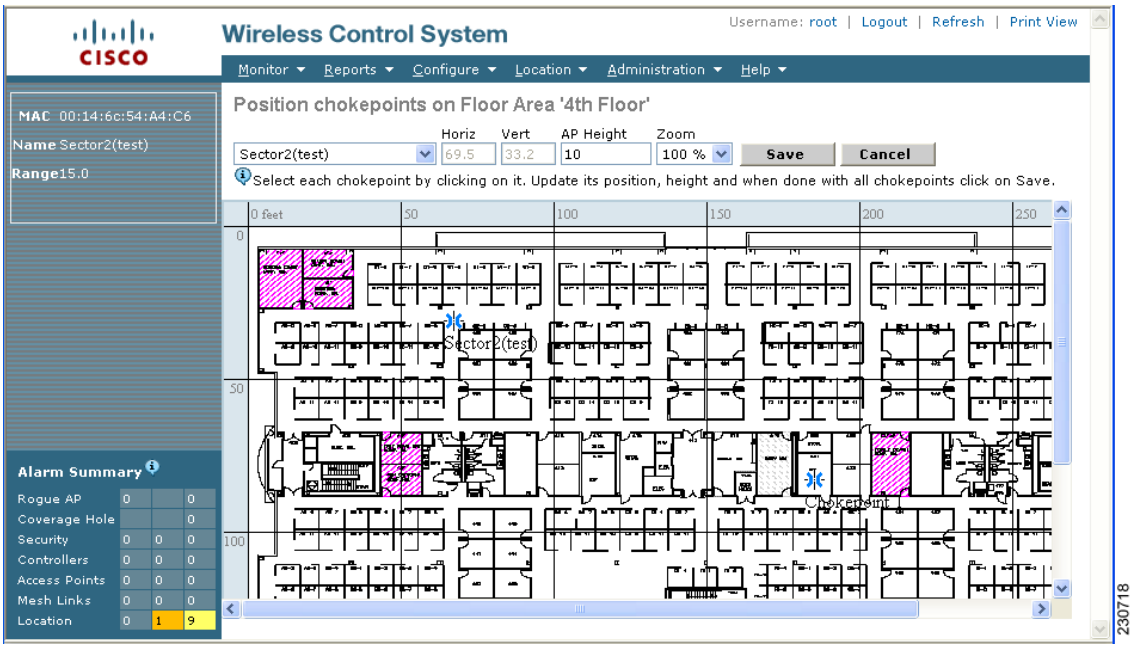
Step 9 Check the box next to the chokepoint to be added to the map. Click **OK**.

A map appears with a chokepoint icon located in the top-left hand corner (Figure 5-28). You are now ready to place the chokepoint on the map.

Figure 5-28 Map for Positioning Chokepoint

Step 10 Left click on the chokepoint icon and drag and place it in the proper location (see Figure 5-29).

Figure 5-29 Chokepoint Icon Positioned on the Floor Map



Note The MAC address, name, and coverage range of the chokepoint appear in the left panel when you click on the chokepoint icon for placement.

Step 11 Click **Save** when the icon is correctly placed on the map.

You are returned to the floor map and the added chokepoint appears on the map.

Note The newly created chokepoint icon may or may not appear on the map depending on the display settings for that floor. If the icon did not appear, proceed with Step 12.

Figure 5-30 New Chokepoint Appears on Floor Map

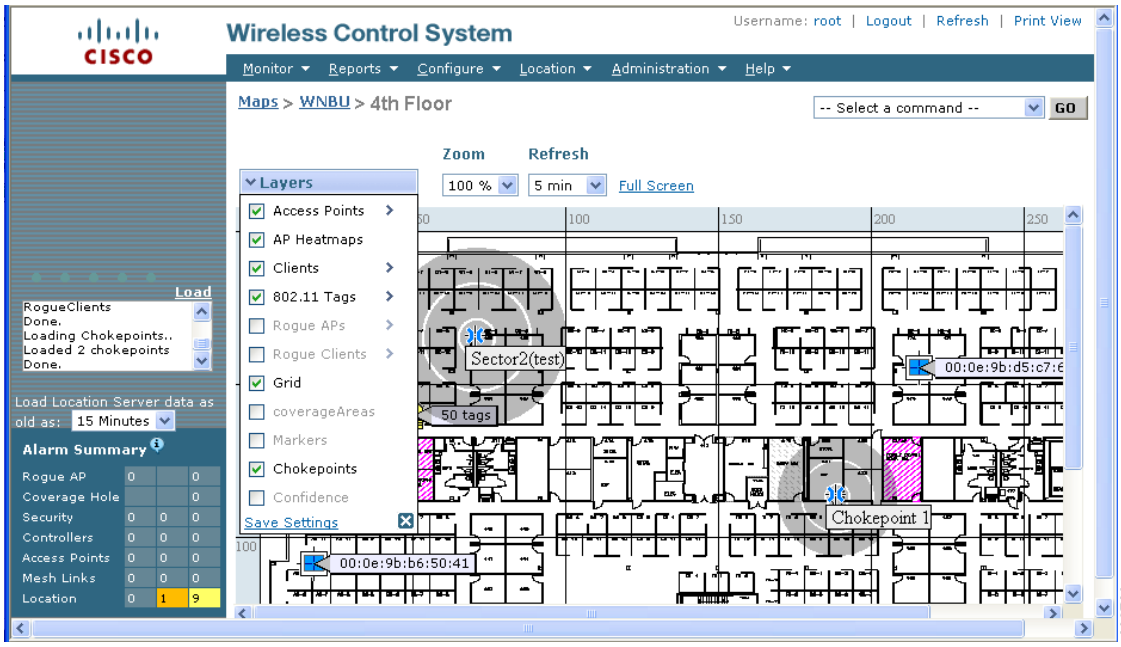
Note The rings around the chokepoint icon indicate the coverage area. When a Cisco Compatible Extensions tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. The chokepoint range is given as a visual only, but chokepoint vendor software is required to actually configure the range. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings. In Figure 5-30, the tag is currently out of range of the chokepoint.

Note MAC address, name, and range of a chokepoint display when you pass a mouse over its map icon.

Step 12 If the chokepoint does not appear on the map, click **Layers** to collapse a selection menu of possible elements to display on the map. Click the **Chokepoints** box.

The chokepoint appears on the map (Figure 5-31).

Figure 5-31 Display Chokepoints on Map



Step 13 Click **X** to close the Layers window.

Note Do not select **Save Settings** unless you want to save this display criteria for all maps.

Removing Chokepoints from the WCS Database and Map

You can remove one or multiple chokepoints at a time.

Follow these steps to delete a chokepoint.

Step 1 Choose **Configure > Chokepoints**. The All Chokepoints page appears.

Step 2 Check the box(es) next to the chokepoint(s) to be deleted.

Step 3 Choose **Remove Chokepoints** from the Select a command drop-down menu. Click **GO**.

Step 4 To confirm chokepoint deletion, click **OK** in the pop-up window that appears.

You are returned to the All Chokepoints page. A message confirming deletion of the chokepoint appears. The deleted chokepoint(s) is no longer listed on the page.

Monitoring Chokepoints

Chokepoints are installed and configured as recommended by the chokepoint vendor. Chokepoints are added to WCS and placed on floor maps, and then they are pushed to the location server during synchronization. Choose **Monitor > Chokepoints** to display a list of found chokepoints. Clicking the link under Map Location for a particular chokepoint displays a map that shows the location of the chokepoint. The following parameters are displayed:

- MAC Address—The MAC address of the chokepoint.
- Chokepoint Name—The user-defined name of the chokepoint.
- Entry/Exit Chokepoint—Specifies whether the chokepoint is an entry or exit chokepoint.
- Range—The range of the chokepoint in feet.
- Map Location—A link to a map showing the location of the chokepoint.

Monitoring Maps

This section describes how to use maps to monitor your wireless LANs and predict coverage. You can use maps to do the following:

- Monitoring Predicted Coverage, page 5-43
- Monitoring Transmit Power Levels on a Floor Map, page 5-50
- Monitoring Coverage Holes on a Floor Map, page 5-51
- Monitoring Clients on a Floor Map, page 5-52
- Monitoring Outdoor Areas, page 5-53

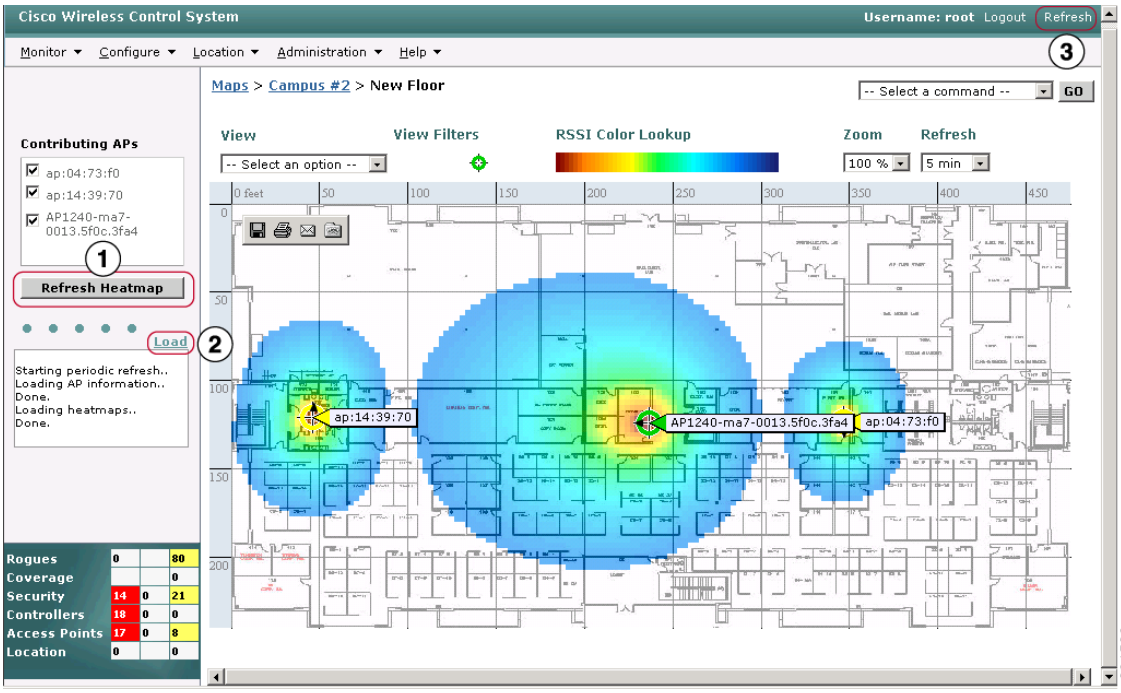
In preparation for monitoring your wireless LANs, familiar yourself with the various refresh options for a map.

- Refresh from network—By clicking **Refresh Heatmap** in the left sidebar menu (see callout 1 in Figure 5-32), 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 5-32). Clicking this refreshes the complete page, or the map and its status and statistics if you are on a map page.
- Load—The Load option in the left sidebar menu refreshes map data from the WCS database on demand (see callout 2 in Figure 5-32). Otherwise, the Refresh option (by the Zoom option on the upper right of the map) provides an interval drop-down menu to set how often to refresh the map data from the database.

Figure 5-32 Monitoring Maps



Note All three options refresh the data based on the layer selection.

Monitoring Predicted Coverage

Follow these steps to monitor the predicted wireless LAN coverage on a map.

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

Step 2 Click an item in the Name column.

Step 3 Click **Layers** to see a check list of the available layers to view. Choosing some layers results in a popup window to further choose what content gets shown in the map. Those layers with popups are described in the next sections. The layer options are as follows:

- Access Points
- AP Heatmaps
- AP Mesh Info —Displays only if mesh access points are present in outdoor areas.
- Clients —Displays data only if a location server was added in WCS.
- 802.11 Tags
- Rogue APs —Displays data only if a location server was added in WCS.
- Rogue Adhocs —Displays data only if a location server was added in WCS.
- Rogue Clients —Displays only if a location server was added in WCS.
- Grid

- Coverage Areas
- Markers
- Chokepoints — Displays only if chokepoints are added in WCS.

Note If you click the arrow to the right of these layers, more filter options are provided.

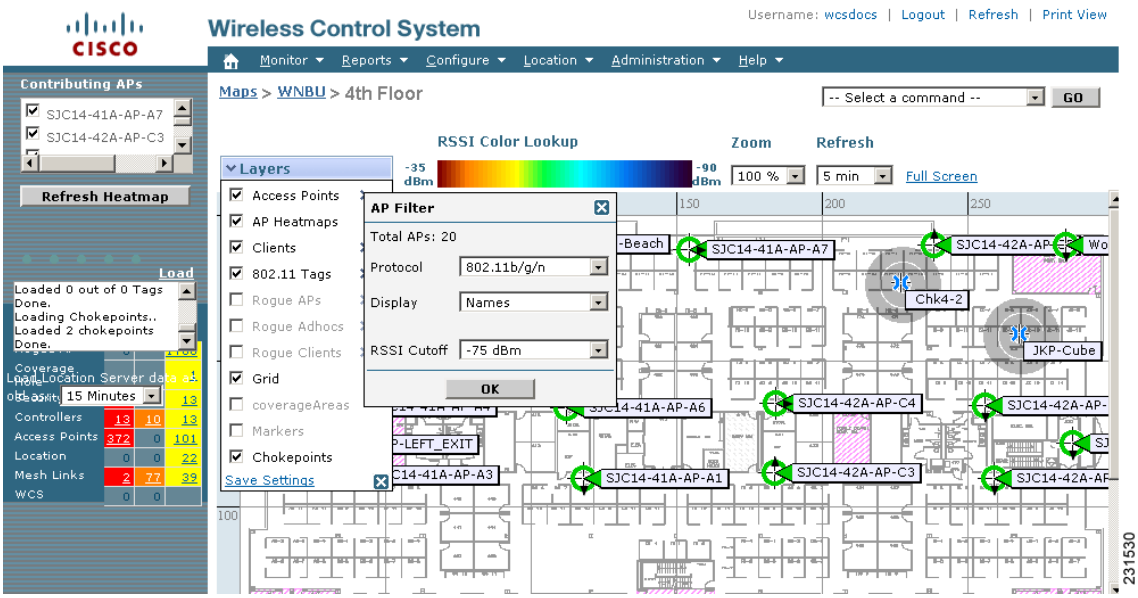
The enabled layers are checked, and the disabled ones are unavailable.

Note When you mouse over the various locations, a popup with general, 802.11a/n, and 802.11b/g/n data appears. It provides the channel, transmit power level, user count, utilization count, antenna name, antenna angle, and elevation angle (for the 802.11a/n and 802.11b/g/n windows), and access point MAC address, model, controller IP address, location, and height in the General tab.

Access Point Layer

If you enable the Access Point layer and then click on the arrow to the right of these layers, an access point filter window appears with further menu options (see Figure 5-33).

Figure 5-33 AP Filter Window



Step 1 From the Protocol drop-down menu, choose one of the following 802.11 protocols to display on the coverage map:

- **802.11a/n & b/g/n**—Displays all the access points in the area.
- **802.11a/n**—Displays a colored overlay depicting the coverage patterns for the 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 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.

Step 2 From the Display drop-down menu, choose one of the following options to specify the information that appears in the flag next to each access point on the map:

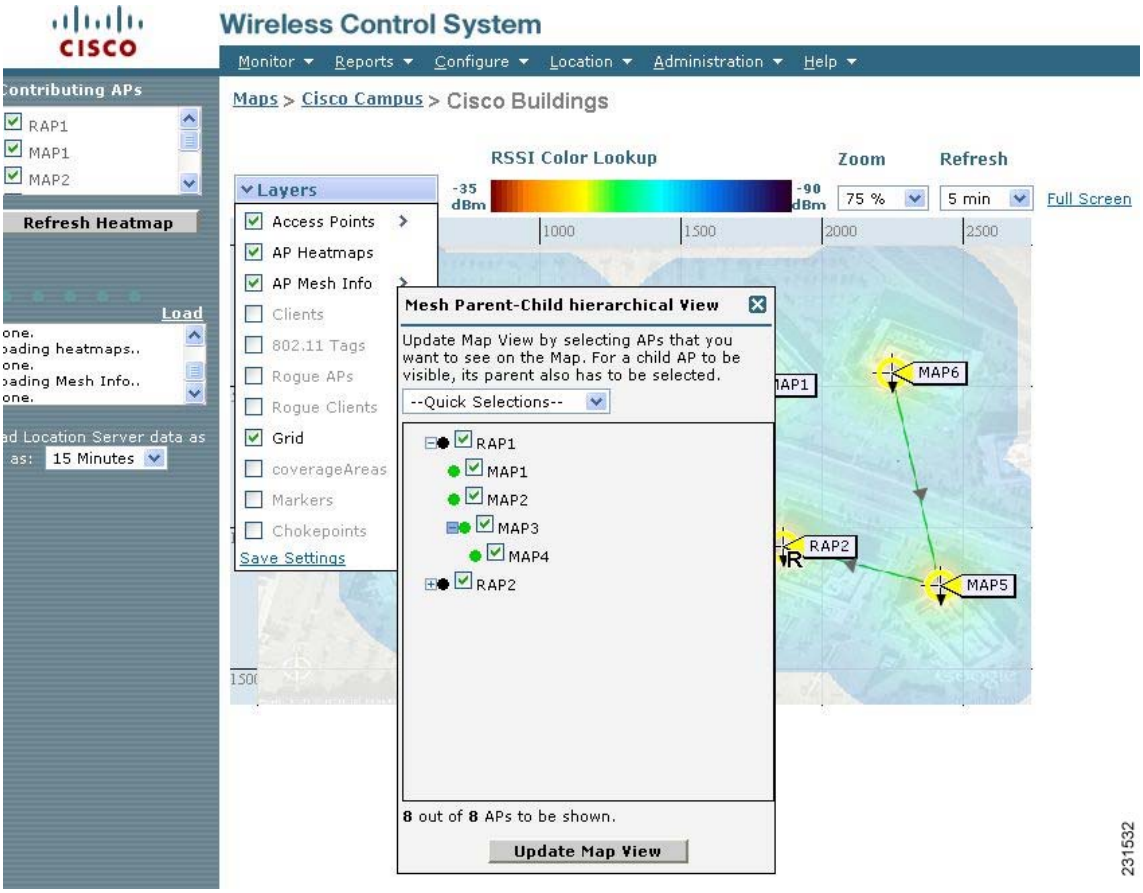
- **Channels**—Shows the Cisco Radio channel number as `Ch#nn`, where *nn* is the channel number, or shows *Unavailable* for unconnected access points.
- **TX Power Level**—Shows the current Cisco Radio transmit power level as Tx Power n, where *n* is power level 1 (high) through 5 (low) or shows *Unavailable* for unconnected access points.
- **Coverage Holes**—Shows the percentage of clients whose signal has become weaker until the client lost its connection, shows *Unavailable* for unconnected access points, or shows *MonitorOnly* for access points in Monitor-Only mode.
- **MAC Addresses**—Displays the MAC address of the access point, regardless of whether 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, "Unavailable" for disassociated access points, or "MonitorOnly" for access points in monitor-only mode.
- **Profiles**—Shows the Load, Noise, Interference and Coverage components of the corresponding operator-defined thresholds: *Okay* for thresholds not exceeded, *Issue* for exceeded thresholds, or *Unavailable* for unconnected access points. You must also then specify the profile type as load, noise, interference, or coverage.
- **Users**—Shows the number of Cisco WLAN Solution clients, shows *Unavailable* for unconnected access points, or shows *MonitorOnly* for access points in Monitor-Only mode.
- Bridge Group Names

Step 3 Click **OK**.

AP Mesh Info Layer

If you enable the AP Mesh Info layer and then click on the arrow to the right of these layers, a Mesh Parent-Child Hierarchical View window appears with further menu options (see Figure 5-34).

Figure 5-34 Mesh Parent-Child Hierarchical View Window



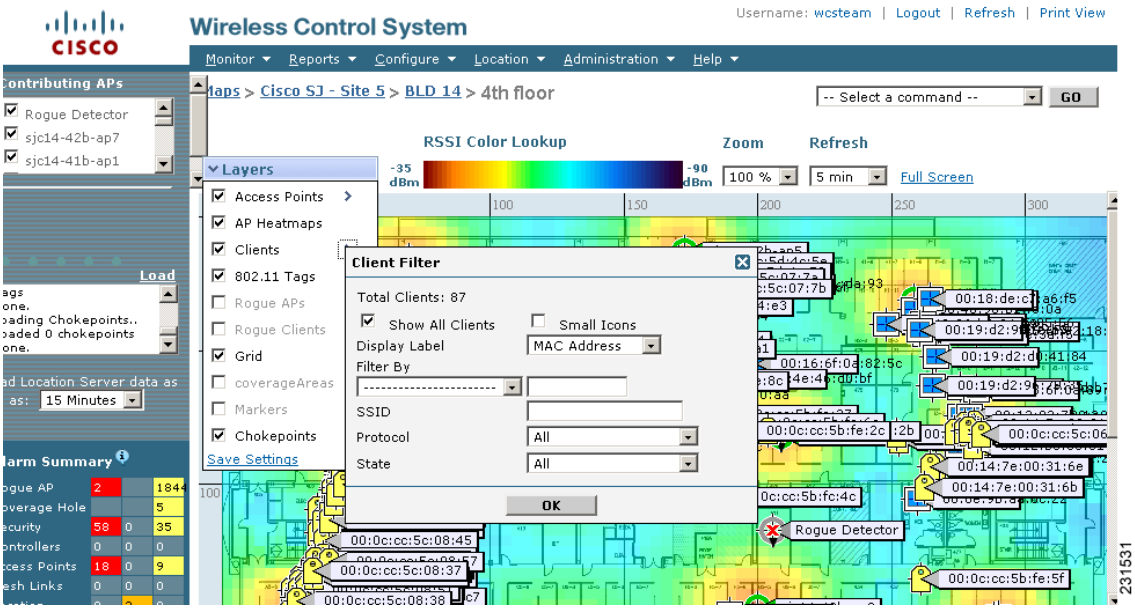
You can update the map view by choosing the access points you want to see on the map. From the Quick Selections drop-down menu, choose to select only root access point, various hops between the first and the fourth, or select all access points.

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

Clients Layer

If you enable the Clients layer and then click on the arrow to the right of these layers, a Client Filter window appears with further menu options (see Figure 5-35).

Figure 5-35 Client Filter Window



If you click the **Show All Clients** check box and **Small Icons** check box, all other drop-down menu options are grayed out.

If you uncheck 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 uncheck the **Show All Clients** check box, you can specify how you want the clients filtered and enter a particular SSID.

The Protocol drop-down menu options are as follows:

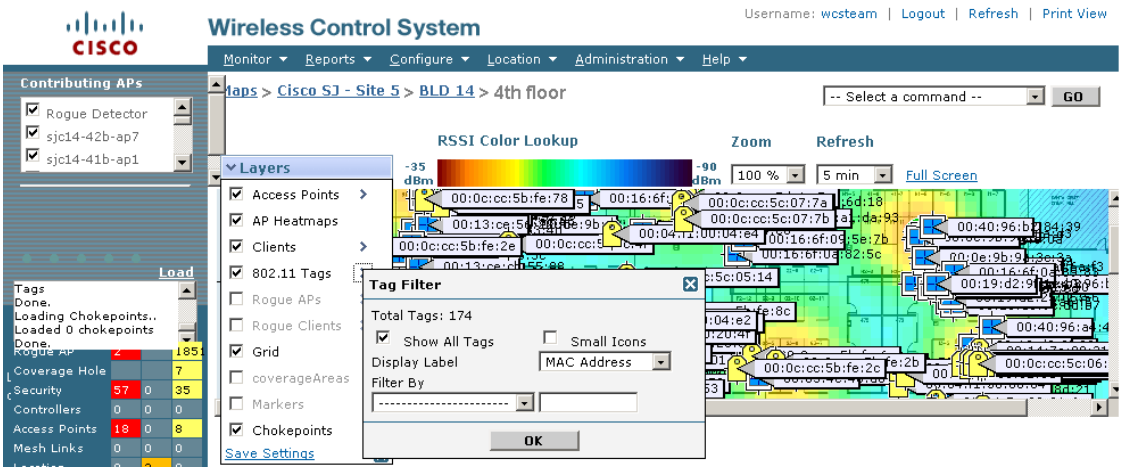
- **All**—Displays all the access points in the area.
- **802.11a/n**—Displays a colored overlay depicting the coverage patterns for the clients with 802.11a/n radios. The colors show the received signal strength from red (–35 dBm) through dark blue (–85 dBm).
- **802.11b/g/n**—Displays a colored overlay 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.

You can further choose to show clients in all states or specifically idle, authenticated, probing, or associated clients.

802.11 Tags Layer

If you enable the 802.11 Tags layer and then click on the arrow to the right of these layers, a Tag Filter window appears with further menu options (see Figure 5-36).

Figure 5-36 Tag Filter Window



If you click the **Show All Tags** check box and **Small Icons** check box, all other drop-down menu options are grayed out.

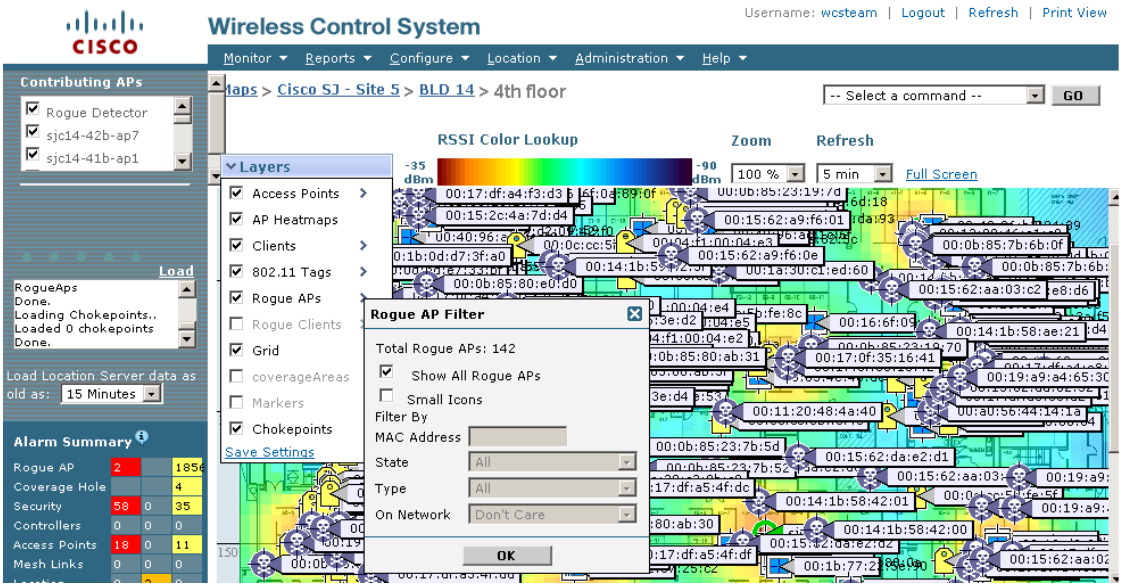
If you uncheck the **Small Icons** check box, you can choose if the want the label to display MAC address, asset name, asset group, or asset category.

If you uncheck the **Show All Clients** check box, you can specify how you want the clients filtered.

Rogue APs Layer

If you enable the Rogue APs layer and then click on the arrow to the right of these layers, a Rogue AP Filter window appears with further menu options (see Figure 5-37).

Figure 5-37 Rogue AP Filter Window



If you click the **Show All Rogue APs** check box and **Small Icons** check box, all other drop-down menu options are grayed out.

If you uncheck the **Show All Rogue APs** check box, you can specify how you want the rogue access points filtered. Follow these steps to define the filter.

Step 1 If you want to view a particular MAC address, enter it in the MAC Address field.

Step 2 From the State drop-down menu, choose if you want to display rogues in the alert, known, acknowledged, contained, threat, or unknown contained state.

Step 3 Specify if you want to display all rogues, access point rogues, or ad hoc rogues.

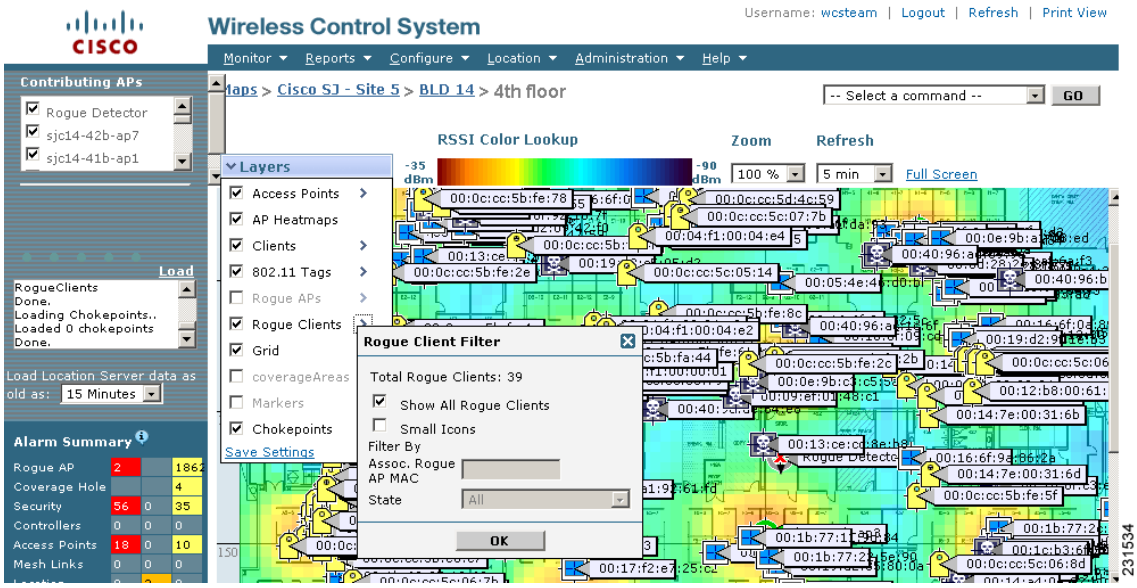
Step 4 Specify whether or not you want to display rogue access points on the network.

Step 5 Click **OK**.

Rogue Clients Layer

If you enable the Rogue Clients layer and then click on the arrow to the right of these layers, a Rogue Client Filter window appears with further menu options (see Figure 5-38).

Figure 5-38 Rogue Client Filter Window



If you click the **Show All Rogue Clients** check box and **Small Icons** check box, all other drop-down menu options are grayed out.

If you uncheck the **Show All Rogue Clients** check box, you can specify how you want the rogue clients filtered. Follow these steps to define the filter.

Step 1 Provide the MAC address of an associated rogue access point.

Step 2 Specify if you want to display all rogue clients or those in the alert, contained, or threat state.

Monitoring Channels on a Floor Map

Follow these steps to monitor channels on a floor map.

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

Step 2 Click an item in the Name column.

Step 3 Click **>Layers**.

Note When you mouse over the various locations, a popup with general, 802.11a/n, and 802.11b/g/n data appears. It provides the channel, transmit power level, user count, utilization count, antenna name, antenna angle, and elevation angle (for the 802.11a/n and 802.11b/g/n windows), and access point MAC address, model, controller IP address, location, and height in the General tab.

Step 4 Click the **Access Points** check box.

Step 5 Click the **>** beside Access Point.

Step 6 From the Display drop-down menu, choose **Channels**.

The number of the channel being used by each radio appears in the flag next to each access point. "Unavailable" appears for disassociated access points.

Note The available channels are defined by the country code setting and are regulated by country. Refer to http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html.

Monitoring Transmit Power Levels on a Floor Map

Follow these steps to monitor transmit power levels on a floor map.

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

Step 2 Click an item in the Name column.

Step 3 Click **Layers**.

Note When you mouse over the various locations, a popup with general, 802.11a/n, and 802.11b/g/n data appears. It provides the channel, transmit power level, user count, utilization count, antenna name, antenna angle, and elevation angle (for the 802.11a/n and 802.11b/g/n windows), and access point MAC address, model, controller IP address, location, and height in the General tab.

Step 4 Click the Access Point check box.

Step 5 Click the **arrow** beside Access Point.

Step 6 Choose **Tx Power Level** from the Display drop-down menu.

Step 7 The number of the transmit power level being used by each radio appears in the flag next to each access point. “Unavailable” appears for disassociated access points.

Table 5-4 lists the transmit power level numbers and their corresponding power settings:

Table 5-4 Transmit Power Level Values

Transmit Power Level Number	Power Setting
1	Maximum power allowed per country code setting
2	50% power
3	25% power
4	12.5 to 6.25% power
5	6.25 to 0.195% power

Note The power levels are defined by the country code setting and are regulated by country. Refer to http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html.

Monitoring Coverage Holes on a Floor Map

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.

Follow these steps to monitor coverage holes on a floor map.

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

Step 2 Click an item in the Name column.

Step 3 Click **Layers**.

Note When you mouse over the various locations, a popup with general, 802.11a/n, and 802.11b/g/n data appears. It provides the channel, transmit power level, user count, utilization count, antenna name, antenna angle, and elevation angle (for the 802.11a/n and 802.11b/g/n windows), and access point MAC address, model, controller IP address, location, and height in the General tab.

Step 4 Click the **Access Points** check box.

Step 5 Click the **arrow** beside Access Point.

Step 6 Choose **Coverage Holes** from the Display drop-down menu.

The percentage of clients that have lost their connection to the wireless network appears in the flag next to each access point. “Unavailable” appears for disassociated access points, and “MonitorOnly” appears for access points in monitor-only mode.

Monitoring Clients on a Floor Map

Follow these steps to monitor client devices on a floor map.

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

Step 2 Click an item in the Name column.

Step 3 Click **Layers**.

Note When you mouse over the various locations, a popup with general, 802.11a/n, and 802.11b/g/n data appears. It provides the channel, transmit power level, user count, utilization count, antenna name, antenna angle, and elevation angle (for the 802.11a/n and 802.11b/g/n windows), and access point MAC address, model, controller IP address, location, and height in the General tab.

Step 4 Click the **Access Points** check box.

Step 5 Click the **arrow** beside Access Point.

Step 6 Choose **Users** from the Display drop-down menu.

The number of client devices associated to each radio appears in the flag next to each access point. “Unavailable” appears for disassociated access points, and “MonitorOnly” appears for access points in monitor-only mode.

Step 7 Click the number of clients to display a list of specific client devices and parameters. Table 5-5 lists the parameters that appear.

Table 5-5 Client Parameters

Parameter	Description
User	The username of the client
Vendor	The manufacturer of the client
IP Address	The IP address of the client
MAC Address	The MAC address of the client
Access Point	The name of the access point to which the client is associated
Controller	The IP address of the controller to which the access point is connected
Port	The port number of the controller to which the access point is connected
802.11 State	Indicates whether the client is associated or disassociated
SSID	The service set identifier (SSID) being broadcast by the access point
Authenticated	Indicates whether authentication is enabled or disabled
Protocol	Indicates whether the 802.11a/n or 802.11b/g/n protocol is being used

Monitoring Outdoor Areas

Follow these steps to add outdoor areas to a campus.

Step 1 Choose **Monitor > Maps**.

Step 2 Click a campus name in the Name column. Verify in the Type column that it is a campus and not a building, floor area, or outdoor area.

Step 3 From the Select a command drop-down menu, choose **New Outdoor Area** and click **GO**.

Step 4 Enter the user-defined name of the new outdoor area.

Step 5 Provide a contact name.

Step 6 Use the drop-down menu to choose what type of structures exist in this area. You can choose cubes and walled offices, drywall office only, or outdoor open space.

Step 7 Enter the height in feet where the access point is mounted.

Step 8 Enter the name of the file containing the outdoor area map or use the **Browse** button to locate the file. Click **Next** to continue with the new outdoor area process.

Step 9 A blue rectangle appears in the upper right-hand corner, superimposed on the map of the campus. Using the mouse, drag this rectangle to the desired outdoor location. To resize the blue rectangle, use Ctrl+Left+Click.

Step 10 The name and contact information carries over to this window. Use the zoom to get a different view of the map.

Step 11 Click the **Maintain Image Aspect Ratio** check box if you want to maintain the ratio of horizontal and vertical pixels of the map image. Maintaining the aspect ratio prevents visual distortion of the map.

Step 12 Enter the horizontal distance from the corner of the outdoor area rectangle to the left edge of the campus map in feet or meters.

Step 13 Enter the vertical distance from the corner of the outdoor area rectangle to the top edge of the campus map in feet or meters.

Step 14 Enter the left to right horizontal span of the outdoor area rectangle in feet or meters.

Step 15 Enter the up and down vertical span of the outdoor area rectangle in feet or meters.

Note To change the unit of measurement (feet or meters), choose **Monitor > Maps** and then choose **Properties** from the Select a command drop-down menu and click **GO**. The first drop-down menu on the Maps > Properties window allows you to choose between feet or meters as a unit of dimension.

Step 16 Choose **Place** to fix the changes on the display or **Save** to add them to the database.

Importing or Exporting WLSE Map Data

When converting from autonomous to LWAPP and from WLSE to WCS, one of the conversion steps is to manually re-enter the access point-related 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**.

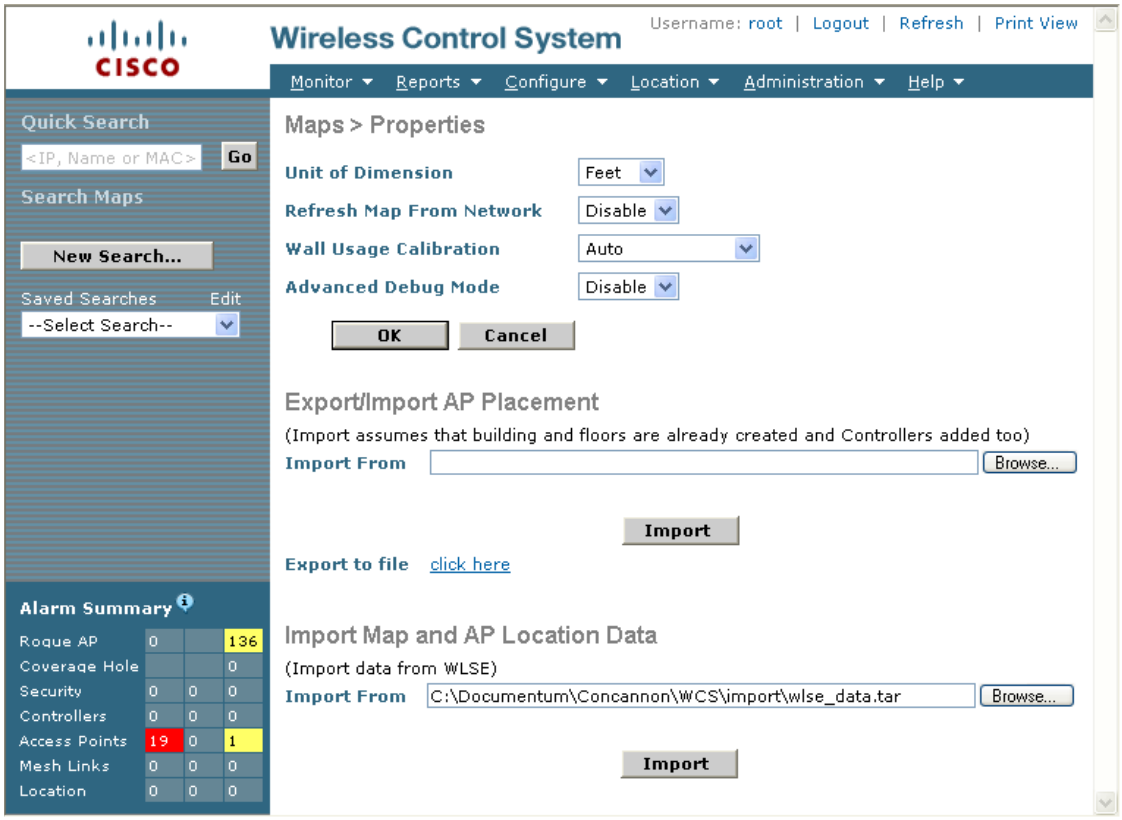
Step 2 Choose **Properties** from the Select a command drop-down menu and click **GO**.

Step 3 In the Import Map and AP Location 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 (see Figure 5-39).

Figure 5-39 Maps > Properties Window



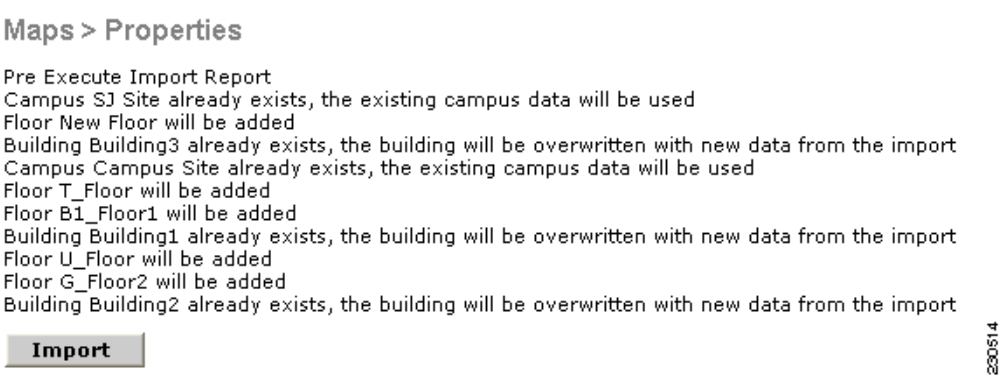
Step 5 Click **Import**.

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 (see Figure 5-40). The report also specifies what cannot be added and why.

Figure 5-40 Pre Execute Import Report

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 (see Figure 5-41).

Figure 5-41 Pre Execute Import Report — Duplicate Data Handling



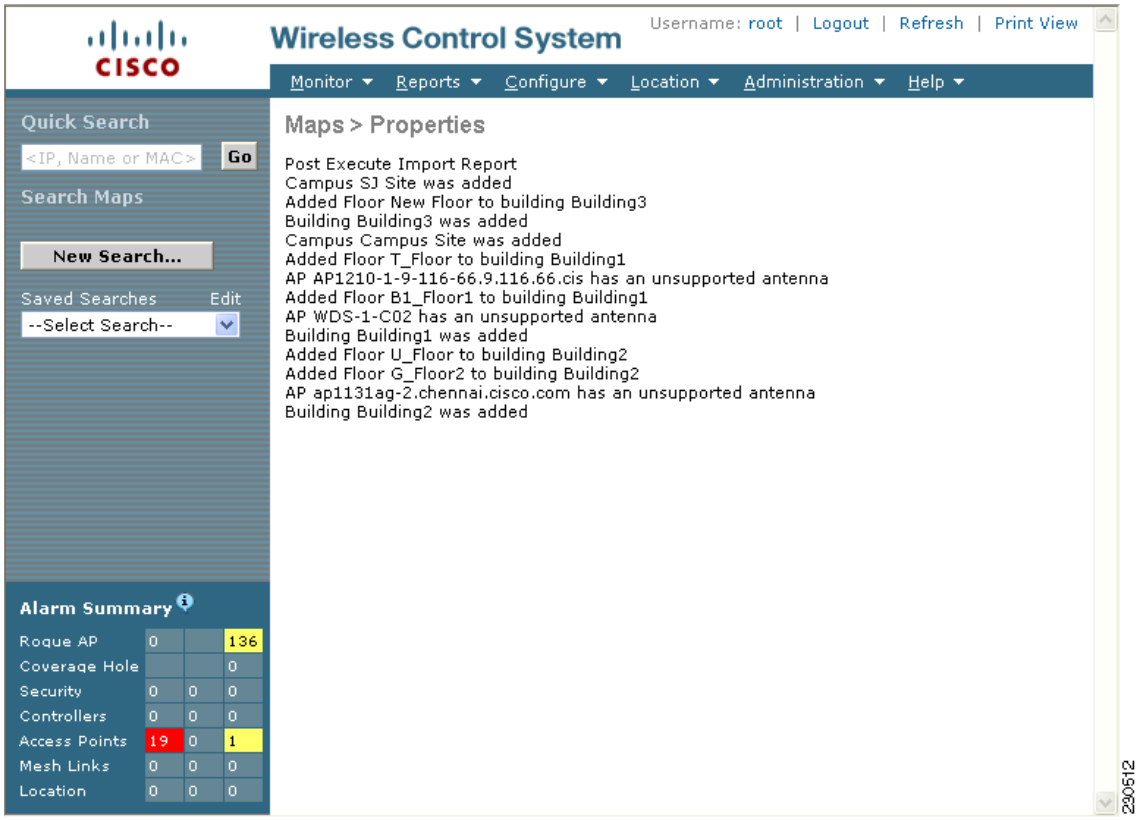
Note If there are duplicate names between a WLSE site and building combination and a WCS campus (or top-level building) and building combination, WCS displays a message in the Pre Execute Import Report indicating that it will delete the existing building.

Step 6 Click **Import** to import the WLSE data.

WCS displays a report indicating what was imported (see Figure 5-42).

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 on the floor image to go directly to the appropriate floor screen.

Figure 5-42 Post Execute Import Report



Step 7 Click **Monitor > Maps** to view the imported data (see Figure 5-42).

Creating and Applying Calibration Models

If the provided RF models do not sufficiently characterize the floor layout, you can create a calibration model that is applied to the floor and better represents the attenuation characteristics of that floor. In environments in which many floors share common attenuation characteristics (such as in a library), one calibration model can be created and then applied to floors with the same physical layout and same deployment.

The calibration models are used as RF overlays with measured RF signal characteristics that can be applied to different floor areas. This enables the Cisco WLAN solution installation team to lay out one floor in a multi-floor area, use the RF calibration tool to measure, save the RF characteristics of that floor as a new calibration model, and apply that calibration model to all the other floors with the same physical layout.

You can collect data for a calibration using one of two methods:

- Data point collection—Calibration points are chosen and their coverage area is calculated one location at a time.
- Linear point collection—A series of linear paths are chosen and then calculated as you traverse the path. This approach is generally faster than the data point collection. You can also employ data point collection to augment data collection for locations missed by the linear paths.

Note A client device that supports both 802.11a/n and 802.11b/g/n radios is recommended to expedite the calibration process for both spectrums.

Use a laptop or other wireless device to open a browser to the WCS server and perform the calibration process.

Step 1 Navigate to **Monitor > Maps** and choose **RF Calibration Models** from the Select a command drop-down menu. Click **GO**.

Step 2 Choose **Create New Model** from the Select a command drop-down menu. Click **GO**.

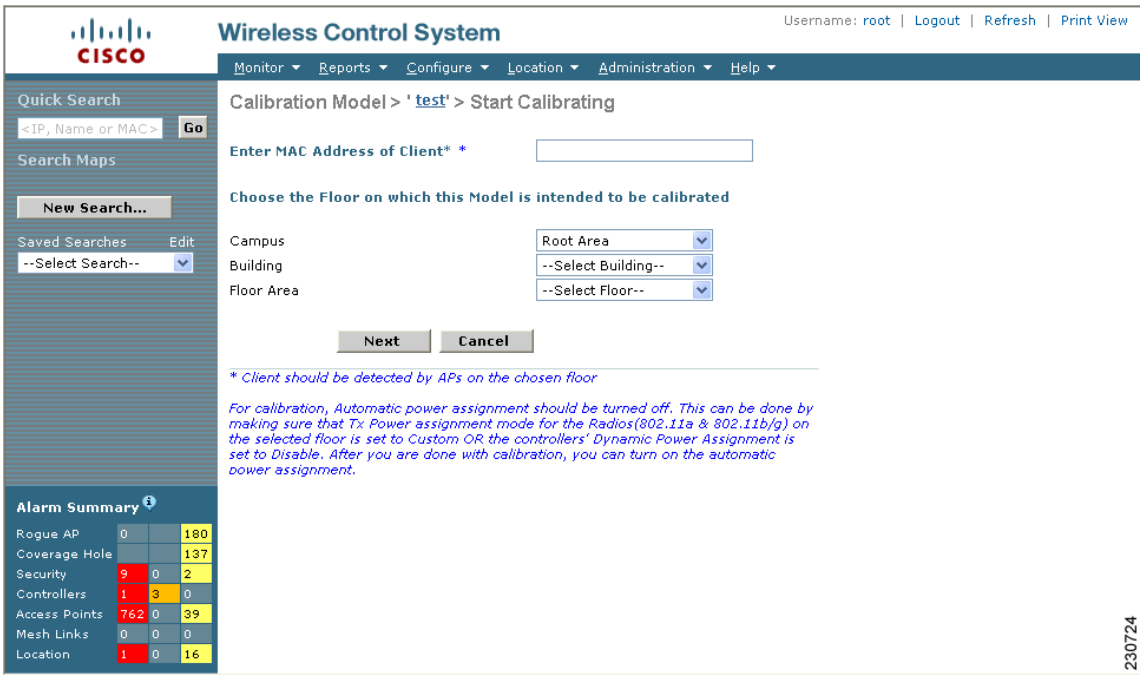
Step 3 Assign a name to the model and click **OK**.

Step 4 The new model appears along with the other RF calibration models, but its status is listed as Not Yet Calibrated. To start the calibration process, click on the hyperlink associated with the new model name. A new window appears which indicates the details of the new model. In the upper right-hand corner, choose **Add Data Points** from the Select a command drop-down menu and click **GO**.

Step 5 If this process is being performed from a mobile device connected to WCS through the Cisco Centralized architecture, the MAC address field is automatically populated with the device's address. Otherwise, you can manually enter the MAC address of the device being used to perform the calibration. MAC addresses that are manually entered must be delimited with colons (such as FF:FF:FF:FF:FF:FF).

Step 6 Choose the appropriate campus, building, and floor where the calibration is performed (see Figure 5-43). Click **Next**.

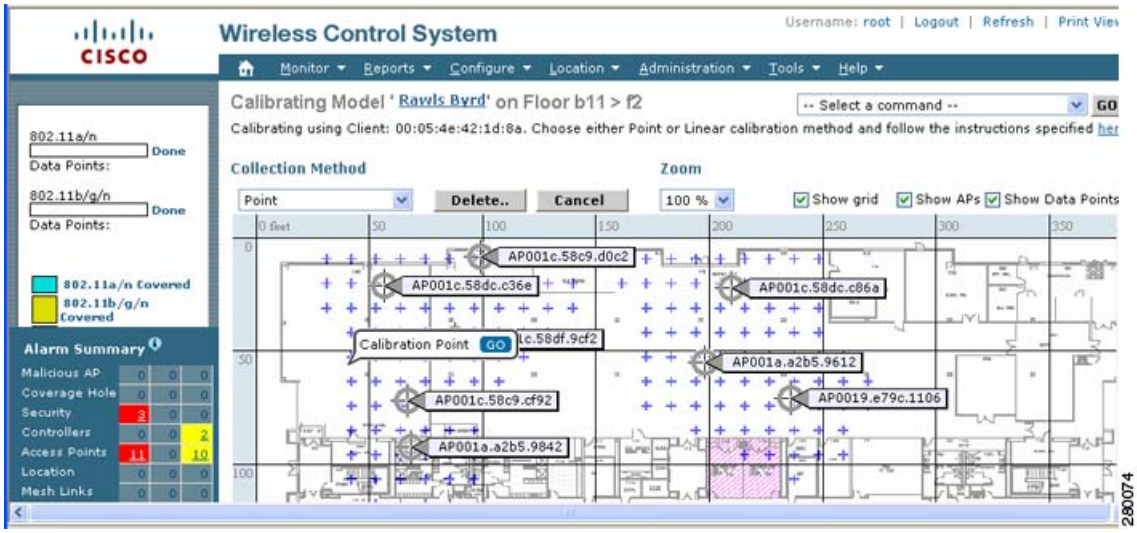
Figure 5-43 Starting to Calibrate



Step 7 When the chosen floor map and access point locations display, a grid of plus marks (+) indicates the locations where data collection for calibration is performed.

Using these locations as guidelines, you can perform either a point or linear collection of data by appropriate placement of either the Calibration Point pop-up (point) or the Start and Finish pop-ups (linear) that display on the map when the respective options are displayed. Figure 5-44 shows the starting window for a point calibration.

Figure 5-44 Positioning Calibration Points



a. If you want to do a point collection of data for the calibration, do the following:

1. Choose **Point** from the Collection method drop-down menu and check the **Show Data points** check box if not already checked. A calibration point pop-up displays on the map.
2. Position the tip of the calibration point pop-up at a data point (+) and click **GO**. A panel appears showing the progress of the data collection.

Note Rotate the calibrating client laptop during data collection so that the client is heard evenly by all access points in the vicinity.

3. When the data collection is complete for a selected data point and the coverage area is plotted on the map, move the calibration point pop-up to another data point and click **GO**.

Note The coverage area plotted on the map is color-coded and corresponds with the specific wireless LAN standard used to collect that data. Information on color-coding is provided in the legend on the left-hand side of the window. Additionally, the progress of the calibration process is indicated by two status bars above the legend, one for 802.11a/n and one for 802.11b/g/n.

Note To delete data points for locations selected in error, click **Delete** and move the black square that appears over the appropriate data points. Resize the square as necessary by pressing **Ctrl** and moving the mouse.

4. Repeat steps a1 to a3 until the calibrations status bar of the relevant spectrums (802.11a/n, 802.11b/g/n) display as *done*.

Note The calibration status bar indicates data collection for the calibration as done, after roughly 50 distinct locations and 150 measurements have been gathered. For every location point saved in the calibration process, more than one data point is gathered. The progress of the calibration process is indicated by two status bars above the legend, one for 802.11b/g/n and one for 802/11a/n.

b. If you want to do a linear collection of data for the calibration, do the following:

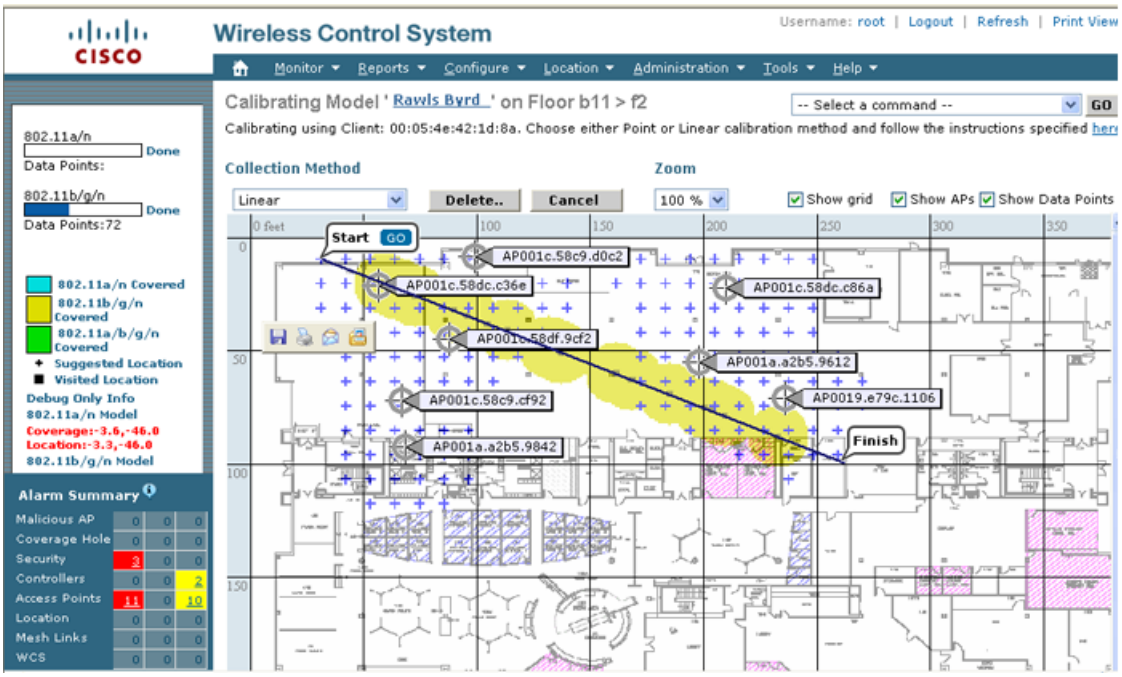
1. Choose **Linear** from the Collection Method drop-down menu and check the **Show Data** points check box if not already checked. A line appears on the map with both Start and Finish pop-ups.
2. Position the tip of the Start pop-up at the starting data point.
3. Position the Finish pop-up at the ending data point.
4. Position yourself with your laptop at the starting data point and click **GO**. Walk steadily towards the end point along the defined path. A panel displays to show that data collection is in process.

Note Do not stop data collection until you reach the end point even if the data collection bar indicates completion.

5. Press the space bar (or **Done** on the data collection panel) when you reach the end point. The collection panel displays the number of samples taken before it closes to reveal the map. The map displays all the coverage areas where data was collected (see Figure 5-45).

Note To delete data points for locations selected in error, click **Delete** and move the black square that appears over the appropriate data points. Resize the square as necessary by pressing **Ctrl** and moving the mouse.

Figure 5-45 Linear Data Collection



Note The coverage area is color-coded and corresponds with the specific wireless LAN standard used to collect that data. Information on color-coding is provided in the legend on the left-hand side of the window.

6. Repeat Steps b2 to b5 until the status bar for the respective spectrum is filled in (done).

Note You can augment linear collection with data point collection to address missed coverage areas.

Step 8 Click on the name of the calibration model at the top of the window to return to the main screen for that model. You can then calibrate the data points.

Step 9 Choose **Calibrate** from the Select a command drop-down menu and click **GO**.

Step 10 Click the **Inspect Location Quality** link when calibration completes. A map displays showing RSSI readings.

Step 11 To use the newly created calibration model, you must apply the model to the floor on which it was created (and on any other floors with similar attenuation characteristics as well). Navigate to **Monitor > Maps** and find the specific floor to which the model is applied. At the floor map interface, choose **Edit Floor Area** from the drop-down menu and click **GO**.

Step 12 From the Floor Type (RF Model) drop-down menu, choose the newly created calibration model. Click **OK** to apply the model to the floor.

Note This process can be repeated for as many models and floors as needed. After a model is applied to a floor, all location determination performed on that floor is done using the specific collected attenuation data from the calibration model.

Analyzing Element Location Accuracy Using Testpoints

You can analyze the location accuracy of rogue and non-rogue clients and asset tags by entering testpoints on an area or floor map. You can use this feature to validate location information generated either automatically by access points or manually by calibration.

Note By checking for location accuracy, you are checking the ability of the existing access point deployment to estimate the true location of an element within 10 meters at least 90% of the time.

Note Before starting this process, record the MAC addresses and locations for all elements within the area or floor to be analyzed. You need this information when placing the testpoints on the map. If analyzing location after calibration, you should analyze the location accuracy of at least as many elements entered during calibration.

Note The **Advanced Debug** option must be enabled on both the location appliance and WCS to allow use of the location accuracy testpoint feature.

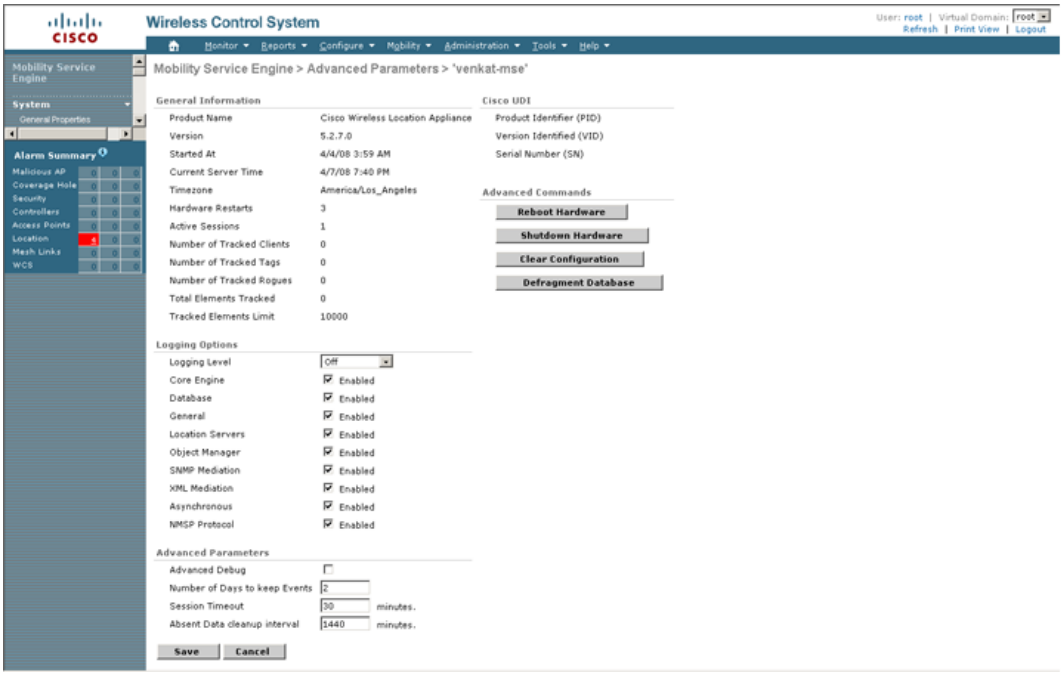
Follow these steps to enable the advanced debug option and assign testpoints to a floor map to check location accuracy.

Step 1 Choose **Mobility > Mobility Service Engines**.

Step 2 Select a server from the All Location Servers page that appears.

Step 3 At the General Properties page for that location server, choose the **System > Advanced Parameters** option from the left sidebar menu (see Figure 5-46).

Figure 5-46 Mobility Service Engine > Advanced Parameters



Step 4 On the page that appears, scroll down to the Advanced Parameters section. Check the **Advanced Debug** box to enable the feature. Click **Save**.

Note If the **Advanced Debug** check box is already checked, you do not need to do anything further. Click **Cancel**.

Assigning Testpoints to a Selected Area

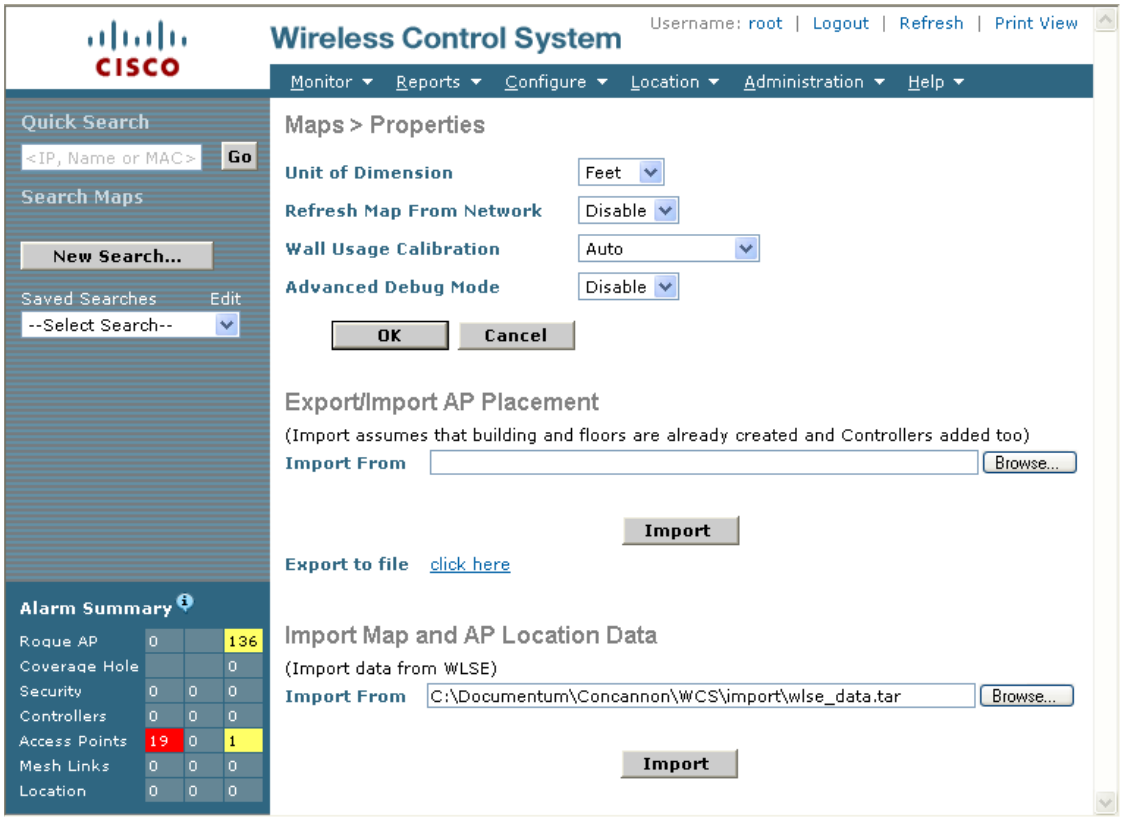
You now must enable the Advanced debug level at the Maps level and begin assigning testpoints to a selected area or map.

Step 1 Choose **Monitor > Maps.**

Step 2 Select **Properties** from the Select a command drop-down menu.

Step 3 On the Maps > Properties page (see Figure 5-47), select **Enable** from the Advanced Debug drop-down menu. Click **OK**.

Figure 5-47 Map > Properties Page

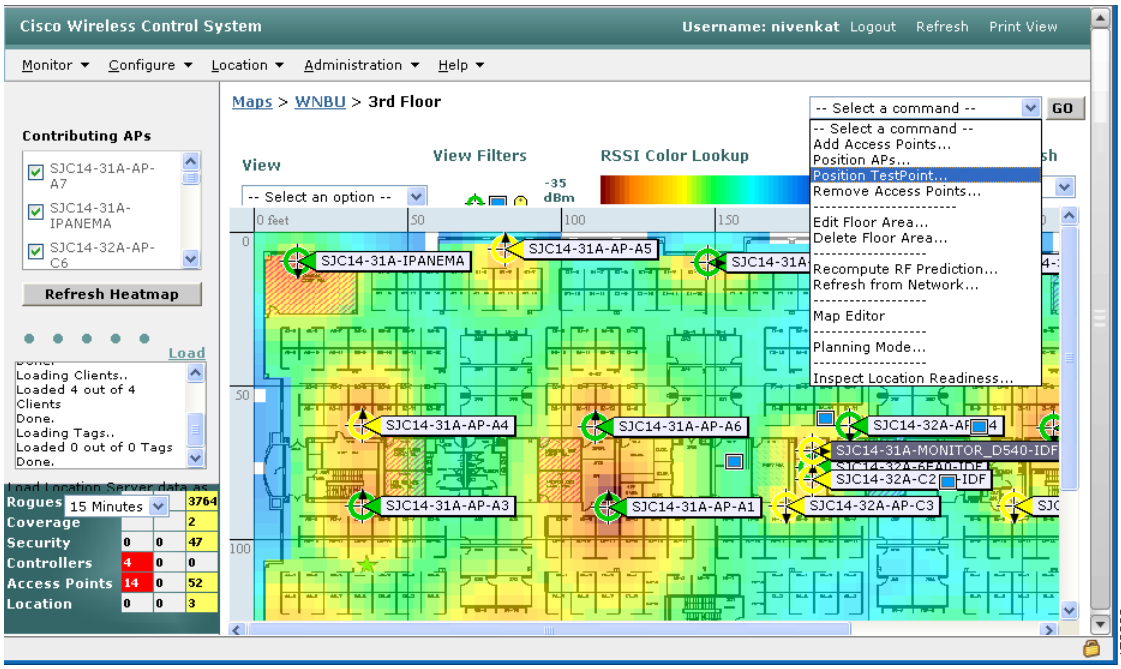


You are returned to the Maps summary window. You are now ready to assign testpoints to a selected area or map.

Step 4 Choose **Monitor > Maps**. Select the area or floor you want to analyze from the map summary that appears.

The page seen in Figure 5-48 appears.

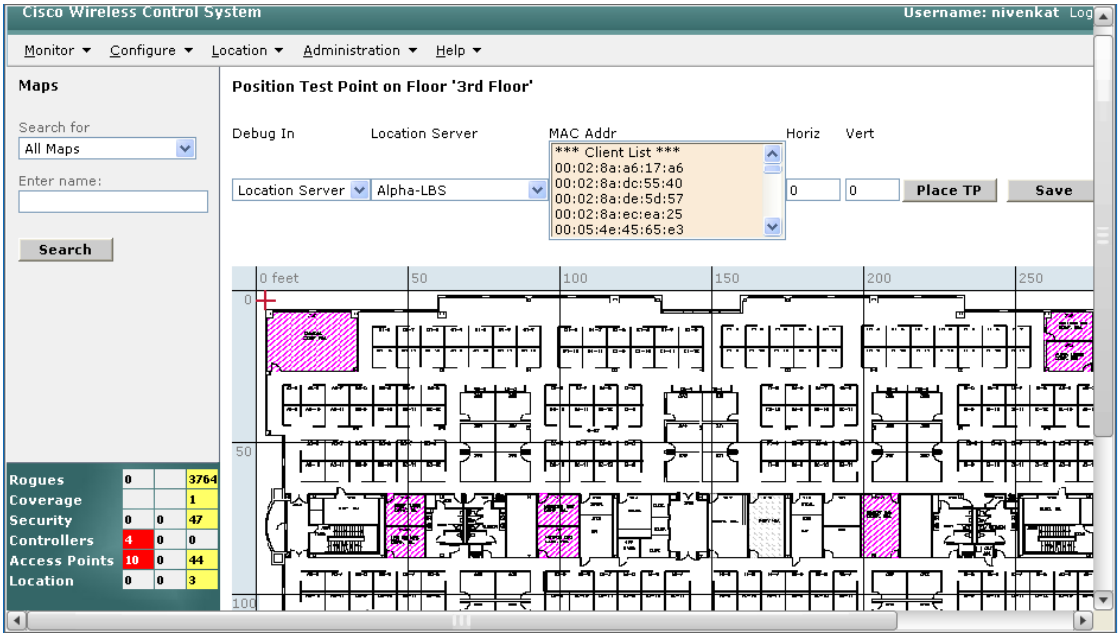
Figure 5-48 Selected Area or Floor Map Chosen at Monitor > Maps Page



Step 5 Select **Position TestPoint** from the Select a command drop-down menu (top-right). Click **GO.**

A blank map of the selected area or floor appears for testpoint assignment (see Figure 5-49).

Figure 5-49 Position TestPoint Assignment Page



Step 6 On the Position Test Point page, select the location server from the drop-down menu and choose a MAC address from the list of MAC addresses (for clients, tags, rogue access point, rogue clients, and so on).

Note If you entered horizontal and vertical coordinates, click **Place TP** instead of Save.

Step 7 Move the red cross-hair cursor (top-left) to the map location that corresponds to the actual position of the element and click **Save**.

Note Instead of using the cursor, you can enter the horizontal (**Horz**) and vertical (**Vert**) coordinates of the asset tag or client to mark its location.

A pop up box appears noting successful addition of the testpoint for the element and its MAC address.

The red cross hair cursor returns to the upper left-band corner after placement is confirmed. You are ready to mark additional testpoints.

Step 8 Wait 2 minutes to collect enough data to analyze. After waiting at least 2 minutes, click **Stop**.

Note If you wait less than 2 minutes before clicking Stop, the accuracy of the data is deteriorated.

Step 9 Repeat Steps 6 and 7 for each client or asset tag you want to add to the map.

Step 10 Click **Analyze** (far-right) to determine location accuracy of the entered testpoints.

A pop up window appears providing accuracy percentage and the number of sample points gathered during that interval.

You can perform this test for multiple elements by selecting multiple MAC addresses from the list of MAC addresses and repeating the above procedure.

Using the Accuracy Tool to Conduct Accuracy Testing

There are two methods of conducting location accuracy testing:

- 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 window.

Note The Advanced Debug option must be enabled in Cisco WCS to allow use of both the Scheduled and On-demand location accuracy testing features.

Follow these steps to enable the advanced debug option in Cisco WCS.

Step 1 In Cisco WCS, click **Monitor > Map**s.

Step 2 Choose **Properties** from the Select a command drop-down menu and click **GO**.

Step 3 Choose **Enabled** from the Advanced Debug drop-down menu. 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 location appliance using the Accuracy Tool.

Using Scheduled Accuracy Testing to Verify Accuracy of Current Location

To configure a scheduled accuracy test, do the following:

Step 1 Click **Tools > Accuracy Tool**.

Step 2 Choose **New Scheduled Accuracy Test** from the Select a command drop-down menu.

Step 3 Enter a test name.

Step 4 Choose the area type from the drop-down menu.

Campus is configured as root area, by default. There is no need to change this setting.

Step 5 Choose the building from the drop-down menu.

Step 6 Choose the floor from the drop-down menu.

Step 7 Choose the begin and end time of the test by entering the days, hours, and minutes. Hours are entered 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 8 You should e-mail the report or download the test results from the Accuracy Tests > Results window because the data in the Results tab is only stored for seven days. Reports are in PDF format.

Note Only the entries for the last seven days appear in the Results window. After seven days, the Results tab disappears.

Note If you select the e-mail option, a SMTP Mail Server must first be defined for the target e-mail address. Click **Administrator > Settings > Mail Server** to enter the appropriate information.

Step 9 Click **Position Testpoints**. The floor map appears with a list of all clients and tags on that floor with their MAC addresses.

Step 10 Click the check box next to each client and tag for which you want to check the location accuracy.

When you check a MAC address check box, two icons overlaying each other appear on the map.

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, check 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 location server but on a different floor, the icon appears in the left-most corner (0, 0 position).

Step 11 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. Only the actual location icon can be dragged.

Step 12 Click **Save** when all elements are positioned. A panel appears confirming successful accuracy testing.

Step 13 Click **OK** to close the confirmation panel. You are returned to the Accuracy Tests summary window.

Note The accuracy test status displays as Scheduled when the test is about to execute. A status of Running appears when the test is in process and Idle when the test is complete. A Failure status appears when the test is not successful.

Step 14 To view the results of the location accuracy test, click the test name and then choose the **Results** tab on the page that appears.

Step 15 At the Results panel, click the **Download** link under the Saved Report heading to view the report.

The Scheduled Location Accuracy Report includes the following information:

- A summary location accuracy report that details the percentage of elements that fall within various error ranges.
- An error distance histogram
- A cumulative error distribution graph
- An error distance over time graph
- A summary of each MAC address whose location accuracy was tested noting its actual location and error distance, and a map showing its spatial accuracy (actual vs. calculated location) and error distance over time for each MAC.

Using On-Demand Accuracy Testing to Test Location Accuracy

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. It is generally used to test the location accuracy for a small number of clients and tags.

Follow these steps to run an on-demand accuracy test.

Step 1 Click **Tools > Accuracy Tool**.

Step 2 Choose **New On demand Accuracy Test** from the Select a command drop-down menu.

Step 3 Enter a test name.

Step 4 Choose the area type from the drop-down menu.

Campus is configured as root area, by default. There is no need to change this setting.

Step 5 Choose the building from the drop-down menu.

Step 6 Choose the floor from the drop-down menu.

Step 7 Tests results are viewed at the Accuracy Tests > Results window. Reports are in .pdf format.

Step 8 Click **Position Testpoints**. The floor map appears with a red cross hair at the (0,0) coordinate.

Step 9 To test the location accuracy and RSSI of a particular location, choose either **client** or **tag** from the drop-down menu on the left. A list of all MAC addresses for the selected option (client or tag) appears in a drop-down menu to its right.

Step 10 Choose a MAC address from the drop-down menu and move the red cross hair to a map location and client the mouse to place it.

Step 11 Click **Start** to begin collection of accuracy data.

Step 12 Click **Stop** to finish collection. You should allow the test to run for at least two minutes before clicking Stop.

Step 13 Repeat Step 9 to Step 12 for each testpoint that you want to plot on the map.

Step 14 Click **Analyze** when you are finished mapping the testpoints.

Step 15 Choose the **Results** tab on the panel 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

Note You can download logs for accuracy tests from the Accuracy Tests summary page.

To do so, check the listed test check box and select either **Download Logs** or **Download Logs for Last Run** from the Select a command drop-down menu and 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).

CHAPTER 6

Monitoring Wireless Devices

This chapter describes how to use WCS to monitor your wireless LANs. It contains these sections:

- Monitoring Rogue Access Points, Adhocs, and Clients, page 6-1
- Rogue Access Point Location, Tagging, and Containment, page 6-16
- Monitoring Clients, page 6-19
- WLAN Client Troubleshooting, page 6-20
- Enabling Automatic Client Troubleshooting, page 6-35
- Finding Clients, page 6-35
- Receiving Radio Measurements, page 6-39
- Monitoring Mesh Networks Using Maps, page 6-40
- Mesh Statistics for an Access Point, page 6-51
- Viewing the Mesh Network Hierarchy, page 6-56
- Monitoring Channel Width, page 6-59
- Viewing Clients Identified as WGBs, page 6-62
- Running a Link Test, page 6-63
- Retrieving the Unique Device Identifier on Controllers and Access Points, page 6-64
- Coverage Hole, page 6-68
- Viewing DHCP Statistics, page 6-70
- RRM Dashboard, page 6-71

Monitoring Rogue Access Points, Adhocs, and Clients

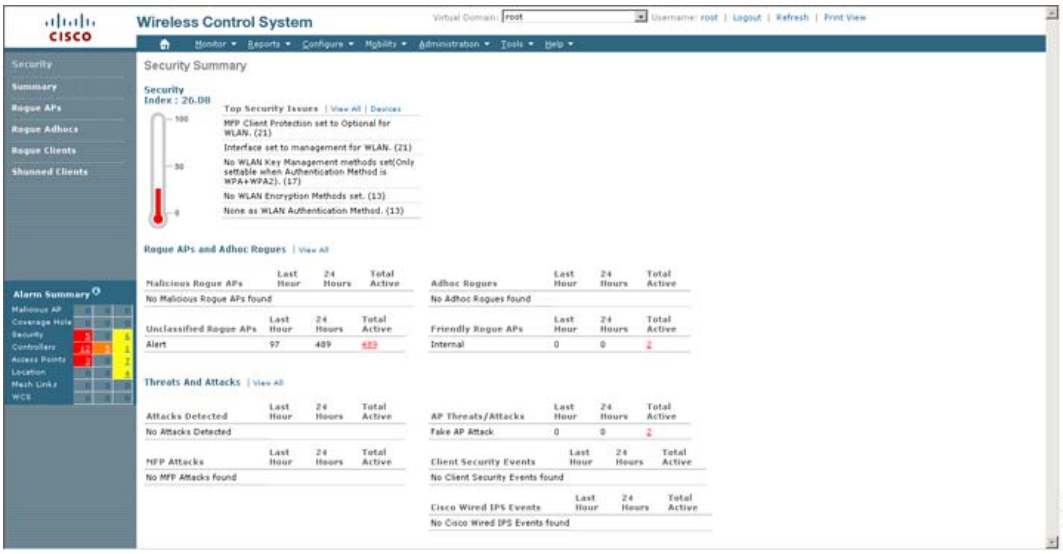
Because unauthorized rogue access points are inexpensive and readily available, employees sometimes plug them into existing LANs and build ad hoc wireless networks without IT department knowledge or consent. These rogue access points can be a serious breach of network security because they can be plugged 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 unsecure 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.

Interpreting Security Summary Window

You can see a summary of existing events and the security state of the network by choosing **Monitor > Security**. The Security Summary window appears (see Figure 6-1).

Figure 6-1 Security Summary Window



The Security Summary window provides information in the following sections:

- Security Index
- Top Security Issues
- Malicious Rogue Access Points
- Adhocs Rogues
- Unclassified Rogue Access Points
- Friendly Rogue Access Points
- Attacks Detected
- Access Point Threats or Attacks
- MFP Attacks
- Client Security Events
- Cisco Wired IPS Events

Security Index

The Security Index gives an indication of 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 calculated as the lowest scoring controller plus the lowest scoring Location Service/Mobility Service Engine.

The security thermometer color range is represented as follows:

- Above 80 - Green
- Below 80 but greater than 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.

Note 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 configuration data from all the controllers. Refer to the "Configuration Sync" section on page 16-4 for steps on enabling the security index.

Top Security Issues

The View All and Devices links sort relevant columns and show a report of security issues occurring across all controllers. If you click **View All**, the Security Index Detailed Report appears (see Figure 6-2). It 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 as you would an alarm), it will be ignored the next time the Configuration Sync task runs (provided Security Index Calculation is enabled).

Note In some cases, when an ACK happens and is ignored in the next iteration, the final security index score may change. There could be multiple reasons for this change:

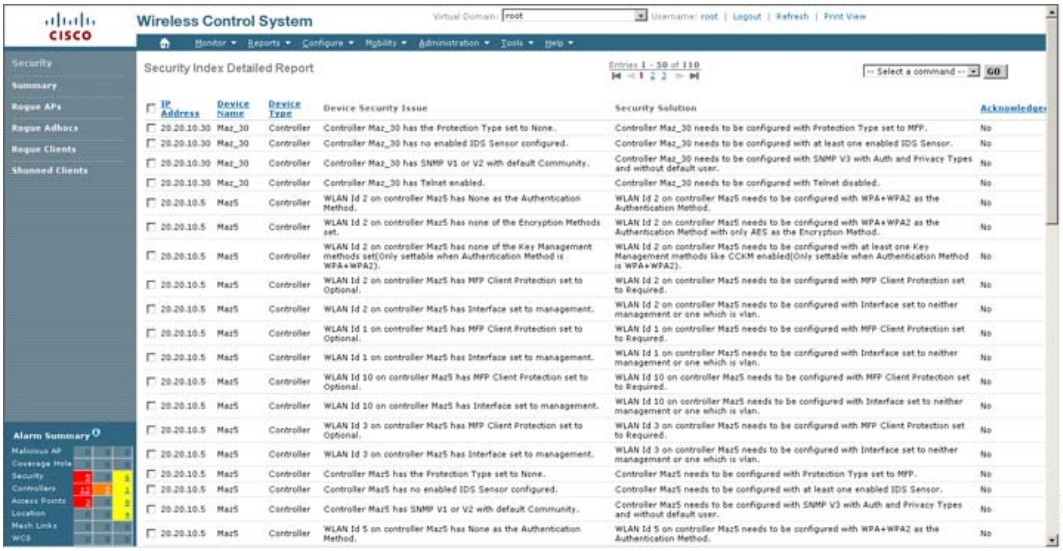
- The acknowledged issue on the controller is not directly affecting the security index score.
- The acknowledged issue on a WLAN is not directly affecting the security index score. Only the lowest scoring WLAN of the lowest scoring controller affects the security index score, so an issue on any other WLAN would not make the score higher.

- Some cases, like SSH and Telnet being enabled on a controller, are both flagged as issues. However, a Telnet issue has a higher precedence than an SSH issue. For instance, if SSH is acknowledged on a controller with the lowest score, no changes would occur for the security index.

The following three different view can be viewed:

- Show Unacknowledged which shows only unacknowledged security issues (the default value). When **View All** is clicked, this view is shown.
- Show Acknowledged shows acknowledged security issues.
- Show All shows all security issues (acknowledged or unacknowledged).

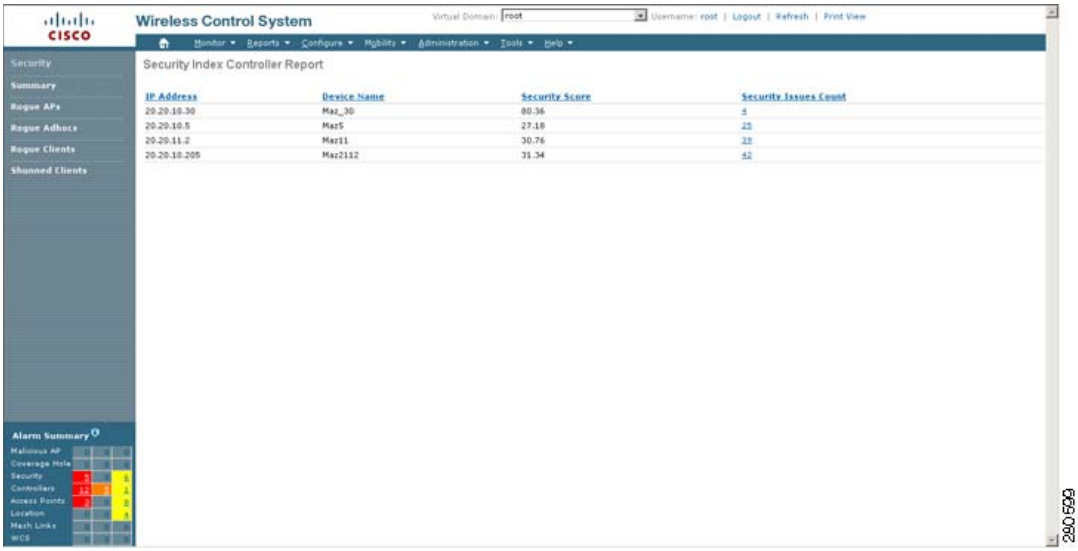
Figure 6-2 Security Index Detailed Report



If you click **Devices** from the Security Summary window (Figure 6-1), the Security Index Controller Report appears (see Figure 6-3). This screen 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.

Note The security score of the lowest scoring controller is not the same as the security index for WCS. Some score comes from the lowest scoring Location or Mobility Server Engine, and the lowest scoring controller score shown is calibrated to out of 100.

Figure 6-3 Security Index Controller Report



If you click the number in the Security Issues Count column, the Security Index Detailed Report appears (see Figure 6-2).

Table 6-1 lists top security issues, provides a description of why the issue occurs, and defines what action should be taken as a solution. Table 6-2 lists top security issues for location and mobility servers, provides a description of why the issue occurs, and defines what action should be taken as a solution.

Table 6-1 Top Security Issues

Controller Security Issue	Why is this an issue?	What is the solution?
Static WEP configured as the authentication method for a WLAN.	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 — WPA+WPA2.
CKIP configured as the authentication method for a WLAN.	Weak authentication method for a WLAN.	Use the most secured authentication method — WPA+WPA2.
An authentication method as *None* for a WLAN.	No authentication method is a clear security risk for a WLAN.	Use the most secured authentication method — WPA+WPA2.
CKIP WEP 10/104 bits (with MMH or Key Permutation or both) as one of the encryption methods for a WLAN.	A weak encryption method for a WLAN.	Use the most secured encryption method —AES. AES is only available when WPA+WPA2 is the authentication method.
WEP 40/104/128 bits as one of the encryption methods (802.1X or WEP Authentication Method) for a WLAN.	A weak encryption method for a WLAN.	Use the most secured encryption method —AES. AES is only available when WPA+WPA2 is the authentication method.

Table 6-1 (continued)Top Security Issues

Controller Security Issue	Why is this an issue?	What is the solution?
One of the encryption methods for a WLAN is TKIP.	A weak encryption method for a WLAN.	Use the most secured encryption method —AES. AES is only available when WPA+WPA2 is the authentication method.
None of the encryption methods for a WLAN are set.	A clear security risk exists for a WLAN when no encryption method is set.	Use the most secured encyrption method —AES. AES is only available when WPA+WPA2 is the authentication method.
None of the key management methods are set for a WLAN. You can set these methods only when the authentication method is WPA+WPA2.	A key management method enhances the security of keys. Without one, WLAN is less secure.	At least one key management method (such as CCKM enabled) must be enabled to improve the security of the WLAN. This method can be set only when the authentication method is WPA+WPA2.
MFP Client Protection is set to *optional* for a WLAN.	With the MFP Client Protection set to *optional*, authenticated clients may not be shielded from spoofed frames.	To shield authenticated clients from spoofed frames, set MFP Client Protection to *required* for a WLAN.
MFP Client Protection is set to *disabled* for a WLAN.	With the MFP Client Protection set to *disabled*, authenticated clients may not be shielded from spoofed frames.	To shield authenticated clients from spoofed frames, set MFP Client Protection to *required* for a WLAN.
The interface is mapped to *management* for a WLAN.	As recommended from SAFE, user traffic should be separated from management traffic.	The WLAN needs its interface mapped to a non-managment interface.
Client Exlusion is disabled for a WLAN.	With Client Exlusion policies disabled, an attacker is free to continuously try for access into the WLAN network.	The WLAN needs to have Client Exclusion policy enabled to prevent a single or a set of clients (rogues) from gaining access to the WLAN network.
The Protection Type is set to AP Authentication.	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 RF groups. Some level of security is introduced, but all management frames are not covered or open to alteration by rogue access points.	The Protection Type set to Management Frame Protection is the most secured option. It includes message integrity check (MIC) into all management frames sent by an access point, and if the management frames are altered, they can be detected by other access points.

Table 6-1 (continued)Top Security Issues

Controller Security Issue	Why is this an issue?	What is the solution?
Protection Type is set to *none*.	No security for 802.11 management messages is passed between the access points and clients.	Protection Type set to Management Frame Protection is the most secured option. It includes message integrity check (MIC) into all management frames sent by an access point, and if the management frames are altered, they can be detected by other access points.
Rogue detection exists only on DCA channels.	Rogue detection done on only a subset of countries or channels is less secure than rogue detection done on all countries or channels.	Rogue detection should be turned on for all countries and channels to improve the chances of discovering rogue access points no matter where they are transmitting.
Detection and reporting of adhoc networks is turned off for rogue policies.	With detection and reporting of adhoc networks turned off, adhoc rogues go undetected.	Adhoc rogues need to be detected; therefore, detection and reporting of adhoc networks needs to be turned on for rogue policies.
The check for all Standard and Custom Signatures is disabled.	If the check for all Standard and Custom Signatures is disabled, various types of attacks from incoming 802.11 packets may go undetected.	The check for all Standard and Custom Signatures needs to be turned on to identify various types of attacks in incoming 802.11 packets.
The Excessive 802.11 Association Failures Client Exclusion Policy is disabled.	Excessive failed association attempts may consume system resources and launch potential denial-of-service attacks to the infrastructure.	Enable Excessive 802.11 Association Failures Client Exclusion Policy to prevent denial-of-service attacks on the infrastructure.
The Excessive 802.11 Authentication Failures Client Exclusion Policy is disabled.	Excessive failed authentication attempts can consume system resources and launch potential denial-of-sevice attacks to the infrastructure.	Enable Excessive 802.11 Authentication Failures Client Exclusion Policy to prevent denial-of-service attacks on the infrastructure.
The Excessive 802.1X Authentication Failures Client Exclusion Policy is disabled.	The excessive 802.1X failed authentication attempts can consume system resources and launch potential denial-of-service attacks to the infrastructure.	Enable the Excessive 802.1X Authentication Failures Client Exclusion Policy to prevent denial-of-service attacks to the infrastructure.
The Excessive 802.11 Web Authentication Failures Client Exclusion Policy is disabled.	If excessive 802.11 web is disabled, web authentication attempts consume system resources and launch potential denial-of-service attacks to the infrastructure.	Enable excessive 802.11 web authentication failures client exclusion policy to prevent denial-of-service attacks to the infrastructure.

Table 6-1 (continued)Top Security Issues

Controller Security Issue	Why is this an issue?	What is the solution?
IP Theft or Reuse Client Exclusion Policy is disabled.	If IP Theft or Reuse Client Exclusion Policy is disabled, an attacker masquerading as another client would not be disallowed.	Enable IP Theft or Reuse Client Exclusion Policy to prevent an attacker from getting into the network as another client.
No enabled IDS sensor is configured.	If no enabled IDS sensor is configured, IP level attacks are not detected.	Configure Enabled IDS Sensors to detect IP level attacks.
SNMP V1 or V2 with a default community is configured.	If SNMP V1 or V2 with default community is configured, the network is open to easy attacks because default communities are well known.	Enable SNMP V3 with Auth and Privacy type and no default user. This is the most secure SNMP connection.
SNMP V1 or V2 with a non-default community is configured.	SNMP V1 or V2 with a non-default community is slightly more secure than a default community but still less secure than SNMP V3.	Enable SNMP V3 with Auth and Privacy type and no default user. This is the most secure SNMP connection.
SNMP V3 with a default user is configured.	Using a default user makes SNMP V3 connections less secure.	Enable SNMP V3 with Auth and Privacy type and no default user. This is the most secure SNMP connection.
SNMP V3 with either Auth or Privacy Type set to *None*.	SNMP V3 with either Auth or Privacy Type set to none reduces the security of an SNMP V3 connection.	Enable SNMP V3 with Auth and Privacy types and no default user. This is the most secure SNMP connection.
HTTP is enabled (Web Mode is enabled but Secure Web Mode is disabled).	HTTP is less secure than HTTPS.	Enable HTTPS.
Telnet is enabled.	If Telnet is enabled, the controller has the risk of attack.	Disable Telnet to reduce the risk of attack.
SSH is enabled and timeout is set to zero.	If SSH is enabled and timeout is zero, the controller runs the risk of attack.	If SSH is enabled, the timeout must be set to zero to reduce the risk of attack.

Table 6-2 Top Security Issues for Location and Mobility Servers

Location Server/Mobility Server Engine Security Issue	Why is this an issue?	What is the solution?
HTTP is enabled.	HTTP is less secure than HTTPS.	Enable HTTPS.
A default password is configured for a location user.	If a default password is configured, the Location Server/Mobility Server Engine is more susceptible to connections from outside the network.	Configure the Location Server/Mobility Server Engine user with a non-default password.

Malicious Rogue Access Points

This section provides information on rogue access points that are classified as *Malicious*. Table 6-3 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 window 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 6-3 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.

Adhocs Rogues

This section provides information on rogue adhocs. This section provides information on rogue adhocs. Table 6-4 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 window with further information appears.

Table 6-4 Rogue Adhocs

Parameter	Description
Alert	Indicates the number of rogue adhocs 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.

Unclassified Rogue Access Points

This section provides information on rogue access points that are not classified. Table 6-5 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 window 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 6-5 Unclassified Rogue

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 6-6 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 window 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 6-6 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.

Attacks Detected

Attacks reflect network patterns that indicate a possible virus or hacker attack. When an attack occurs, the attack table is updated immediately. The table displays the number of attacks during the last one hour, last 24 hours, and the total active. You can use this information to assess the security state or security threats to the network.

If you click an underlined number in any of the time period categories, a window with further information appears.

Access Point Threats or Attacks

Table 6-7 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 window with further information appears.

Table 6-7 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 window with further information appears.

Client Security Events

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 window with further information appears.

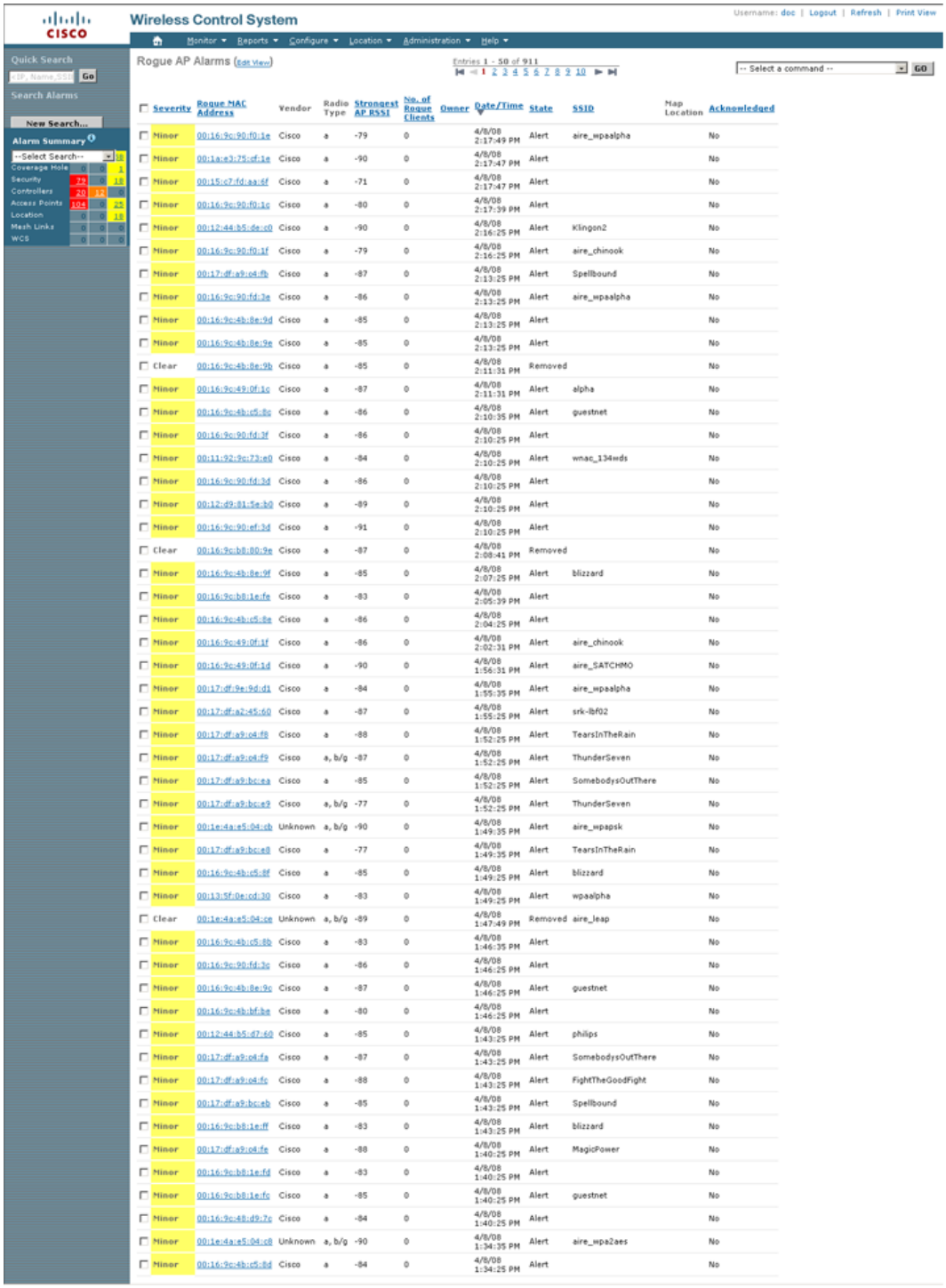
Cisco Wired IPS Events

A value is provided for last hour, last 24 hours, and all. If you click an underlined number in any of the time period categories, a window with further information appears.

Monitoring Rogue Access Point

If you choose **Rogue APs** from the left sidebar menu (of the **Monitor > Security** page), the Rogue AP Alarms window appears (see Figure 6-4). This window allows you to view alarm details and messages regarding any anomalies with the controllers and access points.

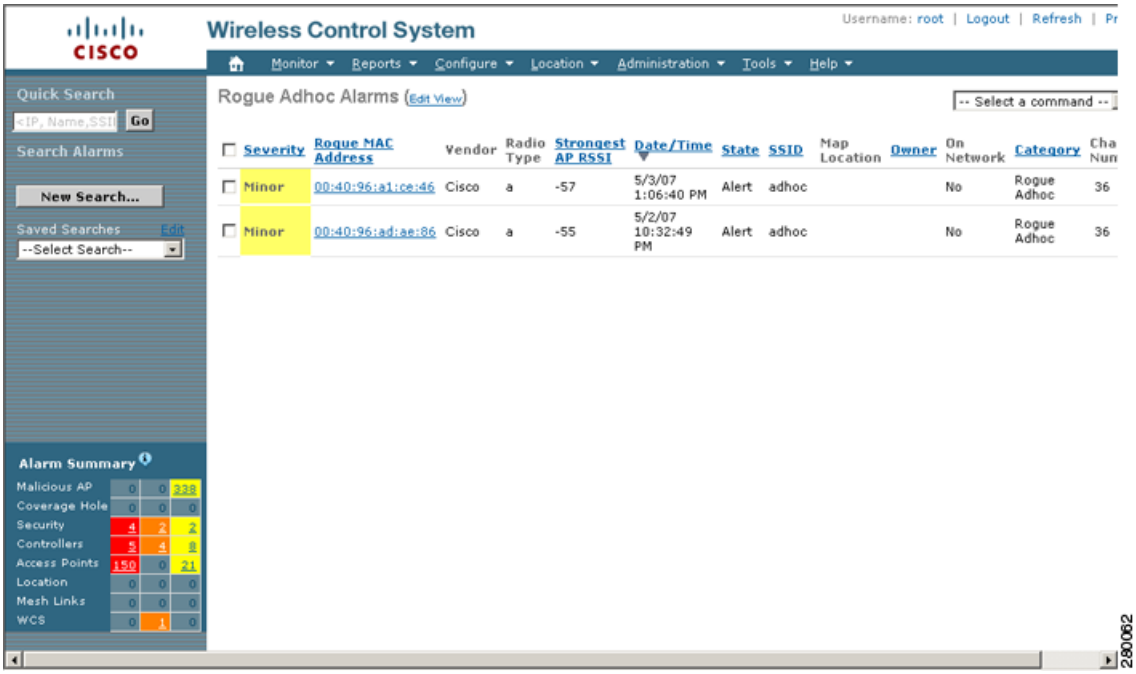
Figure 6-4 Rogue AP Alarms



Monitoring Rogue Adhoc

If you choose **Rogue Adhocs** from the left sidebar menu (of the **Monitor > Security** page), the Rogue Adhoc Alarms window appears (see Figure 6-5). On this window you can view details of rogue adhoc alarms.

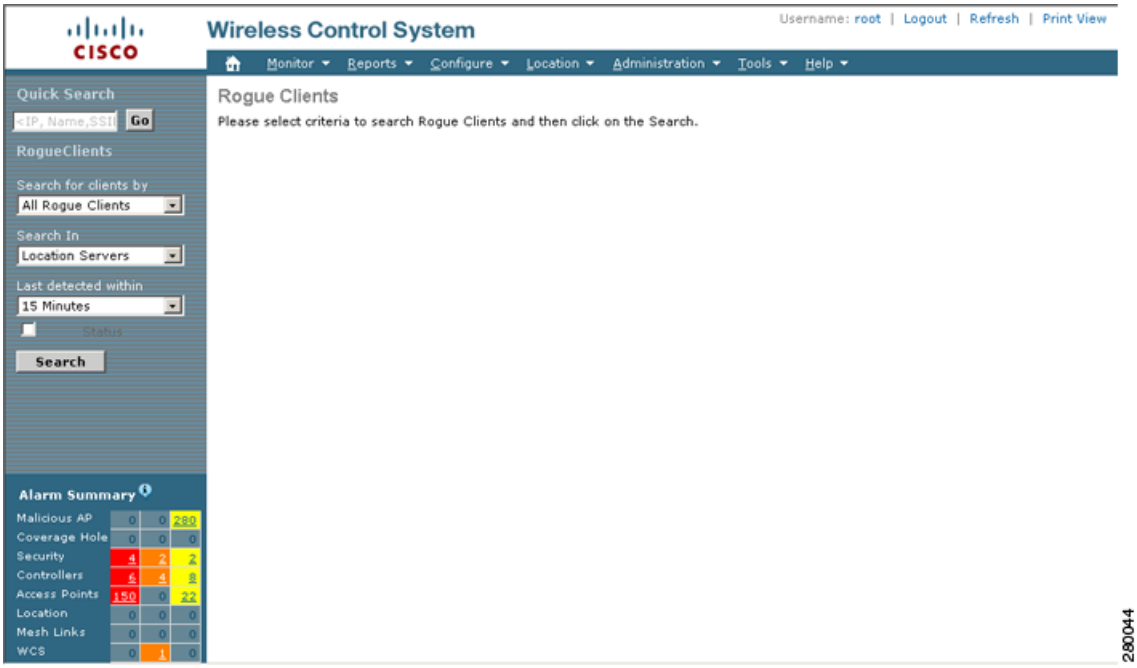
Figure 6-5 Rogue Adhoc Alarms Window



Monitoring Rogue Clients

If you choose **Rogue Clients** from the left sidebar menu (of the **Monitor > Security** page), the Rogue Clients window appears (see Figure 6-6). You can select search criteria in the left sidebar menu and then details about the rogue clients that are found is displayed.

Figure 6-6 Rogue Clients Window



Monitoring Shunned Clients

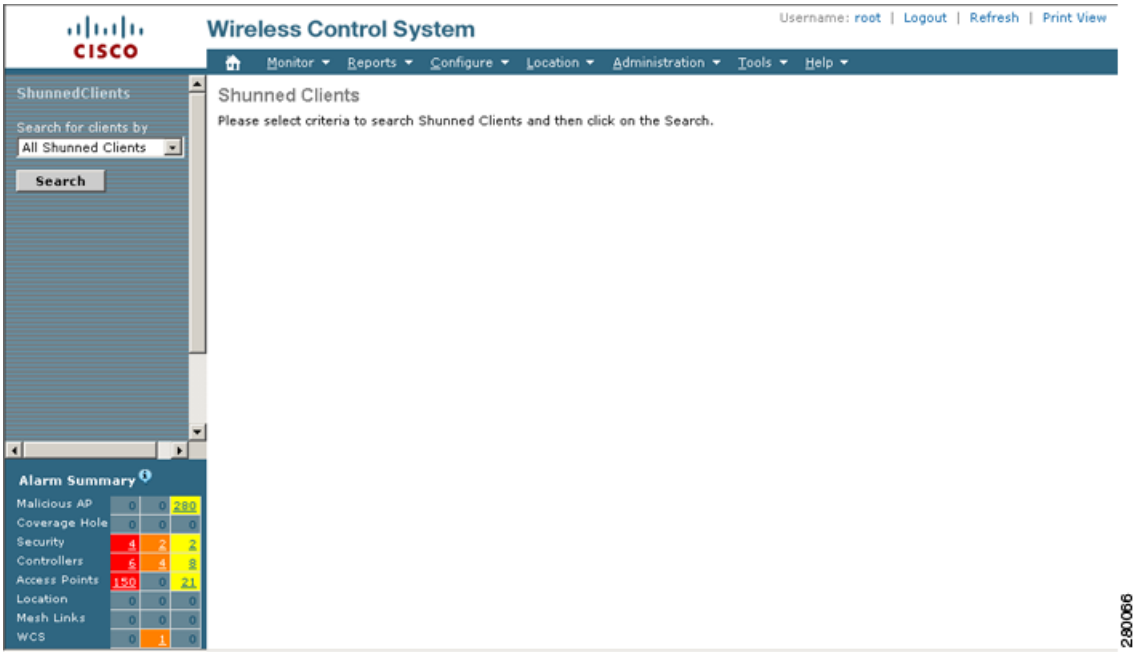
When a Cisco IPS sensor on the wired network detects a suspicious or threatening client, it alerts the controller to shun this client. If the client to be shunned is currently associated to an access point and controller in a mobility group:

1. The shun entry is distributed to all controllers within the same mobility group.
2. The anchor controller adds this client to the dynamic exclusion list.
3. The foreign controller removes the client.

The next time the client tries to connect to a controller, the anchor controller rejects the handcuff and informs the foreign controller that the client is being excluded.

Choose **Monitor > Security** from the left sidebar menu and select **Shunned Clients** to access this window (see Figure 6-7).

Figure 6-7 Shunned Clients Window



The Shunned Client window displays the client IP address, sensor IP address, and the controller for each shunned client.

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

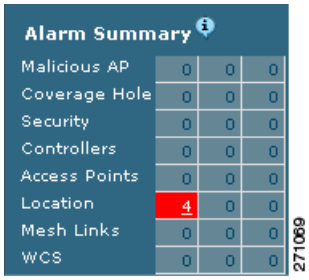
– Tag rogue access points as contained and discourage clients from associating with the rogue access points by having between one and four access points transmit deauthenticate and disassociate messages to all rogue access point clients. This function applies to all active channels on the same rogue access point.

Detecting and Locating Rogue Access Points

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.

When WCS receives a rogue access point message from a controller, an alarm monitor appears in the lower left corner of all WCS user interface pages. The alarm monitor in Figure 6-8 shows 199 rogue access point alarms.

Figure 6-8 Alarm Monitor for Rogue Access Points



Follow these steps to detect and locate rogue access points.

Step 1 Click the **Rogues** indicator to display the Rogue AP Alarms page. This page lists the severity of the alarms, the rogue access point MAC addresses, the rogue access point types, the date and time when the rogue access points were first detected, and their SSIDs.

Step 2 Click any **Rogue MAC Address** link to display the associated Alarms > Rogue - *AP MAC Address* page. This page shows detailed information about the rogue access point alarm.

Step 3 To modify the alarm, choose one of these commands from the Select a Command drop-down menu and click **GO**.

- **Assign to me**—Assigns the selected alarm to the current user.
- **Unassign**—Unassigns the selected alarm.
- **Delete**—Deletes the selected alarm.
- **Clear**—Clears the selected alarm.
- **Event History—**Enables you to view events for rogue alarms.
- **Detecting APs** (with radio band, location, SSID, channel number, WEP state, short or long preamble, RSSI, and SNR)—Enables you to view the access points that are currently detecting the rogue access point.
- **Rogue Clients**—Enables you to view the clients associated with this rogue access point.
- Set State to ‘Unknown - Alert’—Tags the rogue access point as the lowest threat, continues to monitor the rogue access point, and turns off containment.

Set State to 'Known - Internal'—Tags the rogue access point as internal, adds it to the known rogue access points list, and turns off containment.

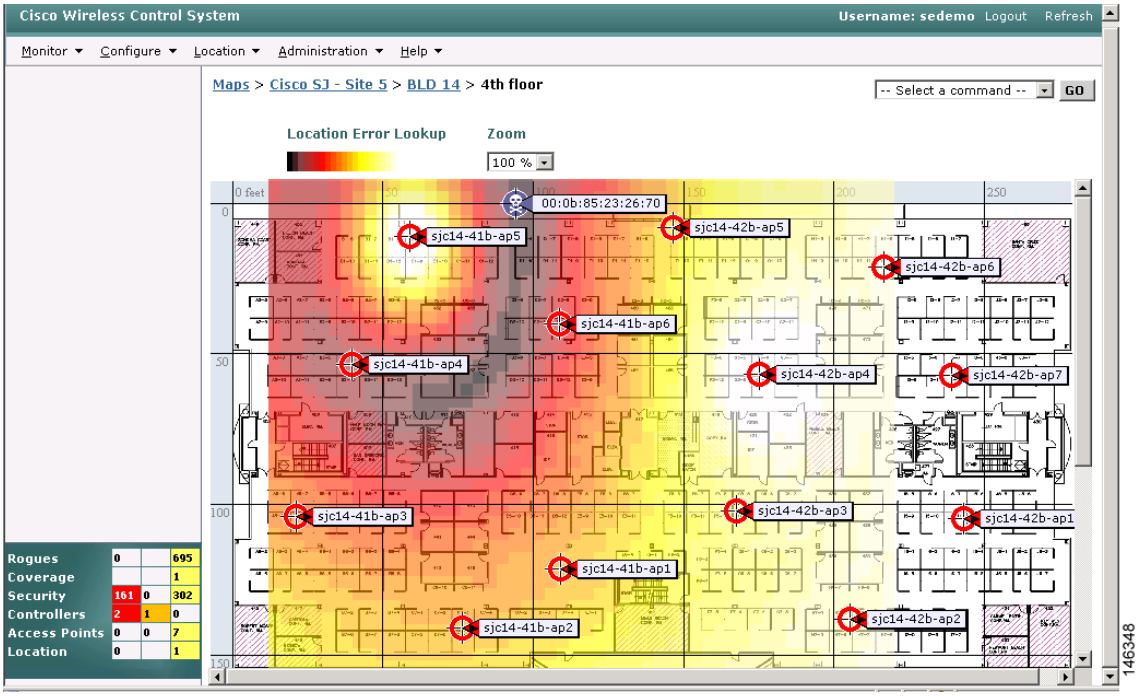
Set State to 'Known - External'—Tags the rogue access point as external, adds it to the known rogue access points list, and turns off containment.

- **1 AP Containment** through **4 AP Containment—**When you select level 1 containment, one access point in the vicinity of the rogue unit sends deauthenticate and disassociate messages to the client devices that are associated to the rogue unit. When you select level 2 containment, two access points in the vicinity of the rogue unit send deauthenticate and disassociate messages to the rogue's clients and so on up to level 4.

Step 4 From the Select a Command drop-down menu, choose **Map (High Resolution)** and click **GO** to display the current calculated rogue access point location on the Maps > *Building Name* > *Floor Name* page.

If you are using WCS Location, WCS compares RSSI signal strength from two or more access points to find the most probable location of the rogue access point and places a small skull-and-crossbones indicator at its most likely location. In the case of an underdeployed network for location with only one access point and an omni antenna, the most likely location is somewhere on a ring around the access point, but the center of likelihood is at the access point. If you are using WCS Base, WCS relies on RSSI signal strength from the rogue access point and places a small skull-and-crossbones indicator next to the access point receiving the strongest RSSI signal from the rogue unit. Figure 6-9 shows a map that indicates that location of a rogue unit.

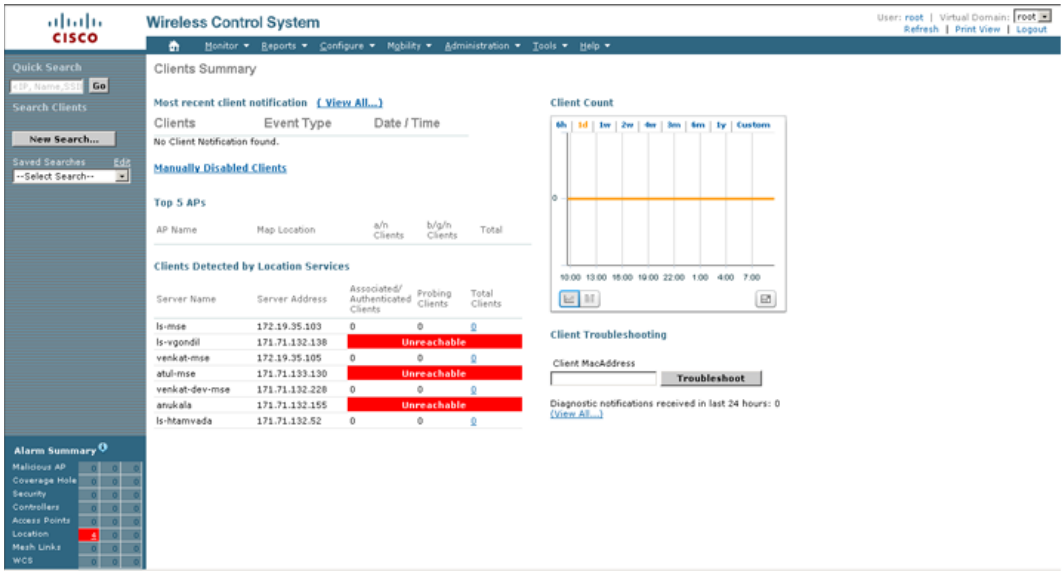
Figure 6-9 Map Indicating Location of Rogue Unit



Monitoring Clients

This section provides access to the controller clients summary details. The information assists in identifying, diagnosing, and resolving client issues. To monitor clients, choose **Monitor > Clients**. The Client Summaries window appears (see Figure 6-10).

Figure 6-10 Clients Summary



The Client Summaries window contains the following portions:

Most Recent Client Notification

- Client—IP address, MAC address, or user-defined name of client.
- Event Type—Reason for client notification. For example, disassociated, WEP decrypt error, or authentication failure.
- Date/Time—Date and time of client notification.

Manually Disabled Clients

Choose **Monitor > Clients** and then click **Manually Disabled Clients** to access this page.

This page enables you to view manually disabled client template information.

- MAC Address—Client MAC address.
- Description—Optional user-defined description.

Top 5 APs

The Top 5 APs section includes the following:

- AP Name—This is the name assigned to the access point. Click an item in the list to see the details of that access point.
- Map Location —The name of the map where the client is located.

- a/n Clients—The number of 802.11a clients currently associated with the controller.
- b/g/n Clients—The number of 802.11b clients and 802.11g clients currently associated with the controller.
- Total Client—Total number of clients currently associated with the controller.

Clients Detected by Location Servers

Displays clients detected by location servers within the last 15 minutes.

- Server Name—User-defined location server name.
- Server Address—IP address of location server.
- Total Clients—Total number of clients currently associated with the location server.

Client Count

A graphic shows the associated clients during a given time frame.

Client Troubleshooting

Client—Enter the IP address, MAC address, or user-defined client name and click **Troubleshoot** to continue to the client details.

Diagnostic Notification Received—Indicates the number of diagnostic notifications received. Click the number to view the list of the diagnostic events.

WLAN Client Troubleshooting

The client reporting protocol is used by the client and the access point to exchange client information. Client reports are collected automatically when the client associates. Follow these steps to run diagnostic tests and reports and to view available logs:

Step 1 Choose **Monitor > Clients**.

Step 2 (optional) In the Quick Search area, type the MAC address of the client in question.

Note To get the current status of the client, you must instead click **New Search** and choose the **Search on Controller Now** option. This option more accurately reflects the 802.11 state of the client because a quick search only periodically updates the database information.

Step 3 To troubleshoot a client, enter the MAC address of the client in the Client field and click **Troubleshoot**. The troubleshooting client options appear (see Figure 6-11).The number of tabs that appear depends on whether the client is a Cisco Compatible Extensions version 5 client or not. The Cisco Compatible Extensions Version 5 clients contain additional tabs like Test Analysis, Messaging, Event Log, and so on. If the MAC address is unknown, enter search criteria of the client (such as user name, floor, and so on) in the Quick Search of the left-hand menu.

Figure 6-11 Troubleshooting Client Tab

The summary page displays a brief description of the problem and recommends a course of action to resolve the issue.

Note Some Cisco Compatible Extension features do not function properly if you use a web browser other than Internet Explorer 6.0 on a Windows workstation.

Step 4 To view log messages logged against the client, click the **Log Analysis** tab (see Figure 6-12).

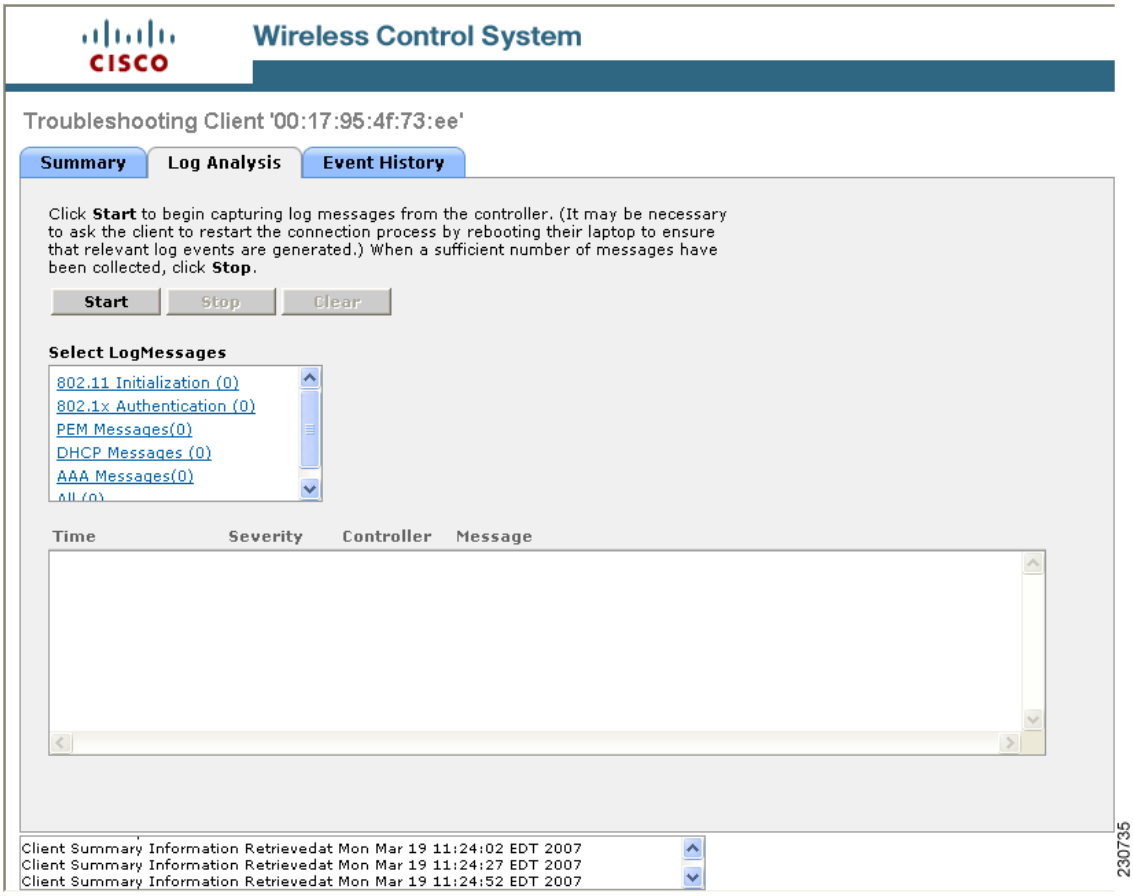
Step 5 To begin capturing log messages about the client from the controller, click **Start**. To stop log message capture, click **Stop**. To clear all log messages, click **Clear**.

Note Log messages are captured for ten minutes and then stopped automatically. A user must click **Start** to continue.

Step 6 To select which 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. It includes the following information:

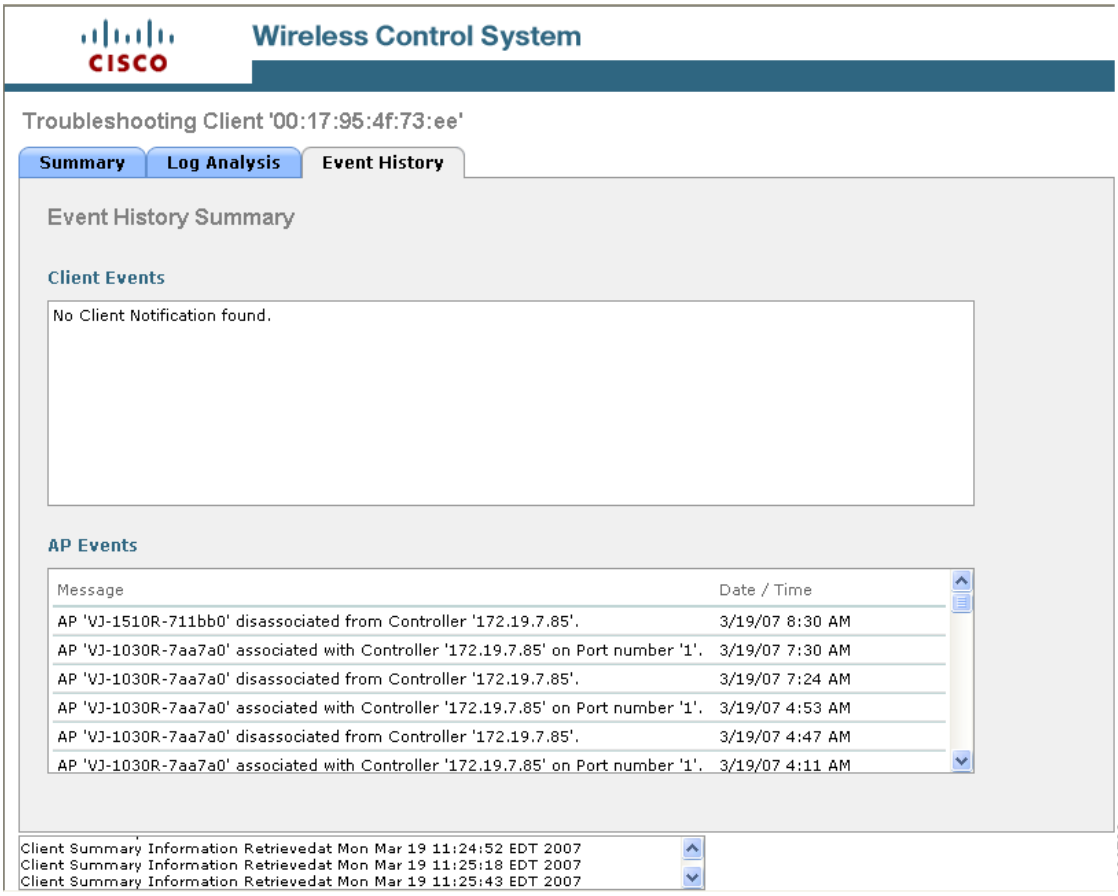
- A status message
- The controller time
- A severity level of info or error (errors are displayed in red)
- The controller to which the client is connected

Figure 6-12 Log Analysis Tab



Step 7 To display a summary of the client's events history, click the **Event History** tab (see Figure 6-13). This page displays client and access point events that occurred within the last 24 hours.

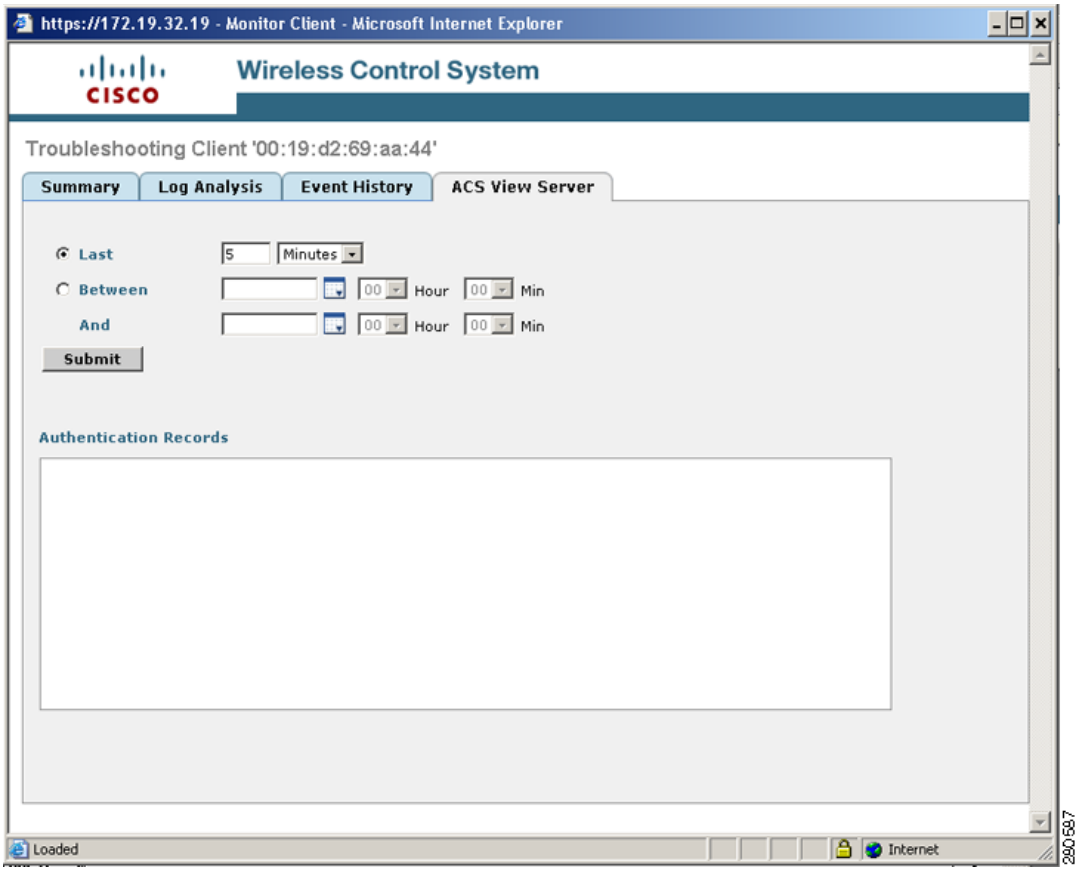
Figure 6-13 Event History Tab



Step 8 If you click the ACS View Server tab, you can inteface with the Cisco Access Control (ACS) System View Server (see Figure 6-14). 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.) Refer to the "Configuring ACS View Server Credentials" section on page 6-34 for steps on establishing credentials.

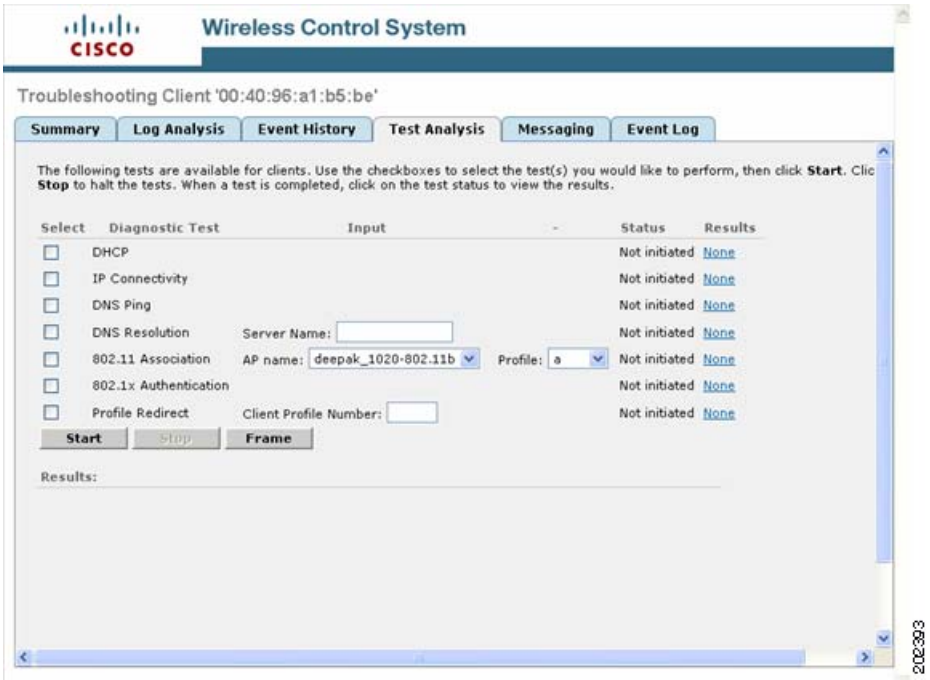
This server provides WCS with aggregated client status information from multiple ACS servers. The client status information allows you to further troubleshoot client issues and determine if they are related to authentication or authorization. Enter the date and time ranges to retrieve the historical authentication and authorization information and click **Submit**. The results of the query are displayed in the Authentication Records portion of the window and is used as a filter for the userid logged into the client.

Figure 6-14 ACS View Server Window



Step 9 (Optional) If Cisco Compatible Extension Version 5 clients are available, a Test Analysis tab as shown in Figure 6-15 appears.

Figure 6-15 Test Analysis Tab



Step 10 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 input information (if applicable), and click **Start**. The following diagnostic tests are available:

- DHCP—Executes a complete DHCP Discover/Offer/Request/ACK exchange to determine that the DHCP is operating properly between the controller and the client.
- IP Connectivity—Causes the client to execute a ping test of the default gateway obtained in the DHCP test to determine that IP connectivity exists on the local subnet.
- DNS Ping—Causes the client to execute a ping test of the DNS server obtained in the DHCP test to determine that IP connectivity exists to the DNS server.
- DNS Resolution—Causes the DNS client to attempt to resolve a network name known to be resolvable to determine that name resolution is functioning correctly.
- 802.11 Association—Directs an association to be completed with a specific access point to determine that the client is able to associate properly with a designated WLAN.
- 802.1X Authentication—Directs an association and 802.1X authentication to be completed with a specific access point to determine 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 6-16 appears. Use this tab to send an instant text message to the user of this client. From the Message Category drop-down menu, choose a message and click **Send**.

Figure 6-16 Messaging Tab

Step 12 Close the Troubleshooting Client window. The **General** tab displays the client details and properties of the access point with which the client is associated. Table 6-8, Table 6-9, and Table 6-10 describe the fields displayed on this General tab.

Table 6-8 General Tab / Client Properties

Parameter	Description
Client User Name	The username the client used for authentication.
Client IP Address	The IP address of the client.
Client MAC Address	The MAC address of the client.
Client Vendor	The client's vendor information.
Controller	The IP address of the controller to which the client is registered. Clicking the controller's IP address displays information about the controller.
Port	The port on the controller to which the client is connected.

Table 6-8 General Tab / Client Properties (continued)

Parameter	Description
802.11 State	802.11 state may be one of the following: • Idle (0)— normal operation: no rejections of client association requests • AAA Pending (1)— completing an AAA transaction • Authenticated (2)— 802.11 authentication completed • Associated (3)— 802.11 association completed • Power Save (4)— client in power save mode • Disassociated (5)— 802.11 disassociation completed • To Be Deleted (6)— to be deleted after disassociation • Probing (7)— client not associated or authorized yet
Interface	The name of the interface to which the client is connected.
VLAN ID	The client has successfully joined an access point for the given SSID. VLAN ID is the reverse lookup of the interface used by the WLAN on the controller side.
802.11 State	The client's state: • Idle— Normal operation; no rejections of client association requests • AAA Pending— Completing an AAA transaction • Authenticated— 802.11 association completed • Associated— 802.11 association completed • Power Save— Client in power save mode • Disassociated— Disassociation completed • To Be Deleted—To be deleted after disassociated • Probing—Client not associated or authorized yet • Blacklisted—Automatically disabled by the system due to perceived security threats
Mobility Role	Local, Anchor, Foreign, Export Anchor, Export Foreign.
Policy Manager State	Internal state of the client's WLAN. Client is working properly when the state is RUN.
Anchor Address	N/A when the client is Local (has not roamed from its original subnet). Anchor IP Address (the IP Address of the original controller) when the client is Foreign (has roamed to another controller on a different subnet). Foreign IP Address (the IP Address of the original controller) when the client is Anchor (has roamed back to another controller on a different subnet).
Mirror Mode	Disable or enable.

Table 6-8 General Tab / Client Properties (continued)

Parameter	Description
Cisco Compatible Extension	Indicates the Cisco Compatible Extension version, if client supports it
E2E	Indicates if E2E is supported.
WGB Status	Indicates the workgroup bridge status as regular client, WGB client, or WGB. If a client is a regular client, the WGB MAC address is not shown. If a client is a workgroup bridge, the state is WGB, and the MAC address is shown. A WGB is a mode that can be configured on an autonomous IOS access point to provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the WGB access point. A WGB connects a wired network over a single wireless segment by learning the MAC addresses of its wired clients on the Ethernet interface and reporting them to the lightweight access point using Internet Access Point Protocol (IAPP) messaging.

Table 6-9 General Tab / RF Properties (read only)

Parameter	Description
AP Name	The name of the access point to which the client is associated. Clicking the link displays information about the access point.
AP Type	The type of access point.
AP Base Radio MAC	The MAC address of the access point's base radio.
Protocol	The protocol used by the radio (802.11a/n or 802.11b/g/n).
AP Mode	The access point mode.
Profile Name	The profile name of the WLAN that the client is associated to or is trying to associate to.
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 is different.
Security Policy	The WLAN security policy that is used.
Association Id	Client's access point association identification number.

Table 6-9 General Tab / RF Properties (read only) (continued)

Parameter	Description
Reason Code	The client reason code may be one of the following: • Normal (0) — Normal operation. • Unspecified reason (1) — Client associated but no longer authorized. • PreviousAuthNotValid(2) — Client associated but not authorized. • DeauthenticationLeaving (3) — The access point went offline, deauthenticating the client. • DisassociationDueToInactivity (4) — Client session timeout exceeded. • DisassociationAPBusy(5) — The access point is busy, performing load balancing, for example. • Class2FrameFromNonAuthStation (6) —Client attempted to transfer data before it was authenticated. • Class2FrameFromNonAssStation (7) — Client attempted to transfer data before it was associated. • DisassociationStnHasLeft (8) — Controller moved the client to another access point using non-aggressive load balancing. • StaReqAssociationWithoutAuth (9) — Client not authorized yet, still attempting to associate with a Cisco WLAN Solution. • Missing Reason Code (99) — Client momentarily in an unknown state.
802.11 Authentication	Which 802.11 authentication algorithm is in force.

Table 6-10 General Tab / Security

Parameter	Description
Authenticated	Indicates whether the client has been authenticated.
Policy Type	The type of security policy used by the client.
Encryption Cipher	Encryption settings.
EAP Type	Type of Extensible Authentication Protocol (EAP) used.

Step 13 To obtain additional troubleshooting information and perform additional diagnostics tests, choose a command from the drop-down menu and click **GO**.

a. To test the link between the client and the access point to which it is associated, choose **Link Test** from the drop-down menu and click **GO**.

b. To disable XYZ, choose **Disable** from the drop-down menu and click **GO**.

c. To remove XYZ, choose **Remove** from the drop-down menu and click **GO**.

d. To enable the Mirror mode, choose **Enable Mirror Mode** from the drop-down menu and click **GO**.

e. To display a high-resolution map of the client's recent location, choose **Recent Map** (**High Resolution**) from the drop-down menu and click **GO**.

f. To display a high-resolution map of the client's present location, choose **Present Map (High Resolution)** from the drop-down menu and click GO.

g. To display a graph showing a history of the client-to-access point associations, choose **AP Association History Graph** from the drop-down menu and click **GO**.

h. To display a table showing a history of the client-to-access-point associations, choose **AP Association History Table** from the drop-down menu and click **GO**.

i. To display information about the reasons for client roaming, choose **Roam Reason** from the drop-down menu and click **GO**.

j. To display details of access points that can hear the client, including at which signal strength/SNR, choose **Detecting APs** from the drop-down menu and click **GO**.

k. To display the history of the client location based on RF fingerprinting, choose **Location History** from the drop-down menu and click **GO**.

l. To display client voice matrix, choose **Voice Metrics** from the drop-down menu and click **GO**.

Step 14 To display client statistics, click the **Statistics** tab (see Figure 6-17).

This page displays four graphs:

- Client RSSI History (dBm)— History of RSSI as detected by the access point to which the client is associated
- Client SNR History— History of SNR as detected by the access point to which the client is associated
- Bytes Sent and Received (Kb/s)— The bytes sent and received by the client from the access point to which it is associated
- Packets Sent and Received (per sec.)—The packets sent and received by the client from the access point to which it is associated

Table 6-11 describes the fields displayed on this Statistics tab.

Figure 6-17 Statistics Tab

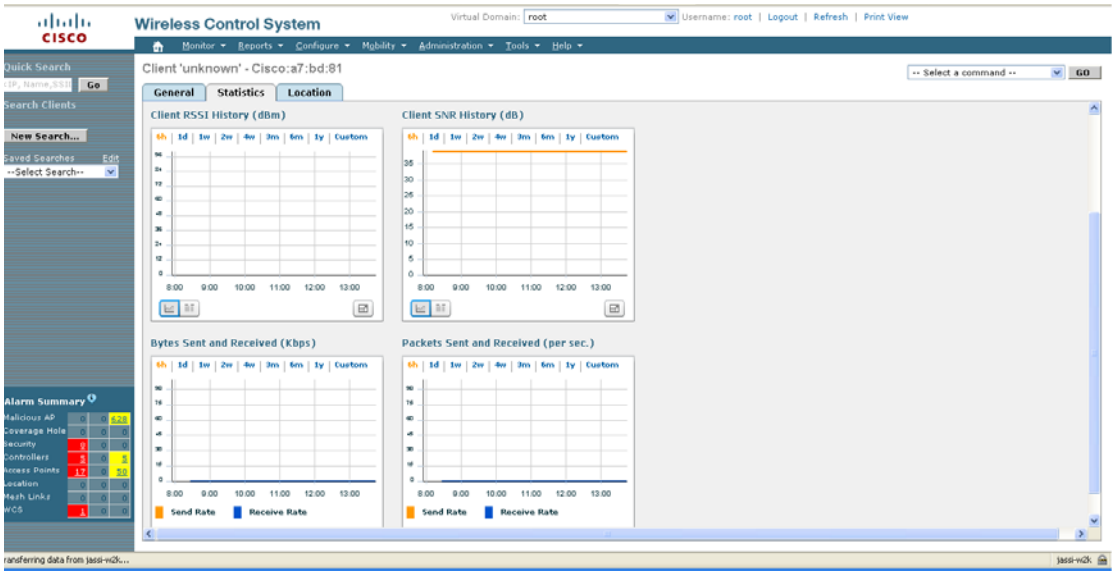


Table 6-11 Statistics Tab / Client Statistics

Parameter	Description
RSSI	Receive signal strength indicator of the client RF session.
SNR	Signal to noise ratio of the client RF session.
Bytes Sent and Received	Total number of bytes sent to the client and received by the controller from the client.
Packets Sent and Received	Total number of packets sent to the client and received by the controller from the client.
Client RSSI History (dBm)	History of RSSI as detected by the access point with which the client is associated.
Client SNR History	History of SNR as detected by the access point with which the client is associated.

Step 15 To display the client's location information, click the **Location** tab (see Figure 6-18). Table 6-12 describes the fields displayed on this Location tab.

Figure 6-18 Location Tab

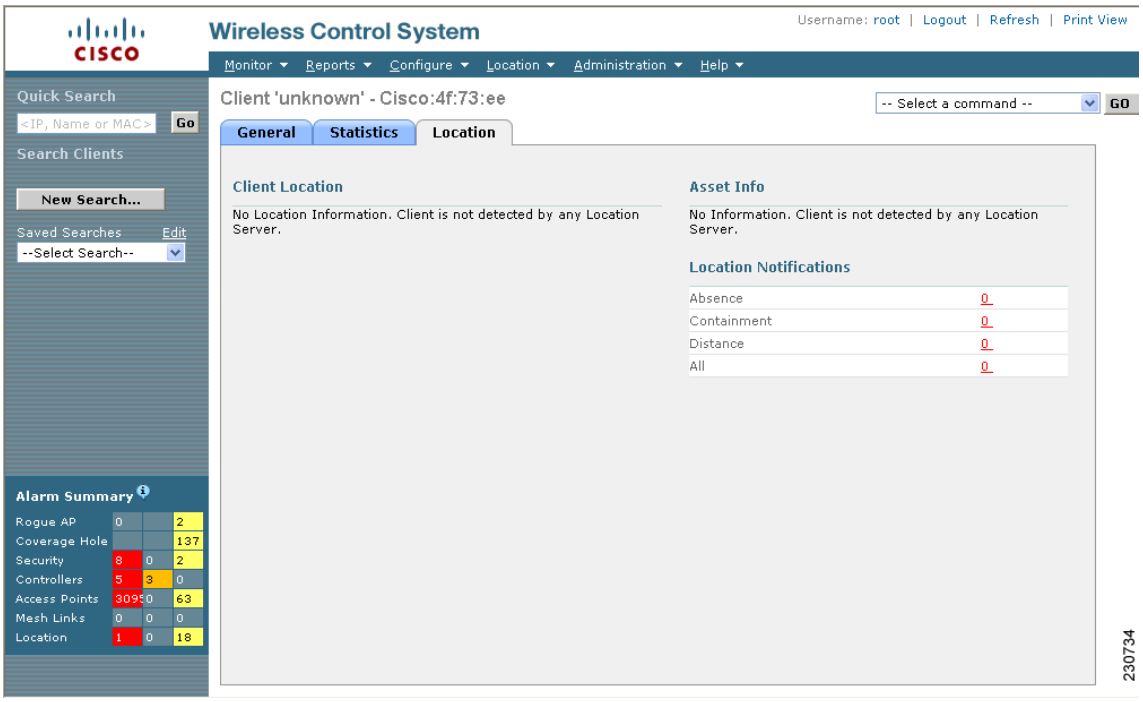


Table 6-12 Location Tab

Parameter	Description
Client Location	Describes the location of the client in the map based on RF fingerprinting.
Asset Information	Describes the asset file destination and name.that
Location Notifications	Displays the number of location notifications logged against the client. Clicking a link displays the notifications.
Absence	The location server generates absence events when the monitored assets go missing. In other words, the location server cannot see the asset in the WLAN for the specified time.
Containment	The location server generates containment events when an asset is moved inside or outside of a designated area. **Tip** You define a containment area (campus, building, or floor) here. You can define a coverage area using the Map Editor.
Distance	The location server generates movement events when an asset is moved beyond a specified distance from a designated marker you define on a map.
All	The total of absence, containment, and distance notifications.

Step 16 Click the **Cisco Compatible Extension (version 5) Info** tab. Reports specific to compatible clients provide client details that enhance client diagnostics and troubleshooting. Table Table 6-13 describes the parameters on the Manufacturer Information portion of the Cisco Compatible Extension (version 5) Info tab.

Note The Cisco Compatible Extensions (version 5) manufacturing information displays for compatible clients only.

- Automated Troubleshooting Report—Displays the automated troubleshooting file.

Note You must click **Export** to save the .zip file. The file contains three logs: automated troubleshoot report, frame log, and watch list log.

Table 6-13 Manufacturer Information

Parameter	Description
Organizationally Unique Identifier	The IEEE assigned organizational unique identifier, for example the first 3 bytes of the MAC address of the wireless network connected device.
ID	The manufacturer identifier of the wireless network adapter.
Model	Model of the wireless network adapter.
Serial Number	Serial number of the wireless network adapter.
Radio	Radio type of the client.
MAC Address	MAC address assigned to the client.
Antenna Type	Type of antenna connected to the wireless network adapter.
Antenna Gain	The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means 4 x 0.5 = 2 dBm of gain.
Radio Receiver Sensitivity	
Provides the receiver sensitivity of the each wireless network adapter. It shows the minimum and maximum RSSI for each radio type as well as the data rate.	
CCXV5 Capability Information	
Lists the client status and service capability of the Cisco Compatible Extensions version 5 clients.	
Radio Channels	
Lists all channels used by each radio.	
Transmit Data Rates	
Lists all data rates used by each radio.	

Table 6-14 describes the parameters displayed in the Cisco Compatibility Extensions (version 5) Capability Information portion of the tab.

Note The Cisco Compatible Extensions (version 5) capability information displays for compatible extension clients only.

Table 6-14 Client Statistics

Parameter	Description
Bytes Sent and Received (Kb/s)	Bytes sent and received with the associated access point.
Packets Sent and Received (per second)	Packets sent and received with the associated access point.

Step 17 To display the client's workgroup bridge information, click the **WGB Clients** tab. Table 6-15 describes the fields that display on this WGB tab.

Table 6-15 WGB Clients Tab

Parameter	Description
User	The user name assigned to the work group bridge.
IP Addr	The IP address of the workgroup bridge.
MAC Addr	The MAC address of the workgroup bridge.
802.11 State	Specifies whether the workgroup bridge is associated or not.

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 Only ACS View 4.1 is supported.

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**.

Enabling Automatic Client Troubleshooting

The Settings > Client page allows you to enable automatic client troubleshooting on a diagnostic channel. This feature is only available for Cisco Compatible Extension clients version 5.

Follow these steps to enable automatic client troubleshooting.

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Client**.

Step 3 Choose the Automatically troubleshoot client on diagnostic channel check box.

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.

Step 4 Click **Save**.

Finding Clients

Follow these steps to use WCS to find clients on your wireless LAN.

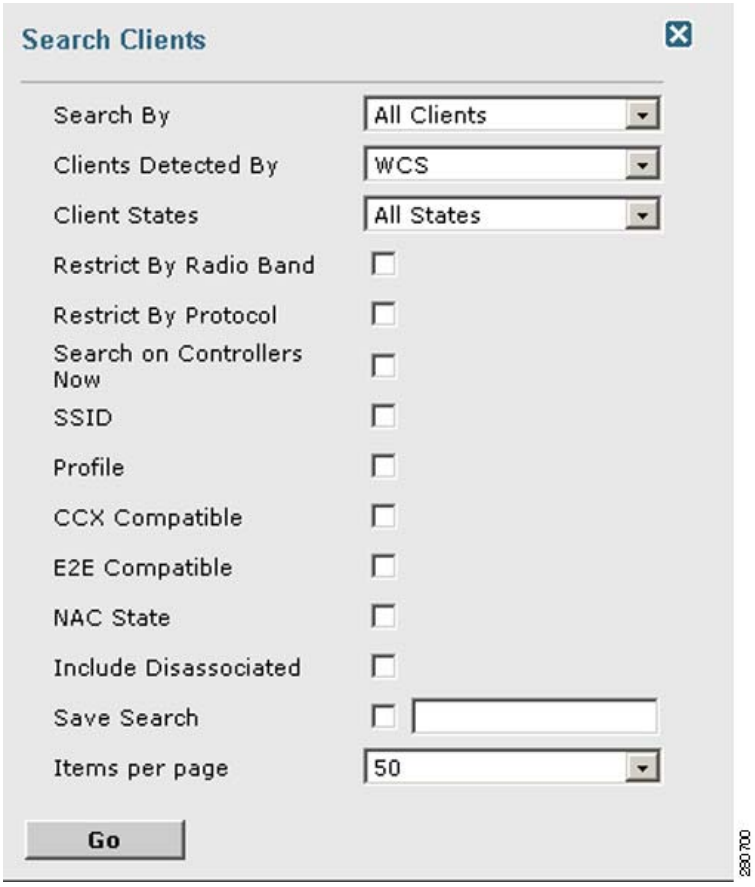
Step 1 Click **Monitor > Clients** to navigate to the Clients Summary page.

Step 2 The sidebar area enables you to select a new configuration panel under the menu area that you have selected. You can make only one choice. The selector area options vary based on the menu that you select.

- **New Search** drop-down menu: Opens the Search Clients window. Use the Search Clients window to configure, run, and save searches.
- **Saved Searches** drop-down menu: Lists the saved custom searches. To open a saved search, choose it from the Saved Searches list.
- **Edit link**: Opens the Edit Saved Searches window. You can delete saved searches in the Edit Saved Searches window.

Step 3 In the sidebar, click **New Search**. The Search Clients window appears (see Figure 6-19).

Figure 6-19 Search Clients



You can configure the following parameters in the Search clients window:

- Search By
- Clients Detected By — Choose WCS for clients stored in WCS that were detected through polling of the controllers from WCS. Choose Location Servers for clients stored on the location server that were detected by the location server through controller polling.
- Client States —Specify if you want to view clients only in a specific state such as idle, authenticated, associated, probing, or excluded.
- Restrict by Radio Band—To see the clients on a particular band, click the check box and choose 2.4GHz (802.11b/g or 802.11n) or 5 GHz (802.11a or 802.11n) from the drop-down menu.
- Restrict by Protocol—To restrict the search by protocol, choose 802.11a/n, 802.11b/n, and 802.11g/n from the drop-down menu.
- Search on Controllers Now—To search controllers rather than just the WCS database, click the check box. This search provides polling results in real time and delayed by 15 minutes, but it may take awhile to perform.
- SSID — To restrict the search by SSID, choose an SSID from the drop-down menu.
- Profile—To restrict the search by the profile that the client is using, click the check box and choose the profile name from the drop-down menu.
- CCX Compatible — To search for Cisco Compatible Extension compatible clients.

- E2E Compatible — To search for E2E compatible clients.
- NAC state—Click the check box and choose the client's network admission control state from the drop-down menu. The choices are invalid (the client is currently probing and not associated), quarantine (the client must go through posture analysis), and access (the client has completed posture analysis and is clean), and not applicable.
- Include Disassociated — To include clients that are no longer on the network but for which WCS has historical records.
- Save Search — To save the search in the Saved Searches drop-down menu.
- Items per page — The number of found items to display on the search results page.

Step 4 Choose **All Clients** in the Search By drop-down menu and click **GO.** The related search results window appears. The search results are listed.

Note You can search for clients under WCS Controllers or Location Servers.

Step 5 Click the username of the client that you want to locate. WCS displays the corresponding Clients *Client Name* page.

Note The Client RSSI History, Client SNR History, Bytes Sent and Received, and Packets Sent and Received reports are displayed. You can specify graph view or table view by clicking the appropriate icon. If it is a report where you can specify time period, enter both the start and end time or a specific time period.

Step 6 To find the client, choose one of these options from the Select a Command drop-down menu and click **GO**:

- **Recent Map (High Resolution)**—Finds the client without disassociating it.
- **Present Map (High Resolution)**—Disassociates the client and then finds it after reassociation. When you choose this method, WCS displays a warning message and asks you to confirm that you want to continue.

If you are using WCS Location, WCS compares the RSSI signal strength from two or more access points to find the most probable location of the client and places a small laptop icon at its most likely location. If you are using WCS Base, WCS relies on the RSSI signal strength from the client and places a small laptop icon next to the access point that receives the strongest RSSI signal from the client. Figure 6-20 shows a heat map that includes a client location.

Figure 6-20 Map with Client Location

Step 7 To view statistics for the selected client, click the **Statistics** tab.

Table 6-16 Client Statistics

Parameter	Description
Bytes received	Total number of bytes received by the controller from the client.
Bytes sent	Total number of bytes sent to the client from the controller.
Packets received	Total number of packets received by the controller from the client.
Packets sent	Total number of packets sent to the client from the controller.
Policy errors	Number of policy errors for the client.
RSSI	Receive signal strength indicator of the client RF session.
SNR	Signal-to-noise ratio of the client RF session.
Client RSSI History (dBm)	History of RSSI as detected by the access point with which the client is associated.
Client SNR History	History of SNR as detected by the access point with which the client is associated.
Bytes Sent and Received (Kb/s)	Bytes sent and received with the associated access point.
Packets Sent and Received (per second)	Packets sent and received with the associated access point.

Step 8 To generate a roam reason report, click **Roam Reason**. This reporting does not require any configuration.

Step 9 To generate a voice TSM report, click **Voice Metrics**.

Step 10 To generate a troubleshooting report, click **Troubleshoot**. You can choose a summary tab, a log analysis tab, or an event history tab.

Step 11 A test analysis generates the following results:

- DHCP—Verifies that DHCP is operating correctly between the controller and the client.
- IP Connectivity—Determines that IP connectivity exists on the local subnet. The IP connectivity test causes the client to execute a ping test to the default gateway.
- DNS Ping—Verifies that IP connectivity exists to the DNS server by having the client perform a ping test to the DNS server.
- DNS Resolution—Verifies that name resolution is functioning correctly. To test, the client tests a network name known to be resolvable, such as www.cisco.com.
- 802.1X Association—Determines that the client is able to associate properly with a designated WLAN and with a specific access point.
- 802.1X Authentication—Determines that the client is able to complete an 802.1X authentication with a designated WLAN and with a specific access point.

Receiving Radio Measurements

On the client window, 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 Clients column or enter a client in the Client Troubleshooting section on the bottom right and click **Troubleshoot**.

Step 3 From the Select a command drop-down menu, choose **Radio Measurement**.

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:

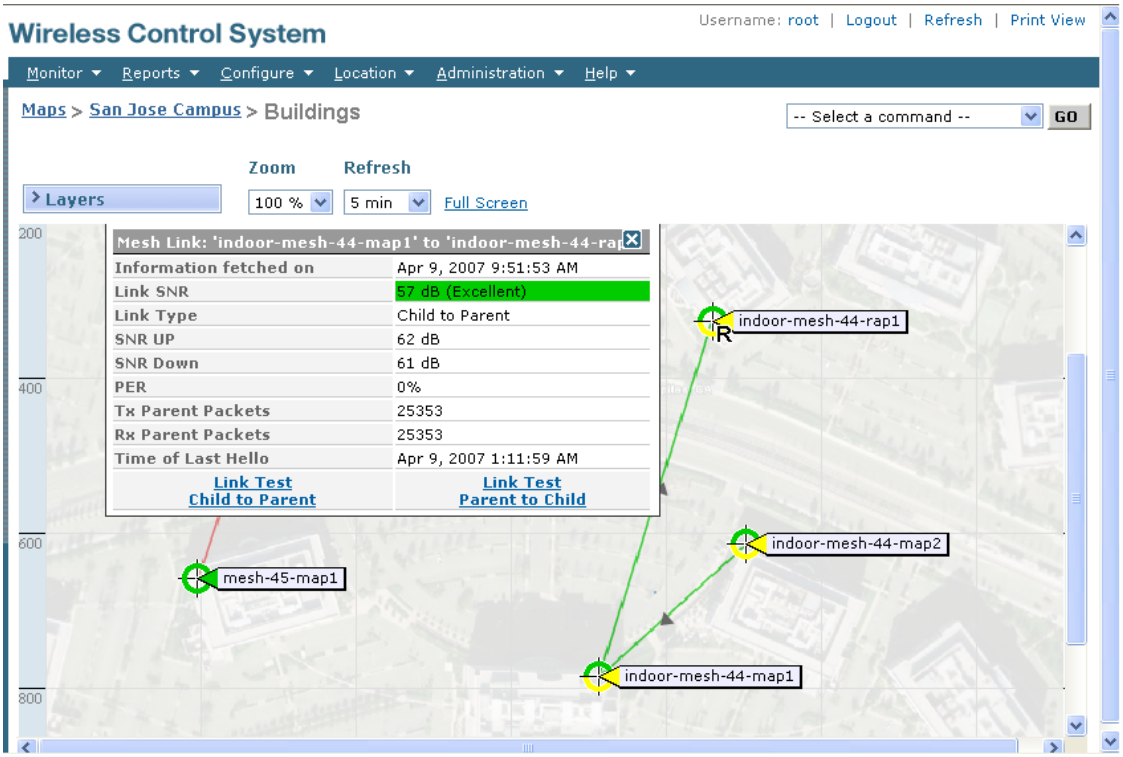
Step 1 In Cisco WCS, choose **Monitor > Maps**.

Step 2 Click the **Map Name** that corresponds to the outdoor area, campus, building, or floor you want to monitor.

Step 3 Move the cursor over the link arrow for the target link (see Figure 6-21). A Mesh Link window appears.

Note The AP Mesh Info check box under the Layers drop-down menu must be checked for links to appear on the map.

Figure 6-21 Mesh Link Details Window

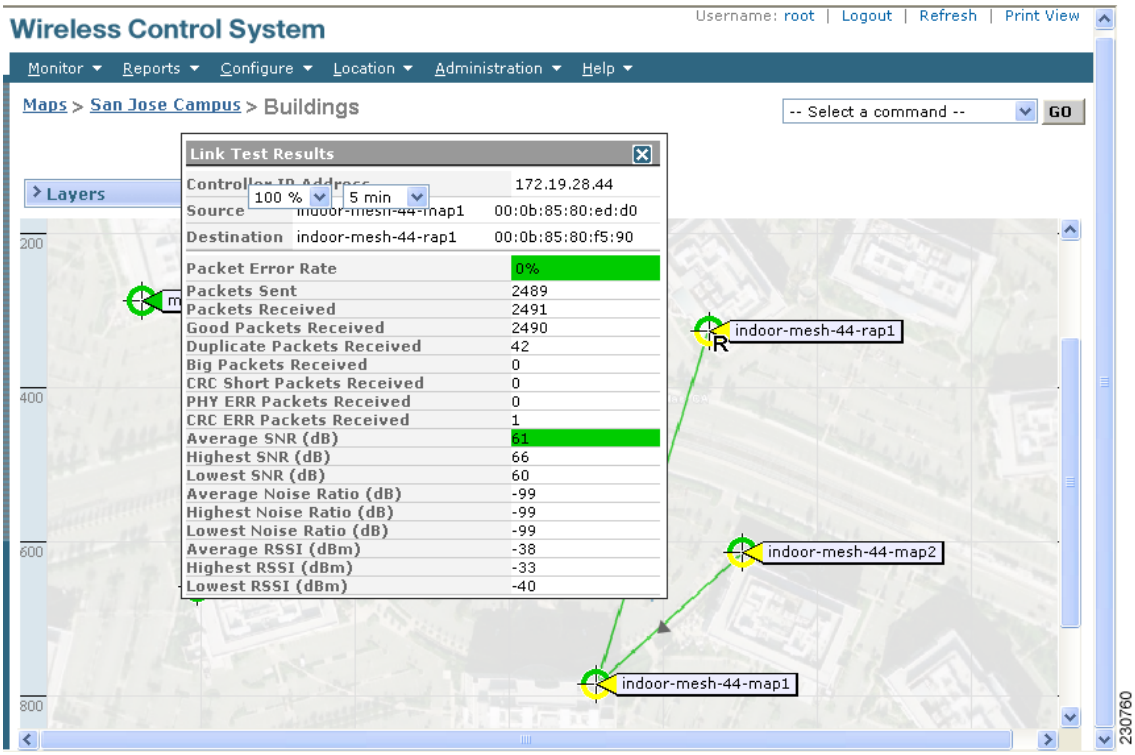


Step 4 Click either **Link Test**, **Child to Parent or Link Test**, or **Parent to Child**. After the link test is complete, a results page appears (see Figure 6-22).

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.

Figure 6-22 Link Test Results

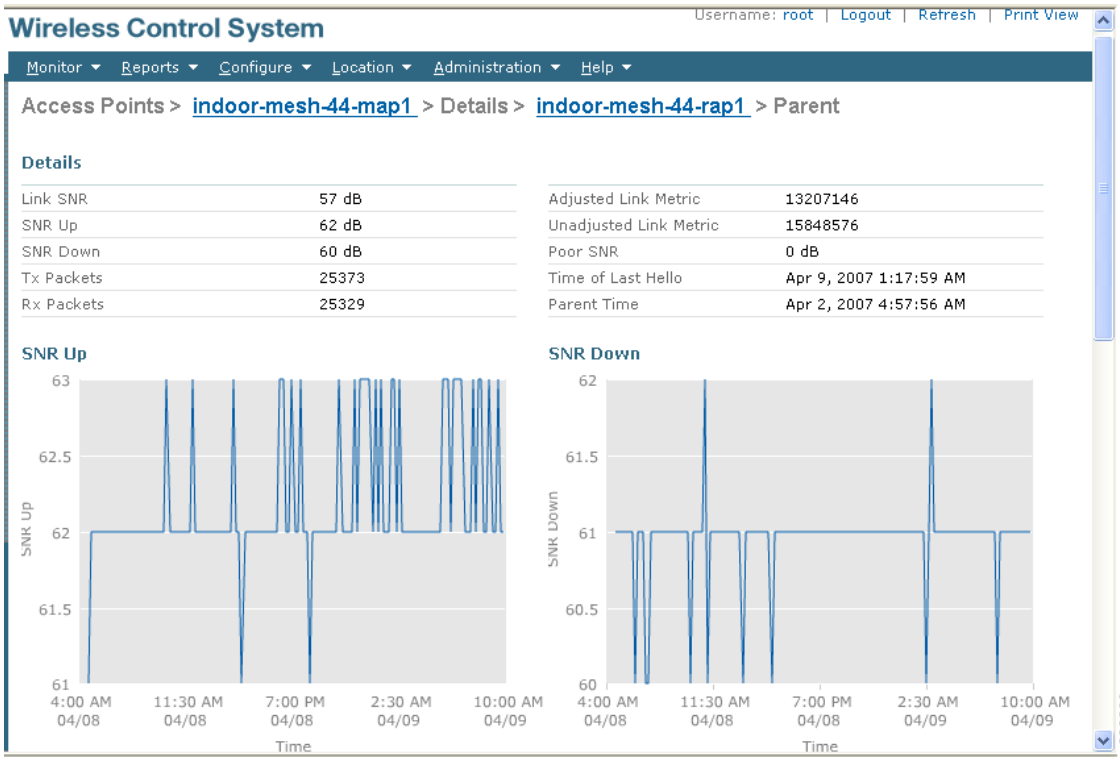


Step 5 To view a graphical representation of SNR statistics over a period of time, click the arrow on the link. A window with multiple SNR graphs appears (see Figure 6-23).

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 6-23 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 14-15.

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 window with configuration information for the selected access point appears (see Figure 6-24).

Figure 6-24 Mesh AP Summary Panel

Step 4 To view detailed configuration information for an access point, click the arrow portion of the mesh access point label. The configuration details for the access point appears (see Figure 6-25).

Note For more details on the View Mesh Neighbors link in the access point panel above, see the "Monitoring Mesh Access Point Neighbors Using Maps" section on page 6-45. 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 6-25 Mesh AP Detail Window

Step 5 At the Access Point configuration window, 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 and LWAPP 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 panel.

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 6-51.

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:

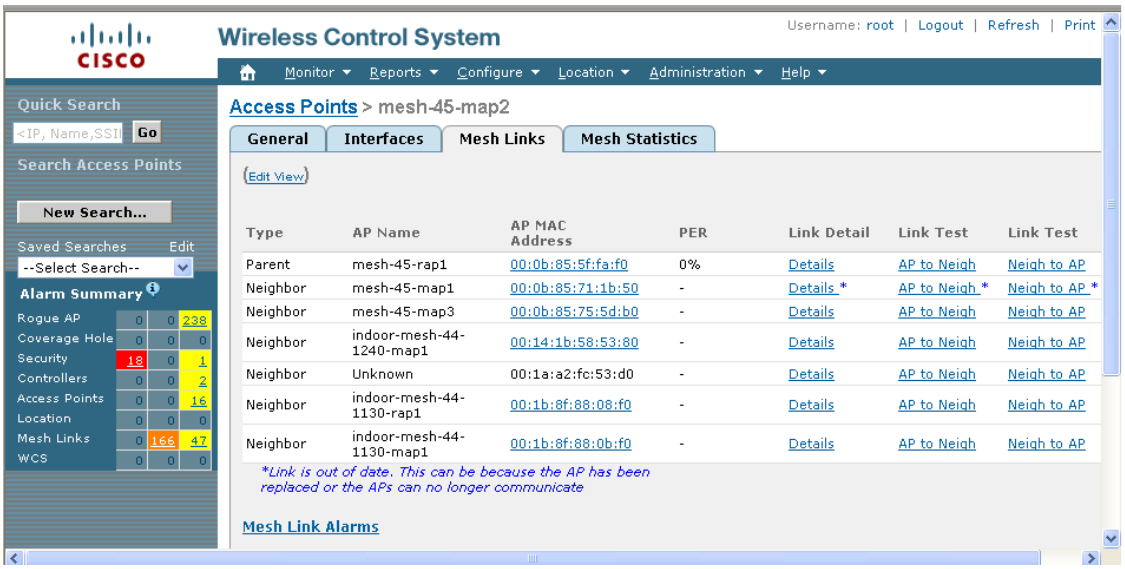
Step 1 In Cisco WCS, choose **Monitor > Maps**.

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 6-26).

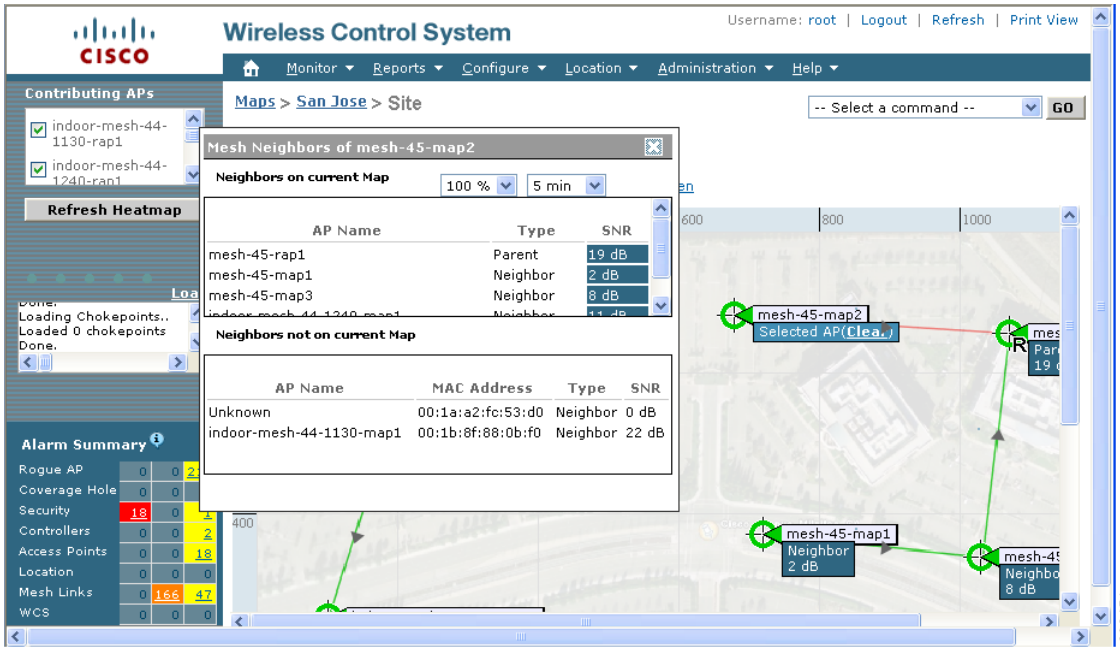
Figure 6-26 Access Points > Mesh Links Panel



Note You can also mesh link details for neighbors of a selected access point by clicking on the View Mesh Neighbors link on the access point configuration summary panel that displays when you mouse over an access point on a map (see Figure 6-25).

Note Signal-to-noise (SNR) only appears on the View Mesh Neighbors panel (see Figure 6-26).

Figure 6-27 View Mesh Neighbors Panel



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 menus at the top of the mesh neighbors window 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).

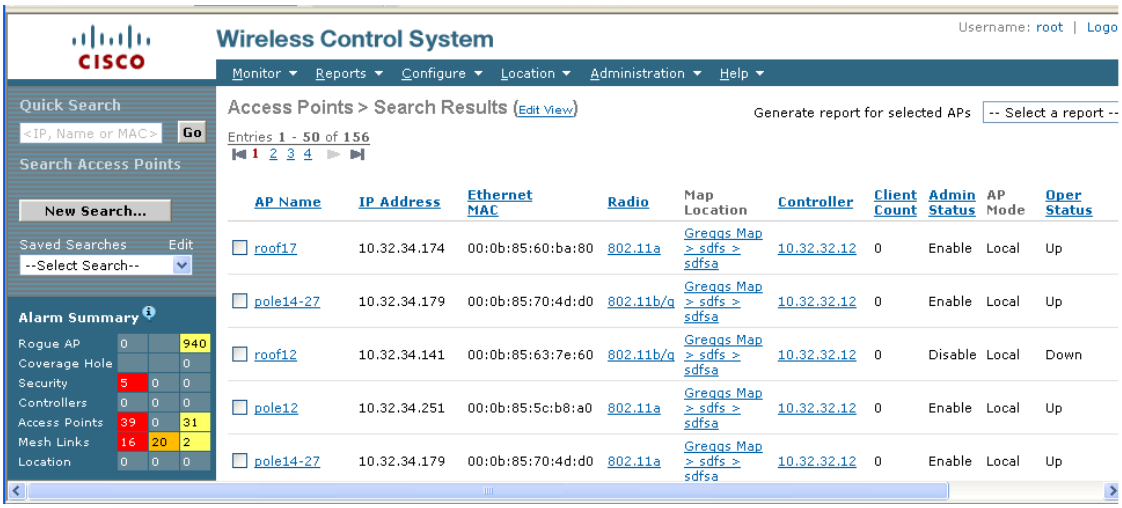
Mesh Health information is displayed in the General Properties panel for mesh access points.

To view the mesh health details for a specific mesh access point, follow these steps.

Step 1 Choose **Monitor > Access Points**. A listing of access points appears (see Figure 6-28).

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 6-28 Monitor > Access Points



Step 2 Click the AP Name link to display details for that mesh access point. The General Properties panel for that mesh access point appears (see Figure 6-29).

Note You can also access the General properties panel for a mesh access point from a Cisco WCS map window. To display the panel, click the arrow portion of the mesh access point label. A tabbed panel appears and displays the General properties panel for the selected access point.

Figure 6-29 AP Name > General Properties Page

To add, remove, or reorder columns in the table, click the Edit View link. Table 6-17 displays optional access point parameters available from the Edit View window.

Table 6-17 Monitor Access Points Additional Search Results Parameters

Column	Options
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 6-17 Monitor Access Points Additional Search Results Parameters

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.
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.
Node Hops	Indicates the number of hops between access point.
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.
Radio MAC	Indicates the radio's MAC address.
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.
WLAN Override Names	Indicates the WLAN override profile names.
WLAN Override	Indicates whether WLAN Override is enabled or disabled.

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 In Cisco WCS, choose **Monitor > Access Points**. A listing of access points appears (see Figure 6-30).

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.

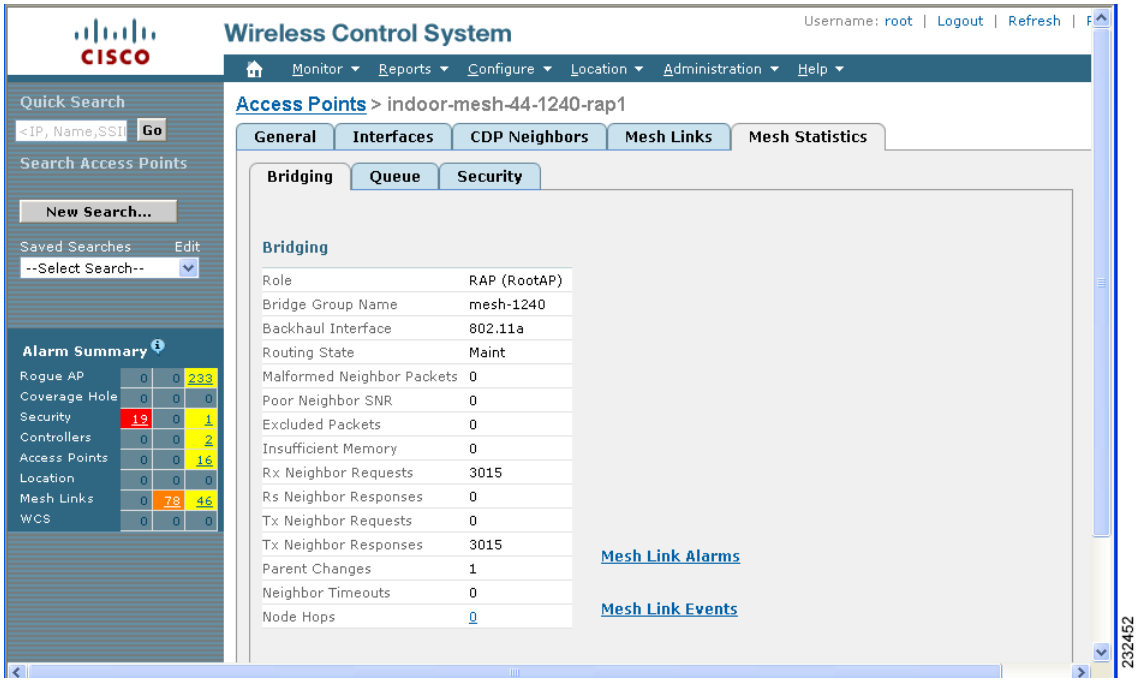
A tabbed panel appears and displays the General Properties page for the selected access point.

Step 3 Click the **Mesh Statistics** tab (see Figure 6-30). A three-tabbed Mesh Statistics panel 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 panel for a mesh access point from a Cisco WCS map. To display the panel, click the arrow portion of the mesh access point label.

Figure 6-30 Monitor > Access Points > AP Name > Mesh Statistics



Summaries of the Bridging, Queue and Security Statistics and their definitions are provided in Table 6-18, Table 6-19 and Table 6-20 respectively.

Table 6-18 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 (BGN)	The name of the bridge group to which the MAP or RAP is a member. Assigning membership in a BGN is recommended. If one is not assigned, a MAP is by default assigned to a default BGN.
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.
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.

Table 6-18 Bridging Mesh Statistics (continued)

Parameter	Description
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 6-19 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 6-19 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 6-20 Security Mesh Statistics

Parameter	Description
Association Request Failures	Summarizes the total number of association request failures that occur between the selected mesh access point and its parent.
Association Request Success	Summarizes the total number of successful association requests 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.
Authentication Request Failures	Summarizes the total number of failed authentication requests 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.
Authentication Request Timeouts	Summarizes the total number of authentication request timeouts that occur 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.
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.

Table 6-20 Security Mesh Statistics (continued)

Parameter	Description
Invalid Reauthentication Request	Summarizes the total number of invalid reauthentication requests received by the parent mesh access point from a child. This may happen when a child is a valid neighbor but is not in a proper state for reauthentication.
Packets Received	Summarizes the total number of packets received during security negotiations by the selected mesh access point.
Packets Transmitted	Summarizes the total number of packets transmitted during security negotiations by the selected mesh access point.
Reassociation Request Failures	Summarizes the total number of failed reassociation requests between the selected mesh access point and its parent.
Reassociation Request Success	Summarizes the total number of successful 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.
Reauthentication Request Failures	Summarizes the total number of failed reauthentication requests 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.
Reauthentication Request Timeouts	Summarizes the total number of reauthentication request timeouts that occurred between the selected mesh access point and its parent.
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.
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.
Unknown Reauthentication Request	Summarizes the total number of unknown reauthentication requests received by the parent mesh access point node from its child. This might occur 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.

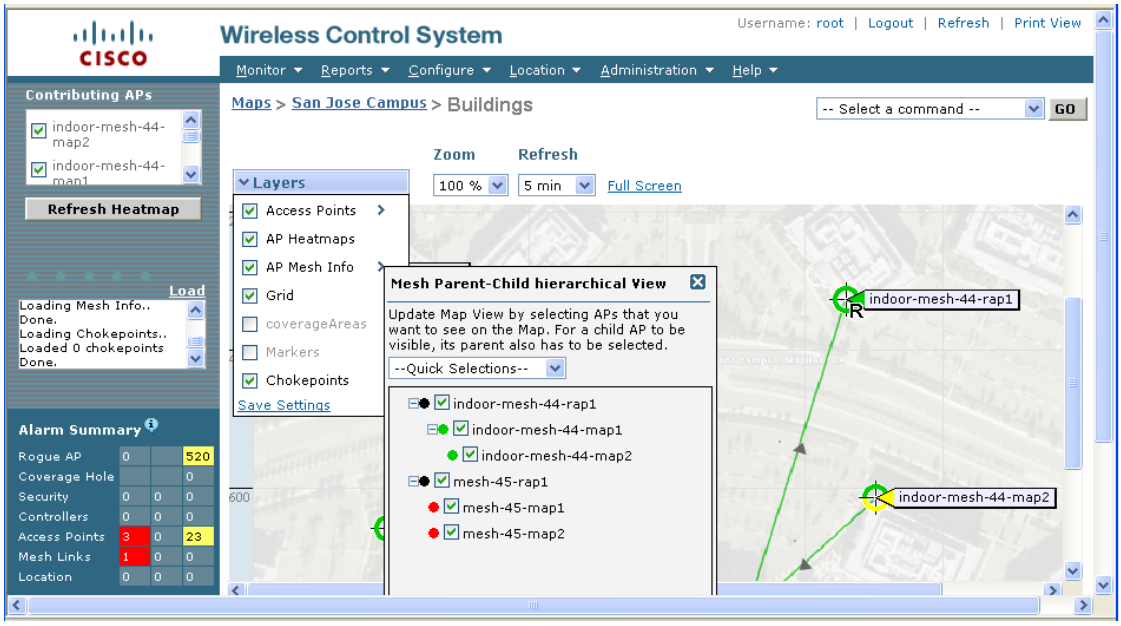
To view the mesh network hierarchy for a selected network, do the following:

Step 1 In Cisco WCS, choose **Monitor > Maps**.

Step 2 Select the map you want to display.

Step 3 Click the **Layers** arrow to expand that menu (see Figure 6-31).

Figure 6-31 Monitor > Maps > Selected Map



Step 4 Check the **AP Mesh Info** check box 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 5 Click the **AP Mesh Info** arrow to display the mesh parent-child hierarchy.

Step 6 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 6-31, the access point, *indoor-mesh-45-rap2*, has only one child, *indoor-mesh-44-map2*.

Step 7 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 6-21 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 6-21 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 window, 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 menu. 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 menu 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 6-22 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 6-32). 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 menu.

b. Select the appropriate option from the menu. A description of the options is provided in Table 6-23.

Table 6-23 Quick Selection Options

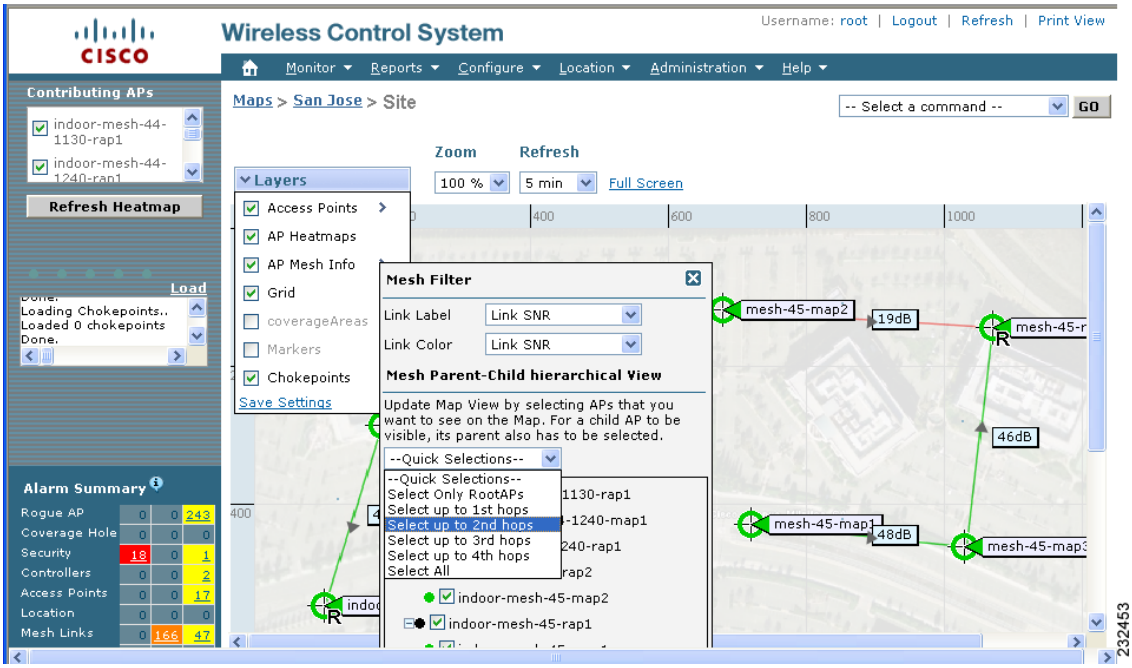
Parameter	Description
Select only Root APs	Choose this setting if you want the map view to display root access points only.
Select up to 1st hops	Choose this setting if you want the map view to display 1st hops only.
Select up to 2nd hops	Choose this setting if you want the map view to display 2nd hops 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 check or uncheck 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.

Figure 6-32 Mesh Filter and Hope Count Configuration Panel



Monitoring Channel Width

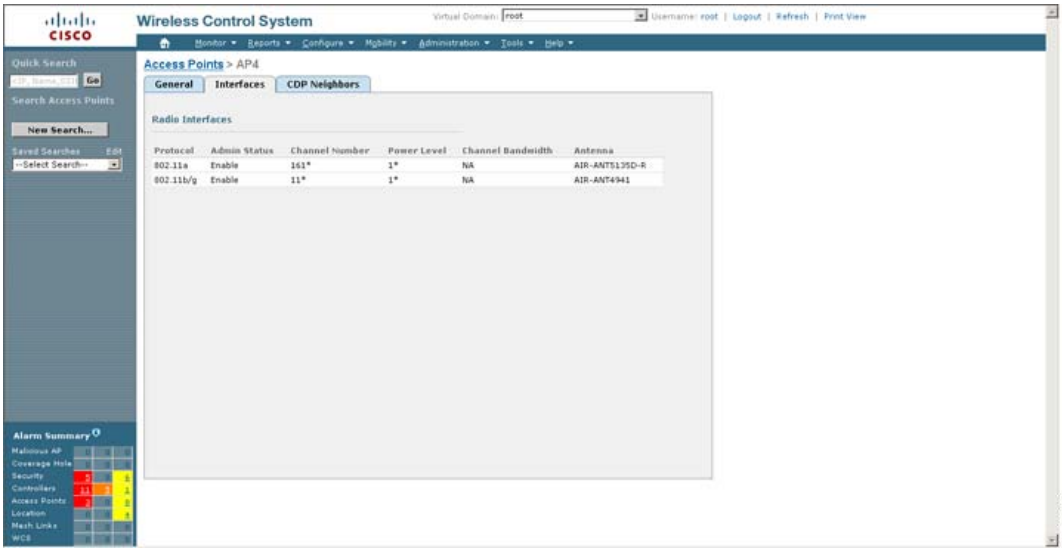
Follow these steps to view the channel width.

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

Step 2 Click an access point from the AP Name column.

Step 3 Click the **Interfaces** tab. The Interfaces tab as shown in Figure 6-33 appears.

Figure 6-33 Interfaces Tab



Step 4 The Interfaces tab displays the following parameters.

Table 6-24 Interfaces Tab Parameters

Parameter	Description
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.
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 Bandwidth	Indicates the channel width for this radio interface. See "Configuring 40-MHz Channel Bonding" section on page 10-15 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 Name	Identifies the type of antenna.

Viewing Google Earth Maps

Follow these steps to view Google Earth maps. Refer to Chapter 18, "Google Earth Maps," for further information.

Step 1 Log in to WCS.

Step 2 Choose **Monitor > Google Earth Maps**. The Google Earth Maps window 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 window 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 web site.

To view details for a Google Earth Map folder, follow these steps:

Step 1 From the Google Earth Map window, click the folder name to open the details window for this folder. The Google Earth Details window 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 window.

Google Earth Settings

Access point related settings can be defined from the Google Earth Settings window. To configure access point settings for the Google Earth Maps feature, follow these steps:

Step 1 Choose **Monitor > Google Earth Maps**.

Step 2 From the Select a command drop-down menu, choose **Settings**.

Step 3 Click **GO**.

Step 4 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 window.

Note These settings apply when Google Earth sends the request for the next refresh.

– Access Points—From the drop-down menu, 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 menu, 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 menu (- 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 menu. Choose **Link SNR** or **Packet Error Rate** from the Link Color drop-down menu.

Note When the AP Mesh Info check box is chosen, Mesh Links are also automatically shown.

Step 5 Click **Save** to confirm these changes or **Cancel** to close the window without saving the changes.

Viewing Clients Identified as WGBs

When you click Monitor > WGB, you get a list of all clients identified as a workgroup bridges (see Figure 6-34). WGB clients bridge wireless to wired. Any 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.

Figure 6-34 Monitor > WGBs

Clients(detected as WGBs) (Edit View)

This page lists the Clients identified as Work Group Bridge.

User	Vendor	IP Addr	MAC Addr	AP	Controller	Port	Loc Server	802.11 State	Profile Name	SSID	Authenticat
<none>	Cisco	10.32.33.139	00:17:94:5c:05:10	SJC14-42A-AP-C2	10.32.32.9	1	<unknown>	Associated	wgbme	wgbme	Yes
<none>	Cisco	10.32.33.110	00:19:30:f0:39:c6	SJC14-42A-AP-C2	10.32.32.9	1	<unknown>	Associated	wgbme	wgbme	Yes

232446

Running a Link Test

A link test uses a ping from parent-to-child or child-to-parent to test the link quality. The RF parameters of the ping reply packets received by the access point are polled by the controller to find the 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. It polls the controller every so many seconds 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.

You can access the link test in one of two ways. The first option is described below.

Step 1 Choose **Monitor > Clients**.

Step 2 From the left sidebar menu, choose **All Clients** in the Search for Clients By drop-down menu.

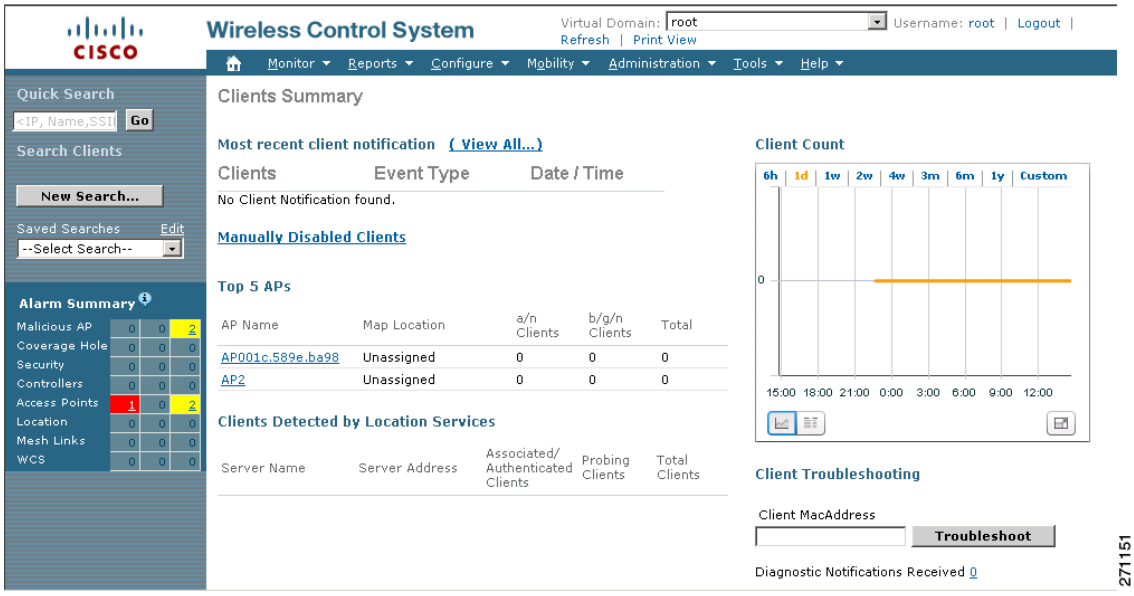
Step 3 In the Client States drop-down menu, choose **All States**. The client list page appears.

Step 4 Click the **Link Test** link in the last column. The link test begins. Figure 6-36 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.

Another method for accessing the link test is as follows:

Step 1 Choose **Monitor > Clients**. The Clients Summary window appears (see Figure 6-35).

Figure 6-35 Clients Summary



Step 2 Click the URL under the Total Clients column of the Clients Detected by Location Servers portion of the window.

Step 3 Click a link in the User column to advance to the detail page.

Step 4 From the Select a command drop-down menu, choose **Link Test**.

Figure 6-36 shows a sample Cisco Compatible Extensions link test result and Figure 6-37 shows a sample ping test result.

Figure 6-36 Cisco Compatible Extensions Link Test Result

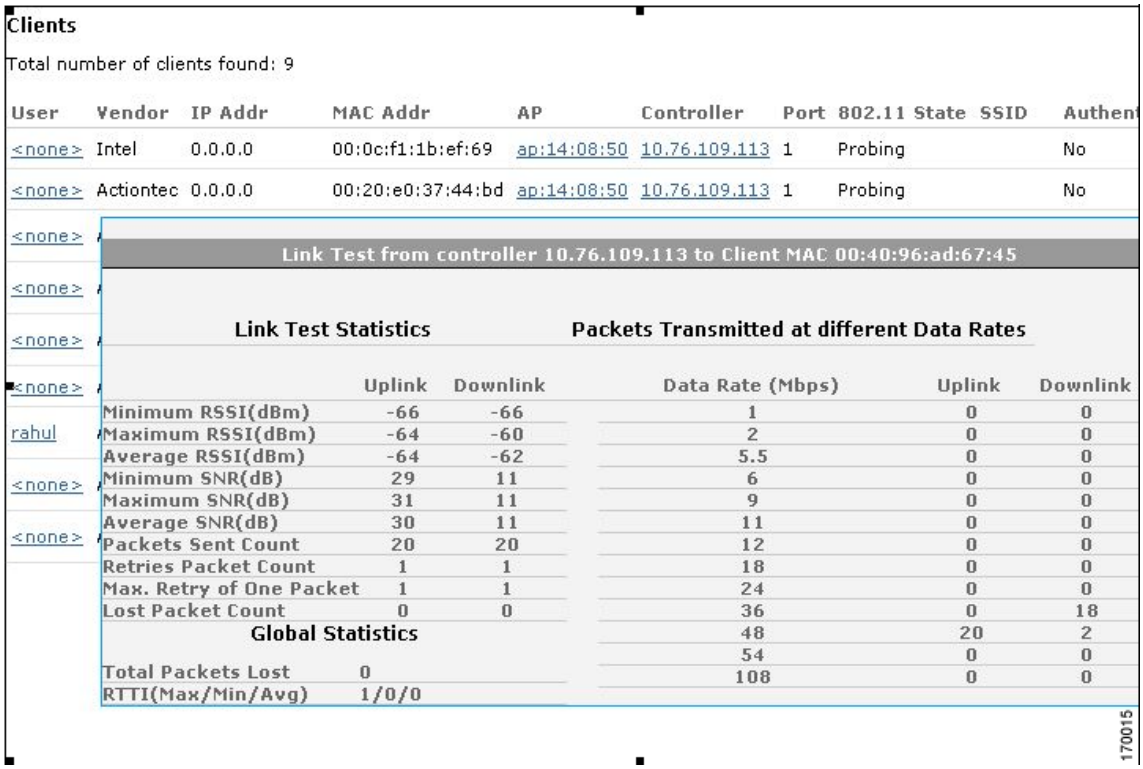
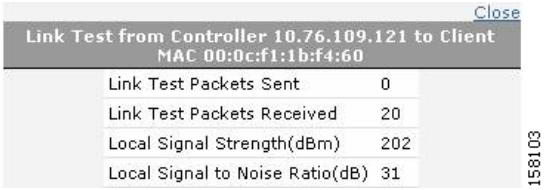


Figure 6-37 Ping Test Result



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:

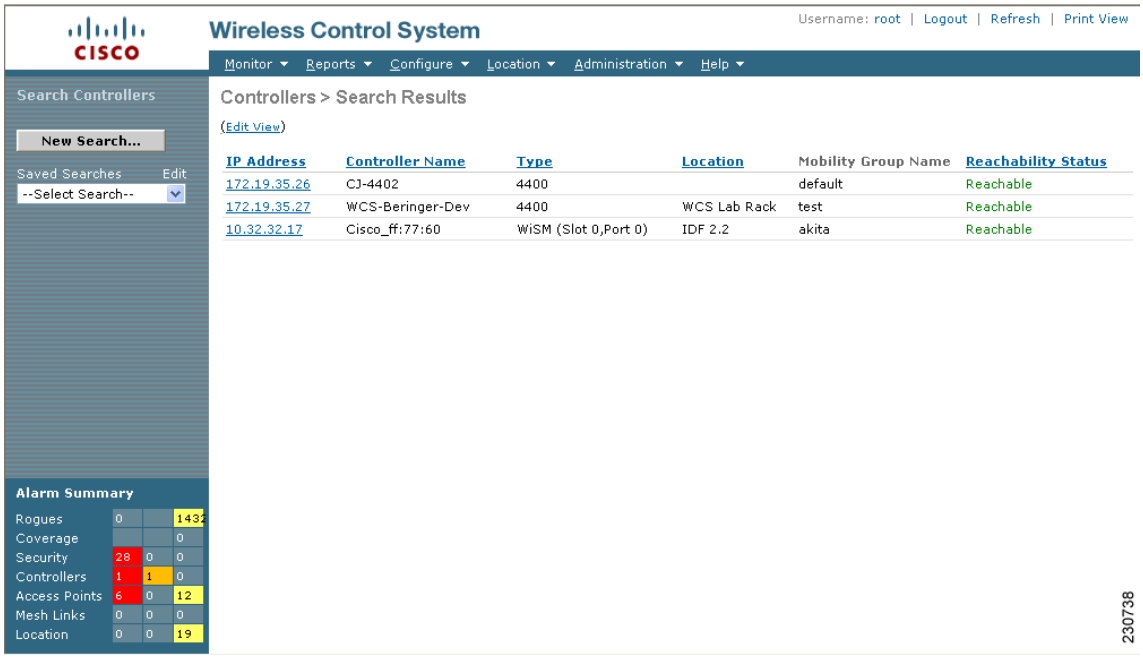
- The orderable product identifier (PID)
- The version of the product identifier (VID)
- The serial number (SN)
- The entity name
- The product description

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.

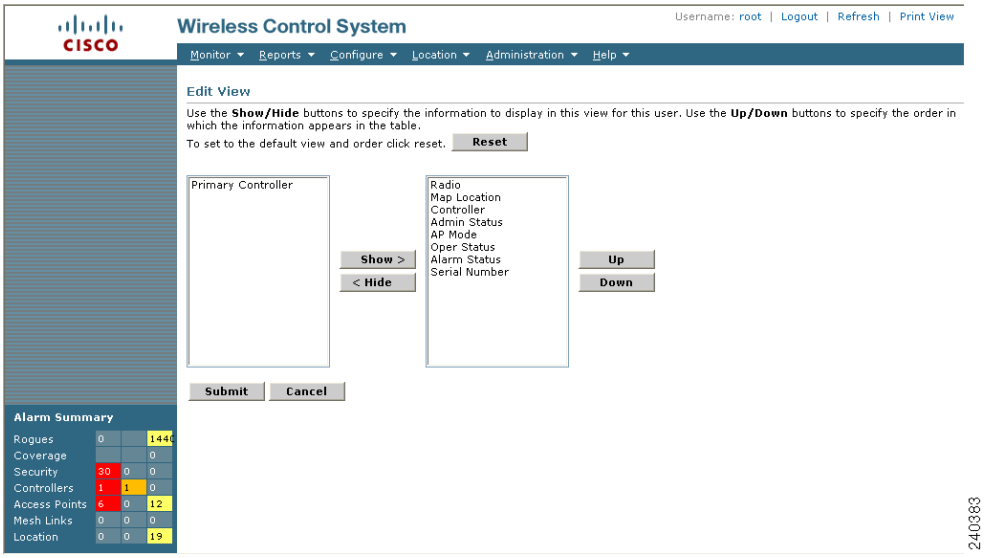
Step 1 Click **Monitor > Controllers**. The Controller > Search Results window displays (see Figure 6-38).

Figure 6-38 Controllers > Search Results



Step 2 (optional) If you want to change how the controller search results are displayed, click **Edit View**. The Edit View window appears (see Figure 6-39). In the left-hand window, highlight the areas you want to view and click **Show** to move them to the right-hand window. You can then highlight the areas in the right-hand menu and click **Up** or **Down** to rearrange the order.

Figure 6-39 Edit View Window



Step 3 Click the IP address of the controller (seen in Figure 6-38) whose UDI information you want to retrieve. Data elements of the controller UDI display. These elements are described in Table 6-25 and Table 6-26:

Table 6-25 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.
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.

Table 6-25 Controllers Summary (continued)

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.
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.
GigE Card Present	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 6-26 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.
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 6-26 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

Table 6-26 Maximum Number of Crypto Cards That Can Be Installed on a Cisco Wireless LAN Controller

Type of Controller	Maximum Number of Crypto Cards
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 the "Finding Coverage Holes" section on page 5-9.

Note 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, choose **Pre-coverage Hole** from the Event Category drop-down menu on the left sidebar and click **Search**.

The Pre-Coverage Hole Events window provides the information described in the following table:

Table 6-27 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.

Table 6-27 Pre-Coverage Hole Parameters (continued)

Parameter	Description
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)
Date/Time	The date and time the event occurred. Click the title to toggle between ascending and descending order.

Step 3 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.

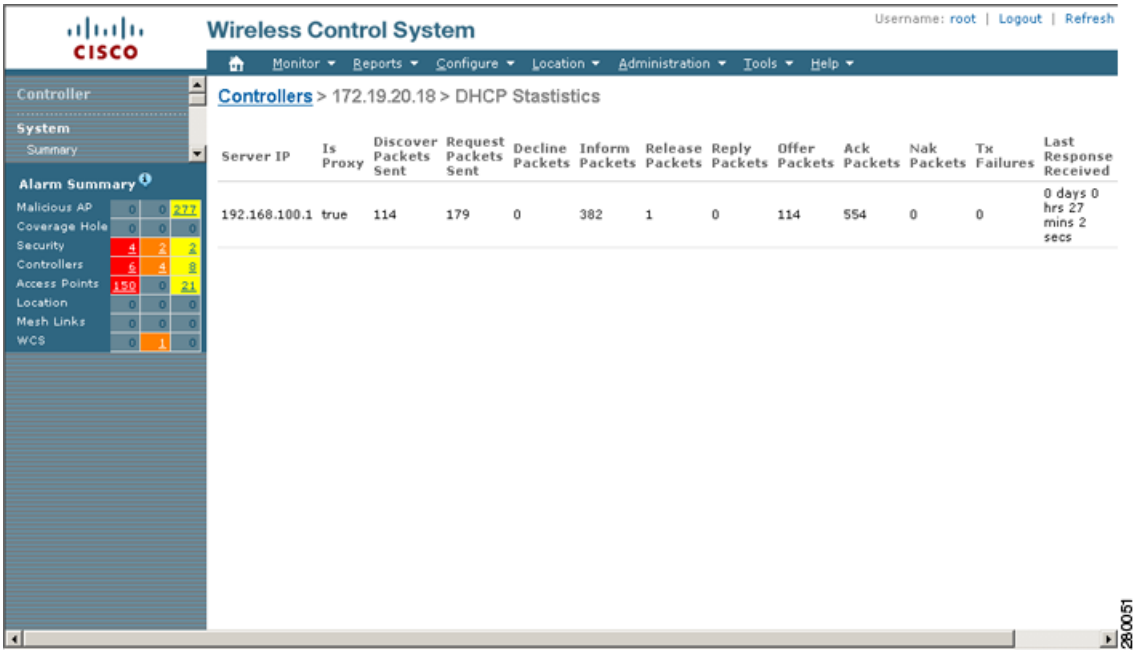
Follow these steps to view DHCP statistics.

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 window appears (see Figure 6-40).

Figure 6-40 DHCP Statistics Window



The DHCP Statistics screen provides the following information:

Table 6-28 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.
Last Response Received	Provides a timestamp of the last response received.
Last Request Sent	Provides a timestamp of the last request sent.

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.

WCS software release 5.1 introduces a snapshot of the Radio Resource Management (RRM) statistics. It helps to identify trouble spots and provides possible reasons for channel or power level changes. The dashboard provides network-wide RRM performance statistics and predicts reasons for channel changes based on grouping the events together (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 LWAPP 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 Mbps. 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 LWAPP 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 channelization allows 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 channelization 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 only reduces an access point's power. However, the coverage hole algorithm can 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.

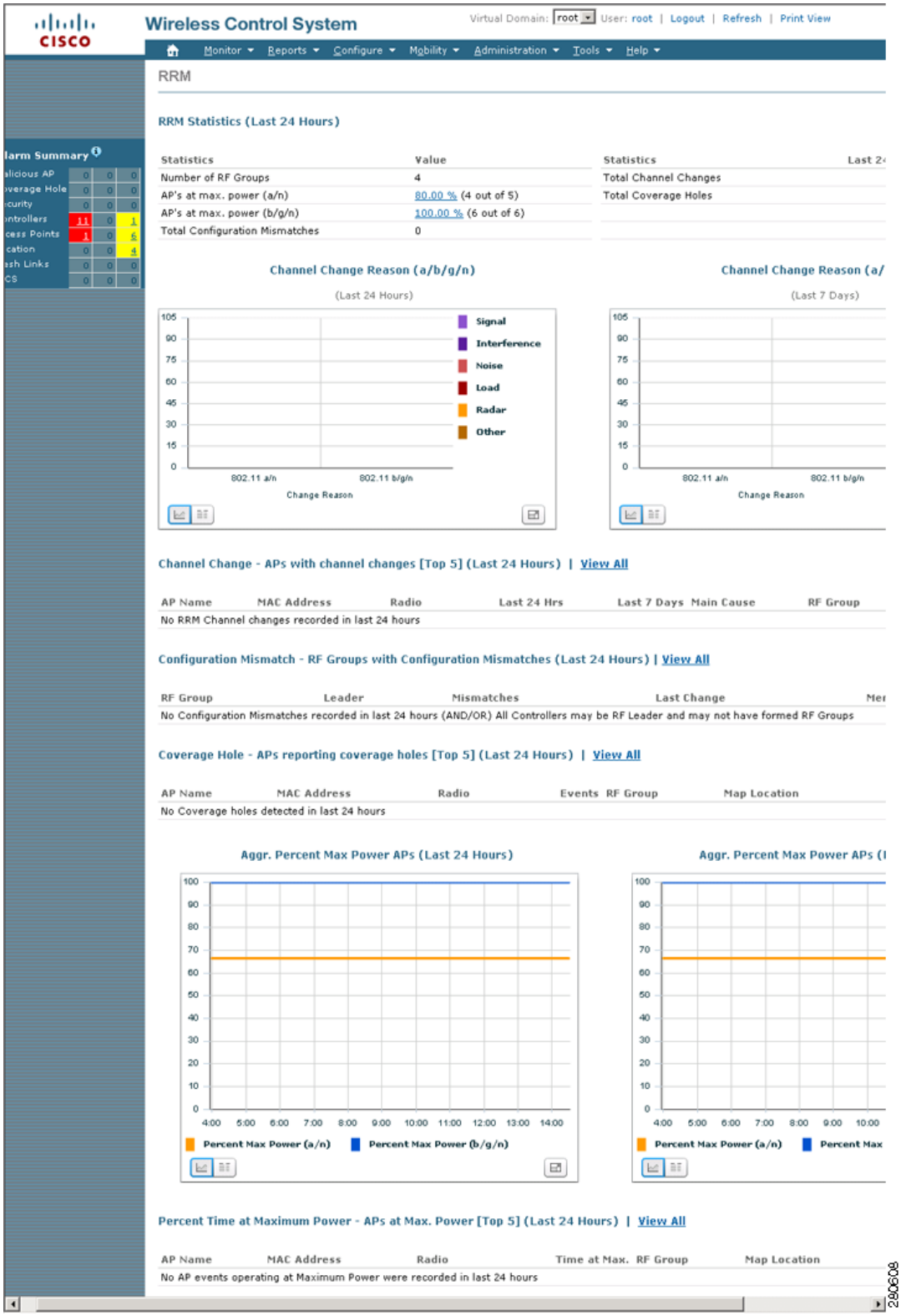
RF Grouping Notifications

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 LWAPP 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 6-41).

Figure 6-41 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 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 LWAPP 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 LWAPP 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 LWAPP 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 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 7-6
- Setting Lobby Ambassador Defaults, page 7-7
- Viewing the Audit Trail, page 7-9
- Enabling Audit Trails for Guest User Activities, page 7-11
- Creating Guest User Accounts, page 7-11
- Managing WCS Guest User Accounts, page 7-14
- Adding a New User, page 7-20

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.

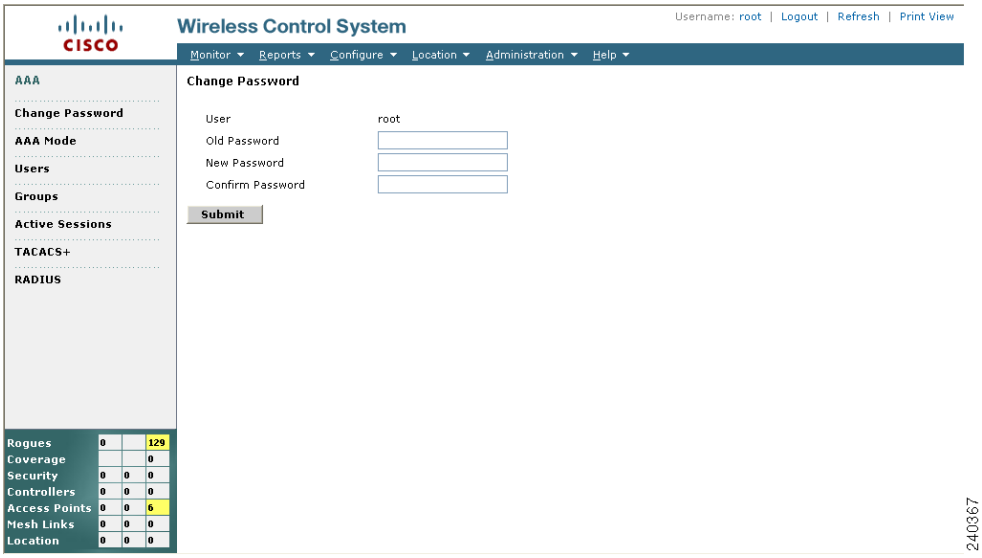
Step 1 Start WCS by following the instructions in the "Starting WCS" section on page 2-12.

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 window appears (see Figure 7-1).

Figure 7-1 Change Password Window



Step 4 In the Old Password field, 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 Under Groups Assigned to this User, check the appropriate check box to assign the new user account to one of the user groups supported by WCS:

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.

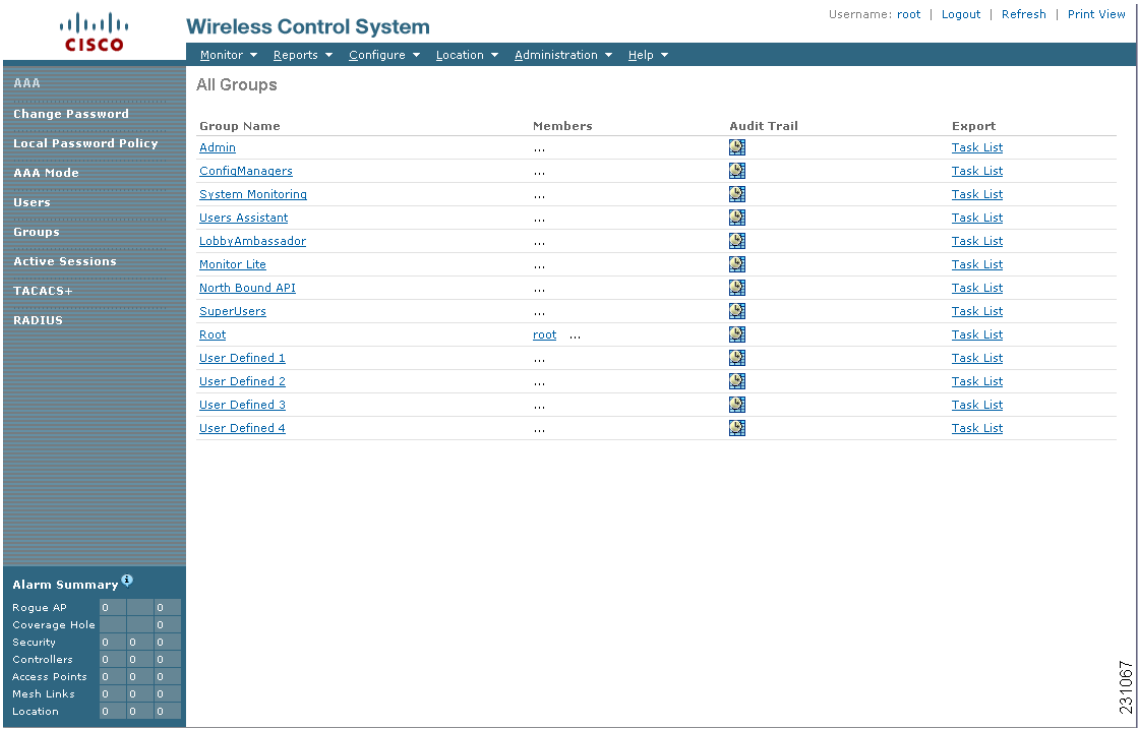
Note If you create a user assistant user, login as that user, and go to Monitor > Controller, you receive a permission denied message as expected behavior.

- 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.

Step 7 Click **Submit**. The name of the new user account appears on the All Users page and can be used immediately.

Step 8 In the sidebar, click **Groups** to display the All Groups page (see Figure 7-2).

Figure 7-2 All Groups Window



Step 9 Click the name of the user group to which you assigned the new user account. The Group > User Group page shows a list of this group's permitted operations.

Step 10 Make any desired changes by checking or unchecking the appropriate check boxes.

Note Any changes you make will affect all members of this user group.

Step 11 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 2-12.

Step 2 Log into the WCS user interface as a user assigned to the SuperUsers group.

Step 3 Click **Administration > Accounts** to display the All Users page.

Step 4 Check the check box to the left of the user account(s) to be deleted.

Step 5 From the Select a command drop-down menu, 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 2-12.

Step 2 Log into the WCS user interface as a user assigned to the SuperUsers group.

Step 3 Click **Administration > Accounts** to display the Change Password page.

Step 4 Click the name of the user account for which you want to change the password. You can change the password here or through the User > Edit window.

Step 5 Enter your old password, unless you are the root user. (A root user can change any password without entering the old password.)

Step 6 On the User > *Username* page, enter the new password in both the New Password and Confirm New Password fields.

Step 7 Click **Submit** to save your changes. The password for this user account has been changed and can be used immediately.

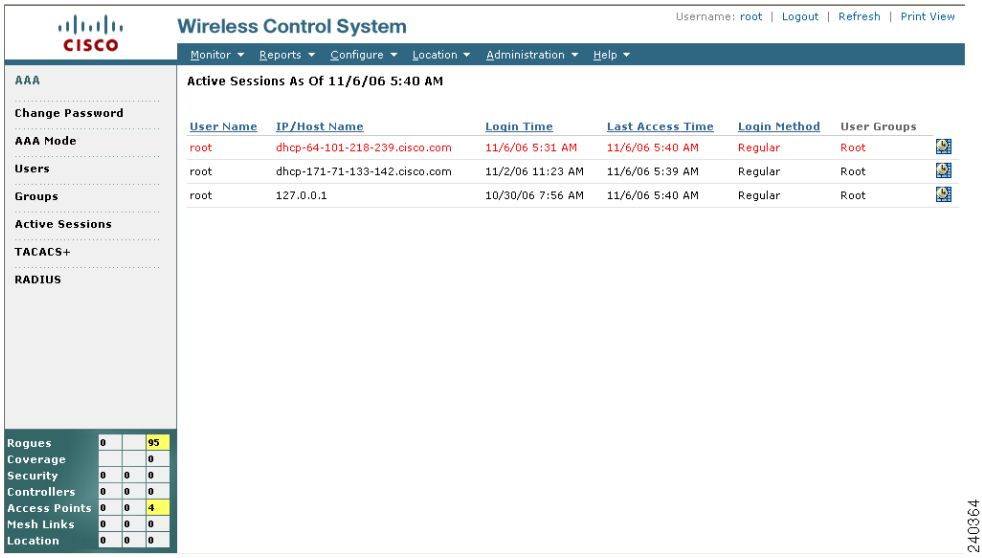
Monitoring Active Sessions

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 window appears (see Figure 7-3).

Figure 7-3 Active Sessions Window



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 window 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.

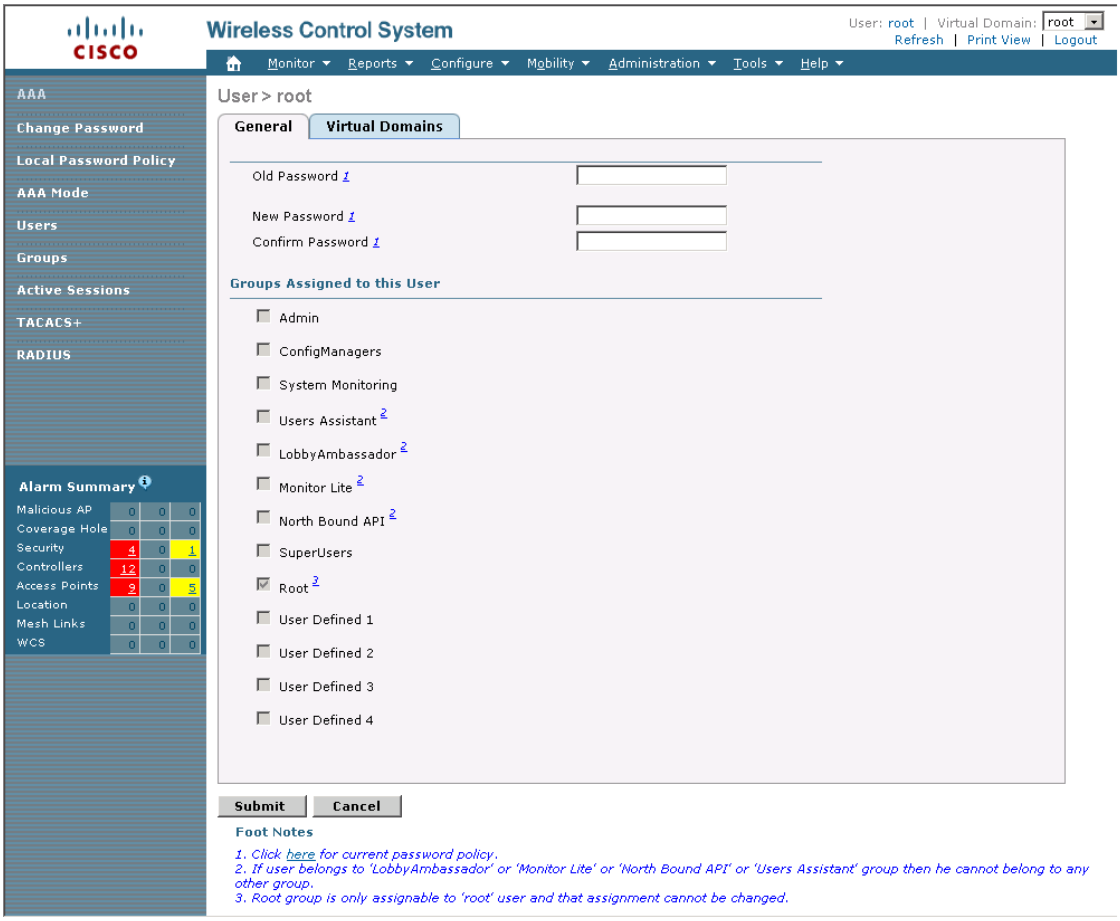
Note The time displayed in this column is usually a few seconds behind the current system time because Last Access Time is updated frequently by the updates to the alarm status panel. However, if a user navigates to a non-WCS Navigator web page in the same browser, the disparity in time is greater upon 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 window that displays the audit trail (previous login times) for that user.

Viewing or Editing User Information

Click in the User Name column of the Users window to see the group the user is assigned to or to adjust a password or group assignment. The detailed users window appears (see Figure 7-4).

Figure 7-4 Detailed Users Window

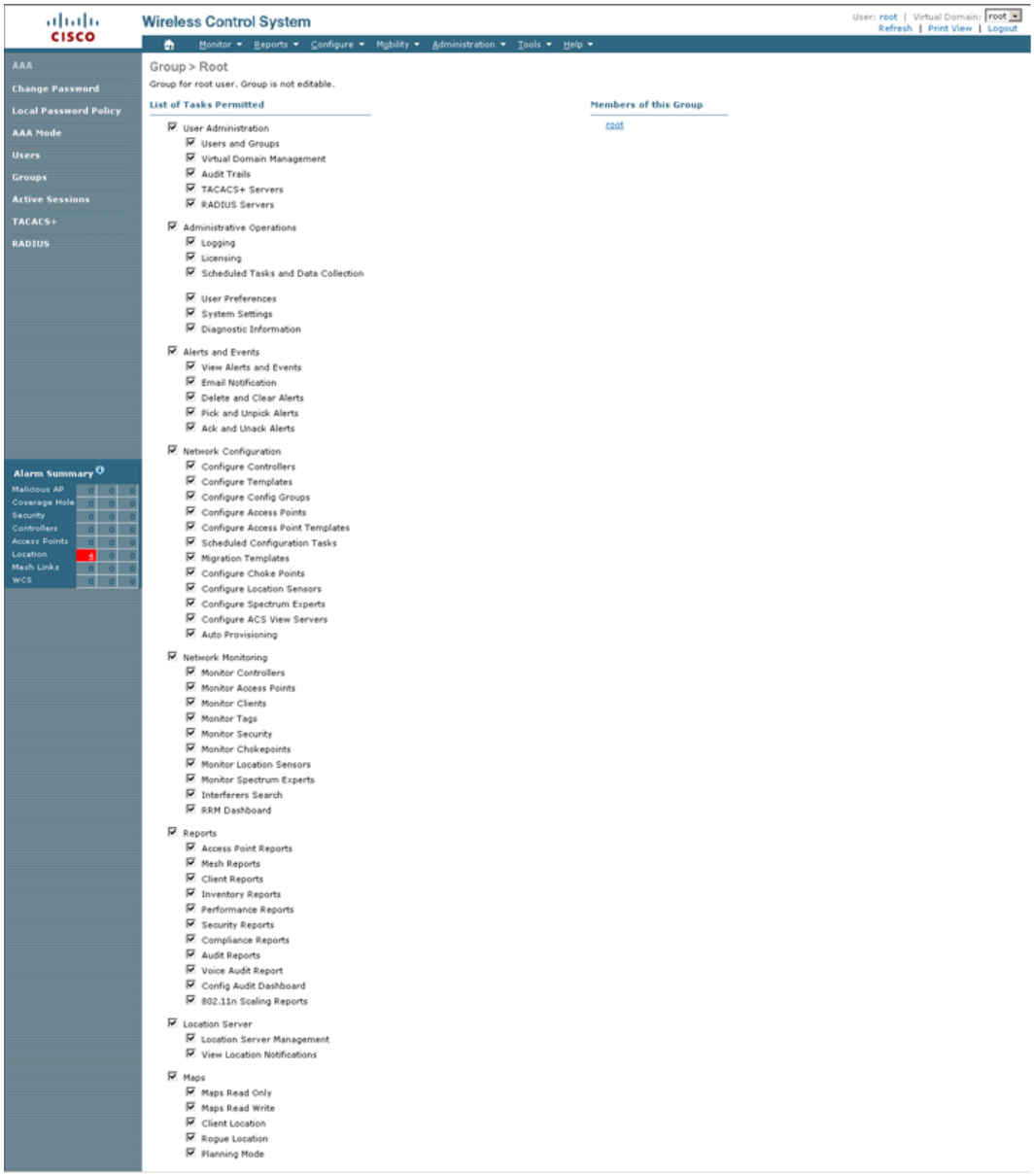


Viewing or Editing Group Information

Click in the Member Of column of the User window to see specific tasks the user is permitted to do within the defined group or to make changes and submit them. The detailed group window appears (see Figure 7-5).

Note The detailed window varies based on what group you choose. Figure 7-5 shows the detailed window of the root group.

Figure 7-5 Detailed Group Window

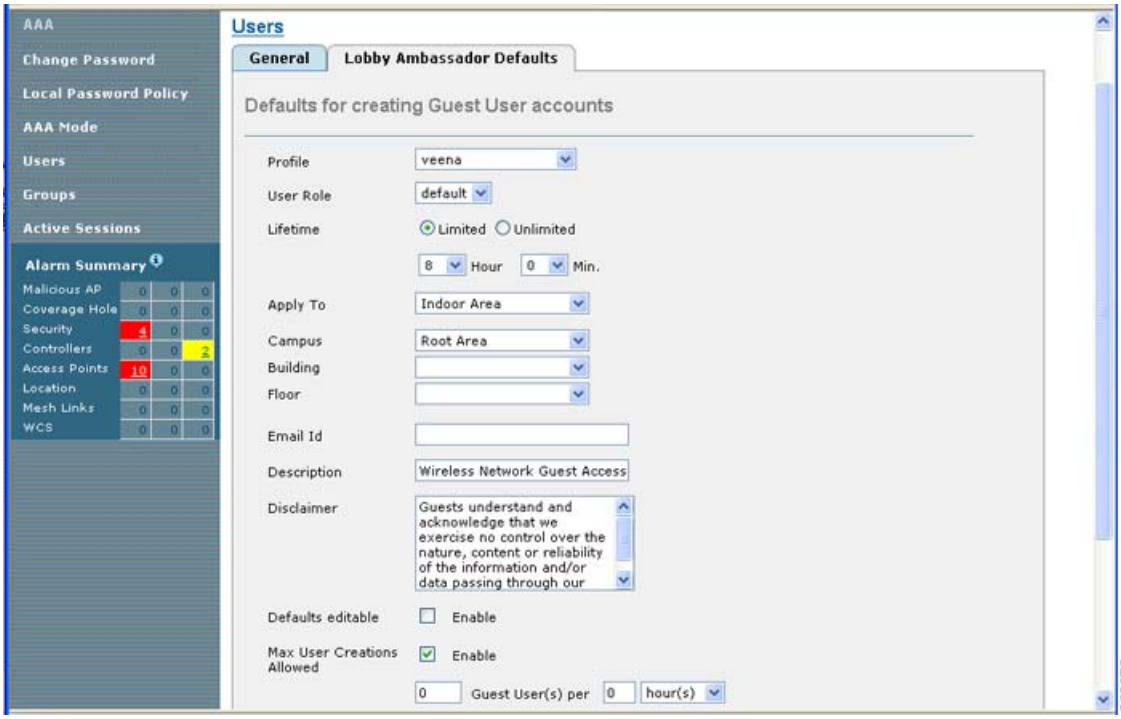


Setting Lobby Ambassador Defaults

If you click the Lobby Ambassador check box when creating a user group, a Lobby Ambassador Defaults tab appears (see Figure 7-6). 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 7-6 Lobby Ambassador Defaults



Step 1 Use the Profile drop-down menu to choose the guest user to connect to.

Step 2 Choose **Limited** or **Unlimited** at the Lifetime parameter. If you choose limited, you can specify the number of hours and minutes. By default the lifetime is limited to 8 hours.

Step 3 Use the Apply to drop-down menu 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 4 Enter the e-mail ID of the host to whom the guest account credentials are sent.

Step 5 Provide a brief description of the account.

Step 6 If you want to supply disclaimer text, enter it.

Step 7 Check the **Defaults Editable Enable** check box if you want to allow the lobby ambassador to override these configured defaults.

Step 8 Check the **Max User Creations Allowed Enable** check box to allow the lobby ambassador to set limits on the number of guest users that can be on the network in a given time period. The time period is defined in hours, days, or weeks.

Editing the Default Lobby Ambassador Credentials

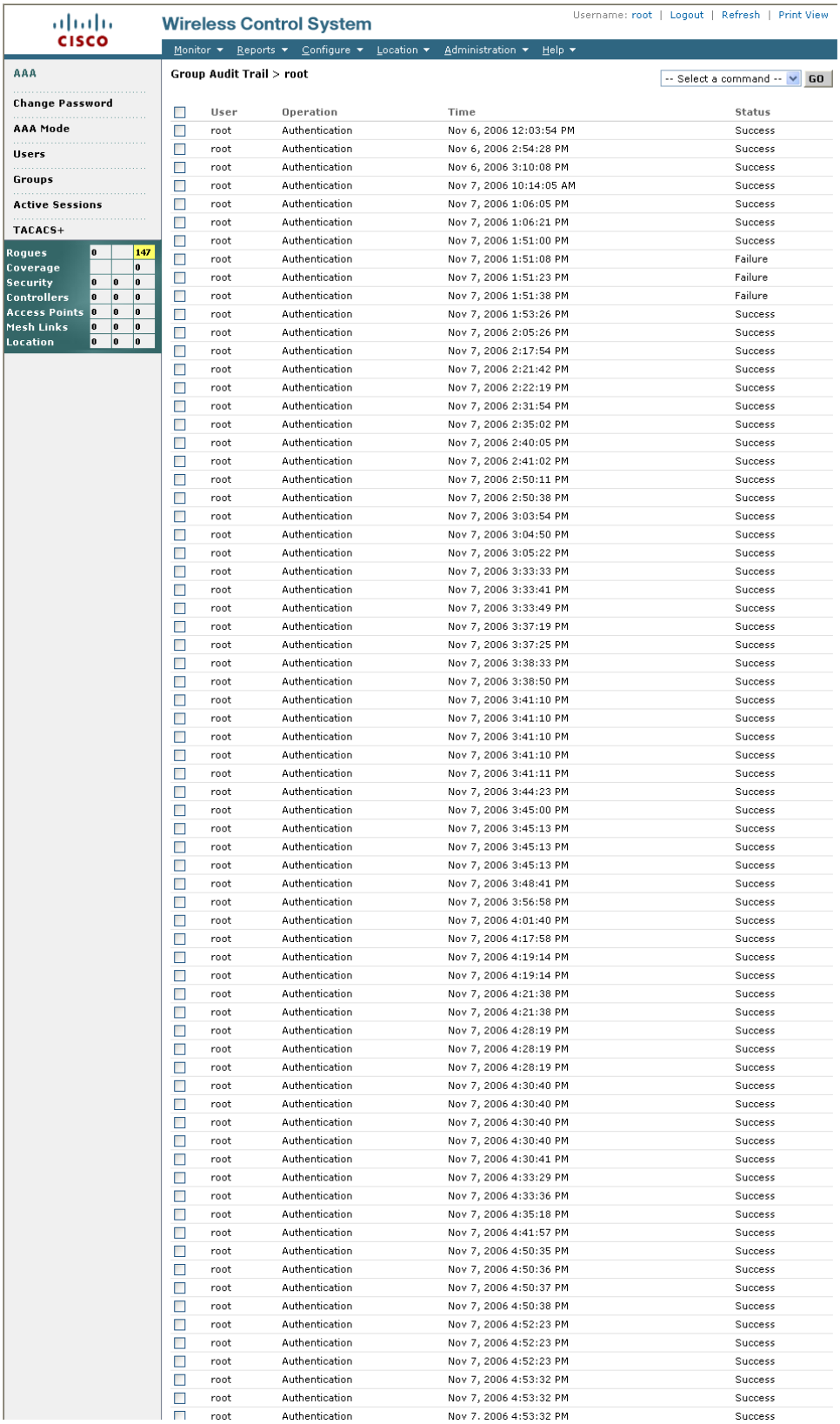
Click the WCS username in the Users window to edit the lobby ambassador default credentials. The Lobby Ambassador Default tab appears, and you can modify the credentials.

Note If you remove the profile selection, the defaults for this lobby ambassador are removed.

Viewing the Audit Trail

Click the **Audit Trail** icon in the Users window to view a log of authentication attempts. The Audit Trail window appears (see Figure 7-7).

Figure 7-7 Audit Trail



Enabling Audit Trails for Guest User Activities

Follow these steps to enable audit trails for guest user activities.

Step 1 Log into the Navigator or WCS user interface as an administrator.

Step 2 Click **Administration > AAA**, then click **Users** in the left sidebar menu to display the Users window.

Step 3 At the Users window, click the **Audit Trail** icon for the lobby ambassador account that you want to view. The Audit Trail window for the lobby ambassador appears.

The window enables you to view a list of lobby ambassador activities over time. Each entry displays the following information:

- User: User login name (for example, *lobby*)
- Operation: Type of operation audited (such as, creation and deletion of guest users reported by name)
- Time: Time operation was audited
- Status: Success or failure of activity

Note WCS keeps all Audit Trail records for up to 7 days. The nightly data cleanup task cleans all records which are older than 7 days.

Step 4 To clear a specific entry from the audit trail listing, check the check box next to that entry and choose **Clear Audit Trail** from the Select a command drop-down menu and click **GO**.

You can select multiple entries for deletion at one time.

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 administrator account. Guest user accounts are for visitors, temporary workers, etc. 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 administrator has no access to online help.

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:

- Creating a Lobby Ambassador Account, page 7-12
- Managing WCS Guest User Accounts, page 7-14
- Logging the Lobby Ambassador Activities, page 7-19

Creating a Lobby Ambassador Account

Follow these steps to create a lobby ambassador account 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 menu, choose **Add User** and click **GO**. The Users window 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, check the **LobbyAmbassador** check box to access the **Lobby Ambassador Defaults** tab.

Step 8 At the Lobby Ambassador Default tab, follow these steps to set the defaults for a guest user account:

a. Choose a Profile for the guest user from the drop-down menu.

Wired-guest is an example of a profile that might be defined to indicate traffic that is originating from wired LAN ports. Refer to the "Configuring Wired Guest Access" section on page 10-23.

b. Choose a user role for the guest user from the drop-down menu. 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. User roles are defined in Cisco WCS on the Local Net User Role Template Window. Refer to the "Configuring Guest User Templates" section on page 11-35.

c. 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 menus. The default value for Limited is one day (8 hours).
   - When *unlimited* is chosen, no expiration date for the guest account exists.

d. Choose the area (indoor or outdoor), controller list, or config group to which the guest user traffic is limited from the Apply to drop-down menu.
   - If you choose the controller list option, a list of controller IP addresses appears. Check the check box next to all controller networks on which guest traffic is allowed.

e. (Optionally) Enter the e-mail ID of the host to whom the guest account credentials are sent.

f. (Optionally) Modify the default guest user description if necessary.

g. (Optionally) Modify the Disclaimer text, if necessary.

h. Check the Defaults Editable check box. This allows the Lobby Ambassadors to modify Guest User default settings on the Lobby Ambassador Default setting window.

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 9 Click **Submit**.

When the lobby ambassador is added, it is part of the lobby ambassador group. The name of the new lobby ambassador account is listed and can be used immediately.

Editing a Lobby Ambassador Account

The Lobby Ambassador default credentials can be edited from the username link on the WCS user list page.

To edit the Lobby Ambassador default credentials, follow these steps:

Step 1 Log into the WCS user interface as an administrator.

Step 2 Choose **Administration > AAA**.

Step 3 From the left sidebar menu, click **Users**.

Step 4 Click the applicable Lobby Ambassador account from the **User Name** column.

Step 5 From the **Lobby Ambassador Defaults** page, edit the credentials as necessary.

Note While editing, if the *Profile* selection is removed (changed to *Select a profile*), the defaults are re moved for this Lobby Ambassador. The user must reconfigure the defaults to reinforce them.

Step 6 Click **Submit**.

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 6.0 or later on your computer.

Note Some WCS features may not function properly if you use a web browser other than Internet Explorer 6.0 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 window, enter your username and password.

Note All entries are case sensitive.

Note The lobby administrator 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 window is displayed. This window provides a summary of all created Guest Users.

To exit the WCS user interface, close the browser window or click **Logout** in the upper right corner of the window. 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 Guest User Accounts, page 7-15
- Deleting Guest User Templates, page 7-17
- Scheduling WCS Guest User Accounts, page 7-18

- Printing or E-mailing WCS Guest User Details, page 7-19

Adding Guest User Accounts

Templates are used to create guest user accounts in WCS. After the template is created, it is applied to all controllers that the guest users can access. Follow these steps to add a new guest user account to WCS.

Step 1 Log into the WCS user interface as lobby ambassador to open the Guest user window.

Step 2 From the Select a command drop-down menu, choose **Add Guest User**.

Step 3 Click **GO. The *Guest User* > New User** window has two tabs: General and Advanced. The lobby ambassador can either manually enter the username and password for an individual or can import a file with user names and passwords defined for multiple users by selecting the Generate Password option.

- If the username and password are entered manually, the password is entered twice for confirmation.
- If the Generate Password option is chosen, the Import From File option should be selected on the Advanced tab. The following fields can be imported for a guest user: username, password, lifetime setting, description, and disclaimer. Format for the fields in the CSV file is noted at the bottom of the Advanced panel.
- If the Import From File check box is checked, no username and password fields appear on the General tab.

Note Passwords are case sensitive and must be a minimum of 8 characters. The password must include at least three of the following elements: lowercase letters, uppercase letters, numbers, and special characters. Reenter and confirm the password.

Step 4 At the Advanced tab, check the **Import From File** option to upload the following information for multiple guest users: username, password, lifetime setting, description, and disclaimer.

Format for the fields in the CSV file is noted at the bottom of the Advanced panel.

Step 5 If Import From file is selected, browse to or enter the file name from which to upload the file.

Step 6 Choose a Profile from the drop-down menu.

The selectable profiles are predefined by a system administrator and define the length of time, user role (allocated bandwidth), and areas of the network (indoor, outdoor, controllers, and config groups) to which a guest user has access. Your administrator can advise which profile to use.

Step 7 Choose a user role from the drop-down menu. (This option is not seen if the Import From File check box is selected.)

Step 8 Choose the lifetime of the guest user account. The options are limited or unlimited. (This option is not seen if the Import From File check box is selected.)

- Limited—From the drop-down menus, choose days, hours, or minutes for the lifetime of this guest user account. The maximum is 35 weeks.
- Unlimited—This user account never expires.

Step 9 Click **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 also restrict the guest user (wired or wireless) to a specific listed controller or a configuration group, which is a group of controllers that has been preconfigured by the administrator.

From the Apply To drop-down menu, choose one of the following:

- Controller List: Check the check box for the controller(s) to which the guest user account applies. Only those controllers configured for guest access (wired or wireless) display.
- Indoor Area: Choose the applicable campus, building, and floor.
- Outdoor Area: Choose the applicable campus and outdoor area.
- Config Group: Choose the config group to which the guest user account applies.

Step 10 Review and modify, if necessary, the description field. (This option is not seen if the Import From File check box was selected.)

Step 11 Review and modify, if necessary, the disclaimer information. Use the scroll bar to move up and down. (This option is not seen if the Import From File check box was selected.)

Step 12 Click the **Make this Disclaimer Default** to use the disclaimer text as the default for all guest user accounts. Click the check box if you want to set new default disclaimer text for all future guest user accounts. (This option is not seen if the Import From File check box was selected.)

Step 13 Click **Save** to save your changes or **Cancel** to leave the settings unchanged. The Guest User Credentials window appears. See the "Guest User Credentials" section on page 7-16.

Guest User Credentials

The Guest User Credentials window displays the following information:

- IP Address: IP address of controller to which the guest user account applies.
- Controller Name: Name of controller.
- Operation Status: Indicates successful or unsuccessful creation of guest user account.
- Reason: Indicates why the creation of the guest user account was unsuccessful.
- Guest User Credentials:
  - Guest User Name: Guest user account login name.
  - Password: Guest user account password.
  - Start time: Date and time that the guest user account begins.
  - End time: Date and time that the guest user account expires.
  - Disclaimer: Disclaimer information for the guest user.
- Print/E-mail Guest User Credentials: Link to print or e-mail guest user information. See the "Printing or E-mailing WCS Guest User Details" section on page 7-19.

Viewing and Editing Guest Users

Follow these steps to view the current WCS guest users.

Step 1 Log into the WCS user interface as described in the "Logging into the WCS User Interface" section on page 2-13.

Step 2 On the Guest User window, click which item number under the User Name column you want to view or edit.

Step 3 On the **Guest Users > Users** window, you can edit the following items:

- Profile ID: The selectable profiles are predefined by the system administrator and define the length of time, user role (allocated bandwidth), and areas of the network (indoor, outdoor, controllers, config groups) to which a guest user has access. Your administrator can advise which profile to use.
- Description: Enter a description of the guest user account.
- Limited or Unlimited:
  - Limited: From the drop-down menus, choose days, hours, or minutes for the lifetime of this guest user account. The maximum is 35 weeks.
  - Unlimited: This user account never expires.
- 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 also restrict the guest user (wired or wireless) to a specific listed controller or a config group, which is a group of controllers that has been preconfigured by the administrator.

  From the Apply To drop-down menus, choose one of the following:
  - Controller List: Check the check box for the controller(s) to which the guest user account applies.
  - Indoor Area: Choose the applicable campus, building, and floor.
  - Outdoor Area: Choose the applicable campus and outdoor area.
  - Config Group: Choose the Config Group to which the guest user account applies.

Step 4 Click **Save** to save your changes or **Cancel** to leave the settings unchanged. When you click **Save**, the screen refreshes.

Note The account expiry displays the controller(s) to which the guest user account was applied and the seconds remaining before the guest user account expires.

Deleting Guest User Templates

During deletion of the guest account, all client stations logged in and using the guest WLAN username are deleted. Follow these steps to delete a WCS guest user template.

Step 1 Log into the WCS user interface as described in the "Logging into the WCS User Interface" section on page 2-13.

Step 2 On the Guest Users window, check the check box to the left of the guest user account(s) to be deleted.

Step 3 From the Select a Command drop-down menu, choose **Delete Guest User** and click **GO**.

Step 4 When prompted, click **OK** to confirm your decision.

Note The IP address and controller name to which the guest user account was applied appears, and you are prompted to confirm the removal of the template from the controller.

The controller sends a notification of a guest account expiry and deletion by invoking a trap. WCS processes the trap and deletes the user account expired from the configuration of that controller. If that guest account is not applied to other controllers, it can be deleted from the templates as well. A notice appears in the event logs also.

Step 5 Click **OK** to delete the guest user template from the controller or **Cancel** to leave the settings unchanged. When you delete the guest user template from the controller, you delete the specified guest user account.

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 username 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 window. After clicking Save, the Guest User Details window displays the password. From this window, 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 On the Guest User window, choose **Schedule Guest User** and click **GO** from the Select a command drop-down menu.

Step 3 On the Guest Users > Scheduling window, enter the guest user name. The maximum is 24 characters.

Step 4 Check 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 (unchecked), one password is supplied for a span of days. The generation of a new username and password on every schedule is optional.

Step 5 Select a Profile ID from the drop-down menu. 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 menu, 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: Check 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 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 menus, choose one of the following:

- Controller List: check 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 window.

Follow these steps to print guest user details from the Guest Users List window.

Step 1 Log into the WCS user interface as lobby ambassador.

Step 2 On the Guest User window, check the check box next to User Name and choose **Print/E-mail User Details** from the Select a command drop-down menu and click **GO**.

- If printing, click **Print** and from the print window, select a printer and click **Print** or **Cancel**.
- If e-mailing, click **E-mail** and from the e-mail window, enter the subject text and the recipient's e-mail address. Click **Send** or **Cancel**.

Logging the Lobby Ambassador Activities

The following activities are logged for each lobby ambassador account:

- Lobby ambassador login: WCS logs the authentication operation results for all users.
- Guest user creation: When a lobby ambassador creates a guest user account, WCS logs the guest user name.

- Guest user deletion: When a lobby ambassador deletes the guest user account, WCS logs the deleted guest user name.
- Account updates: WCS logs the details of any updates made to the guest user account. For example, increasing the life time.

Follow these steps to view the lobby ambassador activities.

Note You must have superuser status to open this window.

Step 1 Log into the Navigator or WCS user interface as an administrator.

Step 2 Click **Administration > AAA**, then click **Groups** in the left sidebar menu to display the All Groups window.

Step 3 On the All Groups windows, click the **Audit Trail** icon for the lobby ambassador account you want to view. The Audit Trail window for the lobby ambassador appears.

This window enables you to view a list of lobby ambassador activities over time.

- User: User login name
- Operation: Type of operation audited
- Time: Time operation was audited
- Status: Success or failure

Step 4 To clear the audit trail, choose **Clear Audit Trail** from the Select a command drop-down menu and click **GO**.

Adding a New User

The Add User window 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.

- Add User Name, Password, and Groups
- Assign a Virtual Domain

Add User Name, Password, and Groups

To add a new user, follow these steps:

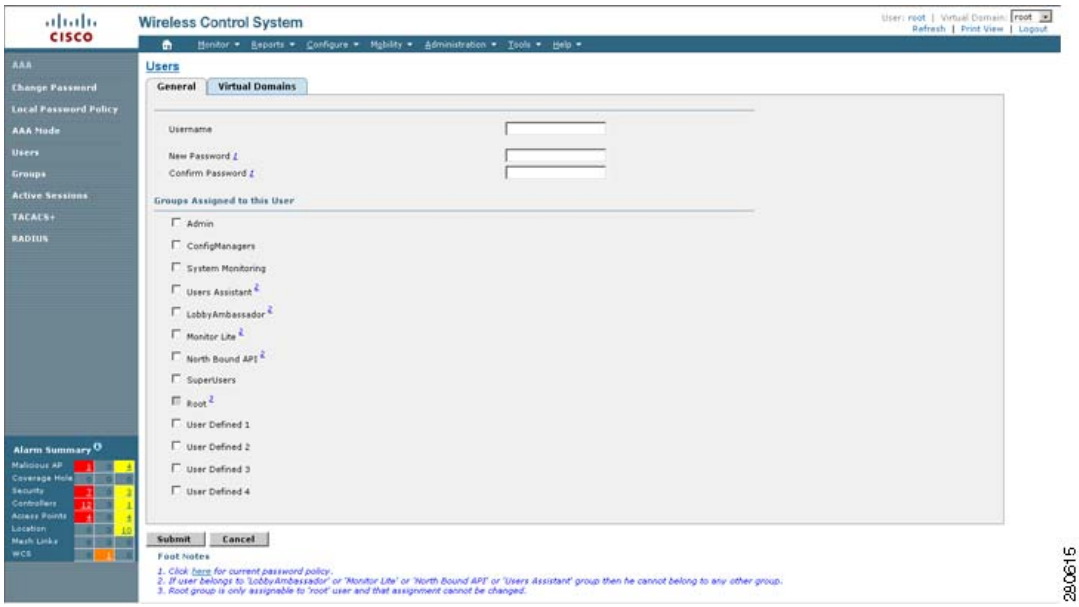
Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, select **Users**.

Step 3 From the **Select a command** drop-down menu, choose **Add User**.

Step 4 Click **GO**. The Users window appears (see Figure 7-8).

Figure 7-8 Users Window



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 adminstration 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. See "Creating a Lobby Ambassador Account" procedure on page 7-12" for more information on setting up a Lobby Ambassador account.
- Monitor Lite—Allows monitoring of assets location.
- North Bound API User—Group used only with WCS Navigator.

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.

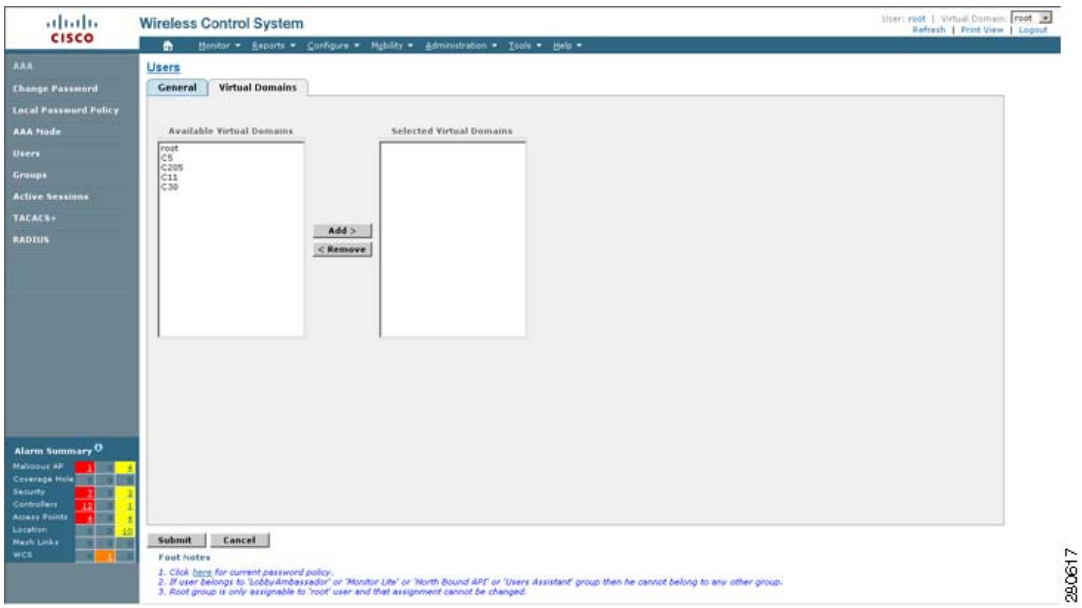
- SuperUsers—Allows users to monitor and configure WCS operations and perform all system administration tasks including administering WCS user accounts and passwords. Superuser tasks can be changed.
- Root—This group is only assignable to 'root' user and that assignment cannot be changed.
- User Defined

Assign a Virtual Domain

Follow these steps to assign a virtual domain to this user:

Step 1 Click the **Virtual Domains** tab. This window 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 hightlight 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 hightlight 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 window without adding or editing the current user.

Virtual Domain RADIUS and TACACS+ Attributes

The Virtual Domain Custom Attributes window 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 (i.e., tasks, roles, virutal 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 field.

Step 8 Click the check boxes to enable these attributes.

Step 9 Click **Submit + Restart**.

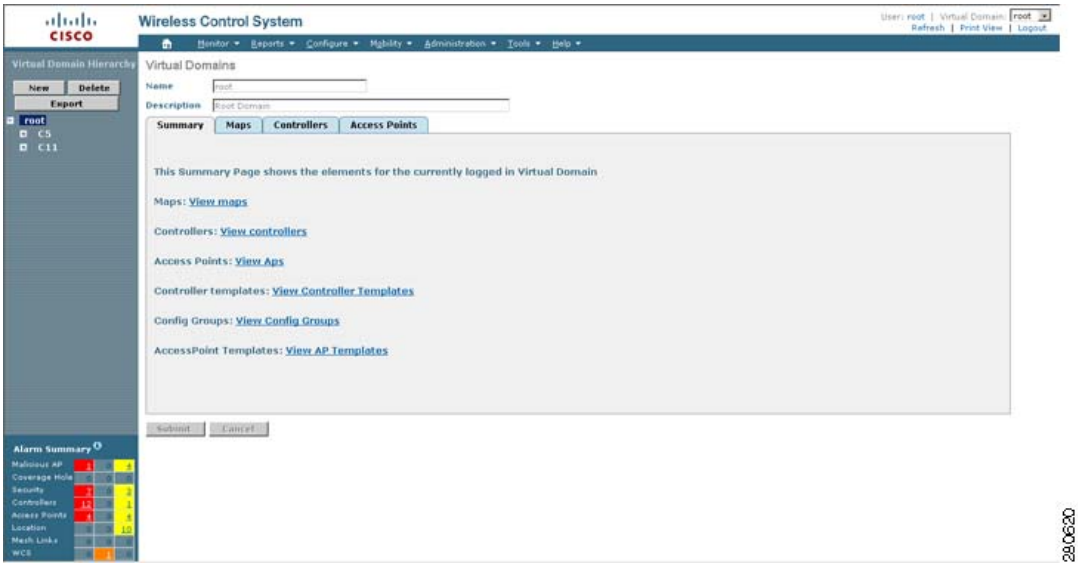
Note For more information on adding RADIUS and TACACS+ attributes to the ACS server, see the "Adding WCS UserGroups into ACS for TACACS+" section on page 16-7 or the "Adding WCS UserGroups into ACS for RADIUS" section on page 16-11.

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 menu at the top of the screen (see Figure 7-10). Only virtual domains that have been assigned to you are available in the drop-down menu.

Figure 7-10 Virtual Domains Summary Tab



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 Service Engines
- 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 WCS. It contains these sections:

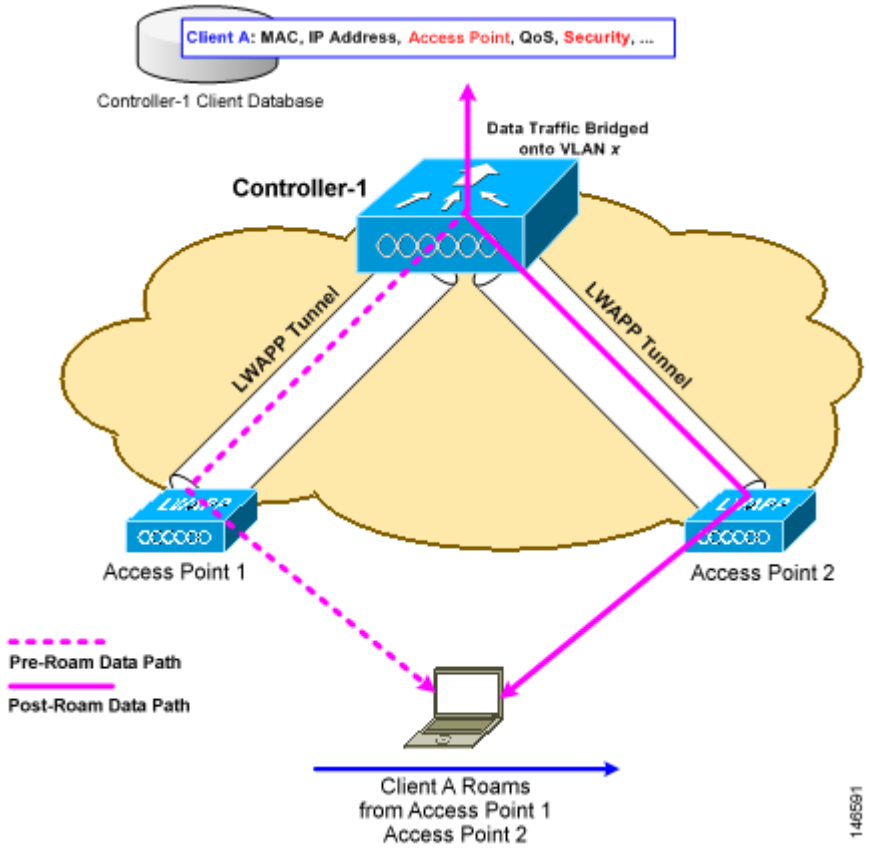
- Overview of Mobility, page 8-1
- Symmetric Tunneling, page 8-5
- Overview of Mobility Groups, page 8-5
- Messaging among Mobility Groups, page 8-7
- Mobility Anchors, page 8-12
- Configuring Multiple Country Codes, page 8-15
- Creating Config Groups, page 8-17
- Downloading Software, page 8-26

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.

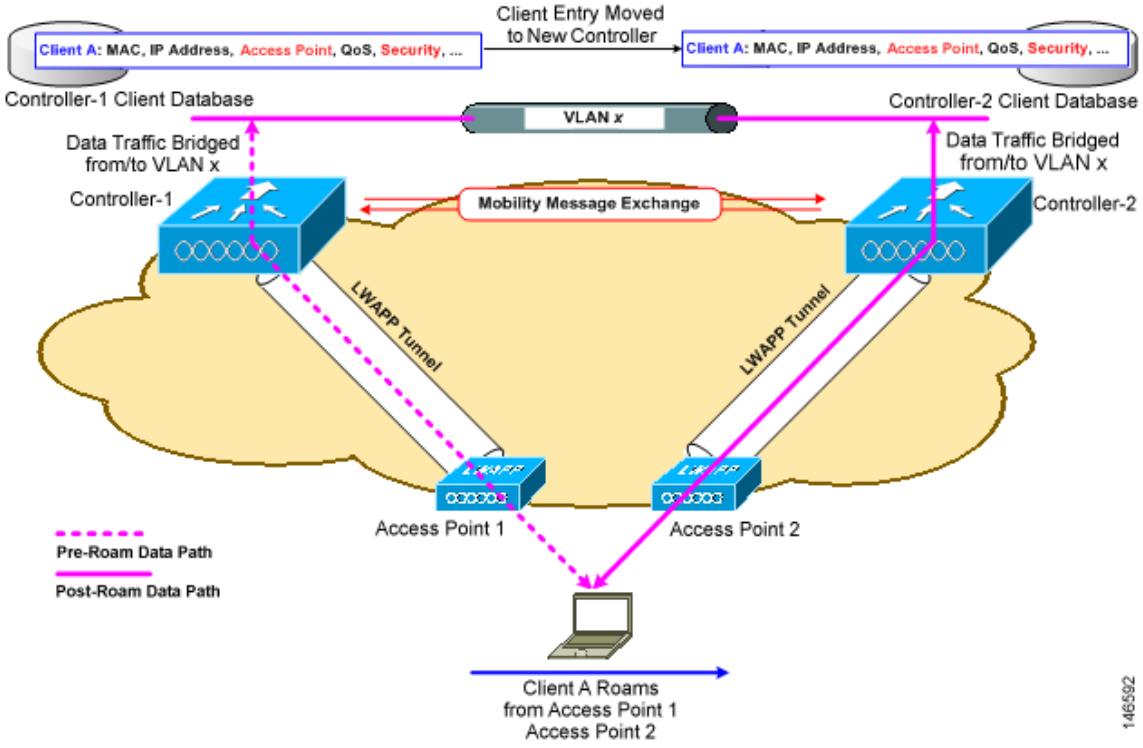
Figure 8-1 Intra-Controller Roaming



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

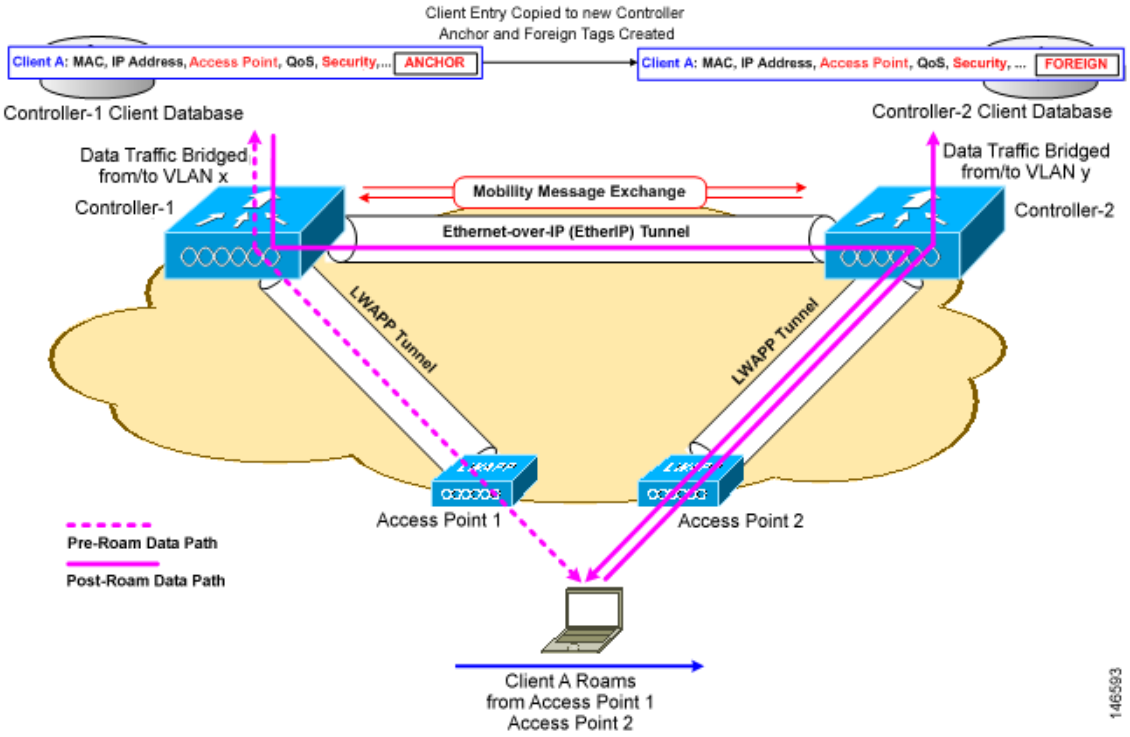


When the client associates to an access point joined to a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database 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.

Refer to the "Configuring General Templates" section on page 11-4 for instructions on configuring this feature within a template.

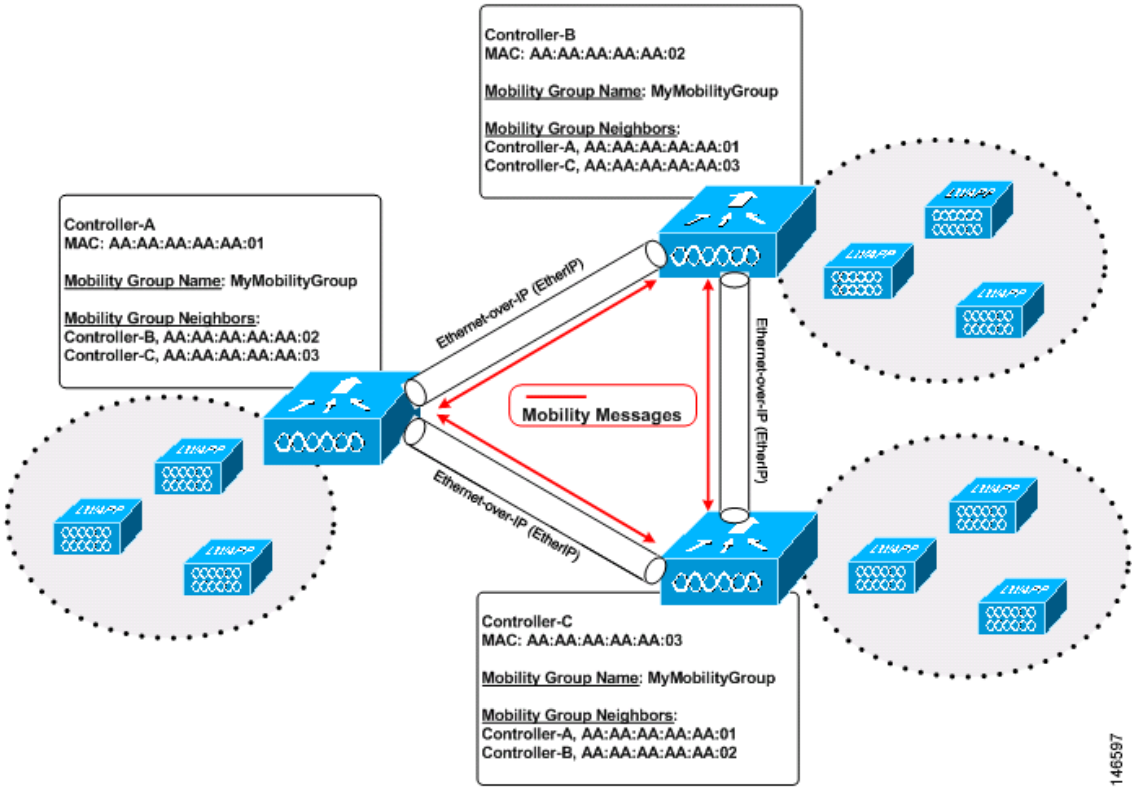
Overview of Mobility Groups

A set of controllers can be configured as a *mobility group* to allow seamless client roaming within a group of controllers. By creating a mobility group, you can enable multiple controllers in a network to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers can share the context and state of client devices and controller loading information. With this information, the network can support inter-controller wireless LAN roaming and controller redundancy.

Note Clients do not roam across mobility groups.

Figure 8-4 shows an example of a mobility group.

Figure 8-4 A Single Mobility Group



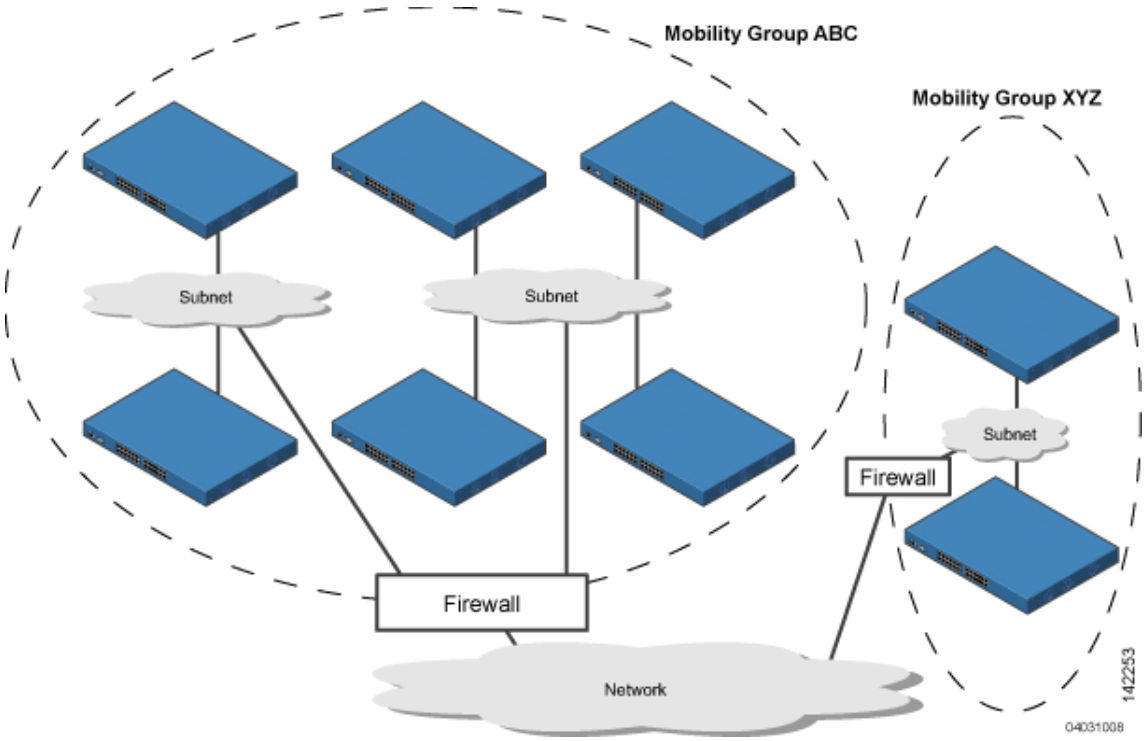
As shown above, each controller is configured with a list of the other members of the mobility group. Whenever a new client joins a controller, the controller sends out a unicast message to all of the controllers in the mobility group. The controller to which the client was previously connected passes on the status of the client. All mobility exchange traffic between controllers is carried over an LWAPP 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. Refer to 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.

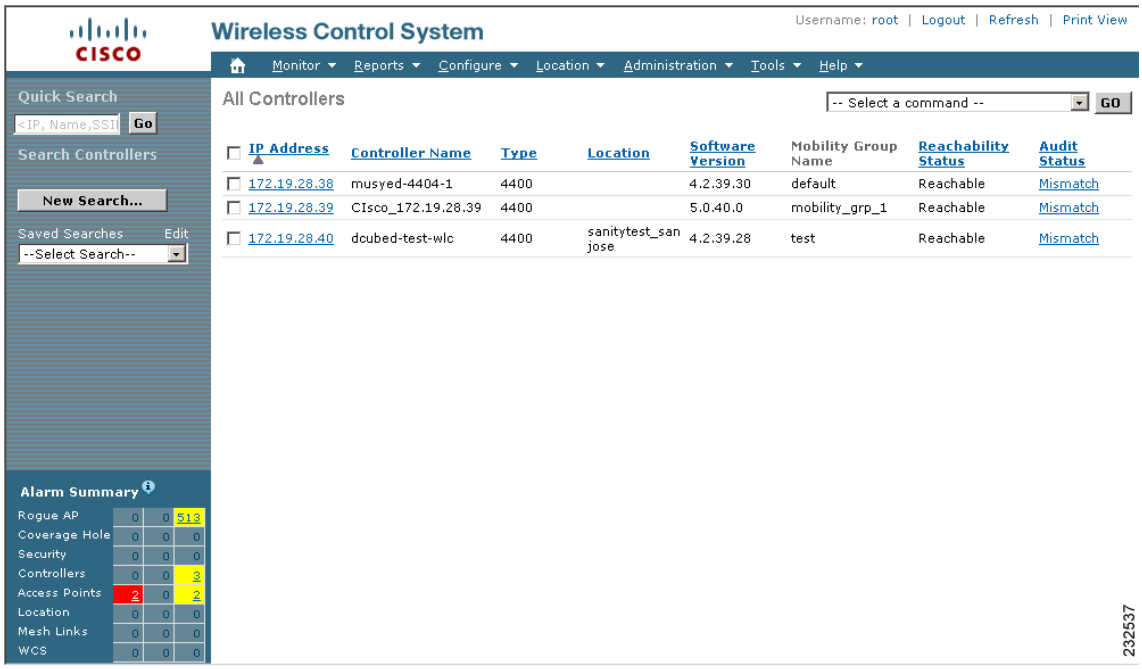
- You must have gathered the MAC address and IP address of every controller that is to be included in the mobility group. This information is necessary because you will be configuring all controllers with the MAC address and IP address of all the other mobility group members.

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 Navigate to **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.

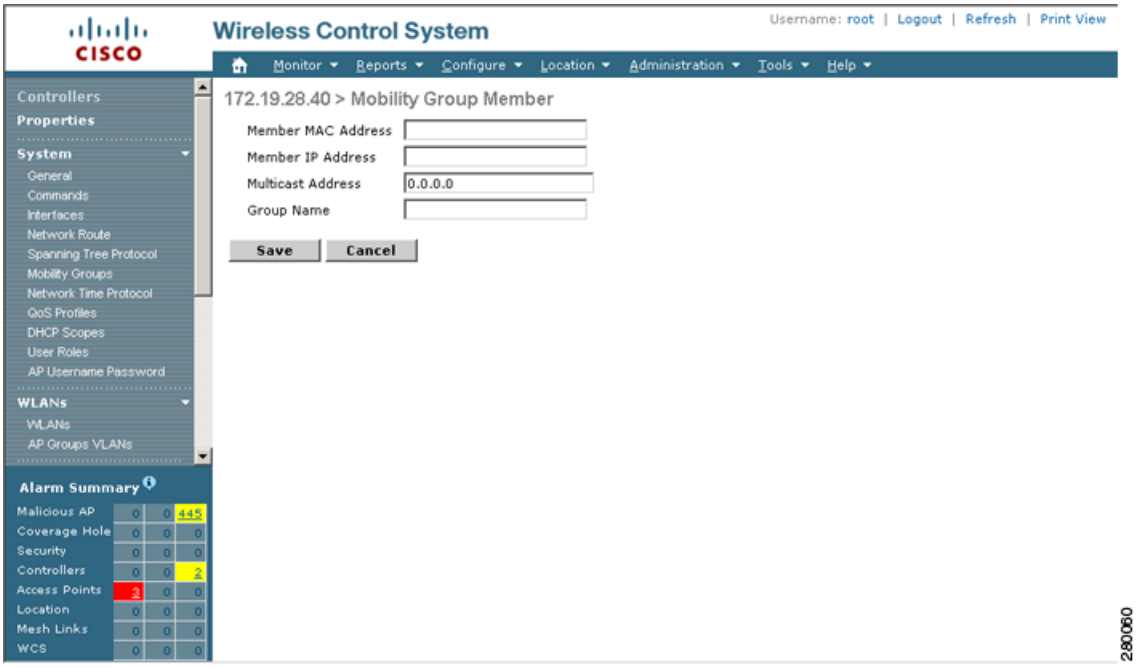
Step 3 Choose **System > Mobility Groups** on the left-hand side. The existing Mobility Group members are listed in the window (see Figure 8-7).

Figure 8-7 Existing Mobility Groups

Step 4 You will see a list of available controllers. From the Select a command drop-down menu 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 window appears.

Figure 8-8 Mobility Group Member Window



Step 6 In the Member MAC Address field, enter the MAC address of the controller to be added.

Step 7 In the Member IP Address field, 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 field. The local mobility member's group address must be the same as the local controller's group address.

Step 9 In the Group Name field, 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.

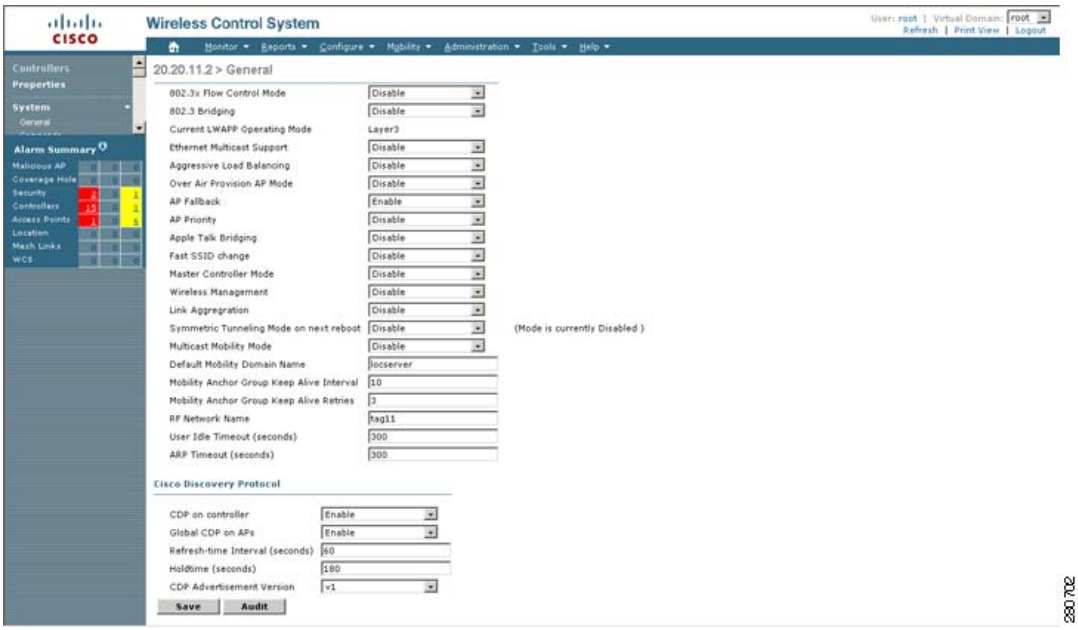
Note You must complete the steps in the "Configuring Mobility Groups" section on page 8-8 prior to setting the mobility scalability parameters.

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 > General** from the left sidebar menu. The General window as shown in Figure 8-9 appears.

Figure 8-9 System > General Window



Step 4 At the Multicast Mobility Mode parameter, specify if you want to enable or disable the ability for the controller to use multicast mode to send Mobile Announce messages to mobility members.

Step 5 If you enabled multicast messaging by setting multicast mobility mode to enabled, you must enter the group IP address at the Mobility Group Multicast-address 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 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.

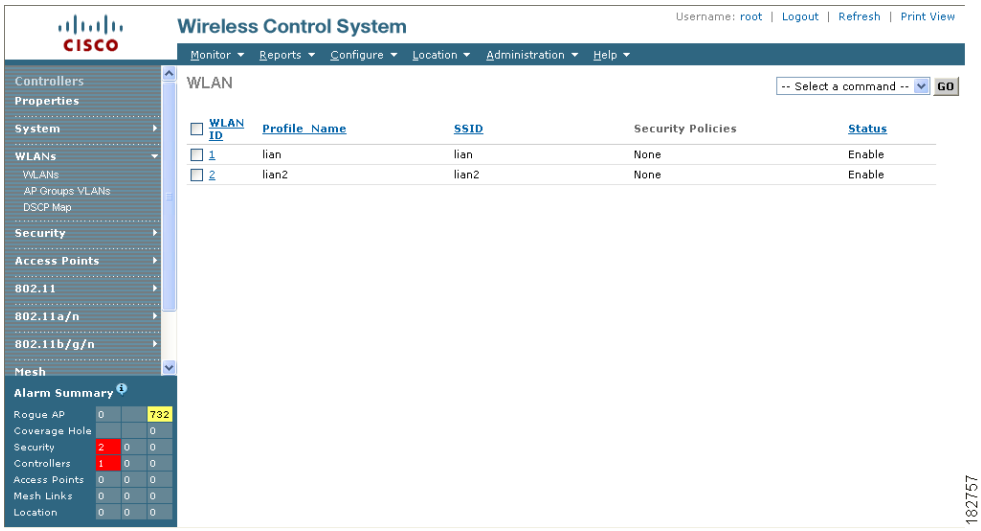
Step 1 Click **Configure > Controllers.**

Step 2 Choose a controller by clicking an IP address.

Step 3 Choose **WLANs > WLANs** from the left sidebar menu.

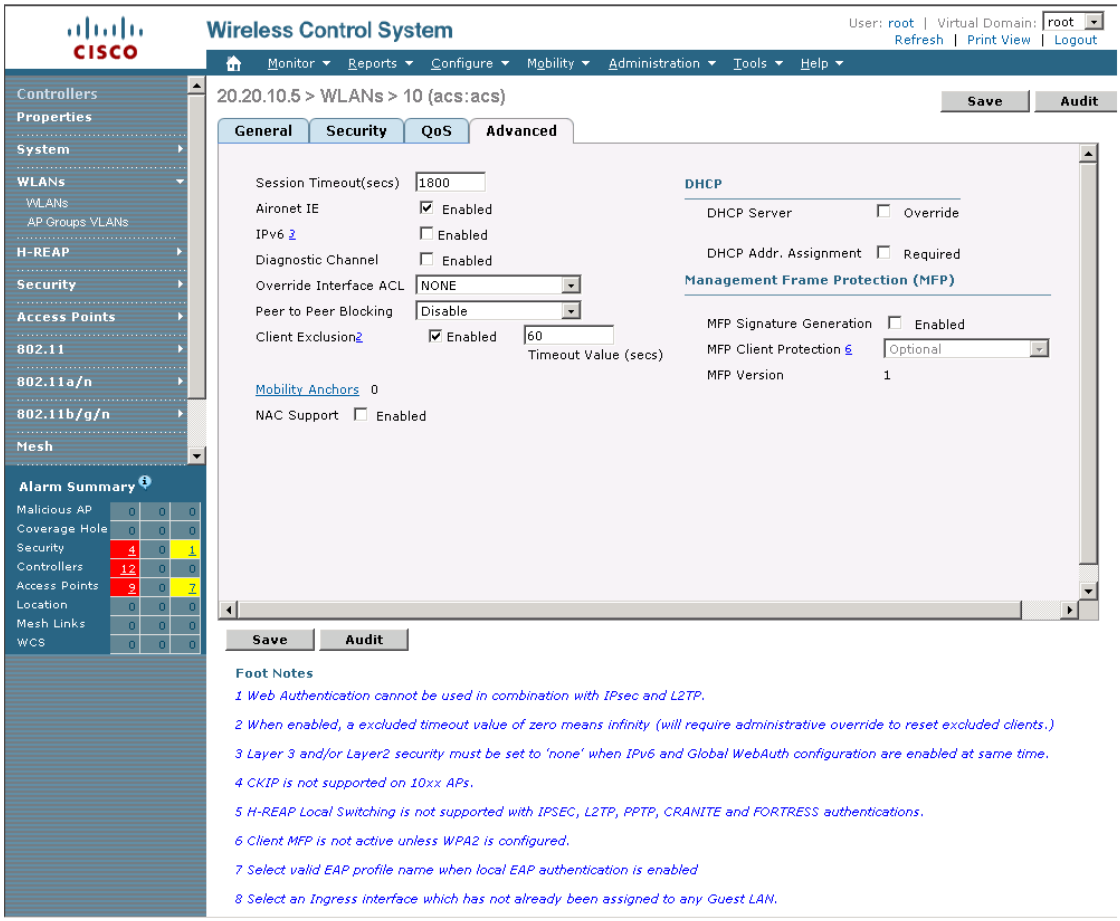
Step 4 Click the desired WLAN ID URL (see Figure 8-10).

Figure 8-10 WLAN Window



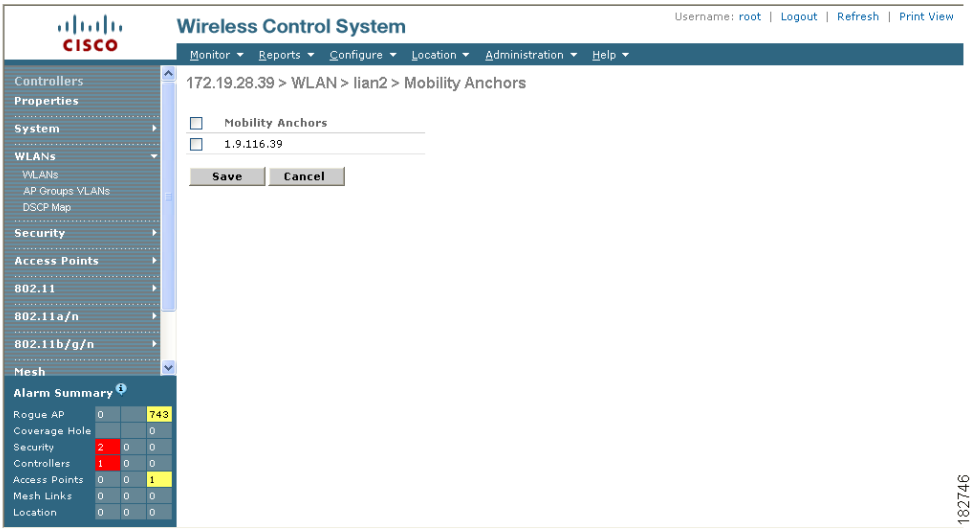
Step 5 After choosing a WLAN ID, a tabbed window appears (see Figure 8-11). Click the **Advanced** tab.

Figure 8-11 Advanced Window



Step 6 Click the **Mobility Anchors** link at the bottom of the page. The Mobility Anchors window appears (see Figure 8-12).

Figure 8-12 Mobility Anchors



Step 7 Check the IP address checkbox 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 10-3.

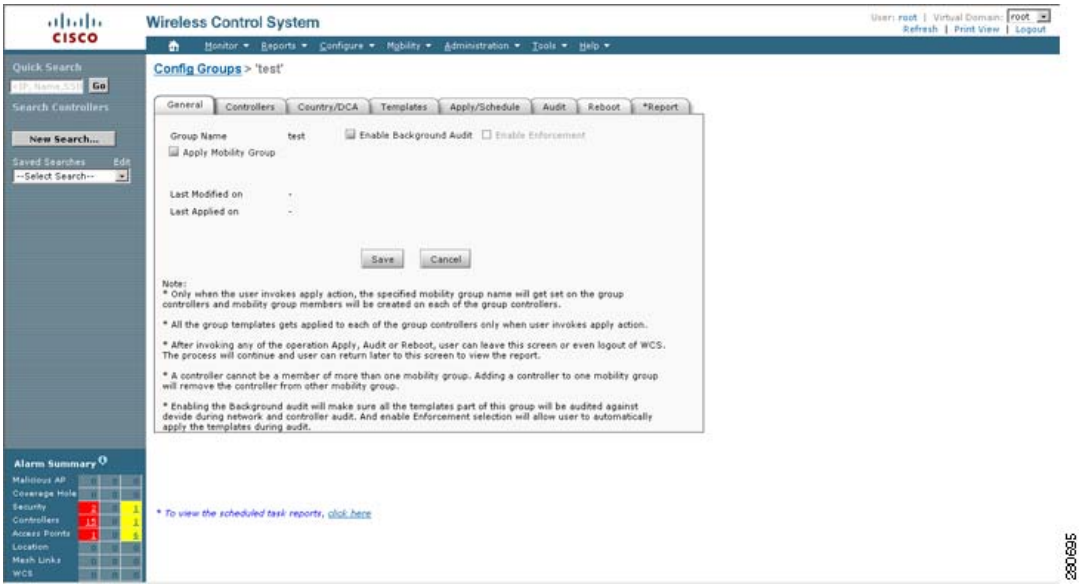
Step 1 Choose **Configure > Config Groups**.

Step 2 Choose **Add Config Groups** from the Select a command drop-down menu.

Step 3 Create a config group by entering the group name and mobility group name.

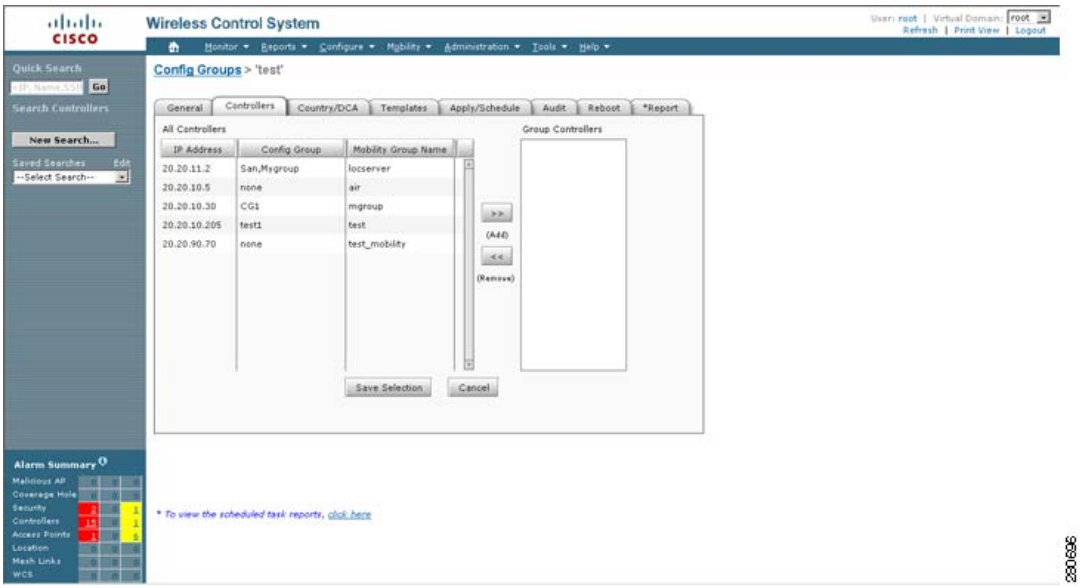
Step 4 Click **Save**. The Config Groups window appears (see Figure 8-13).

Figure 8-13 Config Groups Window



Step 5 Click the **Controllers** tab. The Controllers window appears (see Figure 8-14).

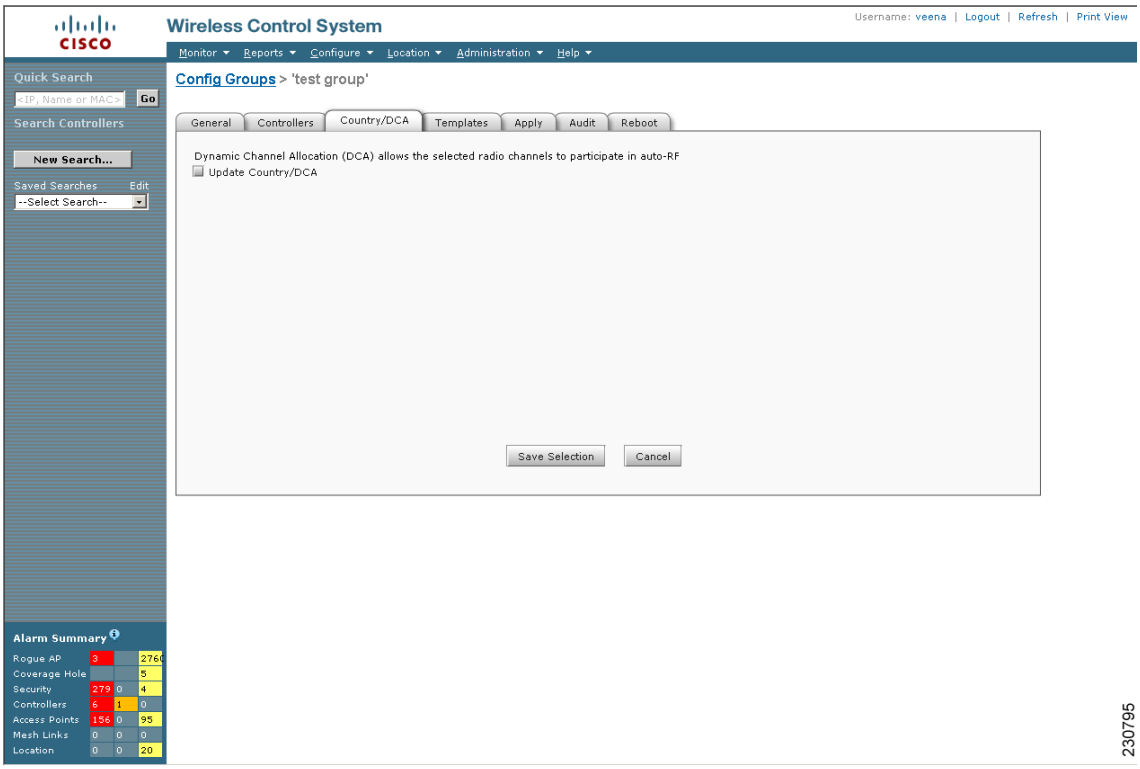
Figure 8-14 Controller Tab



Step 6 Highlight the controllers you want to add and click the **>> Add** button. The controller is added to the Group Controllers window.

Step 7 Click the **Country/DCA** tab. The Country/DCA window 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 Check the **Update Countries** 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 window. 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 11, "Using Templates."

By choosing **Configure > 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 menu, the page displays a table with the following columns:

- Check box: Check to select the config group.
- Group Name: Name of the config group.
- Mobility Group Name: Name of Mobility or WPS Group.
- Controllers: Number of controllers added to Config Group.
- Templates: Number of templates applied to config group.
- Scheduled: Indicates whether or not the provisioning of mobility group, mobility members, and templates has been scheduled.
- Next Scheduled Run: Indicates the date and time of the next scheduled provisioning.
- Last Modified: Date and time config group was last modified.
- Last Applied: Date and time last changes were applied.

Adding New Group

Follow these steps to add a config group.

Step 1 Choose **Configure > Config Groups**.

Step 2 From the Select a command drop-down list, choose **Add Config Group** and click **GO**. The Add New Group window 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.

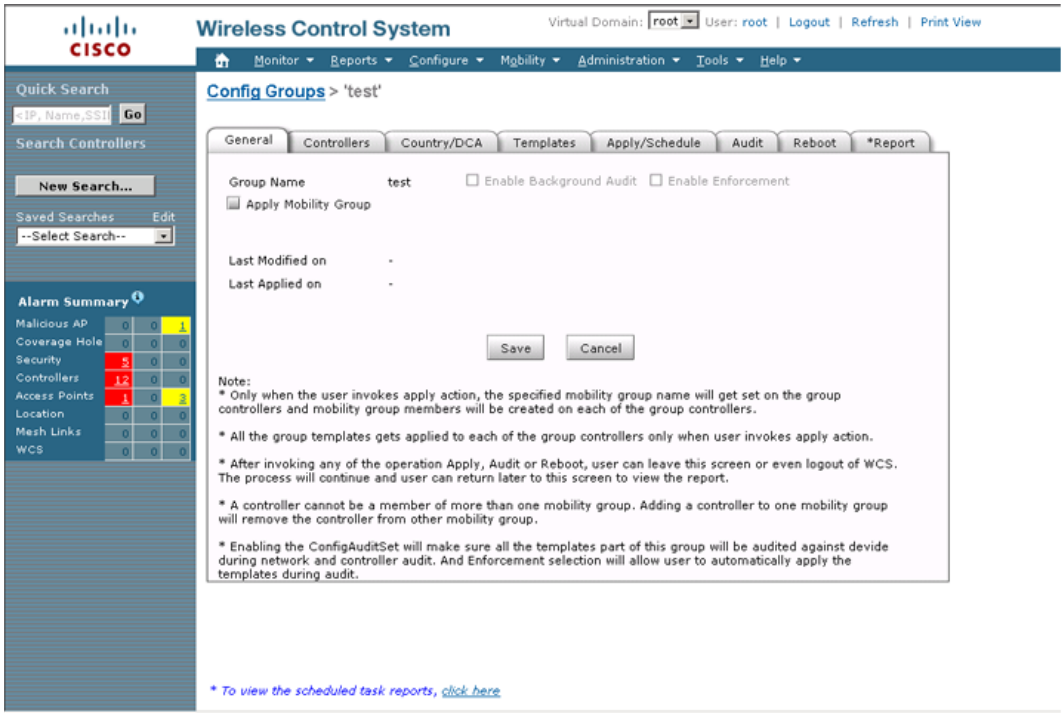
Step 4 Other templates created in WCS can be assigned to a config group. The same WLAN template can be assigned to more than one config group. Choose from the following:

- 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 window appears (see Figure 8-16).

Figure 8-16 Config Groups Window



Configuring Config Groups

Follow these steps to configure a config group.

Step 1 Choose **Configure > Config Groups**, and click a group name under the Group Name column. The Config Group window 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 for 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*.

- 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** 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**.

Enabling a Background Audit

If you enable a background audit on a config group, all of the templates that are part of this group are audited against the controller during network and controller audits.

This option to enable background audit will be disabled if the audit settings in the audit settings page are set to basic audit. This option is available when the Template based audit setting is chosen.

To change the audit settings, go to Administration > Settings > Audit.

After enable background audit is selected, you can select the **Enforce Configuration** checkbox. This ensures that the templates are automatically applied during the audit if any discrepancies are found.

Adding or Removing Controllers from Config Group

Follow these steps to add or remove controllers from a config group.

Step 1 Choose **Configure > 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** button.

Note If you want to remove a controller from the group, highlight the controller in the Group Controllers box and click the **<< Remove** button.

Step 5 You must choose the **Apply** tab and click the **Apply** button to add or remove the controllers to the config groups.

Step 6 Click the **Save Selection** button.

Adding or Removing Templates from the Config Group

Follow these steps to add or remove templates from the config group.

Step 1 Choose **Configure > 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** 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.

Step 1 Choose **Configure > 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 window or log out of Cisco WCS. The process continues, and you can return later to this page and 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 window. 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 window, you must choose landscape page orientation.

Step 4 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 5 Enter a starting date in the text box or use the calendar icon to choose a start date.

Step 6 Choose the starting time using the hours and minutes drop-down menus.

Step 7 Click **Schedule** to start the provisioning at the scheduled time.

Auditing Config Groups

The Config Groups Audit window 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 > Config Groups**, and click a group name under the Group Name column.

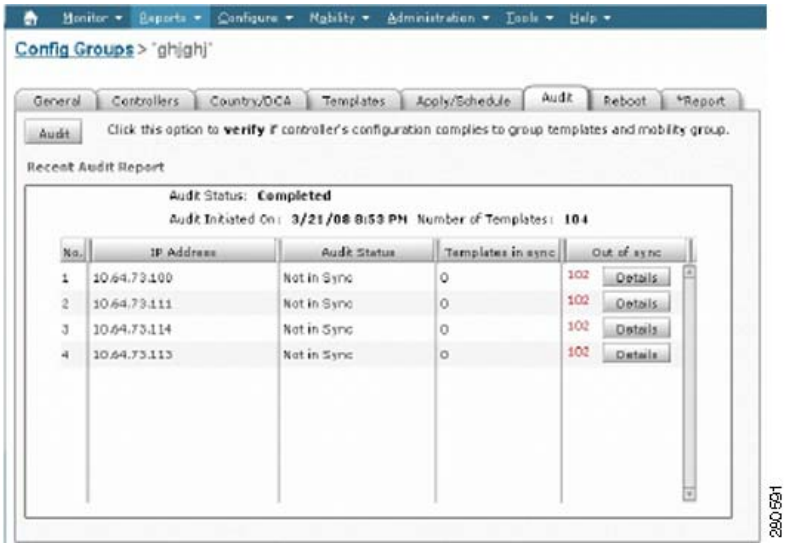
Step 2 Click the **Audit** tab to access this page.

Step 3 Click **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.

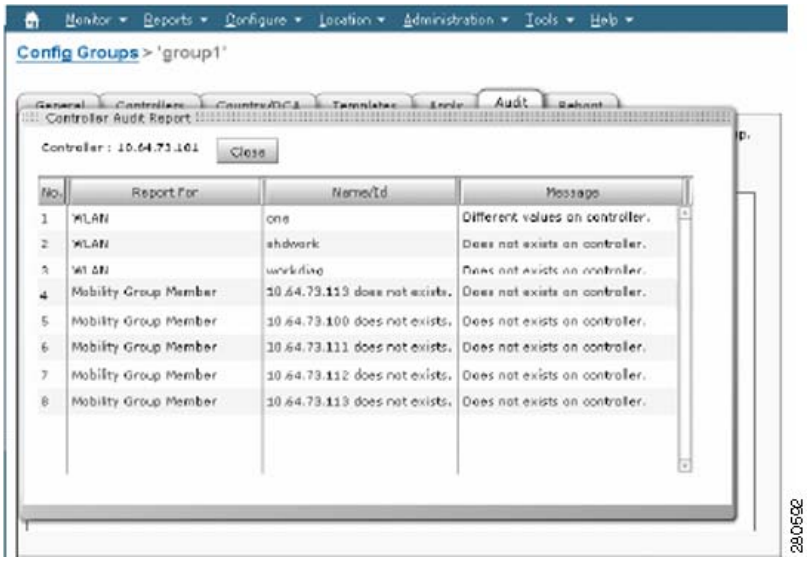
Note This audit does not enforce the WCS configuration to the device. It only identifies the discrepancies.

Figure 8-17 Config Groups Audit Tab



Step 4 Click **Details** to view the Controller Audit Report details (see Figure 8-18).

Figure 8-18 Controller Audit Report Details



Step 5 Double click a line item to open the Attribute Differences window. This window 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 window to the device.

Step 6 Click **Close** to return to the Controller Audit Report window.

Choosing Basic or Template-based Auditing

You can choose between basic and template-based auditing. The default setting is Basic Audit.

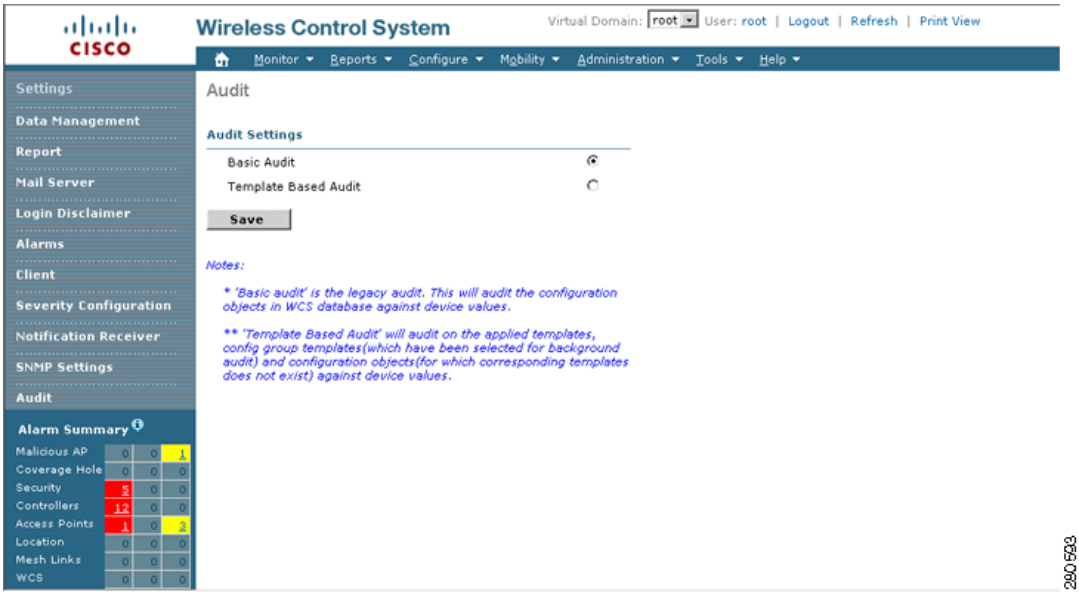
- Basic Audit—Audits the configuration objects in the WCS database against device values. This is the legacy audit. It is selected by default.
- Template-based Audit—Audits on the applied templates, config group templates (which have been selected for the background audit), and configuration audits (for which corresponding templates do not exist) against 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 window appears (see Figure 8-19).

Figure 8-19 Audit Settings Window



Step 3 Choose the radio button for either Basic or Template-Based Audit.

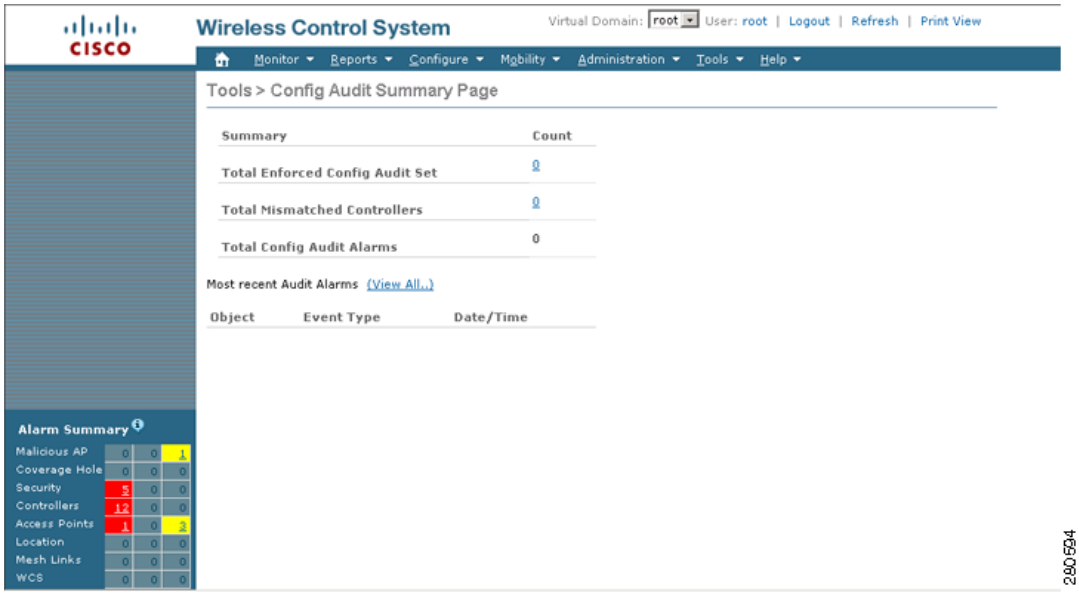
Step 4 Click **Save**.

Note These settings are in effect when the controller audit or network audit is performed.

Viewing Configuration Audit Summary

Choose **Tools > Config Audit** to launch the Configuration Audit Summary page (see Figure 8-20).

Figure 8-20 Tools > Config Audit Summary Window



This page provides a summary of the following:

- Config groups enabled for background audit—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 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.

Rebooting Config Groups

Follow these steps to reboot a config group.

Step 1 Choose **Configure > Config Groups**, and click a group name under the Group Name column.

Step 2 Click the **Reboot** tab.

Step 3 Click 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 window or logout of Cisco WCS. The process continues, and you can return later to this page and view a report.

The Recent Reboot Report window 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 window, 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 > Config Groups**, and click a group name under the Group Name column.

Step 2 Click the **Report** tab. The Recent Apply Report window 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.

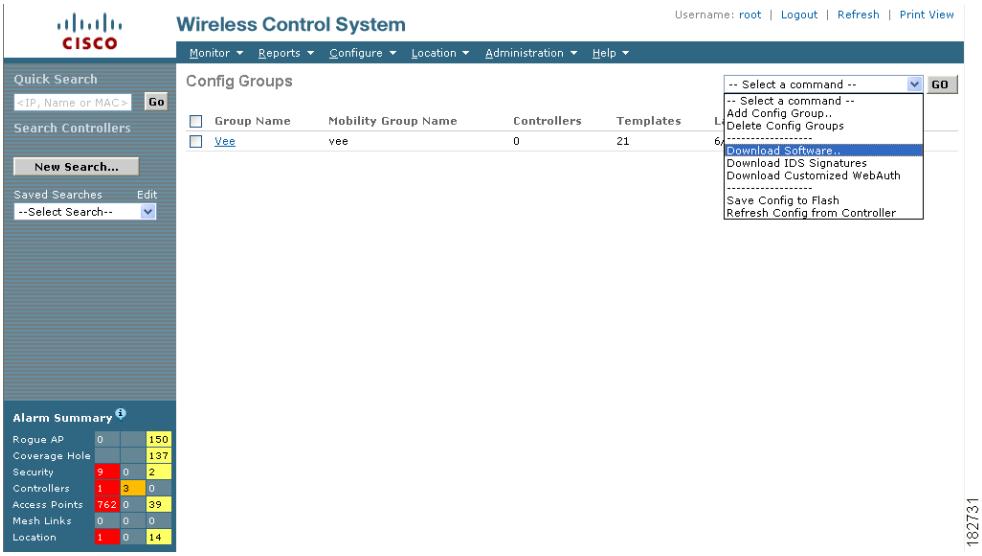
Downloading Software

Follow these steps to download software to all controllers in the selected groups after you have a config group established.

Step 1 From Configure > Config Groups, click the check box to choose one or more config groups names on the Config Groups window.

Step 2 Choose **Download Software** from the Select a command drop-down menu and click **GO** (see Figure 8-21).

Figure 8-21 Download Software Option



Step 3 The Download Software to Controller window 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 4 Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries parameter.

Step 5 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 6 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 7 Click **OK**.

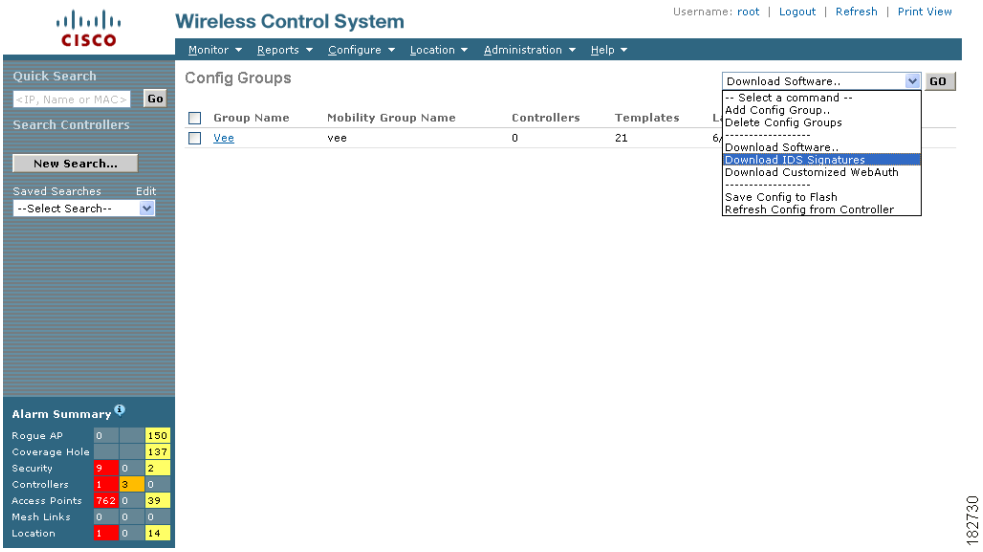
Downloading IDS Signatures

Follow these steps to download intrusion detection system (IDS) signature files from your config group to a local TFTP server.

Step 1 From Configure > Config Groups, click the check box to choose one or more config groups on the Config Groups window.

Step 2 Choose **Download IDS Signature**s from the Select a command drop-down menu and click **GO** (see Figure 8-22).

Figure 8-22 Downloading IDS Signatures Option



Step 3 The Download IDS Signatures to Controller window 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 4 Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries parameter.

Step 5 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 6 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 7 Click **OK**.

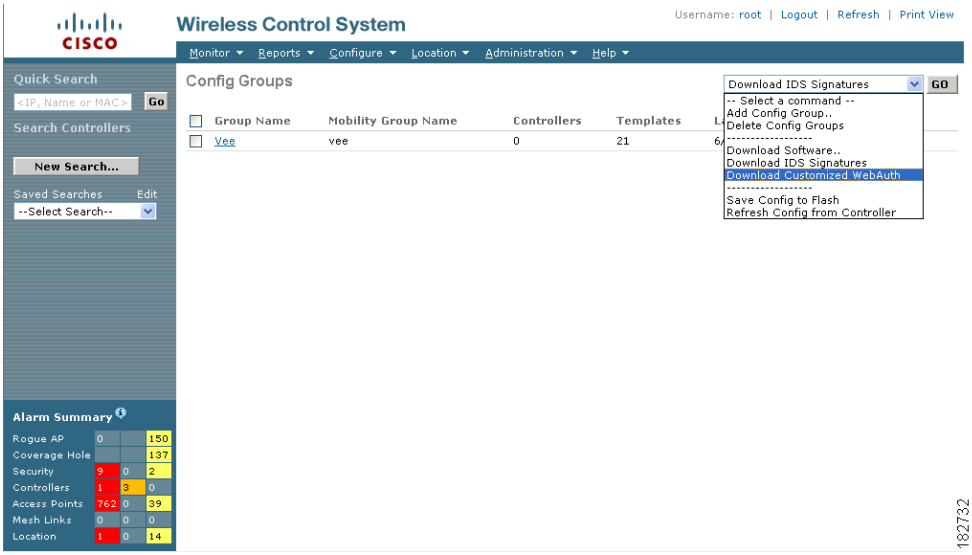
Downloading Customized WebAuth

Follow these steps to download customized web authentication.

Step 1 From Configure > Config Groups, click the check box to choose one or more config groups on the Config Groups window.

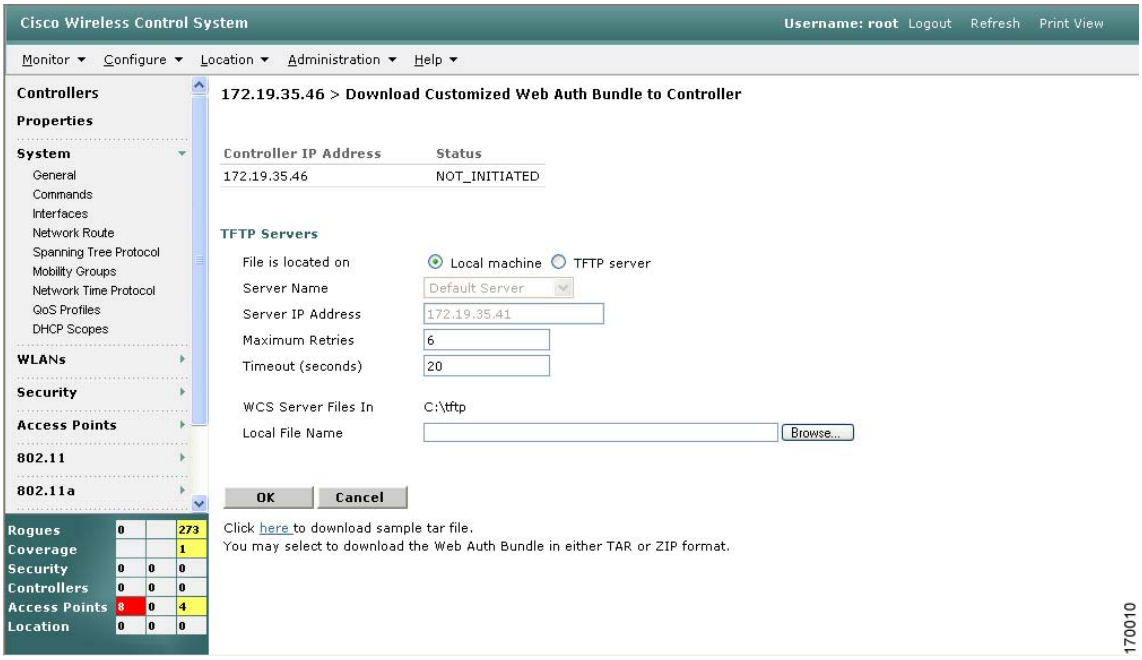
Step 2 Choose **Download Customized WebAuth** from the Select command drop-down menu and click **GO** (see Figure 8-23).

Figure 8-23 Download Customized Web Auth



Step 3 The Download Customized Web Auth Bundle to Controller window appears. The IP address of the controller to receive the bundle and the current status are displayed (see Figure 8-24).

Figure 8-24 Download Customized Web Auth Bundle to Controller



Step 4 Choose **local machine** from the File is Located On parameter.

Step 5 Enter the amount of times the controller should attempt to download the file in the Maximum Retries field.

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

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.

Step 8 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 and retried.

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
- Autonomous to LWAPP Migration Support, page 9-3
- Configuring Access Points, page 9-7
- Configuring Access Point Radios for Location Optimized Monitor Mode, page 9-14
- Searching Access Points, page 9-16
- Viewing or Editing Rogue Access Point Rules, page 9-17
- Configuring Spectrum Experts, page 9-18

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 Priority drop-down, choose **Enabled**.

To then 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 menu, choose the applicable priority (Low, Medium, High, Critical).

Note The default priority is Low.

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. Refer to the "Configuring Access Point Templates" section on page 11-80 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.

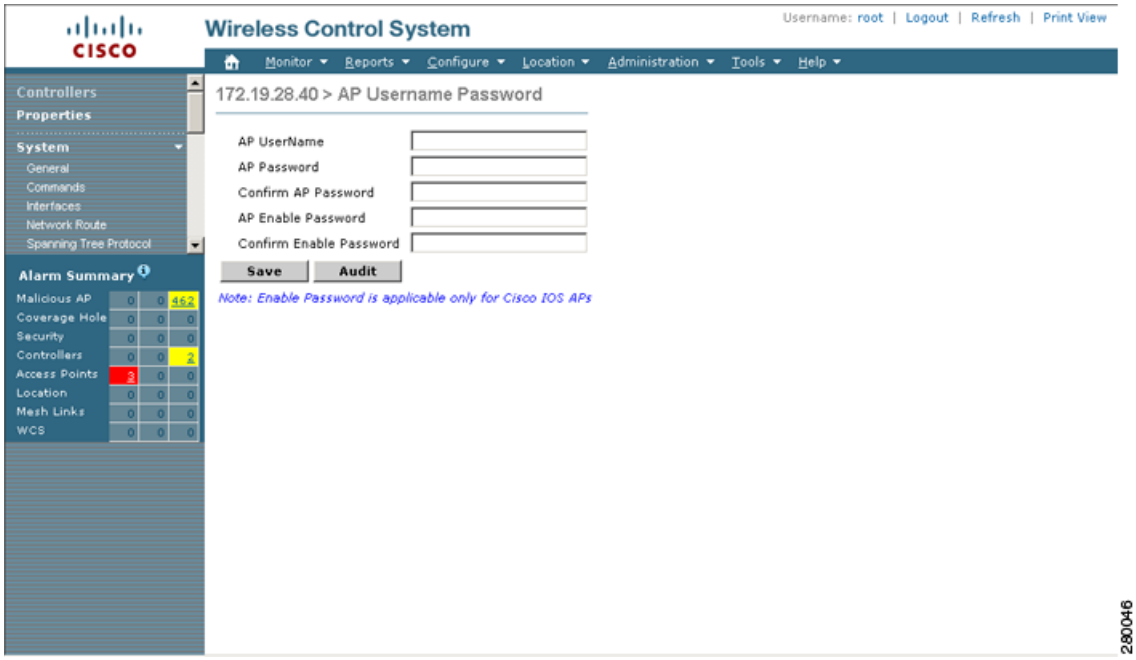
Follow these steps to establish a global username and password.

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 window appears (see Figure 9-1).

Figure 9-1 AP Username Password Window



Step 4 In the AP Username field, enter the username that is to be inherited by all access points that join the controller.

Step 5 In the AP Password field, enter the password that is to be inherited by all access points that join the controller. Re-enter in the Confirm AP Password field.

Step 6 For Cisco autonomous access points, you must also enter and confirm an enable password. In the AP Enable Password field, enter the enable password that is to be inherited by all access points that join the controller. Re-enter in the Confirm Enable Password field.

Step 7 Click **Save**.

Autonomous to LWAPP Migration Support

The autonomous to LWAPP migration support feature provides a common application (WCS) from which you can perform basic monitoring of autonomous access points along with current LWAPP access points. The following autonomous access points are supported:

- Cisco Aironet 1100 Access Point
- Cisco Aironet 1130 Access Point
- Cisco Aironet 1200 Access Point
- Cisco Aironet 1240 Access Point
- Cisco Aironet 1240 Access Point
- Cisco Aironet 1310 Bridge

You may also choose to convert autonomous access points to LWAPP.

From WCS, the following functions are available when managing autonomous access points:

- Adding Autonomous Access Points to WCS
- Configuring autonomous access points
- Viewing Autonomous Access Points in WCS
- 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.
  - See Background Task for more information
- 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 LWAPP 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 menu, 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 Enter the SNMP parameters including version number, number of retries, and timeout in seconds.

Step 7 Enter Telnet credentials for migration (optional).

Note The Telnet credentials are required to convert the access points from autonomous to unified.

Note If the autonomous access point already exists, WCS updates the credentials (SNMP and Telnet) to the existing device.

Step 8 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 menu, 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.

Note The CSV file has the same format as Adding Controllers but includes additional (optional) columns such as telnet_username, telnet_password, and enable_password.

Step 6 Click **OK**.

To remove an autonomous access point from WCS:

Step 1 Select the check box(es) of the appropriate access point(s).

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**.**

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 an LWAPP access point. The WGB and its wired clients are listed as client in WCS.

Choose **Monitor > WGBs** to view a list of all WCS clients that are in WGBs. 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 LWAPP Access Point Migration

To make a transition from an Autonomous solution to a Unified architecture, autonomous access points must be converted to LWAPP access points. The migration utility is available from the **Configure > Migration Templates** page where existing templates are listed.

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, 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 migrating an already-managed autonomous access point to LWAPP, its location and antenna information is migrated as well. You do not need to re-input the information. WCS automatically removes the autonomous access point after migration.

Adding/Modifying a Migration Template

To add a new template, select **Add Template** from the **Select a command** drop-down list.

To modify an existing template, click the template name from the summary list.

Enter or modify the following migration parameters:

General

- Template 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 WAN Link—Increases the default timeouts for the CLI commands executed on the access point.
- DNS Address
- Domain Name

Controller Details

Note Ensures that the access point authorization information (SSC) can be configured on this controller and the converted access points can join.

- Controller IP—Enter the IP address of the WLAN controller you are wanting to add to the newly migrated access point.
- 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 LWAPP conversion file defined in the TFTP directory during WCS setup (for example, c1240-rcvk9w8-tar.123-11JX1.tar).

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.
- **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:

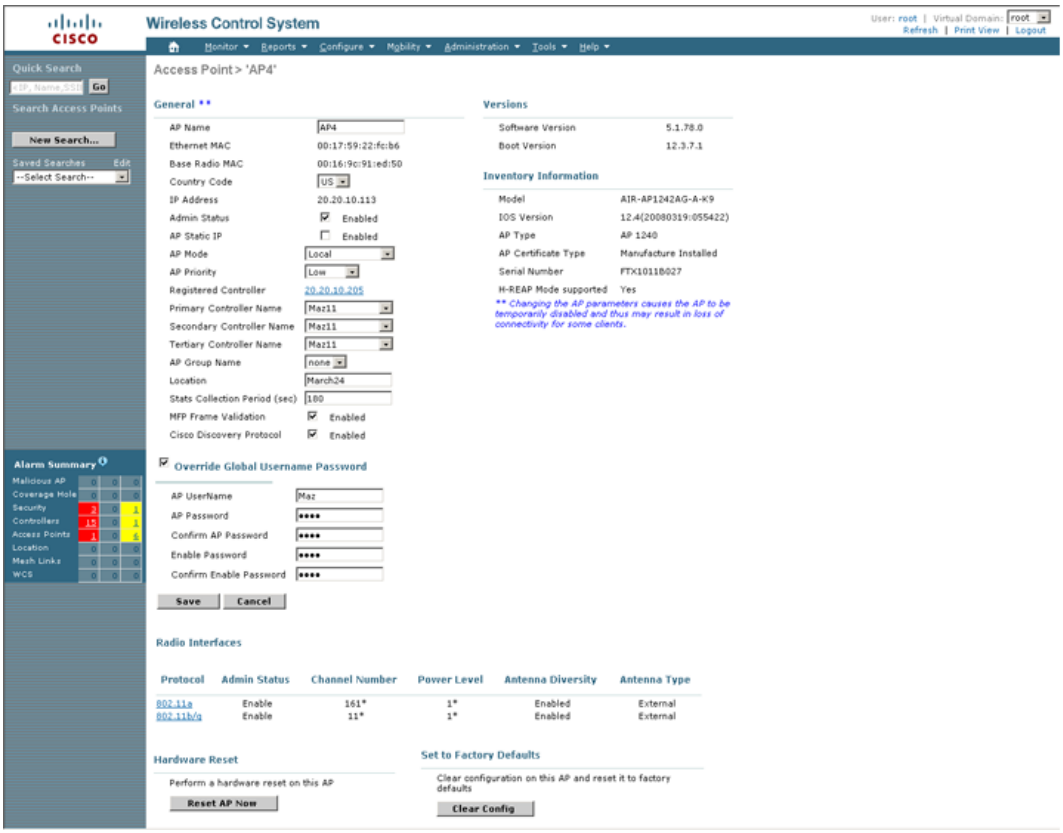
- Ethernet MAC
- IP Address
- Radio
- Map Location
- AP Type
- Controller
- Operation Status
- Alarm Status
- Audit Status

Note If you hover 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 following window appears (see Figure 9-2).

Figure 9-2 Detailed Access Point Information

.



Note There is no need to add access points to the Cisco WCS database. 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.

Some of the parameters on the window are supplied.

- The General portion displays the Ethernet MAC, the Base Radio MAC, and IP Address.
- The Versions portion of the window displays the software and boot version.
- The Inventory Information portion displays the model, IOS version, and serial number and type of the access point, provides which certificate type is required, and determines whether H-REAP mode is supported or not.
- 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.

Step 2 Enter the name assigned to the access point.

Step 3 Use the drop-down menu 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 http://www.cisco.com/warp/public/779/smbiz/wireless/approvals.html.

Step 4 If you want to enable the access point for administrative purposes, check the **Enabled** check box.

Step 5 If you click **Enabled** 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 menu. 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.
- 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 location optimized monitor mode (LOMM) feature. When LOMM is enabled, you can specify which four channels within the 2.4GHz 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 LOMM, you must also make additional edits on the 802.11b/g radio of the access point. Refer to the "Configuring Access Point Radios for Location Optimized Monitor Mode" section on page 9-14 for configuration details.

- Rogue Detector — In this mode, the access point radio is turned off, and the access point listens to wired traffic only. 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 Mode — 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.
- HREAP —Choose **HREAP** from the AP Mode drop-down menu to enable hybrid REAP for up to six access points. The HREAP access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost.

Step 7 In the Primary, Secondary, and Tertiary Controller fields, you can define the order in which controllers are accessed.

Step 8 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.

Step 9 Enter a description of the physical location where the access point was placed.

Step 10 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 11 Choose Enabled 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 12 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, and the receiving access points which were configured to detect MFP frames 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 13 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 14 On the System > AP Username Password window, 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 window. If you want to override the global credentials for this particular access point, click 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 15 Select the role of the mesh access point from the AP Role drop-down menu. 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 16 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 17 Select the data rate for the backhaul interface from the drop-down menu. 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 18 Choose the Enable option from the Ethernet Bridging drop-down menu to enable Ethernet bridging for the mesh access point.

Step 19 Click **Save** to save the configuration.

Step 20 If you need to perform a hardware reset on this access point, click **Reset AP Now**.

Step 21 If you need to clear the access point configuration and reset all values to the factory default, click **Clear Config**.

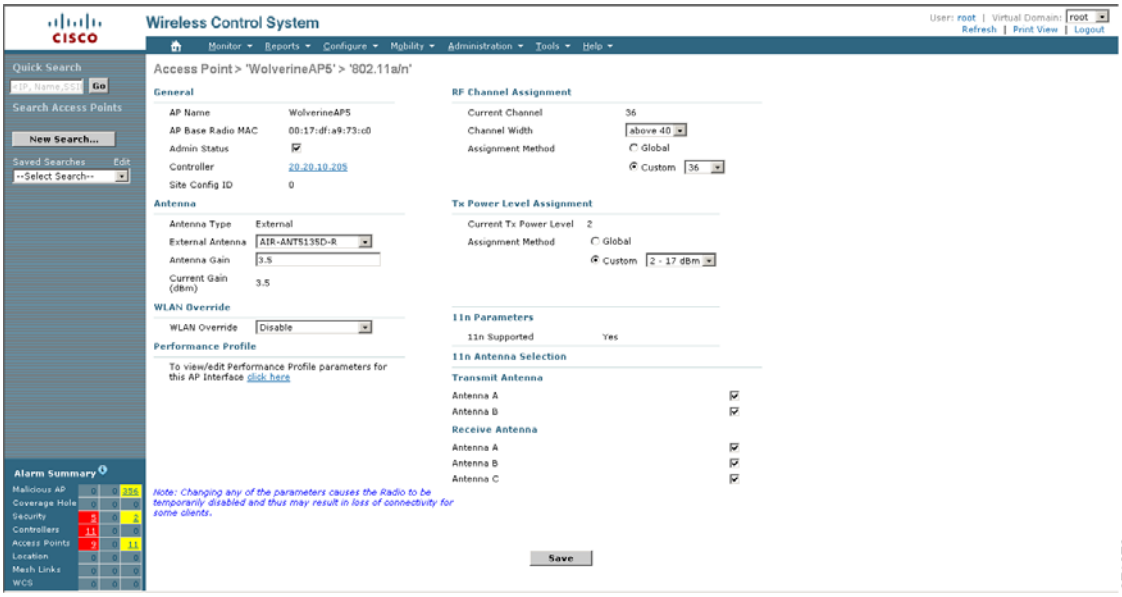
11n Antenna Selection

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 9-3).

Figure 9-3 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—Check 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.

Antenna

- Antenna Type—Indicates an external or internal antenna.
- External Antenna—Use the drop-down menu to choose the appropriate external 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.
- Current Gain—The current antenna gain.

WLAN Override

- WLAN Override—Enable or disable WLAN override for this access point. .

Performance Profile

Click the URL to view or edit performance profile parameters for this access point interface.

RF Channel Assignment

- Current Channel—The current channel being utilized.
- Channel Width—Select the channel bandwidth from the drop-down menu.
- 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. Choose a channel from the drop-down list.

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 Parameters

- 11n Supported—Indicates whether or not 802.11n radios are supported.

11n Antenna Selection

- 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.

Configuring Access Point Radios for Location Optimized Monitor Mode

To optimize monitoring and location calculation of tags, you can enable LOMM 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 LOMM 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 9-7.

Follow the steps below to set enable LOMM 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 At the All Access Points Summary window, choose the **802.11 b/g Radio** link for the appropriate access point.

Step 3 At the Radio parameters window, disable **Admin Status** by unchecking the check box. This disables the radio.

Step 4 Check the **Location Optimized Channel Assignment** checkbox. Drop-down menus 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 menu.

Step 6 Click **Save**. Channel selection is saved.

Step 7 At the Radio parameters window, re-enable the radio by checking the **Admin Status** check box.

Step 8 Click **Save**. The access point is now configured as a LOMM access point.

The AP Mode displays as Monitor/LOMM on the **Monitor > Access Points** window.

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 menu, choose **Schedule Radio status**.

Step 4 Click **GO**.

Step 5 Choose **Enable** or **Disable** from the Admin Status drop-down menu.

Step 6 Use the **Hours** and **Minutes** drop-down menus 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 **Submit** 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 menu, choose **View Scheduled 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 window 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 menu. 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 controls in the left sidebar to create and save custom searches:

- **New Search** drop-down menu: Opens the Search Access Points window. Use the Search Access Points window to configure, run, and save searches.
- **Saved Searches** drop-down menu: Lists the saved custom searches. To open a saved search, choose it from the Saved Searches list.
- **Edit Link**: Opens the Edit Saved Searches window. You can delete saved searches in the Edit Saved Searches window.

You can configure the following parameters in the Search Access Points window:

- Search By
- Radio Type
- Search in
- Save Search
- Items per page

After you click GO, the access point search results appear:

Table 9-1 Access Point Search Results

Parameter	Options
AP Name	Name assigned to the access point. Click the access point name item to display details.
WCS	WCS name where access point was detected.
Ethernet MAC	MAC address of the access point.
IP Address	IP address of the access point.
Radio	Protocol of the access point is either 802.11a/n or 802.11b/g/n.
Map Location	Campus, building, and floor location.
Controller	IP address of the controller.
Admin Status	Administration site of the access point (Enabled or Disabled).
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

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. Refer to the "Configuring a Rogue AP Rules Template" section on page 11-43 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**.

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 menu.

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** panel.

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 10-1
- Setting Multiple Country Codes, page 10-3
- Searching Controllers, page 10-4
- Managing User Authentication Order, page 10-5
- Viewing Audit Status (for Controllers), page 10-5
- Viewing Latest Network Audit Report, page 10-7
- Setting AP Failover Priority, page 10-8
- Pinging a Network Device from a Controller, page 10-8
- Enabling Load-Based CAC for Controllers, page 10-9
- Enabling High Density, page 10-11
- Configuring 802.3 Bridging, page 10-14
- Configuring an RRM Threshold Controller (for 802.11a/n or 802.11b/g/n), page 10-14
- Configuring 40-MHz Channel Bonding, page 10-15
- Configuring EDCA Parameters for Individual Controller, page 10-16
- Configuring SNMPv3, page 10-17
- Viewing All Current Templates, page 10-17
- Configuring NAC Out-of-Band Integration, page 10-18
- Configuring Wired Guest Access, page 10-23
- Using Switch Port Tracing, page 10-27

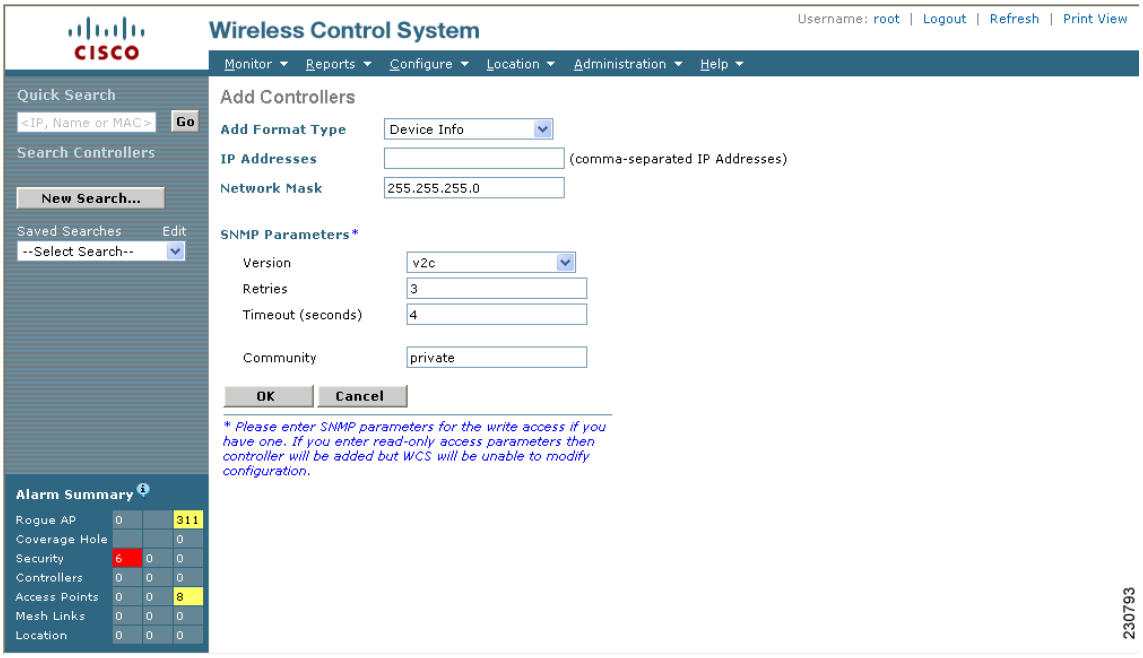
Adding Controllers

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 menu choose **Add Controllers** and click **GO**. The Add Controller window appears (see Figure 10-1).

Figure 10-1 Add Controller Window



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 menu at Device Info.

If you want to add multiple controllers by importing a CSV file, choose **File** from the Add Format Type drop-down menu. The CSV file allows you to generate your own import file and add the devices you want.

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 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.

Step 5 Click **OK**.

Setting Multiple Country Codes

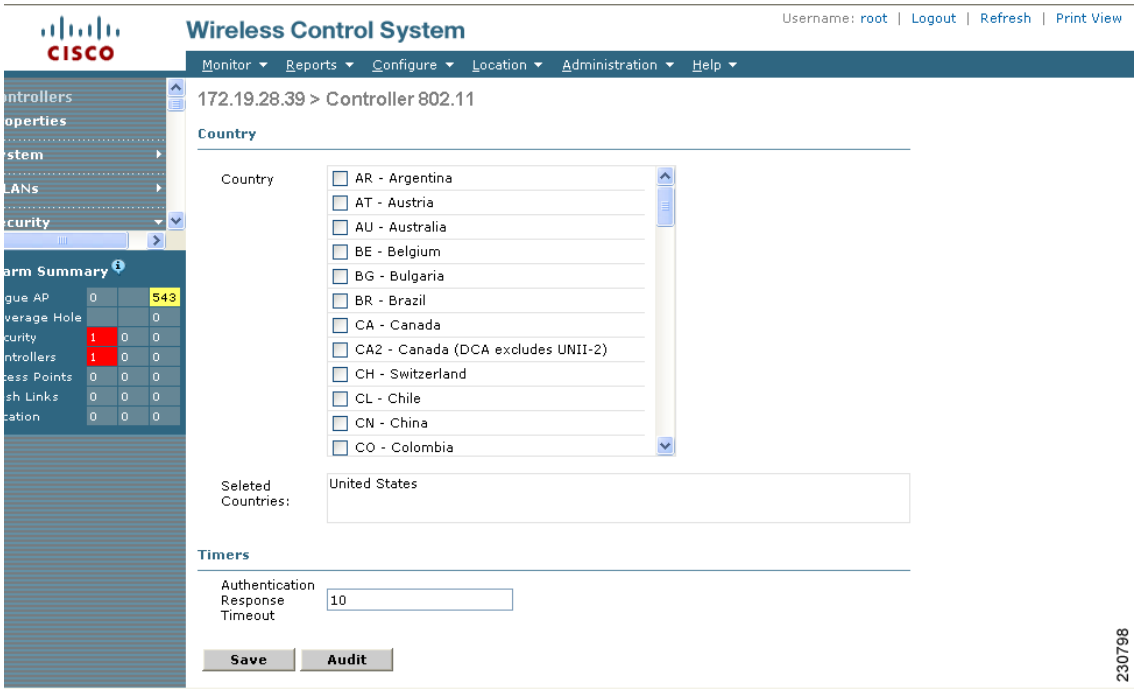
To set multiple country support for a single controller(s) that is not part of a mobility group, follow the steps below.

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the controller for which you are adding countries.

Step 3 Select **802.11 > General** from the left sidebar menu. The Controller 802.11 window appears (see Figure 10-2).

Figure 10-2 Controller 802.11



Step 4 Click the check box to choose which country you want to add. Access points are designed for use in many countries with varying regulatory requirements. You can configure a country code to ensure that it complies with your country'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**.

Searching Controllers

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

- **New Search** drop-down menu: Opens the Search Controllers window. Use the Search Controllers window to configure, run, and save searches.
- **Saved Searches** drop-down menu: Lists the saved custom searches. To open a saved search, choose it from the Saved Searches list.
- **Edit Link**: Opens the Edit Saved Searches window. You can delete saved searches in the Edit Saved Searches window.

You can configure the following parameters in the Search Controllers window:

- Search for controller by— Choose all controllers, IP address, or controller name.
- Select a Network— Choose all networks or an individual network.
- Save Search— Check the Save Search check box and enter a name in the Save Search text field to save the search in the Saved Searches drop-down list.
- Search by 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 window. The range is 10 to 100 items per window. The default is 20.

After you click **GO**, the controller search results appear:

Table 10-1 Search Results

Parameter	Options
IP Address	Local network IP address of the controller management interface. Clicking the title toggles from ascending to descending order. Clicking an IP address in the list displays a summary of the controller details.
WCS	User-defined WCS name.
Controller Name	Clicking the title toggles from ascending to descending order.
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 from ascending to descending order.

Table 10-1 Search Results

Parameter	Options
Mobility Group Name	Name of the controller or WPS group.
Reachability Status	Reachable or Unreachable. Clicking the title toggles from ascending to descending order.

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 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 menu in the Configure > Controllers window or by clicking **Audit Now** directly from the Controller Audit Report.

Note A current Controller Audit Report can be accessed from the Configure > Controllers window by choosing an object from the Audit Status column.

To audit a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the check box for the applicable controller.

Step 3 From the Select a command drop-down menu, choose **Audit Now.**

Step 4 Click **GO**.

Step 5 When you perform the Refresh values from controller action from the View Audit Status page, a confirmation is shown.

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 (i.e, 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 8-17 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 8-17 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 following sections are displayed if the audit is selected to be a basic audit:

Config WCS discrepancies

- 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 8-17 for more information on enforcing configurations.

– If you choose *Refresh Config from Controller*, a Refresh Config window appears displaying 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.

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 WLCs.

Note On the Refresh Config window, 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 menu, choose **View Latest Network Audit Report**.

Step 4 Click **GO**.

The Audit Summary displays the time of the audit, the IP address of the selected controller, and the audit status. The Audit Details display the config differences, if applicable.

You can use the General and Schedule tabs to revise the Audit Report parameters.

Note From the **All Controllers** page, click the **Audit Status** column value to view the latest audit details page for the selected controller. This method has similar information as the Network Audit report 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 menu. 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.

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 Priority drop-down, choose **Enabled**.

To then 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 menu, choose the applicable priority (Low, Medium, High, Critical).

Note The default priority is Low.

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 menu and click **GO**.

Step 5 In the Enter an IP Address (x.x.x.x) to Ping window, enter the IP address of the network device that you want the controller to ping and click **OK**.

WCS displays the Ping Results window, 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 window.

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 11-61.

To enable load-based CAC for a controller using the WCS web interface, follow these steps.

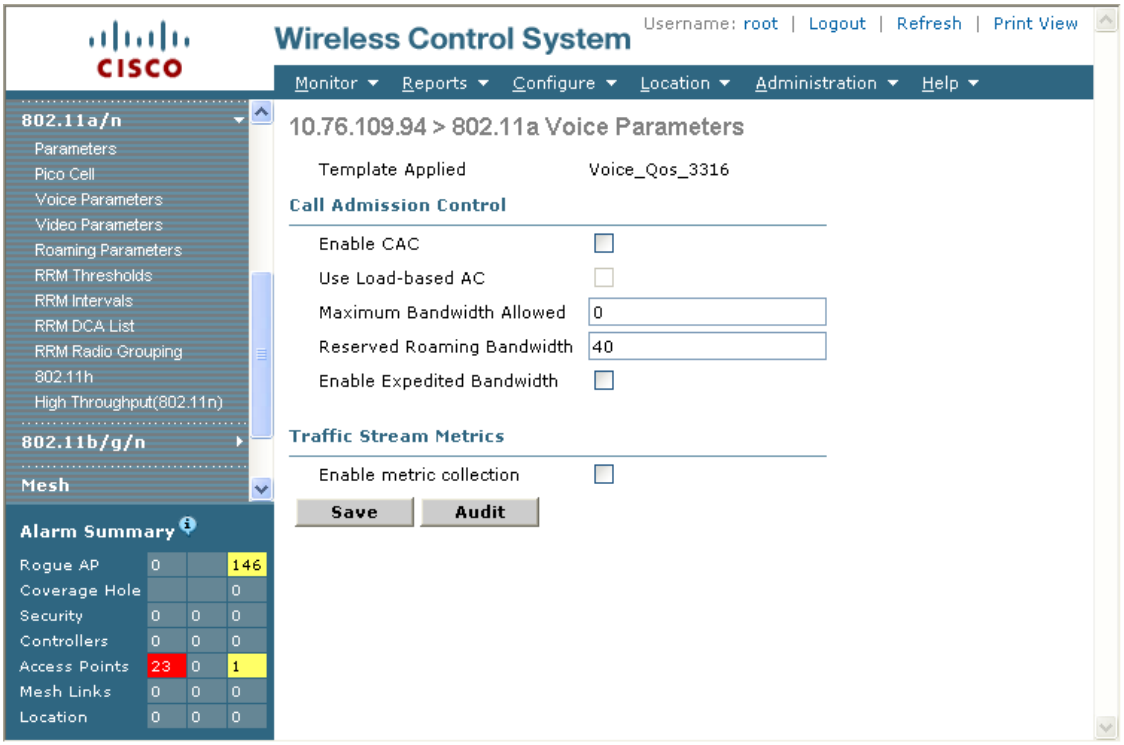
Step 1 Click **Configure > Controllers**.

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 10-3).

Figure 10-3 802.11a/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**.

Enabling High Density

The high density deployments are enabled with Cisco Unified Wireless Network software release 4.1 in conjunction with the Cisco and Intel Business Class Suite Version 2 initiative.

The high density networking feature is designed for large, multi-cell high density wireless networks in which it can be challenging to populate a site with a large number of lightweight access points to manage the cumulative bandwidth load while diminishing the contention between access points and still maintaining quality of service. To optimize RF channel capacity and improve network performance, the high density (or pico cell) mode parameters are introduced.

With this feature you can manually configure the transmit power, receiver sensitivity thresholds, and clear channel assessment sensitivity threshold of Intel client devices and Cisco Aironet lightweight access points in order to create optimal high-density deployments. When a client that supports high density associates to an access point with high-density enabled, they exchange specific 802.11 information element s (IEs) that instruct the client to adhere to the access point's advertised received sensitivity threshold, CCA sensitivity threshold, and transmit power levels. These three parameters reduce the effective cell size by adjusting the received signal strength before an access point and client consider the channel accessible for the transfer of packets. When all access points and clients raise the signal standard in this way throughout a high density area, access points can be deployed closer together, minimizing interference with each other and managing environmental and distant rogue signals.

Note High density is off by default. There are deployment risks involved if you change from the predetermined values. Do not attempt to configure pico cell functionality within your wireless LAN without the advice of Cisco technical support. Non-standard installation is not supported.

Along with these configuration changes, you can further optimize the pico cell deployment as follows:

Requirements

High density has the following restrictions:

- Only Cisco lightweight access points (except the AP1030 and 1500 series mesh access points) and the Intel PRO/Wireless 3945ABG and Intel Wireless WiFi Link 4965AGN clients are supported.
- Only 802.11a/n networks with high density deployments are supported.

Note Cisco recommends the use of high density only in new WLAN deployments in which all clients and lightweight access points support the high-density feature.

Optimizing the Controller to Support High Density

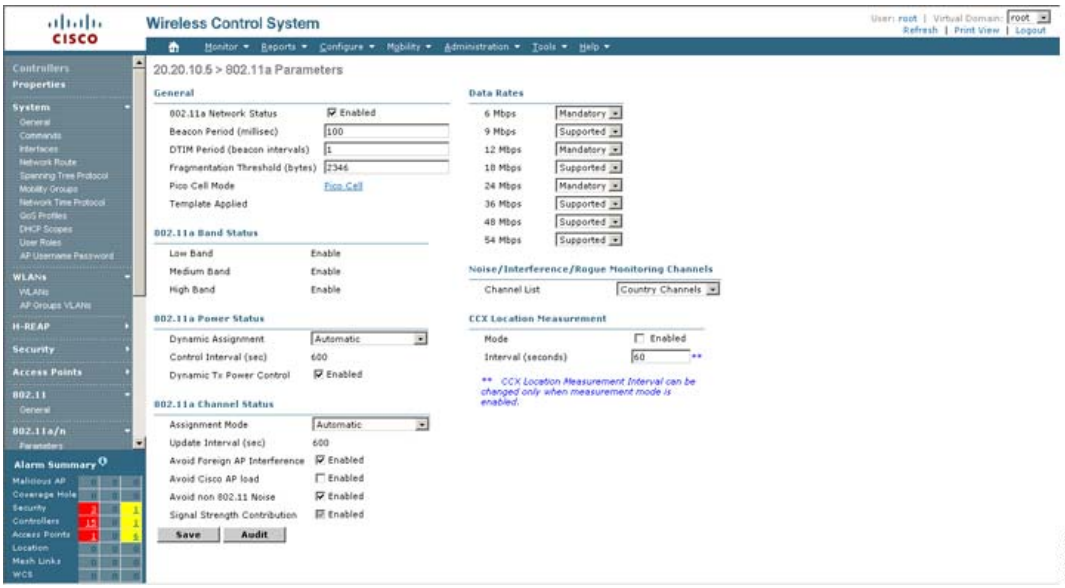
To optimize a controller to support high density, you need to enable pico cell mode v2. A method to mitigate the inter-cell contention problem in high-density networks is to adjust the access point and client receiver sensitivity, CCA sensitivity, and transmit power parameters in a relatively cooperative manner. By adjusting these variables, the effective cell size can be reduced, not by lowering the transmit power but by increasing the necessary received power before an access point and client consider the channel sufficiently clear for packet transfer. These similar values can be set in the Controller Templates portion of the GUI. Refer to Applying Controller Templates, page 11-79. Follow these steps to configure high density.

Note If you enable pico cell, the default values for auto RF adjust according to the values suggested for Intel 3945ABG clients. The transmit power is set to 10 dBm, CCA sensitivity threshold to –65 dBm, and receiver sensitivity threshold to –65 dBm.

Step 1 Choose **Configure > Controllers**.

Step 2 From the left sidebar menu, choose **802.11a/n > Parameters** or **802.11b/g/n > Parameters**. The window as shown in Figure 10-4 appears. Ensure that the 802.11a/n (or 802.11b/g/n) Network Status check box is not enabled.

Figure 10-4 Pico Cell Parameter



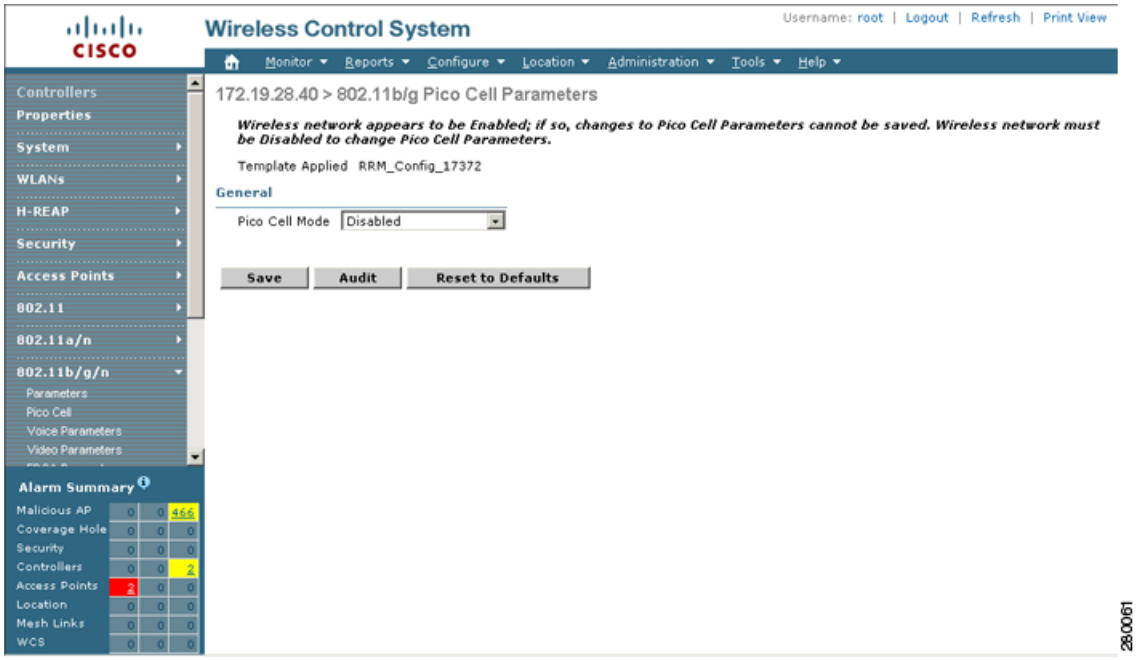
Step 3 In the General portion of this window, you see a Pico Cell Mode parameter. Click **Enable**.

Note Pico cell mode cannot be enabled while Aggressive Load Balancing is enabled on the controller.

Step 4 Click **Save**.

Step 5 Choose **802.11a/n > Pico Cell** or **802.11b/g/n > Pico Cell** from the left sidebar menu. The Pico Cell Parameters screen appears (see Figure 10-5).

Figure 10-5 Pico Cell Parameters Window



Note If the Pico Cell Mode parameter is set to Disabled or V1, the Pico Cell V2 parameters are grayed out.

Step 6 From the Pico Cell Mode drop-down menu, choose **V2**. By choosing V2, the high-density parameters for the access point and clients share the same values and make communication symmetrical. This selection also allows you to enter values for Rx sensitivity, CCA sensitivity, and transmit power, although the defaulted minimum and maximum values represent the Cisco recommended values for most networks.

Note Choose V1 only if you are using a legacy Airespace branded product acquired prior to their acquisition by Cisco. Cisco recommends that you choose V2 if you want to enable pico cell mode.

Step 7 Set the Rx sensitivity threshold based on the desired receiver sensitivity for 802.11a/n radios. The Current column shows what is currently set on the access point and clients, and the Min and Max columns show the range to which the access points and clients should adapt. The valid ranges for Current, Min, and Max columns are -127 to 127 dBm. The defaults are -65 dBm (current), -127 dBm (Min), and 127 dBm (Max). Receiver signal strength values outside of this range are blocked.

Step 8 Set the CCA sensitivity threshold based on when the access point or client considers the channel clear enough for activity. The Current column shows what is currently set on the access point and clients, and the Min and Max columns show the range to which the access points and clients should adapt. The valid ranges for Current, Min, and Max columns are -127 to 127 dBm. The defaults are -65 dBm (current), -127 dBm (Min), and 127 dBm (Max). CCA values outside of this range are blocked.

Step 9 Specify the transmit power of the radio that will be used by the client. The valid ranges for Current, Min, and Max columns are -127 to 127 dBm. The defaults are 10 dBm (current), 0 dBm (Min), and 17 dBm (Max).

Step 10 Click **Save** to save these values. Click **Audit** to see a comparison of how WCS configuration matches up with controller configurations. Before choosing **Reset to Defaults**, you must turn off the 802.11a/n network.

Step 11 Return to **802.11a/n > Parameters** and check the 802.11a /n Network Status check box to turn the network back on.

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 s the General page.

Step 3 From the 802.3 Bridging drop-down menu, 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.

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 > Controller**.

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 Thresholds, Load Thresholds, Other Thresholds, and Noise/Interference/Rogue Monitoring Channels.

Note When the Coverage Thresholds Min SNR Level (dB) parameter is adjusted, the value of the Signal Strength (dB) automatically reflects this change. The Signal Strength (dB) parameter provides information regarding what the target range of coverage thresholds is when adjusting the SNR value.

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:

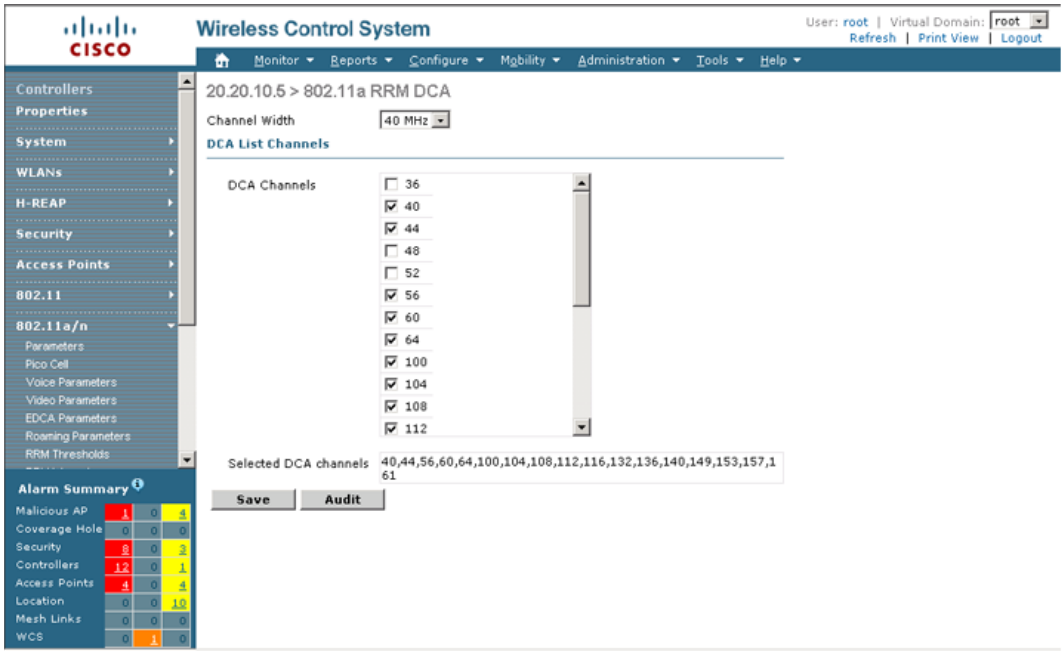
Step 1 Choose **Configure > Controllers**.

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 window appears (see Figure 10-6).

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 10-6 802.11a/n RRM DCA Window



Step 4 From the Channel Width drop-down menu, 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 Choose the check box(es) for the applicable DCA channel(s). The selected channels are listed in the **Selected DCA channels** text box.

Step 6 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. Refer to the "Configuring EDCA Parameters through a Controller Template" section on page 11-63 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 the **EDCA Profile** from the drop-down menu.

Note Profiles include Wi-Fi Multimedia (WMM), Spectralink Voice Priority (SVP), Voice Optimized, and Voice & Video Optimized. WMM is the default EDCA profile.

Note You must shut down radio interface before configuring EDCA Parameters.

Step 5 Click the **Enable Streaming MAC** check box to enable this feature.

Note Only enable Streaming MAC if all clients on the network are WMM compliant.

Configuring 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. 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 menu.

Step 3 On the SNMP Parameters portion of the window, choose **v3** from the Version drop-down menu.

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 menu, 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 menu, choose **Discover Templates from Controller**.

Step 4 Click **GO**. The Discover Templates window displays the number of discovered templates and each template's name.

Note The configuration from the controller is refreshed if you select this option.

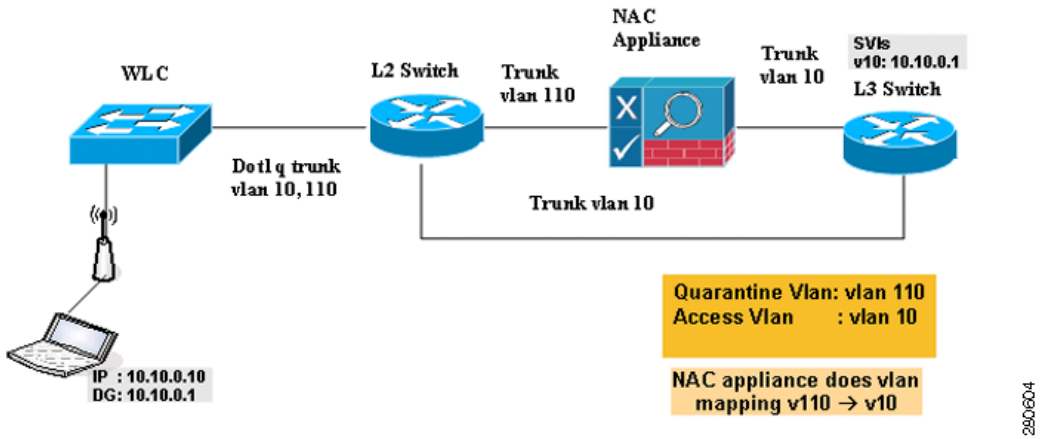
Configuring NAC Out-of-Band Integration

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 10-7 provides an example of NAC out-of-band integration.

Figure 10-7 NAC Out-of-Band Integration



In Figure 10-7, 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 Refer to Chapter 13 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 Refer to 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:

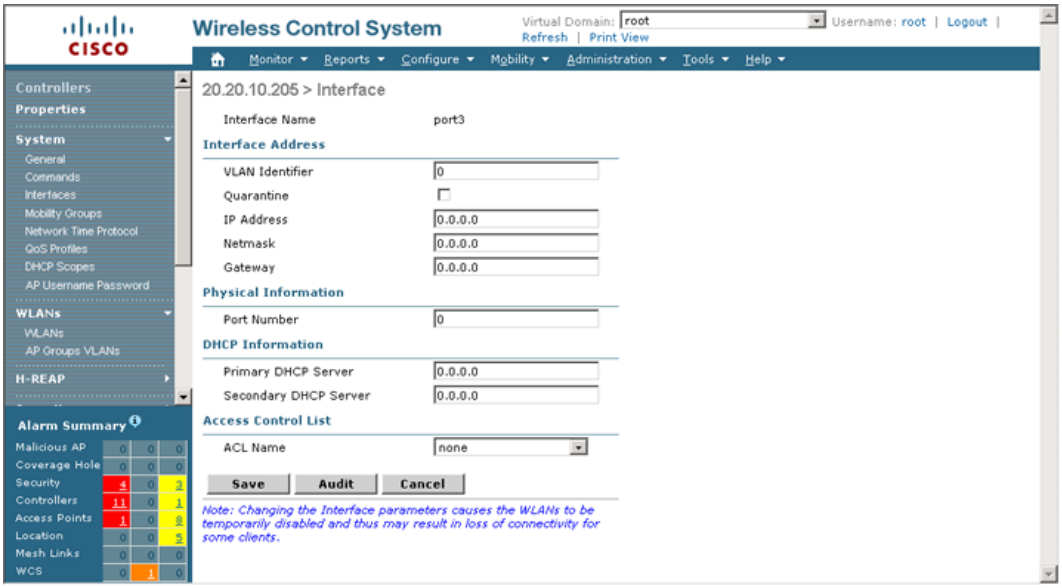
a. Choose **Configure > Controller**.

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 menu. The Interface window appears (see Figure 10-8).

Figure 10-8 Interface Window



e. In the Interface Name field, enter a name for this interface, such as “quarantine.”

f. In the VLAN Identifier field, enter a non-zero value for the access VLAN ID, such as “10.”

g. Check 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.

h. Configure any remaining fields for this interface, such as the IP address, netmask, and default gateway.

i. Enter an IP address address for the primary and secondary DHCP server.

j. Click **Save**. You are now ready to create a NAC-enabled WLAN or guest LAN

Step 2 To configure NAC out-of-band support on a WLAN or guest LAN, follow these steps:

a. Click **WLANs > WLANs** from the left sidebar menu.

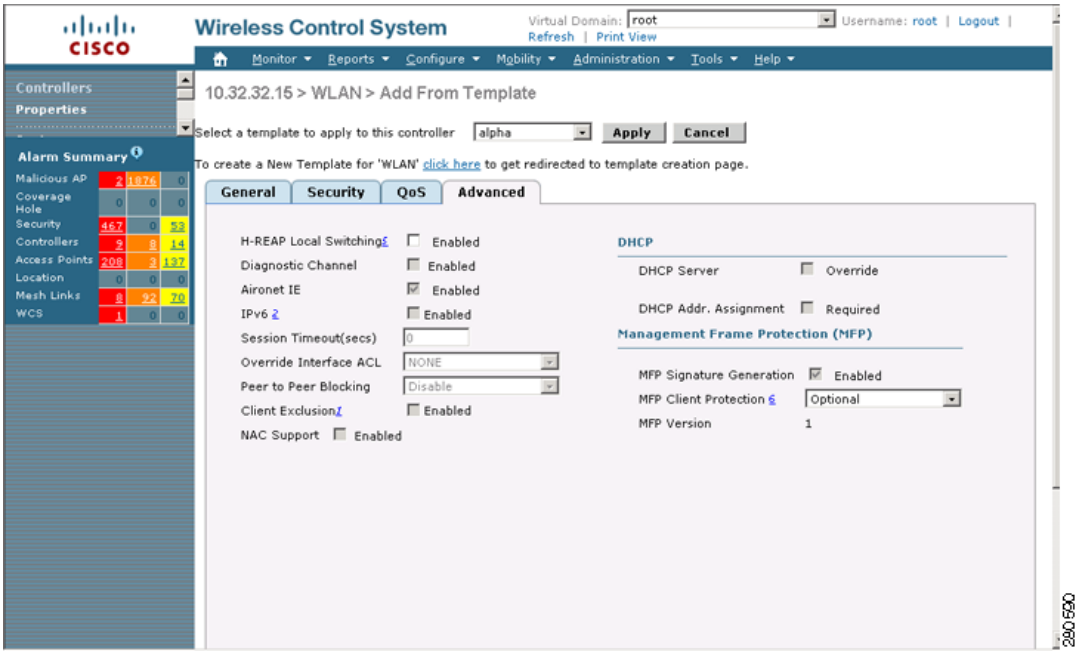
b. Choose **Add WLAN** from the Select a command drop-down menu and click **GO**.

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 menu. 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 10-23.

Note Ensure that WLAN IDs within the same network match before you forward the WLAN template.

d. Click the **Advanced** Tab (see Figure 10-9).

Figure 10-9 WLAN > Add From Template Window



e. To configure NAC out-of-band support for this WLAN or guest LAN, check the **NAC Support** check box. To disable NAC out-of-band support, leave the check box unchecked, 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 VLANs** in the left sidebar menu to open the AP Groups VLANs page.

b. Click the name of the desired AP group.

c. From the Interface Name drop-down box, choose the quarantine-enabled VLAN.

d. To configure NAC out-of-band support for this AP group VLAN, check the **NAC Support** check box. To disable NAC out-of-band support, leave the check box unchecked, which is the default value.

e. Click **Apply** to commit your changes.

Step 4 To see the current state of the client (either Quarantine or Access), follow these steps:

a. Click **Monitor > Clients** to open the Clients page and perform a search for clients.

b. Click the MAC address of the desired client to open the Clients > Detail page. The NAC state appears as access or quarantine under the Security Information section (see Figure 10-10).

Figure 10-10 Monitor > Client Window

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. Refer to the "Creating Guest User Accounts" section on page 7-11.

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.

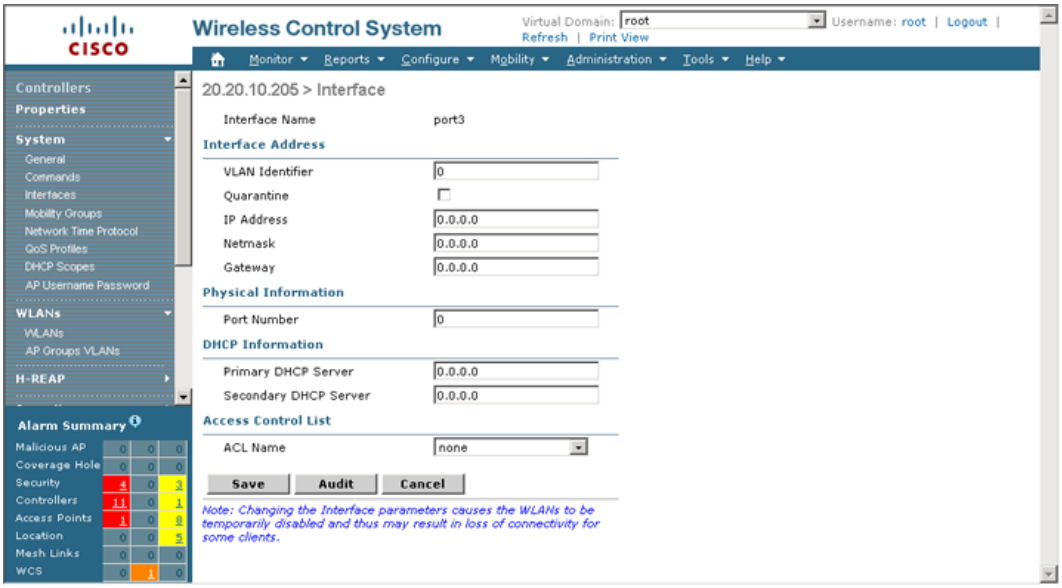
If two controllers are being used, the controller (foreign) that receives the wired guest traffic from the switch then forwards the wired guest traffic to an anchor controller that is also configured for wired guest access. After successful hand off of the wired guest traffic to the anchor controller, 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 7-11.

To create dynamic interfaces for wired guest user access, click **Configure > Controllers** and after choosing a particular IP address, choose **System > Interfaces**. 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 10-24 and the "Creating an Egress Interface" section on page 10-25 before continuing to "Creating a Wired LAN for Guest Access" section on page 10-25. Both the Ingress and Egress Interfaces use the screen as shown in Figure 10-11.

Figure 10-11 Interfaces Summary Window



Creating an Ingress Interface

Follow these steps to create an Ingress interface.

Step 1 Choose **Add Interface** from the Select a command drop-down menu and click **GO**.

Step 2 In the Interface Name field, enter a name for this interface, such as guestinterface.

Step 3 Enter a VLAN ID for the new interface.

Step 4 Check the **Guest LAN** check box.

Step 5 Enter the primary and secondary port numbers.

Step 6 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 menu and click **GO**.

Step 2 In the Interface Name field, enter a name for this interface, such as quarantine.

Step 3 In the VLAN Identifier field, enter a non-zero value for the access VLAN ID, such as 10.

Step 4 Check 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 5 Enter the IP address, netmask, and default gateway.

Step 6 Enter the primary and secondary port numbers.

Step 7 Provide an IP address for the primary and secondary DHCP server.

Step 8 Configure any remaining fields for this interface and click **Save**.

You are now ready to create a wired LAN for guest access.

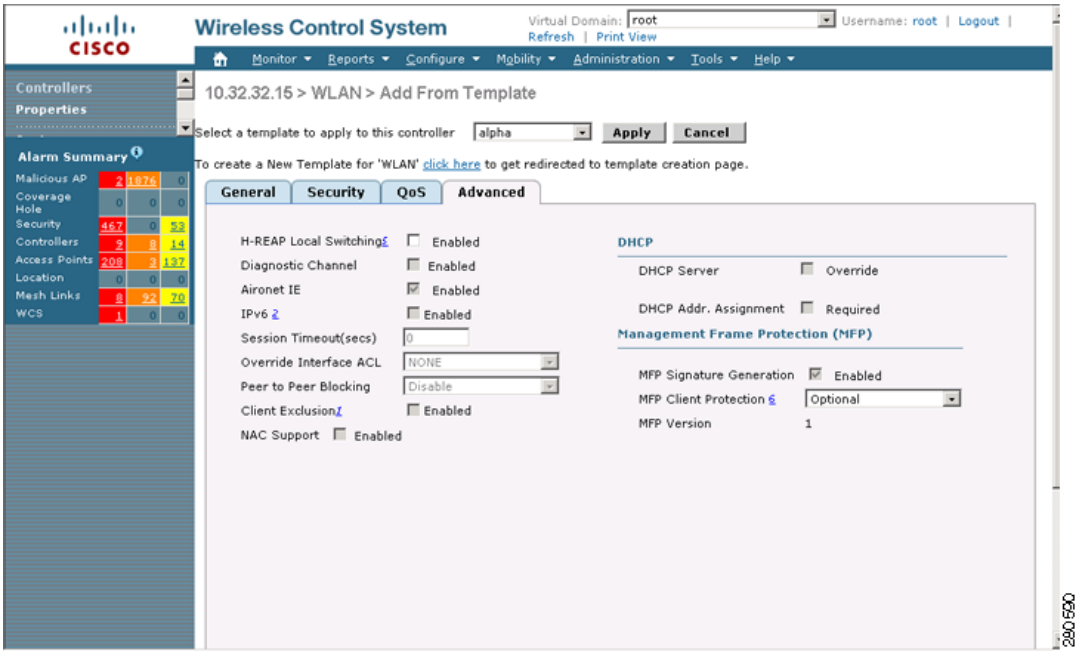
Creating a Wired LAN for Guest Access

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** from the left sidebar menu.

Step 2 Choose **Add WLAN** from the Select a command drop-down menu and click **GO**. The WLAN > Add From Template window appears (see Figure 10-12).

Figure 10-12 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 menu. 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 At the New Template general tab, enter a name in the Template Name field 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 Check the **Enabled** check box for the WLAN Status parameter.

Step 8 From the Ingress Interface drop-down menu, choose the Ingress interface that you created in the "Creating an Ingress Interface" section on page 10-24. The provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Step 9 From the Egress Interface drop-down menu, choose the Egress interface that you created in the "Creating an Egress Interface" section on page 10-25. 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 menu.

Step 10 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, 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 e-mail address when attempting to connect to the network.

b. To specify custom web authentication windows, uncheck the Global WebAuth Configuration **Enabled** check box.

1. When the Web Auth Type drop-down menu 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 menus 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 menu 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 3-17.

   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 field.

   You can select specific RADIUS or LDAP servers to provide external authentication on the **Security > AAA** panel. To do so, continue with Step 11.

Note The RADIUS and LDAP external servers must be already configured to have selectable options on the Security > AAA panel. You can configure these servers on the RADIUS Authentication Servers page, TACACS+ Authentication Servers page, and LDAP Servers page..

Step 11 If you selected External as the Web Authentication Type in Step 10, click **Security > AAA** and select up to three RADIUS and LDAP servers using the drop-down menus.

Step 12 Click **Save**.

Step 13 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 an LWAPP 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 connected to rogue access point information is used to track the switch port to which the rogue access point is connnected 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.

Step 1 Choose **Monitor > Security.**

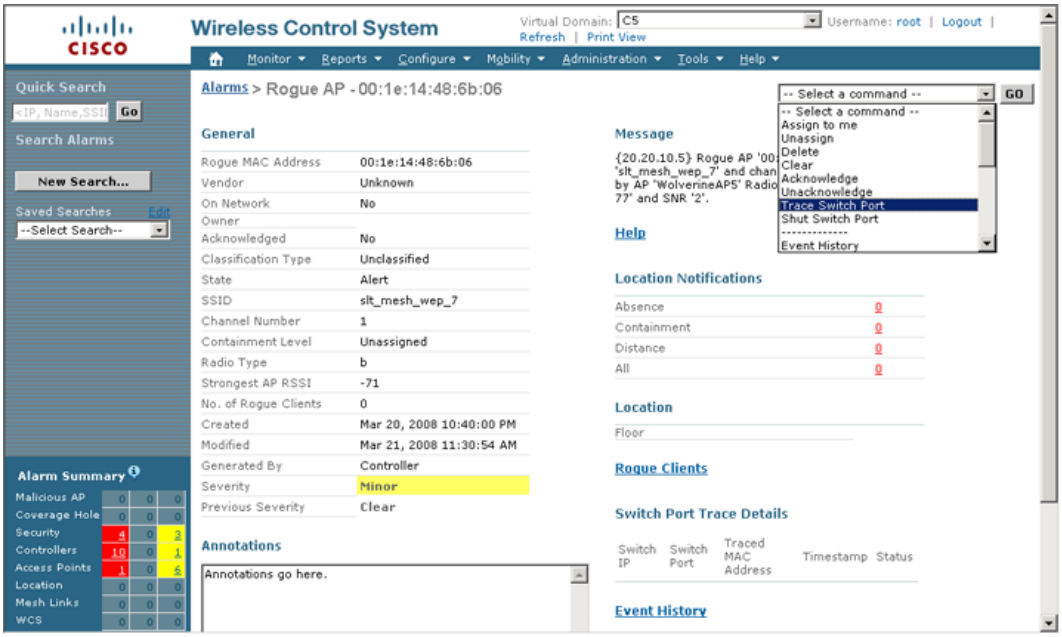
Step 2 Click **View All** in the Rogue APs and Adhoc Rogues section.

Step 3 Choose for which rogue you are setting switch port tracking by clicking the URL in the MAC Address column.

Step 4 From the Select a command drop-down menu, choose **Trace Switch Port** (see Figure 10-13).

Figure 10-13 Trace Switch Port option on the Alarms > Rogue Page

.

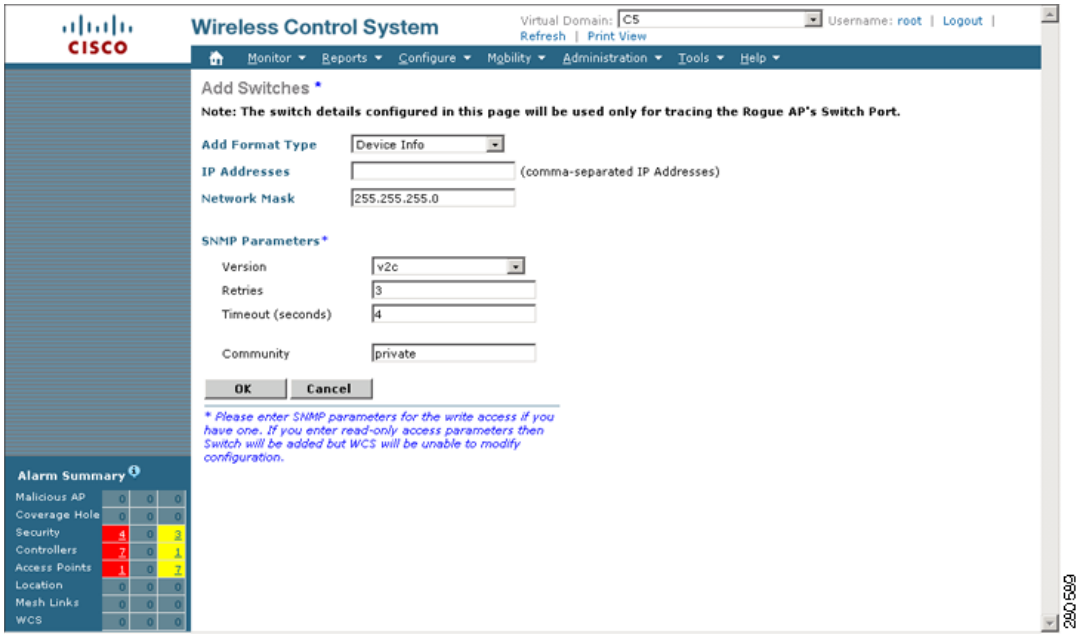


Step 5 When one or more searchable MAC addresses are available, the WCS uses CDP to discover any switches connected up to two hops away from the detecting access point. The MIBs of each CDP discovered switch is examined to see if it contains any of the target MAC addresses. If any of the MAC addresses are found, the corresponding port number is returned and reported as the rogue's switch port.

The SNMP communities for the switches are provided in Configure > Switches (see Figure 10-14).

Figure 10-14 Configure > Switches

.



Step 6 The switch details configured on this page are used only for tracing the rogue access point's switch port. Choose one of the following:

If you want to add one switch or use commas to separate multiple switchess, leave the Add Format Type drop-down menu at Device Info.

If you want to add multiple switches by importing a CSV file, choose **File** from the Add Format Type drop-down menu. The CSV file allows you to 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 On the SNMP Parameters portion of the window, choose your version choice from the Version drop-down menu.

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.

Step 10 You can change the retries and timeout values that were established for this switch if desired.

Step 11 Enter the community for this switch.

Step 12 Click **OK**.

Removing Switches

You can remove switches by choosing **Configure > Switches** and choosing **Remove Switches** from the Select a command drop-down menu.

Shutting Switch Port

You can suppress the switch port to which the rogue access point is connected. From the Alarms Rogue page (shown in Figure 10-13), choose **Shut Switch Port** from the Select a command drop-down menu.

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.

CHAPTER 11

Using Templates

This chapter describes how to add and apply controller templates. Information on creating (adding) access point templates is also provided.

Templates allow you to set parameters that you can then apply to multiple devices without having to re-enter the common information.

Note Template information can be overridden on individual devices.

This chapter contains these sections:

- Adding Controller Templates, page 11-1
- Applying Controller Templates, page 11-80
- Adding Access Point Templates, page 11-80
- Configuring Access Point Templates, page 11-81

Adding Controller Templates

Follow these steps to add a new controller template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 Choose **Add Template** from the Select a command drop-down menu and click **GO**.

Step 3 Enter the template name.

Step 4 Provide a description of the template.

Step 5 Click **Save**.

A summary of the templates that can be added is highlighted below:

- Configuring an NTP Server Template, page 11-3
- Configuring General Templates, page 11-4
- Configuring QoS Templates, page 11-6
- Configuring a Traffic Stream Metrics QoS Template, page 11-8
- Configuring WLAN Templates, page 11-9

- Configuring H-REAP AP Groups, page 11-21
- Configuring a File Encryption Template, page 11-23
- Configuring a RADIUS Authentication Template, page 11-24
- Configuring a RADIUS Accounting Template, page 11-27
- Configuring a LDAP Server Template, page 11-28
- Configuring a Local EAP General Template, page 11-30
- Configuring a Local EAP Profile Template, page 11-31
- Configuring an EAP-FAST Template, page 11-33
- Configuring Network User Credential Retrieval Priority Templates, page 11-35
- Configuring a Local Network Users Template, page 11-35
- Configuring Guest User Templates, page 11-37
- Configuring a User Login Policies Template, page 11-38
- Configuring a MAC Filter Template, page 11-39
- Configuring an Access Point or LBS Authorization, page 11-40
- Configuring a Manually Disabled Client Template, page 11-41
- Configuring a CPU Access Control List (ACL) Template, page 11-42
- Configuring a Rogue Policies Template, page 11-43
- Configuring a Rogue AP Rules Template, page 11-44
- Configuring a Rogue AP Rule Groups Template, page 11-46
- Configuring a Friendly Access Point Template, page 11-48
- Configuring a Client Exclusion Policies Template, page 11-49
- Configuring an Access Point Authentication and MFP Template, page 11-51
- Configuring a Web Authentication Template, page 11-52
- Configuring Access Control List Templates, page 11-56
- Configuring a Policy Name Template (for 802.11a/n or 802.11b/g/n), page 11-57
- Configuring High Density Templates, page 11-60
- Configuring a Voice Parameter Template (for 802.11a/n or 802.11b/g/n), page 11-62
- Configuring EDCA Parameters through a Controller Template, page 11-64
- Configuring EDCA Parameters through a Controller Template, page 11-64
- Configuring an RRM Threshold Template (for 802.11a/n or 802.11b/g/n), page 11-66
- Configuring an RRM Interval Template (for 802.11a/n or 802.11b/g/n), page 11-68
- Configuring an 802.11h Template, page 11-69
- Configuring a High Throughput Template (for 802.11a/n or 802.11b/g/n), page 11-69
- Configuring a Mesh Template, page 11-71
- Configuring a TFTP Server Template, page 11-72
- Configuring a Trap Receiver Template, page 11-73
- Configuring a Trap Control Template, page 11-73
- Configuring a Telnet SSH Template, page 11-75

- Configuring a Legacy Syslog Template, page 11-76
- Configuring a Multiple Syslog Template, page 11-77
- Configuring a Local Management User Template, page 11-78
- Configuring a User Authentication Priority Template, page 11-79
- Configuring Radio Templates, page 11-88

Configuring an NTP Server Template

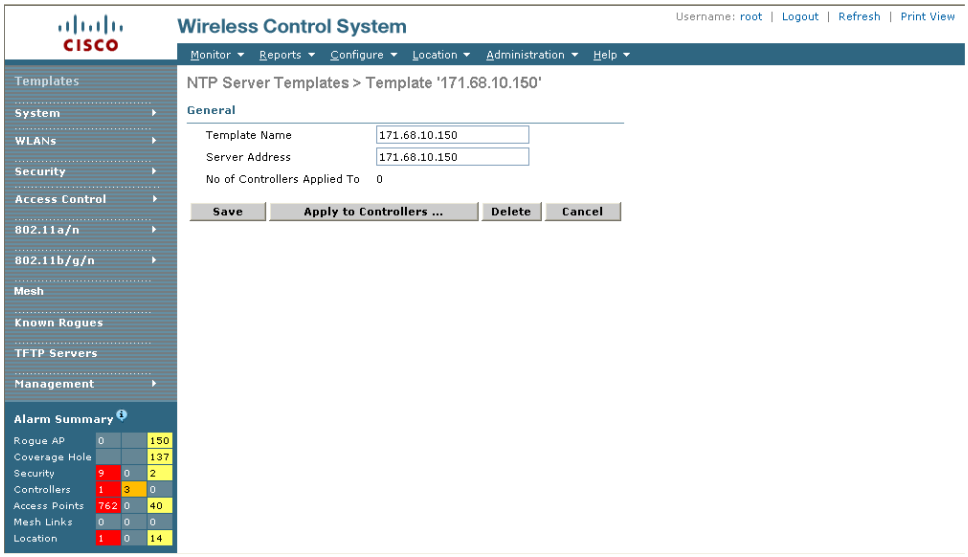
Follow these steps to add a new network time protocol (NTP) server template to the controller configuration or make modifications to an existing NTP template. NTP is used to synchronize computer clocks on the internet.

Step 1 Choose **Configure > Controller Templates**.

Step 2 Choose **System > Network Time Protocol** from the left sidebar menu.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO.** To modify an existing template, click to select a template in the Template Name column. The NTP Server Template window appears (see Figure 11-1), and the number of controllers the template is applied to automatically populates.

Figure 11-1 NTP Servers Template



Step 4 Enter the NTP server IP address.

Step 5 Click **Save**.

Configuring General Templates

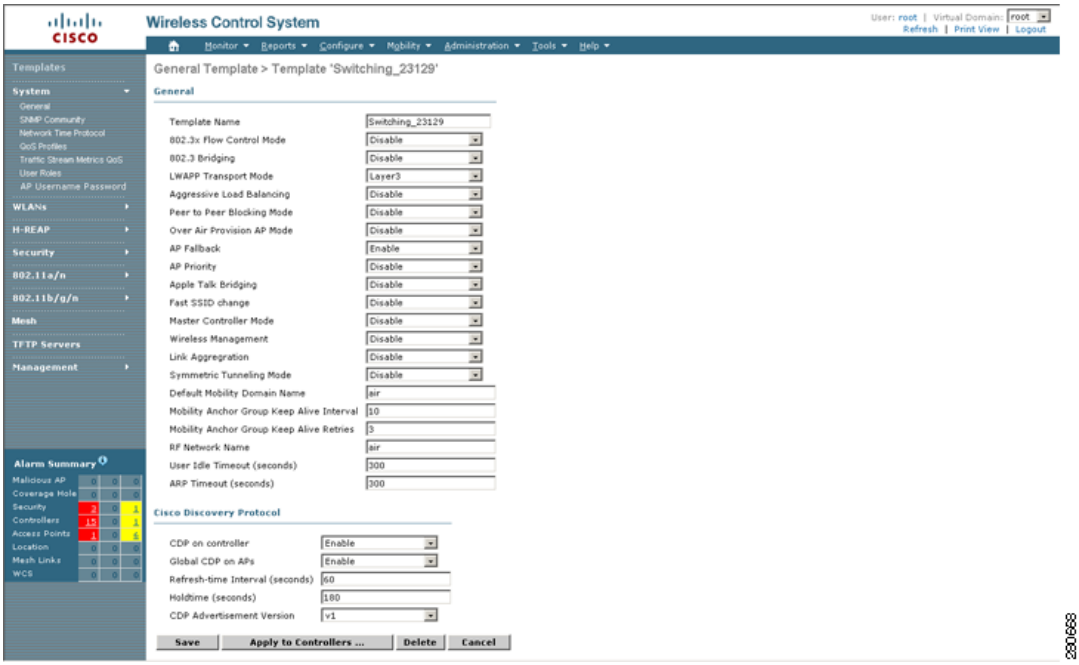
Follow these steps to add a new template with general information for a controller or make a change to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **System > General**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO.** To modify an existing template, click to select a template in the Template Name column. The General Template window appears (see Figure 11-2).

Figure 11-2 General Template



Step 4 Use the drop-down menu to enable or disable flow control mode.

Step 5 Use the drop-down menu to enable or disable 802.3 bridging.

Step 6 Specify Layer 2 or Layer 3 transport mode. When set to Layer 3, the LWAPP 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 LWAPP uses proprietary code to communicate with the access points.

Step 7 At the Ethernet Multicast Support drop-drop menu, choose **Disable** to disable multicast support on the controller or **Multicast** to enable multicast support on the controller. Choose **Unicast** if the controller, upon receiving a multicast packet, forwards the packets to all the associated access points. H-REAP supports only unicast mode.

Step 8 Choose if you want to enable or disable aggressive load balancing.

Step 9 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 10 At the Over Air AP Provision Mode drop-down menu, choose enable or disable.

Step 11 At the AP Fallback drop-down menu, choose enable or disable. Enabling fallback causes an access point which lost a primary controller connection to automatically return to service when the primary controller returns.

Step 12 Choose to enable or disable Apple talk bridging.

Step 13 Choose to enable or disable the fast SSID option. If enabled, the client connects instantly to the controller between SSIDs without having appreciable 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 14 Because the master controller is normally not used in a deployed network, the master controller setting is automatically disabled upon reboot or OS code upgrade. You may enable the controller as the master controller from the Master Controller Mode drop-down menu.

Step 15 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, Static WEP, or VPN Pass Through WLANs. Wireless management is not available to clients attempting to log in via an IPSec WLAN.

Step 16 Choose to enable or disable link aggregation. Link aggregation allows you to reduce the number of IP addresses needed to configure the ports on your controller by grouping all the physical ports and creating a link aggregation group (LAG). In a 4402 model, two ports are combined to form a LAG whereas in a 4404 model, all four ports are combined to form a LAG.

If LAG is enabled on a controller, the following configuration changes occur:

- Any dynamic interfaces that you have created are deleted. This is done to prevent configuration inconsistencies in the interface database.
- Interfaces cannot be created with the “Dynamic AP Manager” flag set.

Note You cannot create more than one LAG on a controller.

The advantages of creating a LAG 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.
- Multiple AP-manager interfaces are not required since only one logical port is visible to the application.

Note When you make changes to the LAG configuration, the controller has to be rebooted for the changes to take effect.

Step 17 Choose to enable or disable symmetric mobility 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.

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 18 Enter the operator-defined RF mobility group name in the Default Mobility Domain Name field.

Step 19 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 20 At the Mobility Anchor Group Keep Alive Retries, specify the number of queries to anchor before the client declares it unreachable.

Note When you hover over the parameter field with the mouse, the valid range for that field appears.

Step 21 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 22 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 23 Specify the timeout in seconds for the address resolution protocol. The factory default is 300 seconds.

Step 24 At the CDP on controller drop-down menu, choose if you want 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 25 At the Global CDP on APs drop-down menu, choose if you want to enable CDP on the access point.

Step 26 At the Refresh Time Interval parameter, enter the interval at which CDP messages are generated. With the regeneration, the neighbor entries are refreshed.

Step 27 At the Holdtime parameter, enter the time in seconds before the CDP neighbor entry expires.

Step 28 At the CDP Advertisement Version parameter, enter which version of the CDP protocol to use.

Step 29 Click **Save**.

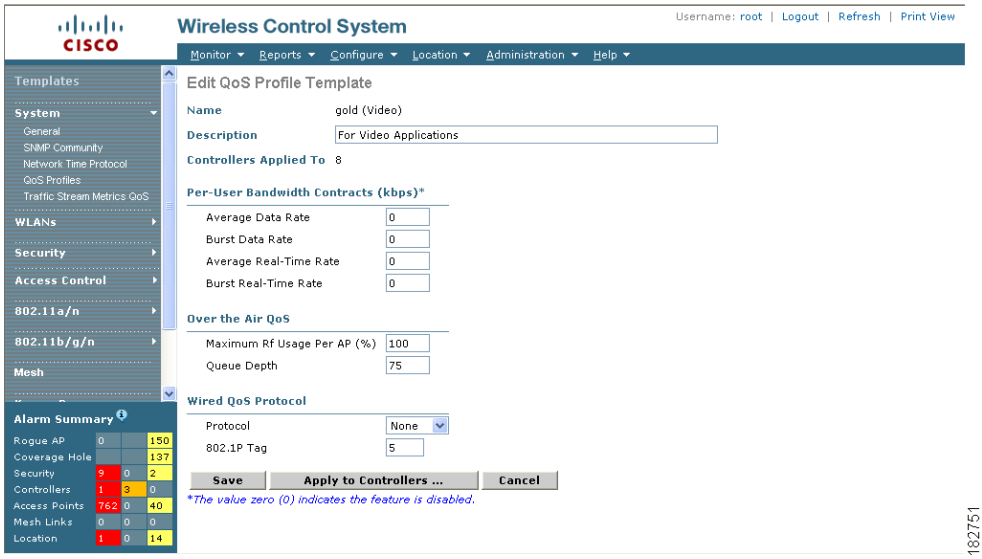
Configuring QoS Templates

Follow these steps to make modifications to the quality of service profiles.

Step 1 Choose **Configure > Controller Templates**.

Step 2 On the left sidebar menu, choose **System > QoS Profiles**. The QoS Template window appears (see Figure 11-3), and the number of controllers the template is applied to automatically populates.

Figure 11-3 QoS Profile Template



Step 3 Set the following values in the Per-User Bandwidth Contracts portion of the window. 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 4 Set the following values for the Over-the-Air QoS portion of the window.

- 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 5 Set the following values in the Wired QoS Protocol portion of the window.

- 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 LWAPP packets.

Step 6 Click **Save**.

Configuring a Traffic Stream Metrics QoS Template

Traffic stream metrics are a series of statistics about VoIP over your wireless LAN and informs you of the QoS of the wireless LAN. These statistics are different than the end-to-end statistics provided by VoIP systems. End-to-end statistics provide information on packet loss and latency covering all the links comprising the call path. However, traffic stream metrics are statistics for only the WLAN segment of the call. Because of this, system administrators can quickly determine whether audio problems are being caused by the WLAN or by other network elements participating in a call. By observing which access points have impaired QoS, system administrators can quickly determine the physical area where the problem is occurring. This is important when lack of radio coverage or excessive interference is the root problem.

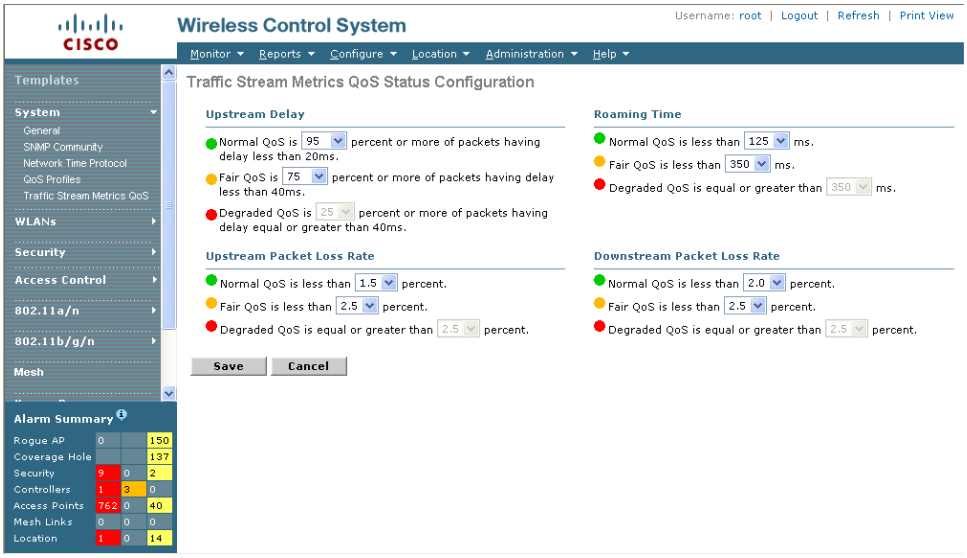
Four QoS values (packet latency, packet jitter, packet loss, and roaming time), which can affect the audio quality of voice calls, are monitored. All the wireless LAN components participate in this process. Access points and clients measure the metrics, access points collect the measurements and then send them to the controller. The access points update the controller with traffic stream metric information every 90 seconds, and 10 minutes of data is stored at one time. 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 Templates**.

Step 2 On the left sidebar menu, choose **System > Traffic Stream Metrics QoS**. The Traffic Stream Metrics QoS Status Configuration window appears (see Figure 11-4).

Figure 11-4 Traffic Stream Metrics QoS Status Template



The Traffic Stream Metrics QoS Status Configuration window 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 new WLAN template or make modifications to an existing WLAN template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 Choose **WLANs > WLAN** from the left sidebar menu.

The WLAN Template window 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 window (see Figure 11-5).

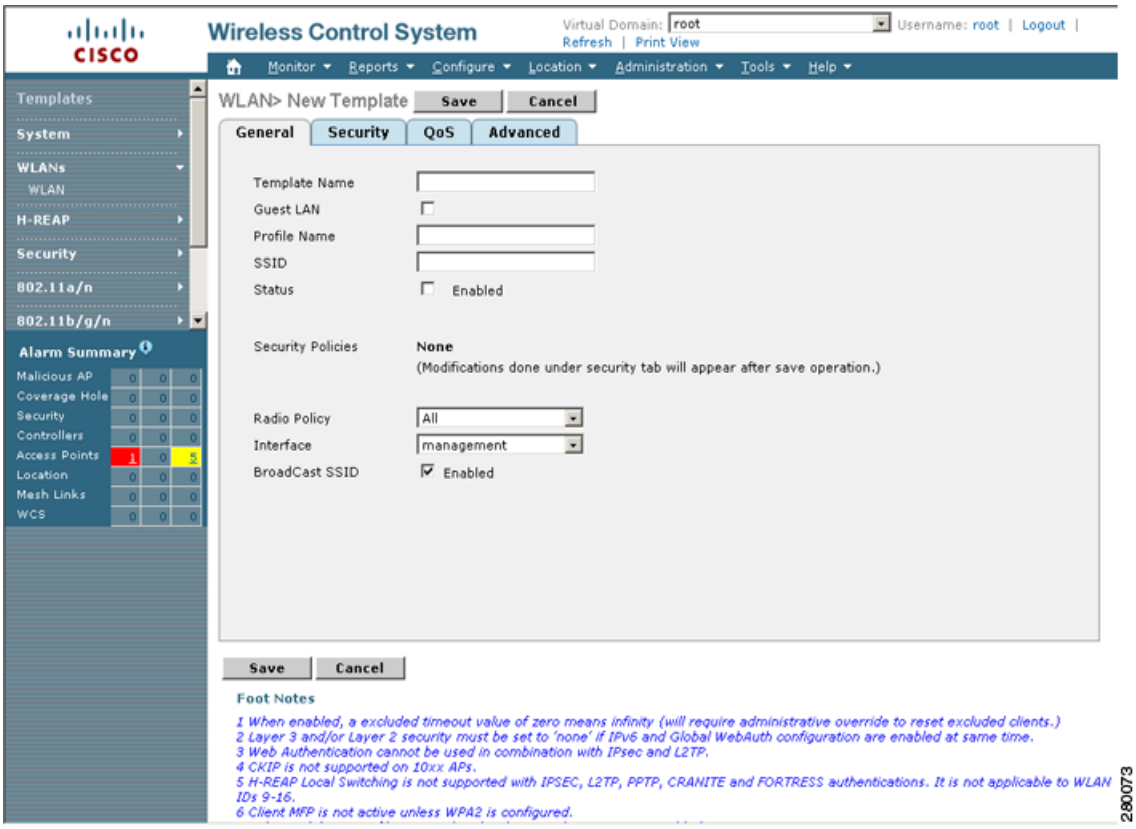
- Template Name - The user-defined name of the template. Clicking the name displays parameters for this template.
- Profile Name - User-defined profile name used to distinguish WLANs with the same SSID.

Note This heading is not present in software release prior to 4.0.96.0.

- SSID - Displays the name of the WLAN.
- WLAN Status - Sets the status of the WLAN to enabled when checked.
- Security Policies - Determines whether 802.1X is enabled. None indicates no 802.1X.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO.** To make modifications to an existing template, click a URL in the Template Name column. The WLAN Template window appears (see Figure 11-5).

Figure 11-5 WLAN Template



Step 4 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. Wired guest access accounts are added to the network using the Lobby Ambassador portal. (Refer to the "Creating Guest User Accounts" section on page 7-11).

Step 5 Enter a name in the Profile Name field that identifies the guest LAN. Do not use any spaces in the name entered.

Step 6 Check the **Enabled** check box for the Status parameter.

Step 7 Use the Radio Policy drop-down menu to set the WLAN policy to apply to All (802.11a/b/g/n), 802.11a only, 802.11g only, 802.11b/g/n only, or 802.11a/g/n only.

Step 8 Use the Interface drop-down menu to choose the available names of interfaces created by the Controller > Interfaces module.

Step 9 Click **Broadcast SSID** to activate SSID broadcasts for this WLAN.

Step 10 Click **Save**.

Step 11 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 11-11.
- Click the **QoS** tab to establish which quality of service is expected for this WLAN. Continue to the "QoS" section on page 11-17.
- 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 11-18.

Security

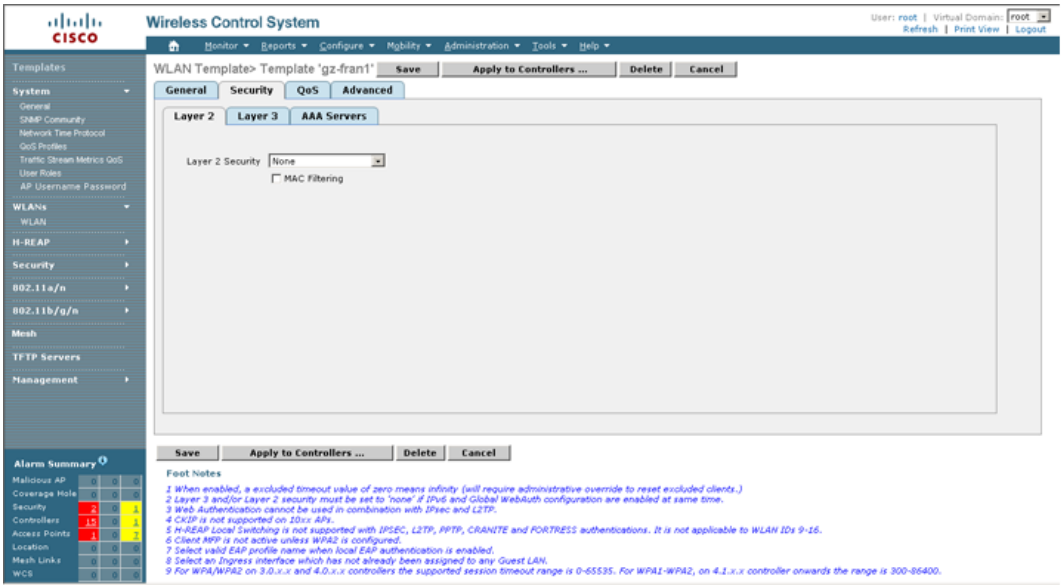
After choosing Security, you have an additional three tabs: Layer 2, Layer 3, and AAA Servers.

Layer 2

When you choose the Layer 2 tab, the window as shown in Figure 11-6 appears.

Note The screen contains different views depending on what option is chosen in the Layer 2 Security drop-down menu.

Figure 11-6 Layer 2 Window



Step 1 Use the Layer 2 Security drop-down menu to choose between None, WPA, WPA-2, Static WEP, 802.1X, Cranite, Fortress, Static WEP-802.1X, CKIP, and WPA1 + WPA2 as described in the table below.

Table 11-1 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. 104/128 bit key. 128/152 bit key.
WPA	This is a 3.2 controller code option and is not supported in 4.0 or later versions.
WPA-2	This is a 3.2 controller code option is not supported in 4.0 or later versions.

Table 11-1 Layer 2 Security Options (continued)

Parameter	Description
Static WEP	Static WEP encryption parameters: Key sizes: 40/64, 104/128, and 128/152 bit key sizes. Key Index: 1 to 4 (Note 2). Encryption Key: Encryption key required. Key Format: Select encryption key format in ASCII or HEX. **Note** Regardless of which format you choose, for security reasons, only ASCII is visible on the WLC. 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.
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.
Fortress	FIPS 40-2 compliant Layer 2 security feature.
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: 40/64, 104/128. and 128/152 bit key sizes. Key index: 1 to 4 (Note 2). Encryption Key: Enter encryption key. Key Format: Select encryption key format in ASCII or HEX. WEP 802.1X data encryption type (Note 1): 40/64 bit key. 104-128 bit key. 128/152 bit key.

Table 11-1 Layer 2 Security Options (continued)

Parameter	Description
WPA1+WPA2	Use this setting to enable WPA1, WPA2, or both. See the WPA1 and WPA2 parameters displayed on the window when WPA1+WPA2 is selected. WPA1 enables Wi-Fi Protected Access with TKIP-MIC Data Encryption. When WPA1+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 WPA1+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. When selected, these CKIP parameters are displayed. Key size: Specify key length. Encryption Key: Specify encryption key. Key Format: ASCII or HEX. **Note** Regardless of which format you choose, for security reasons, only ASCII is visible on the WLC. 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: Enabled or disabled (check box). Key Permutation: Enabled or disabled (check box).

Step 2 Check the **MAC Filtering** check box if you want to filter clients by MAC address.

Step 3 If you selected either WPA1 or WPA2 in Step 1, you must specify the type of WPA encryption: either TKIP or AES.

Step 4 Choose the desired type of authentication key management. The choices are 802.1X, CCKM, PSK, or CCKM+802.1X.

Note If you choose PSK, you must enter the password and type (ASCII or hexadecimal).

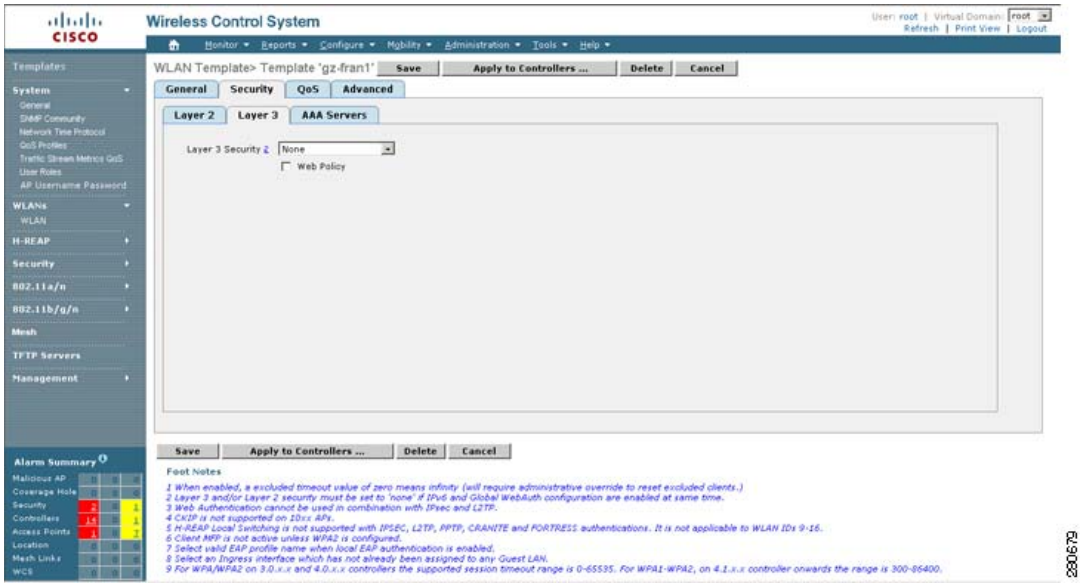
Step 5 Click **Save**.

Layer 3

When you choose the Layer 3 tab, the window shown in Figure 11-7 appears.

Note The screen contains different views depending on what option is chosen in the Layer 3 Security drop-down menu.

Figure 11-7 Layer 3 Window



Follow these steps to configure the Layer 3 tab.

Step 1 Use the Layer 3 security drop-down menu to choose between None and VPN Pass Through. The window parameters change according to the selection you make. If you choose VPN pass through, you must enter the VPN gateway address.

Step 2 You can modify the default security policy (web authentication) or assign specific web authentication (login, logout, login failure) pages and the server source.

a. To change the security policy 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 windows, uncheck the Global WebAuth Configuration **Enabled** check box.

1. When the Web Auth Type drop-down menu 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 menus 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 menu 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 3-17.

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 field.

You can select specific RADIUS or LDAP servers to provide external authentication on the **Security > AAA** panel. To do so, continue with Step 4.

Note The RADIUS and LDAP servers must be already configured to have selectable options on the Security > AAA panel. You can configure these servers on 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 menus.

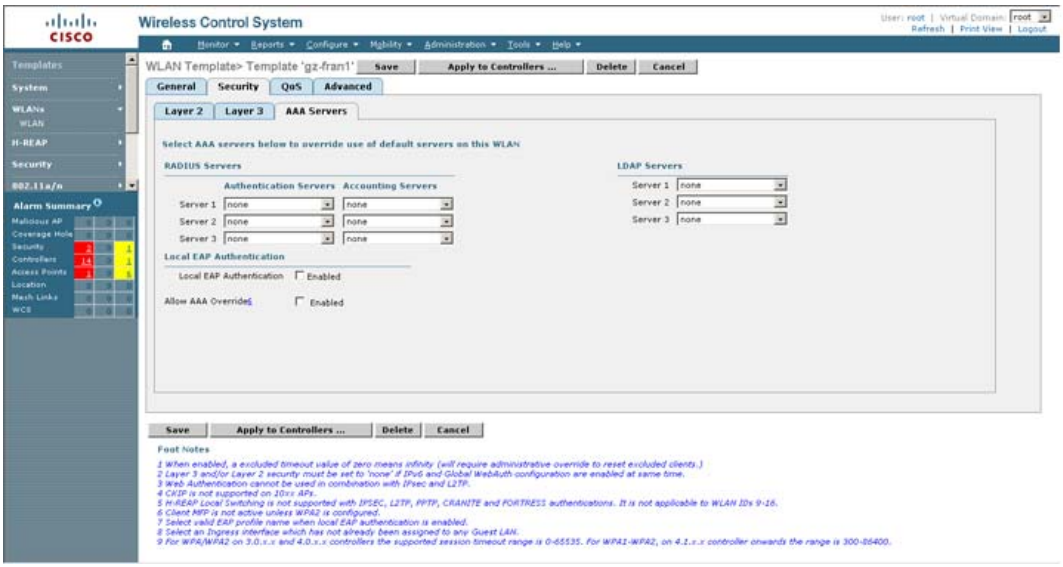
Step 4 Click **Save**.

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 window shown in Figure 11-8 appears.

Figure 11-8 AAA Servers Window



Follow these steps to configure the AAA Servers tab.

Step 1 Use the drop-down menus 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 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.

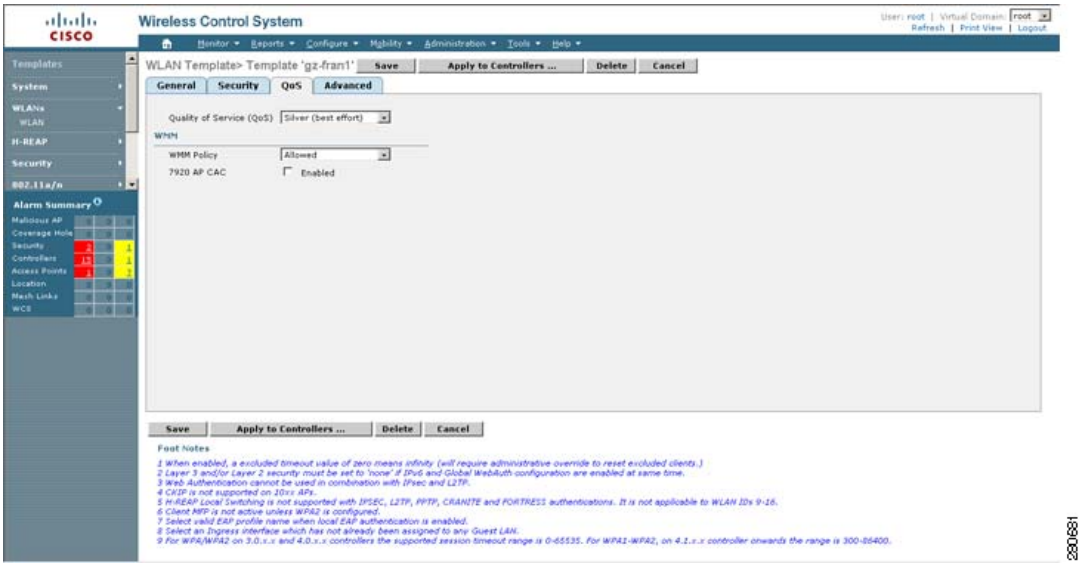
The AAA override values may come from a RADIUS server, for example.

Step 4 Click **Save**.

QoS

When you select the QoS tab from the WLAN Template window, the window as shown in Figure 11-9 appears.

Figure 11-9 QoS Window



Follow these steps to configure the QoS tab.

Step 1 Use the QoS drop-down menu 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 menu 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.

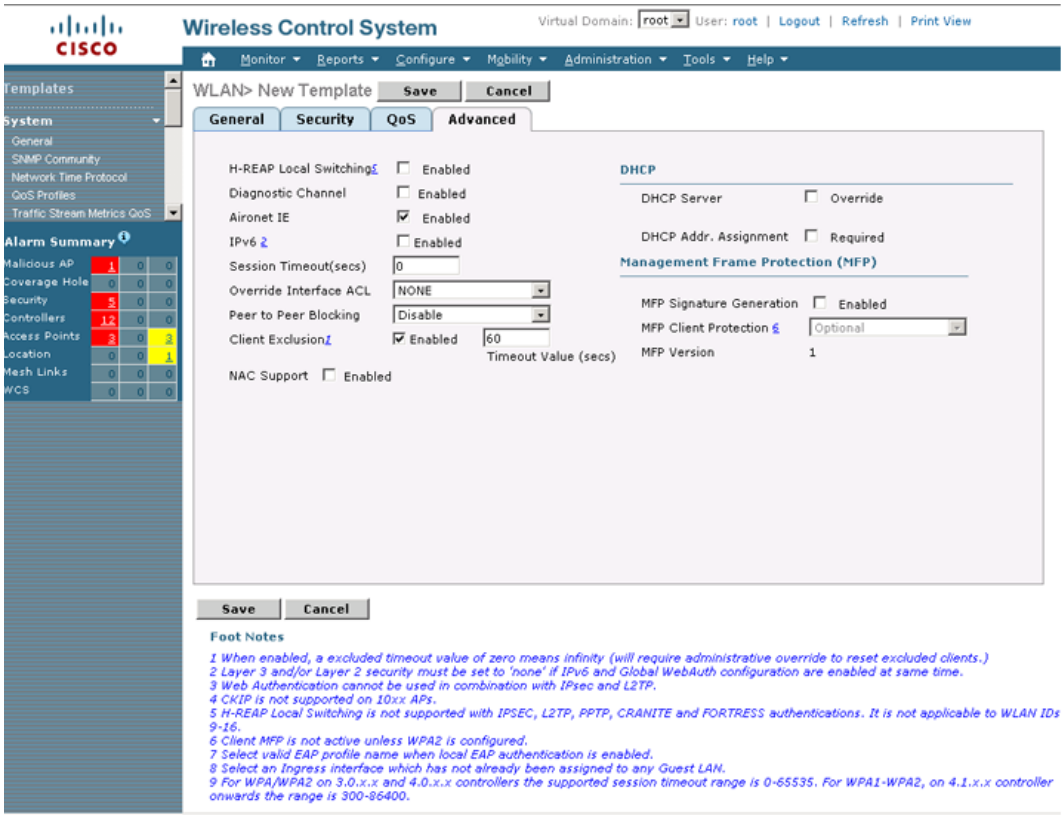
Step 4 If you want WLAN to support older versions of the software on 7920 phones, click to enable the **7920 Client CAC** check box. The CAC limit is set on the access point for newer versions of software.

Step 5 Click **Save**.

Advanced

When you click the Advanced tab on the WLAN Template window, the window shown in Figure 11-10 appears.

Figure 11-10 Advanced Window



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 13-4. 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, PPTP, CRANITE, and FORTRESS authentications, and it is not applicable to WLAN IDs 9-16.

Step 2 At the Session Timeout parameter, set the maximum time a client session can continue before requiring reauthorization.

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 if you want to enable IPv6. You can configure IPv6 bridging and IPv4 web auth on the same WLAN. WCS disallows Layer 2 security with IPv6 bridging.

Note Layer 3 security must be set to *None* for this to be enabled.

Step 5 A list of defined access control lists (ACLs) is provided at the Override Interface ACL drop-down menu. (Refer to the "Configuring Access Control List Templates" section on page 11-56 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 6 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 menu, 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—The packet is forwarded on the upstream VLAN, and the decision is made about what to do with the packet.

If HREAP local switching is enabled for the WLAN, which prevents traffic from passing through the controller, this drop-down menu is grayed out.

Note Peer-to-peer blocking does not apply to multicast traffic.

Step 7 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 8 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. Refer to the "Configuring NAC Out-of-Band Integration" section on page 10-18 for more information.

Step 9 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 10 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 11 At the MFP Client Protection drop-down menu, choose Optional, Disabled, or Required for configuration of individual WLANs of a controller. If infrastructure MFP is not enabled, this drop-down menu 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 12 Click **Save**.

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.

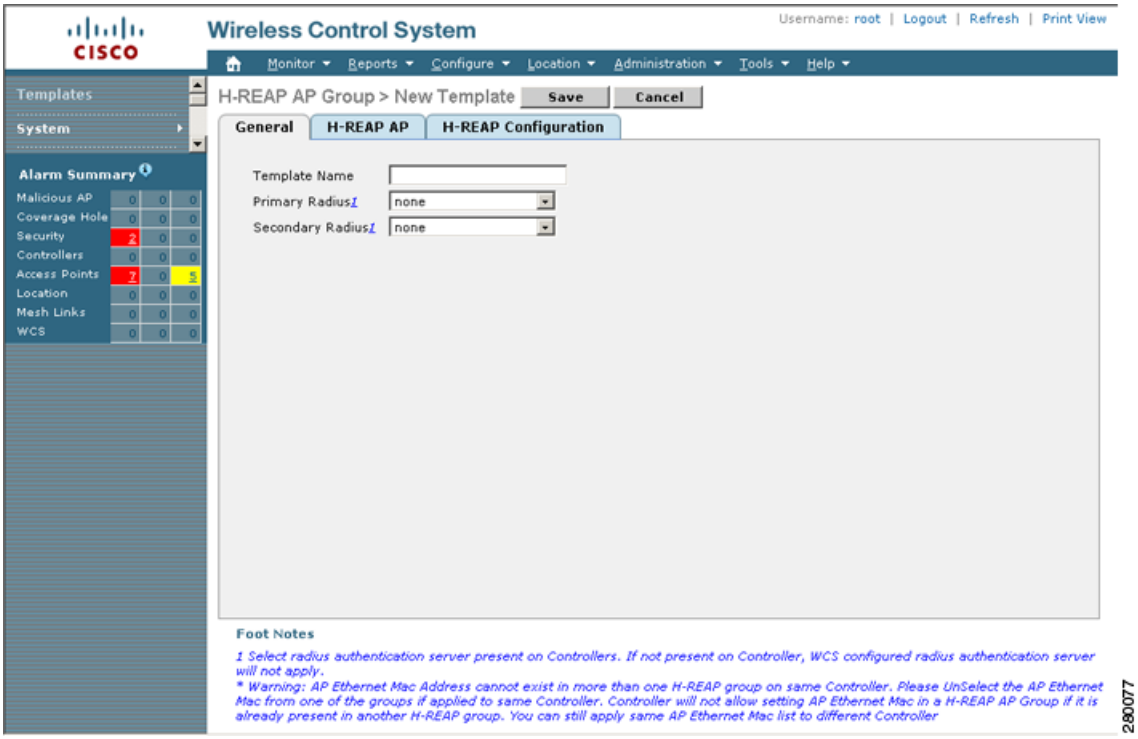
Follow these steps to set up an H-REAP AP group.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **HREAP > HREAP AP Groups**.

Step 3 The Template Name column shows the group names assigned to the HREAP access point groups. If you want to add an additional group, choose **Add HREAP AP Group** from the Select a command drop-down menu.
- or -
To make modifications to an existing template, click to select a template in the Template Name column. The General tab of the HREAP AP Groups template appears (see Figure 11-11).

Figure 11-11 AP Groups HREAP 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 window 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 Check the **H-REAP Local Authentication Enabled** check box to enable local authentication for this hybrid-REAP group. The default value is unchecked.

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 field. 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 Authority ID field, enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.

Step 15 In the EAP-FAST Authority Info field, 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 field, 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

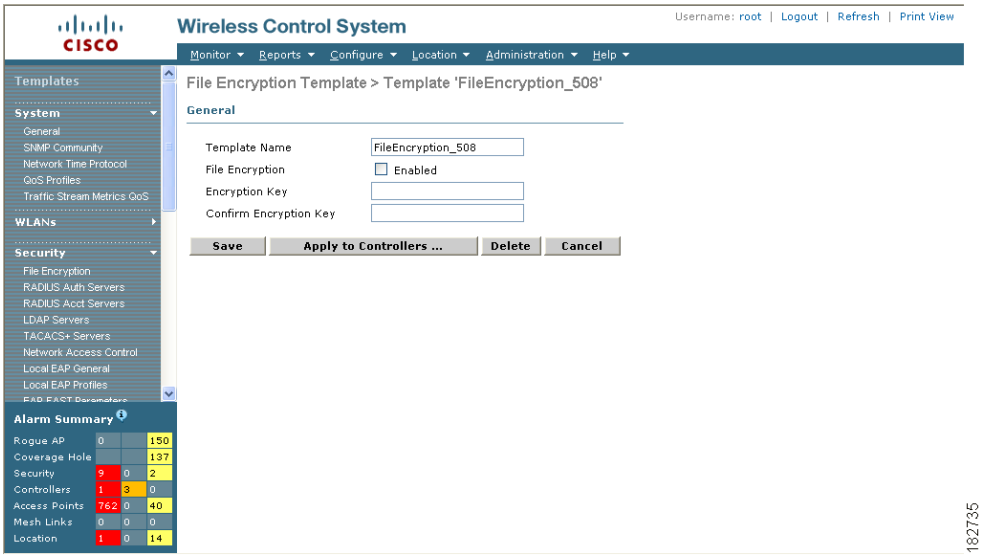
This page enables you to add a new file encryption template or make modifications to an existing file encryption template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > File Encryption**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The File Encryption Template appears (see Figure 11-12).

Figure 11-12 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 template for RADIUS authentication server information 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.

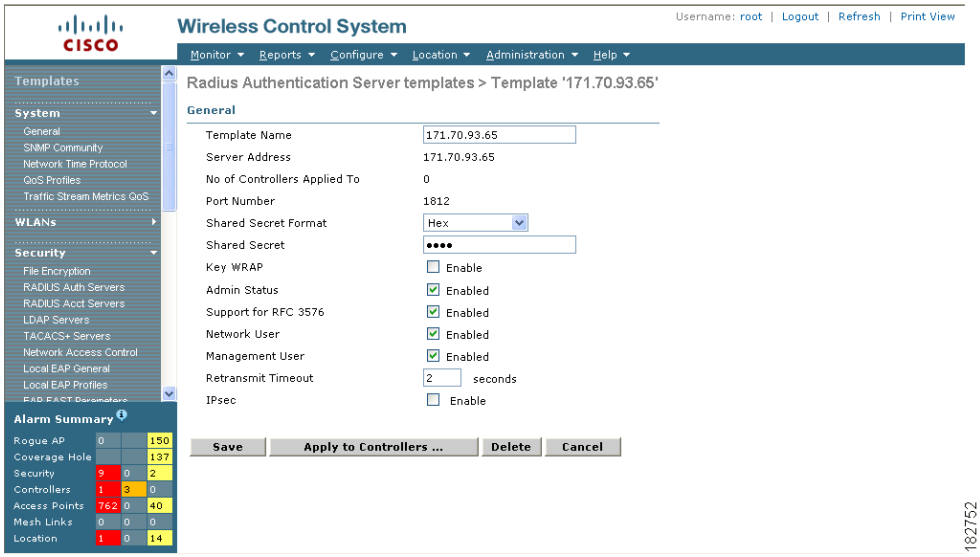
Step 1 Choose **Configure > Controller Templates**.

Step 2 On the left sidebar menu, choose **Security > RADIUS Authentication Servers**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select the template in the Template Name column. The RADIUS Authentication Server Template window appears (see Figure 11-13), and the number of controllers the template is applied to automatically populates.

The IP address of the RADIUS server and the port number for the interface protocol is also displayed.

Figure 11-13 RADIUS Authentication Server Template



Step 4 Use the drop-down menu 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. 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 which format you choose, for security reasons, only ASCII is visible on the WLC. 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 window, 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 menu 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 field. 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 menu 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

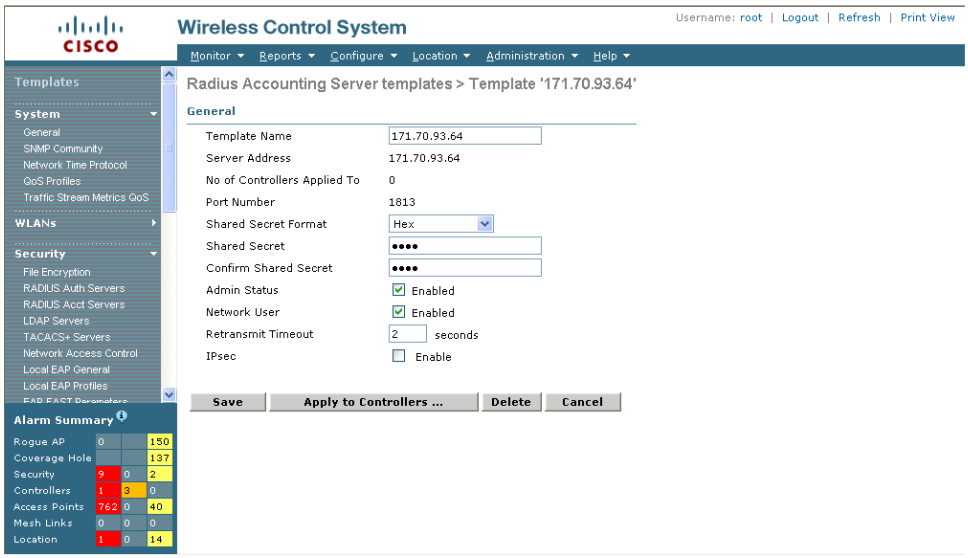
This page allows you to add a new template for RADIUS accounting server information or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > RADIUS Acct Servers**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The RADIUS Accounting Template appears (see Figure 11-14), and the number of controllers the template is applied to automatically populates. The IP address of the RADIUS server and the port number for the interface protocols are also displayed.

Figure 11-14 RADIUS Accounting Server Templates



Step 4 Use the Shared Secret Format drop-down menu to choose either ASCII or hexadecimal.

Note Regardless of which format you choose, for security reasons, only ASCII is visible on the WLC. 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 LDAP Server Template

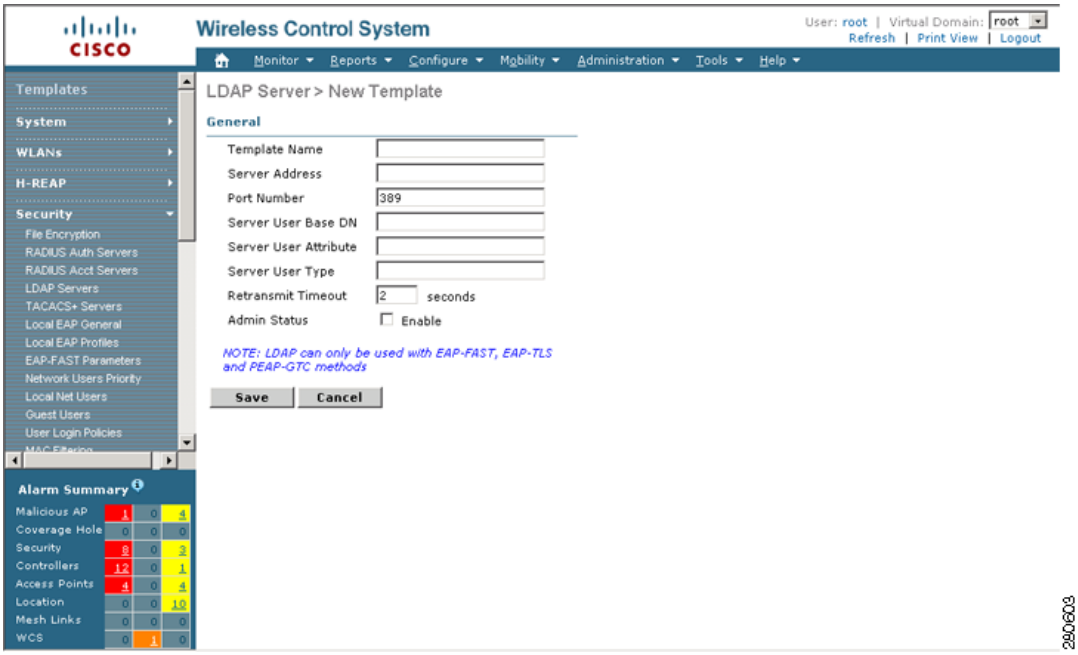
This section explains how to configure a Lightweight Directory Access Protocol (LDAP) server as a backend database, similar to a RADIUS or local user database. An LDAP backend database allows the controller to query an LDAP server for the credentials (username and password) of a particular user. These 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. This page allows you to add a new template for an LDAP server or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > LDAP Servers**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The LDAP Server Template appears (see Figure 11-15). The IP address of the LDAP server and the port number for the interface protocols are displayed.

Figure 11-15 LDAP Server Template



Step 4 In the Server User Base DN field, 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 field, enter the attribute that contains the username in the LDAP server.

Step 6 In the Server User Type field, enter the ObjectType attribute that identifies the user.

Step 7 In the Retransmit Timeout field, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

Step 8 Check the Admin Status check box if you want the LDAP server to have administrative privileges.

Step 9 Click **Save**.

Configuring a TACACS+ Server Template

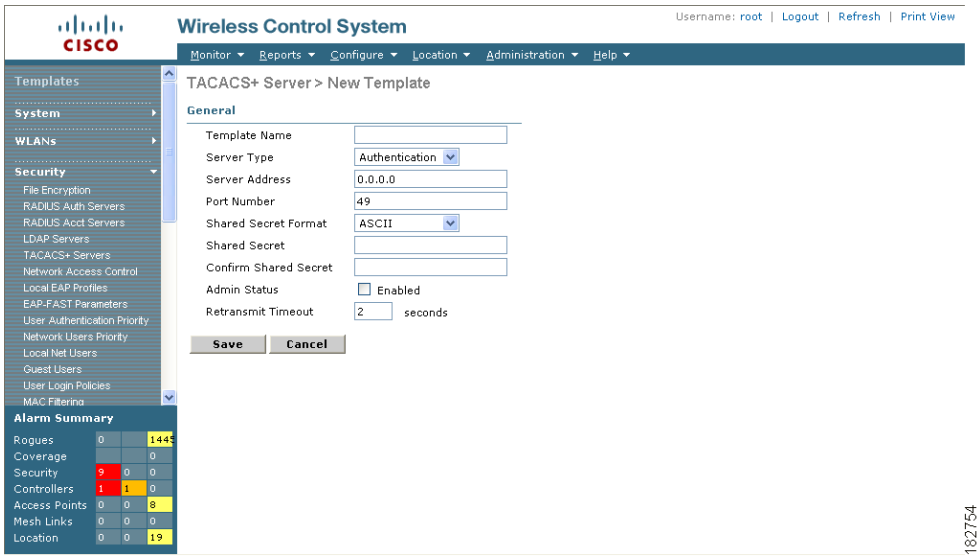
This page allows you to add a new TACACS+ server template or make modifications to an existing template. After these server templates are configured, controller users who log into the controller through the CLI or GUI are authenticated.

Step 1 Choose **Configure > Controller Templates**.

Step 2 On the left sidebar menu, choose **Security > TACACS+ Server**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a user in the Template Name column. The TACACS+ Server Template appears (see Figure 11-16). The IP address and the port number of the TACACS+ template are displayed.

Figure 11-16 TACACS+ Server Template



Step 4 Select the server type. The choices are authentication, authorization, or accounting.

Step 5 Use the drop-down menu 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. 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 field.

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 a template with this timeout value or make changes to an existing template.

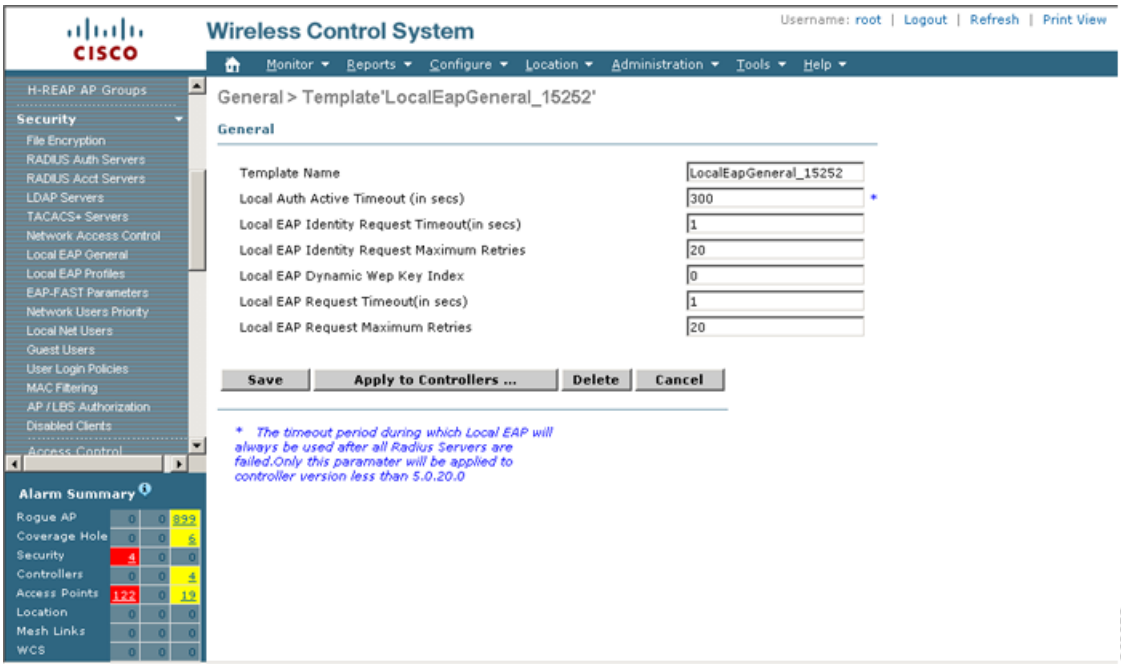
Note If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to then reauthenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > Local EAP General**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The Local EAP General Template appears (see Figure 11-17).

Figure 11-17 Local EAP General Template



Step 4 In the Local Auth Active Timeout field, 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 new template for the local EAP profile 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.

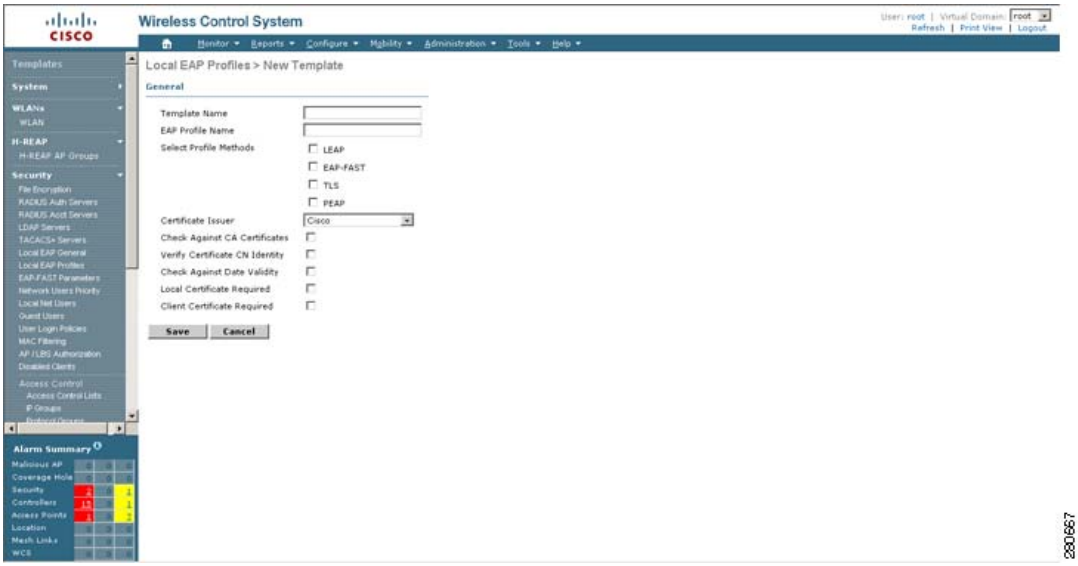
Note The LDAP backend database supports only these local EAP methods: EAP-TLS and EAP-FAST with certificates. LEAP and EAP-FAST with PACs are not supported for use with the LDAP backend database.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > Local EAP Profiles**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The Local EAP Profiles Template appears (see Figure 11-18).

Figure 11-18 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 (Flexile 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 Issues drop-down menu 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 you want the device certificate on the controller to be used for authentication, check the **Local Certificate Required** check box. This certification is applicable only to EAP-FAST.

Step 10 If you want the wireless clients to send their device certificates to the controller in order to authenticate, check the **Client Certificate Required** check box. This certification is only applicable to EAP-FAST.

Step 11 Click **Save**.

Step 12 Follow these steps to enable local EAP:

a. Choose **WLAN > WLANs** 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

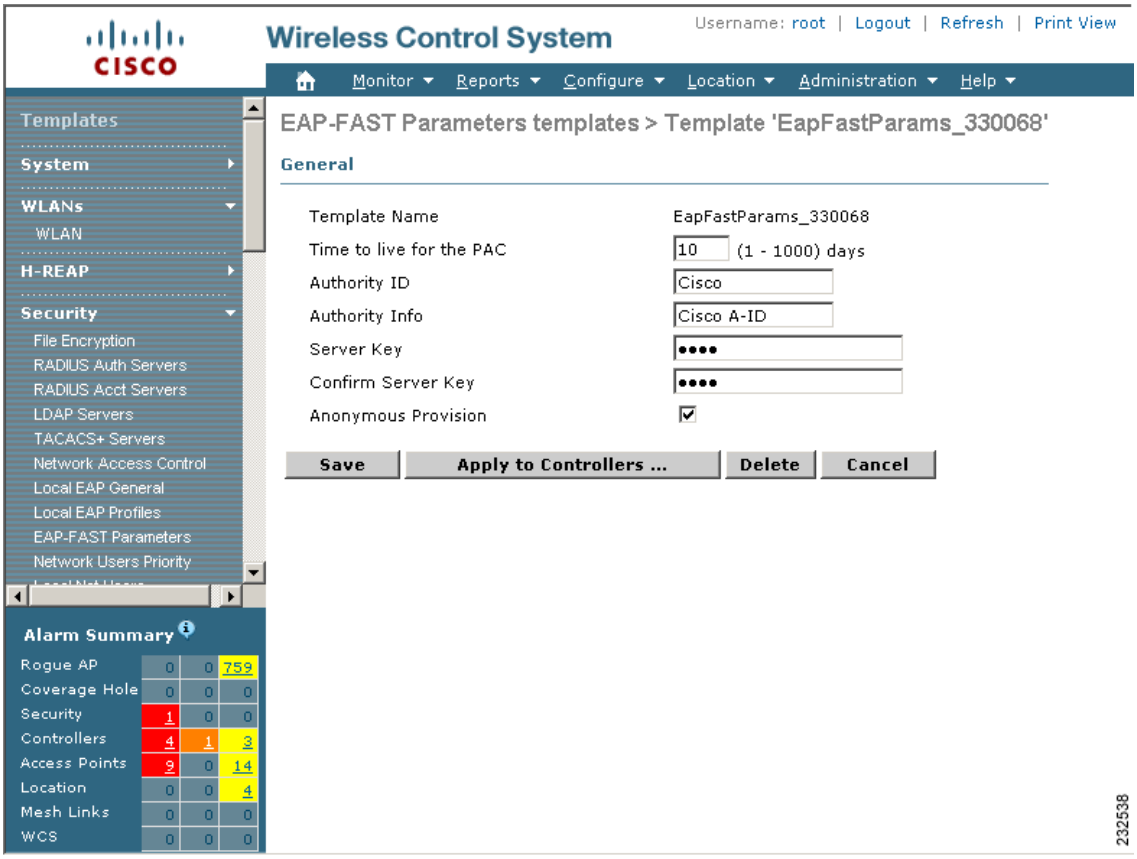
This authentication type (Flexible Authentication via Secure Tunneling) uses a three-phased tunnel authentication process to provide advanced 802.1X EAP mutual authentication. A username, password, and PAC are used to perform mutual authentication with the RADIUS server through the access point. This page allows you to add a new template for the EAP-FAST profile or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > EAP-FAST Parameters**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The EAP-FAST Parameters Template appears (see Figure 11-18).

Figure 11-19 EAP-FAST Parameters Template



Step 4 In the Time to Live for the PAC field, 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 field, 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 field, enter the ID for the authority identifier of the local EAP-FAST server.

Step 7 In the Authority Info field, 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 a local certificate is required, click the check box.

Step 10 If a client certificate is required, click the check box.

Step 11 If an anonymous provision is required, click the check box.

Step 12 If you want to enable anonymous provisioning, check the **Client Authentication 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 13 Click **Save**.

Configuring Network User Credential Retrieval Priority Templates

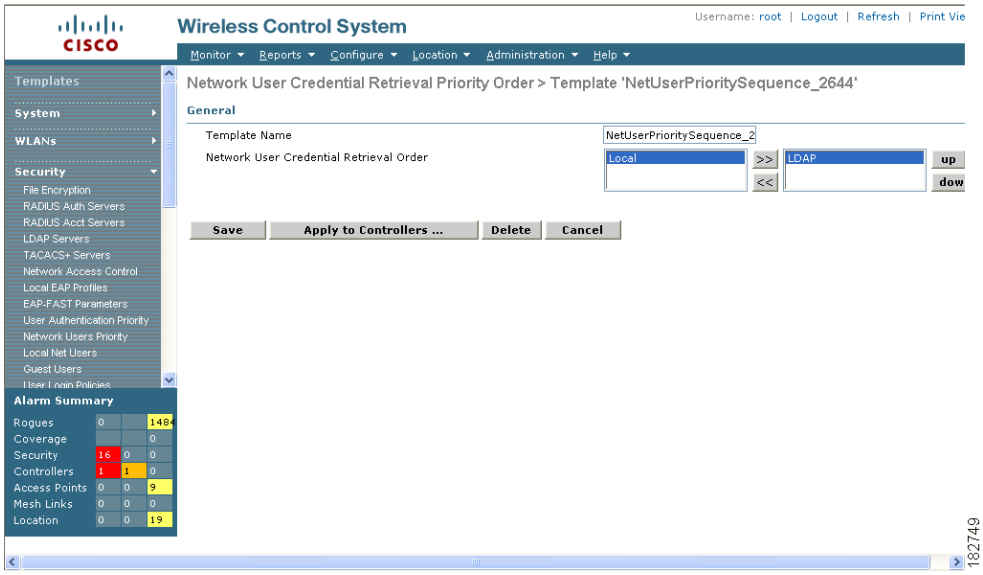
You can specify the order that LDAP and local databases use to retrieve user credential information. This page allows you to add a new template for the network user credential retrieval priority or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > Network Users Priority**.

To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The Network User Credential Retrieval Priority Template appears (see Figure 11-20).

Figure 11-20 Network User Credential Retrieval Priority Order Template



Step 3 Use the left and right pointing arrows to include or disclude network user credentials in the right-most window.

Step 4 Use the up and down buttons to determine the order credentials are tried.

Step 5 Click **Save**.

Configuring a Local Network Users Template

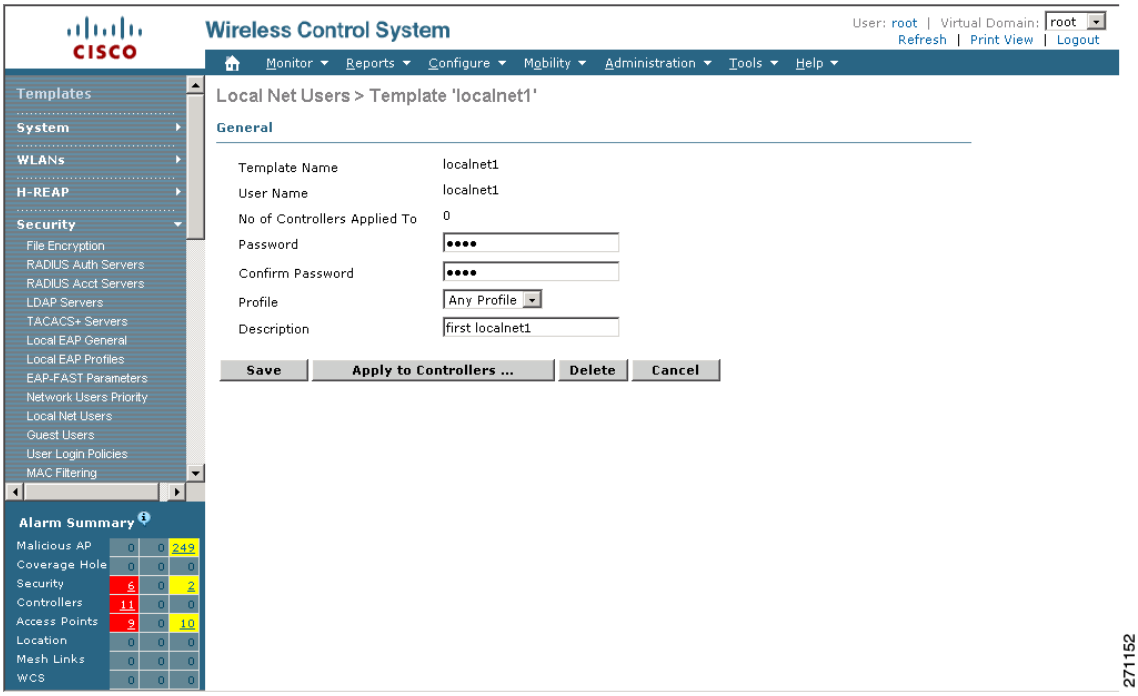
With this template, you can store the credentials (username and password) of all the local network users. These credentials are then used to authenticate the users. For example, local EAP may use the local user database as its backend database to retrieve user credentials. This page allows you to add a new local authentication template or make modifications to an existing 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 Templates**.

Step 2 On the left sidebar menu, choose **Security > Local Net Users**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a user in the User Name column. The Local Net Users Template appears (see Figure 11-21).

Figure 11-21 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 10. 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.

Enter a username and password. It is mandatory to fill the Username and Password fields 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 menu 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 Step 10.

Step 9 If you want to override the existing template parameter, click to enable this parameter.

Step 10 Click **Save**.

Configuring Guest User Templates

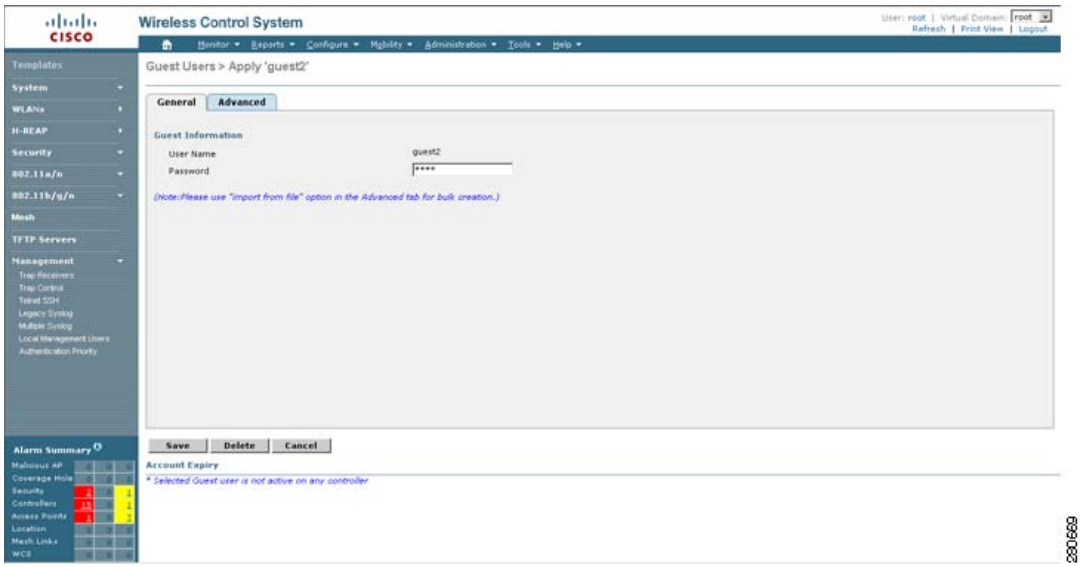
This page allows you to create a new template for guest user information or make modifications to an existing template. The purpose of a guest user account is to provide a user account for a limited amount of time. A Lobby Ambassador is able to configure a specific time frame for the guest user account to be active. After the specified time period, the guest user account automatically expires. Refer to the "Creating Guest User Accounts" section on page 7-11 for further information on guest access.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > Guest Users**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a user in the User Name column. The General Guest User Template window appears (see Figure 11-22).

Figure 11-22 Guest User Template



Step 4 Enter a guest name. Maximum size is 24 characters.

Step 5 Click the **Generate Password** check box if you want a password automatically generated. The Password and Confirm Password parameters are automatically populated. If automatic generation is not enabled, you must supply a password twice.

Note If this is enabled, a different password is supplied for each day (up to the number of days chosen). If this is disabled (unchecked), one password is supplied for a span of days.

Step 6 Click the **Advanced** tab.

Step 7 If you want to import multiple users, click the **Import From File** check box.

Step 8 Click **Browse** to go to the file path where the CSV is located. The Sample CSV file is as follows:

```
User Name| Password| Life Time| Description| Disclaimer
Guest-1,pwd1,864000,Description-1,Disclaimer-1
Guest-2,pwd2,864000,Description-2,Disclaimer-2
```

Note Table headings are not required, and description and disclaimer are not mandatory.

Step 9 Choose a user role for the guest user from the drop-down menu. 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 10 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 menus. The default value for Limited is one day (8 hours).
- When Unlimited is chosen, there is no expiration date for the guest account.

Step 11 Choose the area (indoor, outdoor), controller list, or config group to which the guest user traffic is limited from the Apply to drop-down menu.

If you choose the controller list option, a list of controller IP addresses appears. Check the check box next to all controller networks on which guest traffic is allowed.

Step 12 (Optionally) Modify the default guest user description if necessary.

Step 13 (Optionally) Modify the Disclaimer text, if necessary. If you want the supplied text to be the default, click the **Make this Disclaimer default** check box.

Step 14 Click **Save**.

Configuring a User Login Policies Template

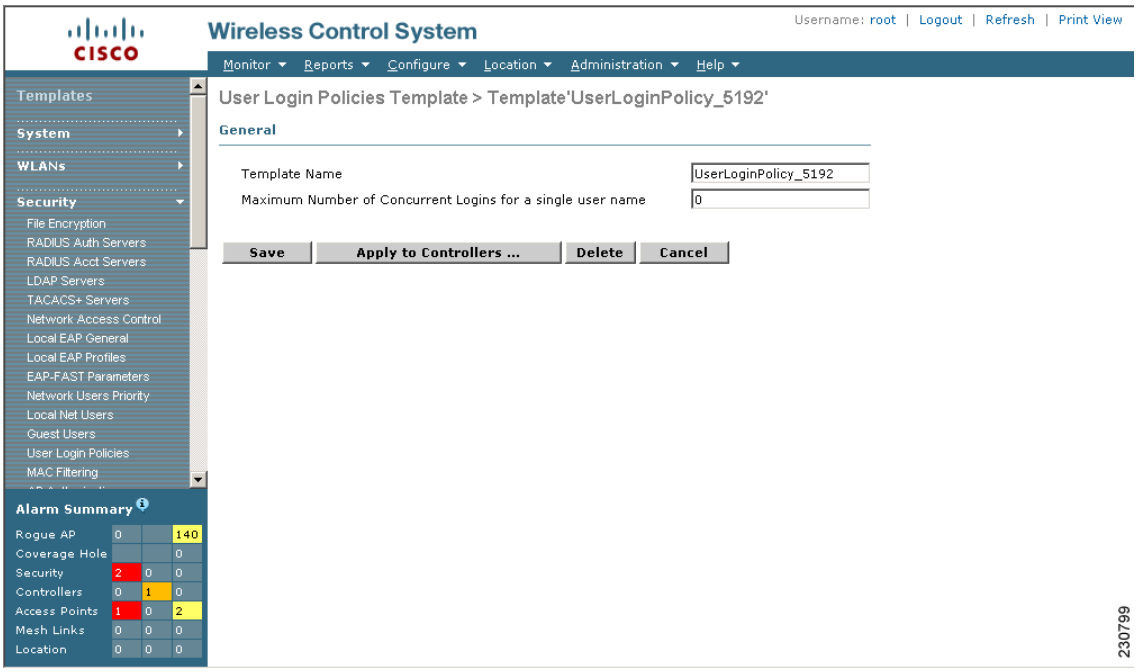
This page allows you to add a new user login policies template or make modifications to an existing template. On this template you set the maximum number of concurrent logins that each single user can have.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > User Login Policies**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a user login policy in the Template Name column. The User Login Policies Template window appears (see Figure 11-23).

Figure 11-23 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

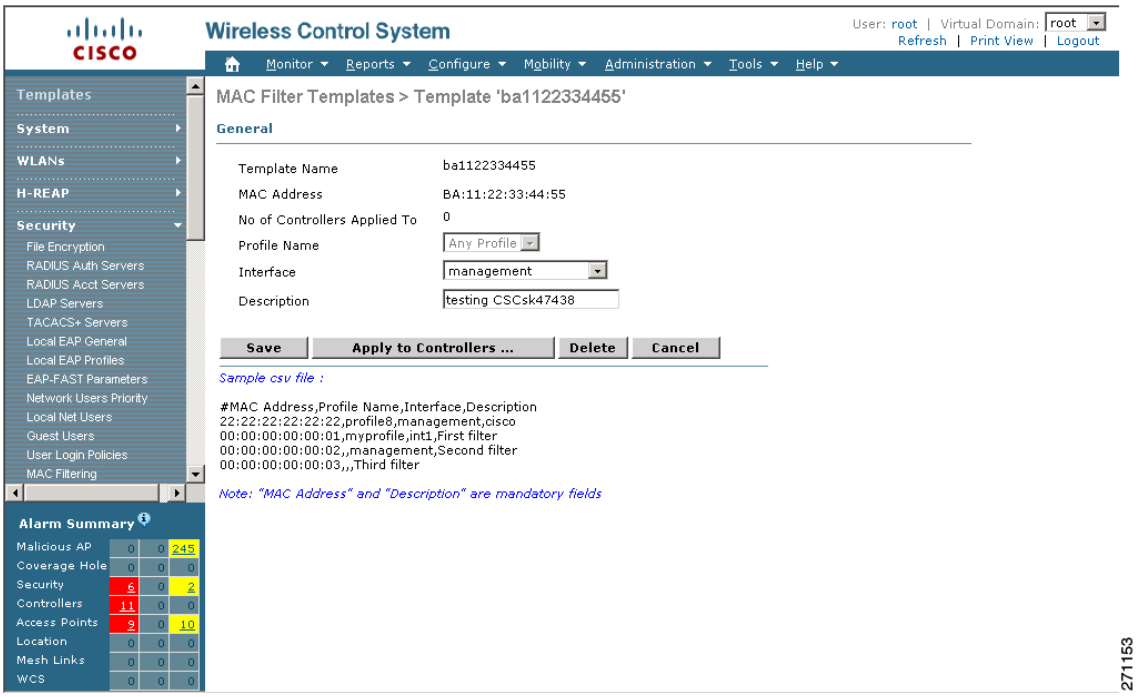
This page allows you to add a new MAC filter template or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > MAC Filtering**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a MAC address in the MAC Address column. The MAC Filter Templates window appears (see Figure 11-24).

Figure 11-24 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 9.

The client MAC address appears.

Step 5 Choose the SSID which this MAC filter is applied to or choose the *any SSID* option.

Step 6 Use the drop-down menu 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 LBS Authorization

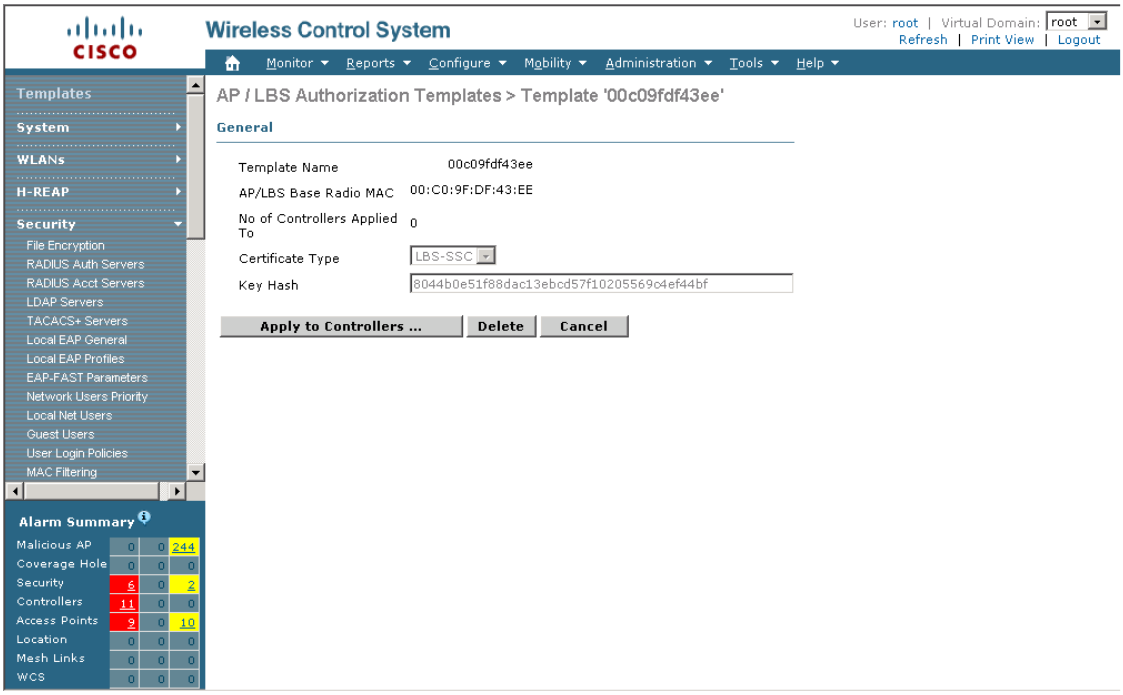
Follow these steps to add an access point or LBS authorization template or make changes to an existing template. These templates are devised for Cisco 11xx/12xx series access points converted from IOS to LWAPP or for 1030 access points connecting in bridge mode. Refer to the *Cisco Location Appliance Configuration Guide* for further information.

Step 1 Choose **Configure > Controller Templates**

Step 2 From the Security selections in the left sidebar menu, choose **AP/LBS authorization**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click a MAC address in the AP Base Radio MAC column. The AP/LBS Authorization Template appears (see Figure 11-25), and the number of controllers the template is applied to automatically populates.

Figure 11-25 AP/LBS 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, Certificate Type (MIC or SSC), and key hash (such as 00:0f:90:b5:f7:c8,SSC,856D20CE8AFCE1C0E7A136F34E3F130FAFAA78A8). 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

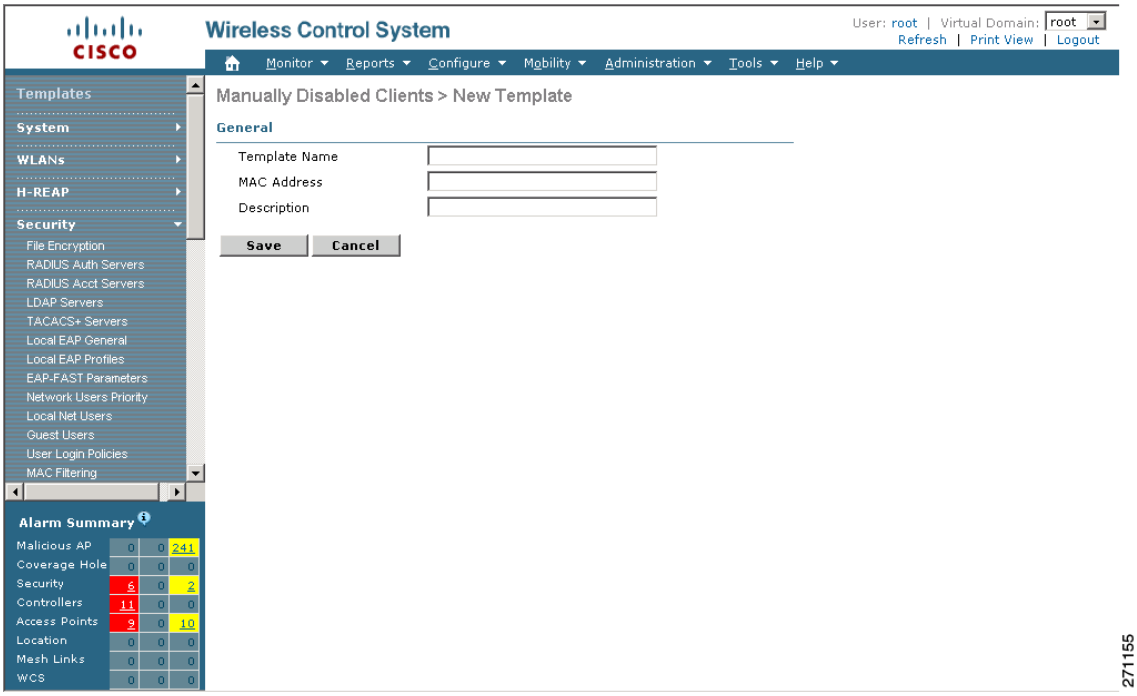
This page allows you to add a new manually disabled client template or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > Disabled Clients**.

To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a disabled client in the Template Name column. The Manually Disabled Clients Template window appears (see Figure 11-26).

Figure 11-26 Manually Disabled Clients Template



Step 3 Enter the MAC address of the client you want to disable.

Step 4 Enter a description of the client you are setting to disabled.

Step 5 Click **Save**.

Configuring a CPU Access Control List (ACL) Template

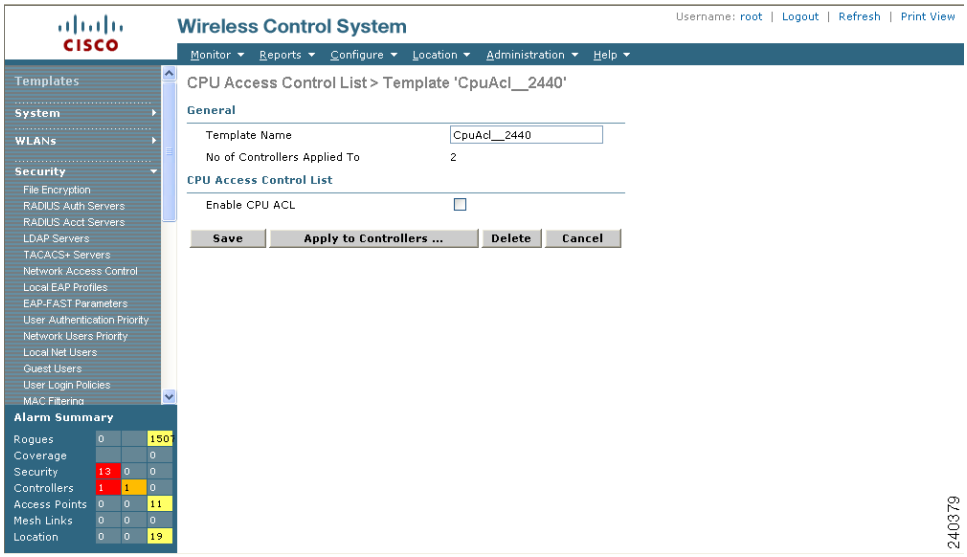
The existing ACLs established in the "Configuring Access Control List Templates" section on page 11-56 is used to set traffic controls between the central processing unit (CPU) and network processing unit (NPU). Follow these steps to add a CPU ACL template or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 Choose **Security > CPU Access Control List** in the left sidebar menu.

Step 3 If you want to create a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template name in the ACL Name column. The CPU Access Control List Template appears (see Figure 11-27).

Figure 11-27 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 menu, choose a name from the list of defined names.

Step 6 From the CPU ACL Mode drop-down menu, 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 window enables you to configure the rogue policy (for access points and clients) applied to the controller. Follow these steps to add a rogue policy template or modify an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > Rogue Policies**.

Step 3 If you want to create a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template name in the Template Name column. The Rogue Policy Setup Template appears (see Figure 11-28).

Figure 11-28 Rogue Policy Setup Template

Step 4 Check the **Rogue Location Discovery Protocol** to enable the discovery of rogue access points. Rogue Location Discovery Protocol (RLDP) determines whether or not the rogue is connected to the enterprise wired network.

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 adhoc 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 Templates > Security > 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 9-17.

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.

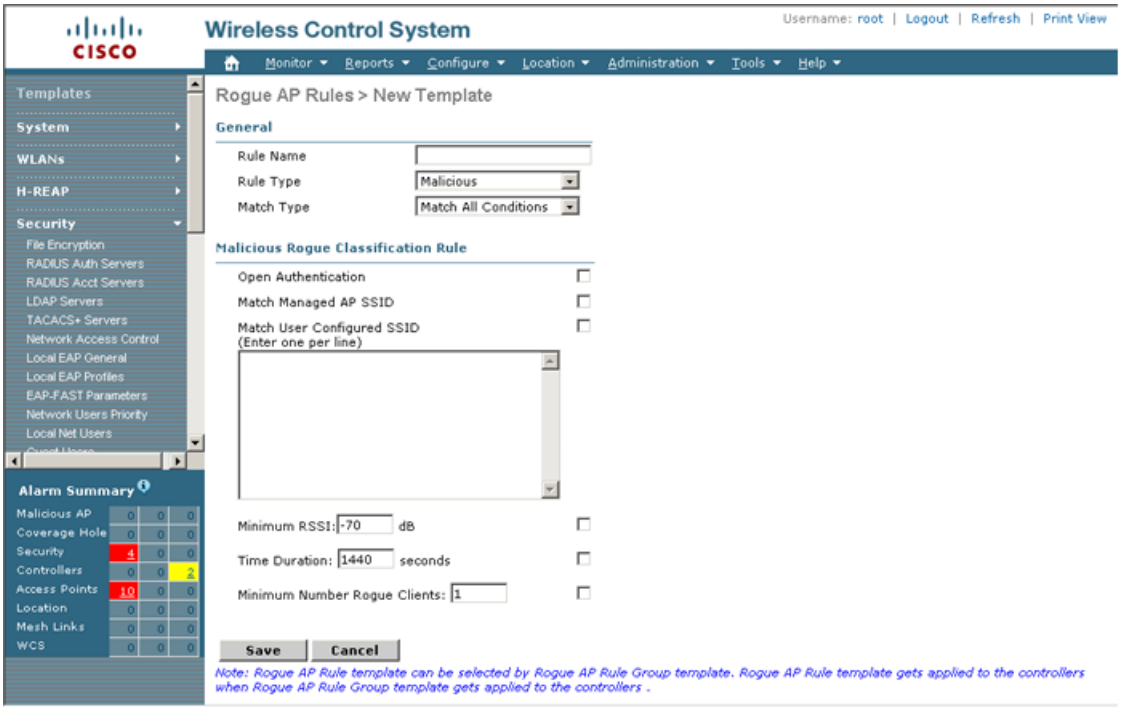
Follow these steps to create a new classification rule template for rogue access points.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > Rogue AP Rules**.

Step 3 From the Select a command drop-down menu, choose **Add Classification Rule** and click **GO**. The Rogue AP Rules > New Template window appears (see Figure 11-29). To make modifications to an existing rogue access point rules template or to apply a current template to the controllers, choose **Configure > Controller Templates > Security > Rogue AP Rules** and click a template name in the Template Name column.

Figure 11-29 Rogue AP Rules > New Template Window



Step 4 In the General portion of the window, 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 menu. 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 menu.

Step 5 In the Malicious Rogue Classification Rule portion of the window, 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 text box below **Match User Configured SSID**.

- 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.

To view current rogue access point rule groups templates, choose **Configure > Controller Templates > Security > Rogue AP Rule Groups**.

Follow these steps to create a new Rogue AP Rule Groups template.

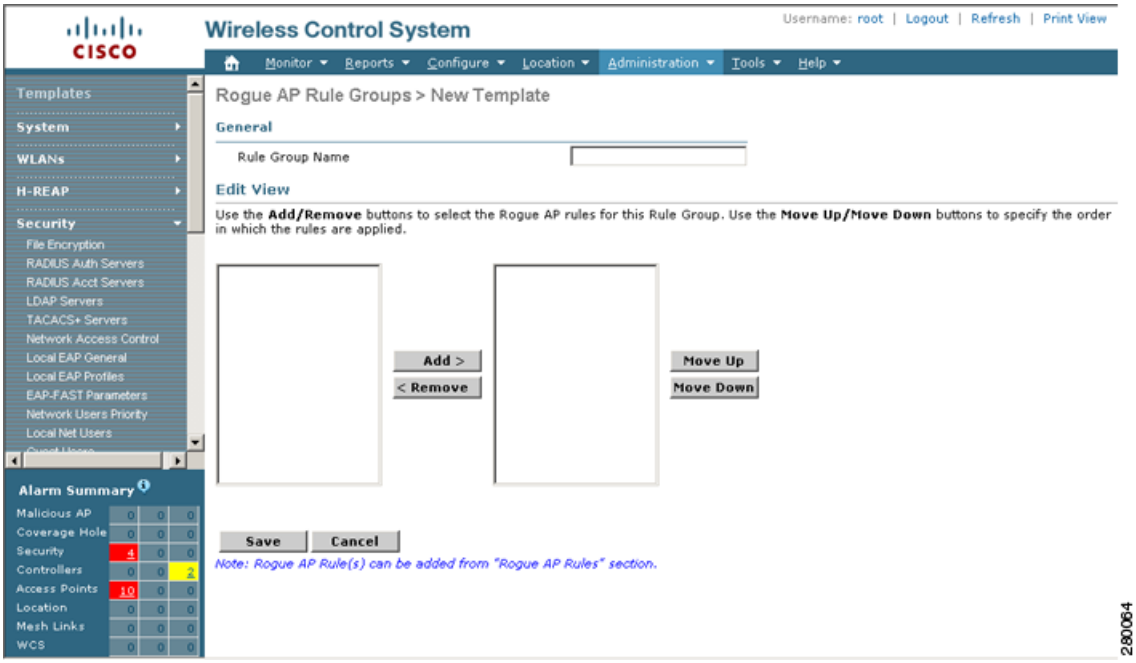
Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > Rogue AP Rule Groups**.

Step 3 From the Select a command drop-down menu, click **Add Rogue Rule Group**.

Step 4 Click **GO**. The Rogue AP Rule Groups > New Template window appears (see Figure 11-30).

Figure 11-30 Rogue AP Rule Groups > New Template



Note To make modifications to an existing rogue policy template or to apply a current template to controllers, choose **Configure > Controller Templates > Security > Rogue AP Rule Groups** and click a template name in the Template Name column. 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 window.

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. Refer to the "Configuring a Rogue AP Rules Template" section on page 11-44 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 window 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-LWAPP access points from being falsely identified as rogues.

Note *Friendly Internal* access points were previously referred to as *Known APs*.

To view or edit the current list of friendly access points, choose **Configure > Controller Templates > Security > Friendly AP**. 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.

To add a new friendly access point, follow these steps:

Step 1 Choose **Configure > Controller Templates**.

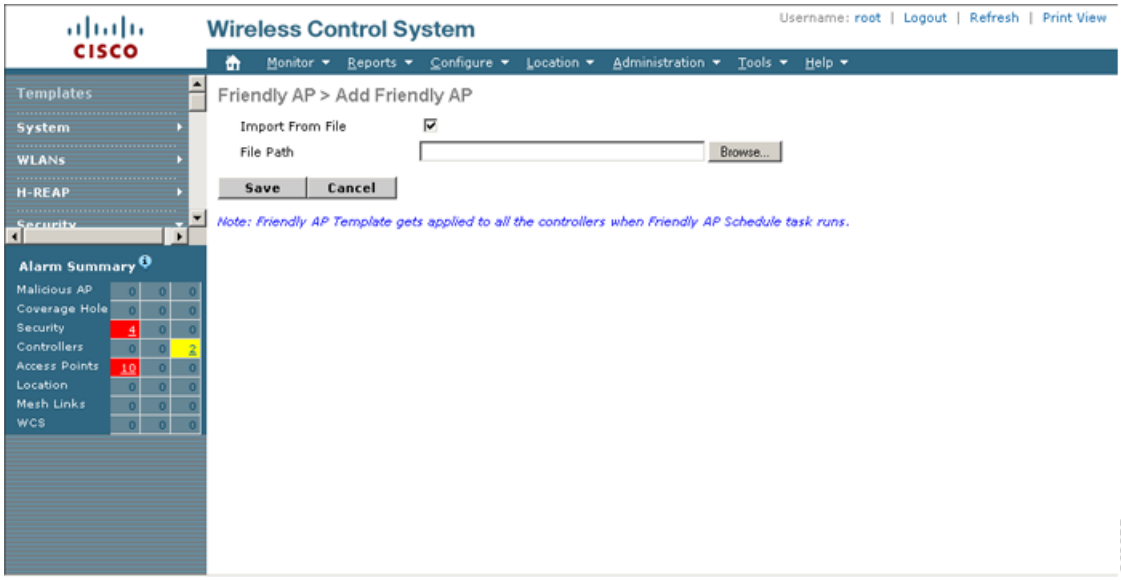
Step 2 From the left sidebar menu, choose **Security > Friendly AP**.

Step 3 From the Select a command drop-down menu, choose **Add Friendly**.

Step 4 Click **GO**. The Friendly AP window appears (see Figure 11-31).

Note To make modifications to an existing friendly access point, choose **Configure > Controller Templates > Security > Friendly Internal** and click the access point's MAC address. Make the necessary changes to the access point and click **Save**.

Figure 11-31 Friendly AP > Add Friendly AP Window



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 menu.
  - 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 window without adding the access point to the list.

Configuring a Client Exclusion Policies Template

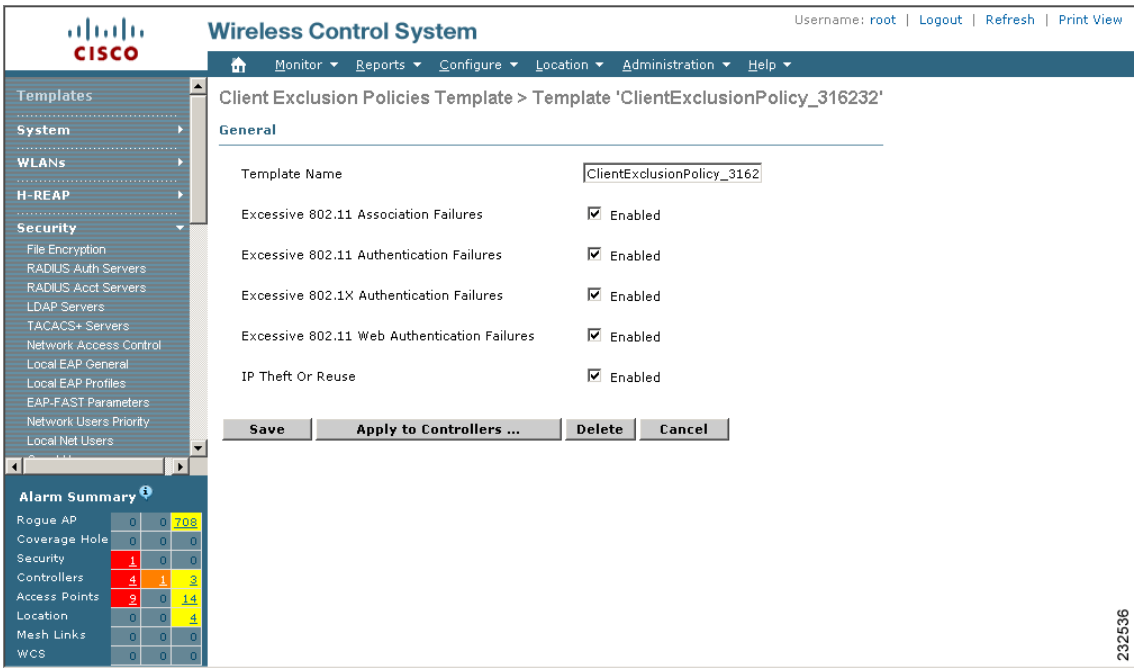
Follow these steps to add a client exclusion policies template or modify an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 Choose **Security > Client Exclusion Policies** in the left sidebar menu.

If you want to create a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template name in the Template Name column. The Client Exclusion Policies Template appears (see Figure 11-32).

Figure 11-32 Client Exclusion Policies Template



Step 3 To edit an existing client exclusion policies template, click its name in the Template Name column to go the Client Exclusion Policies Template window. Create or edit a client exclusion policies template by configuring its parameters.

Table 11-2 Client Exclusion 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.
External Policy Server Failures	Enable to exclude clients with excessive external policy server failures.

Table 11-2 (continued)Client Exclusion 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 4 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.

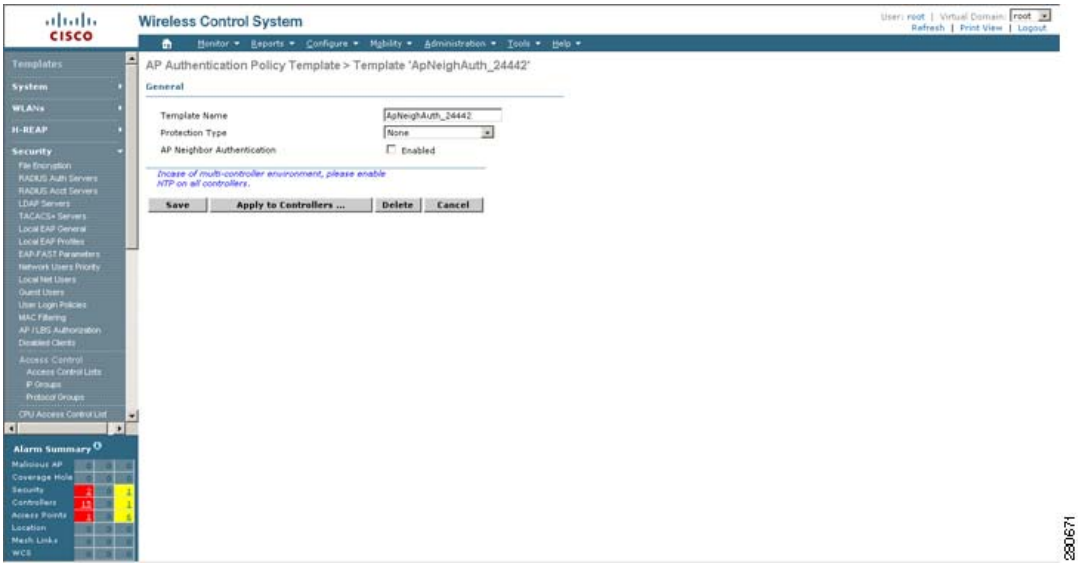
Follow these steps to add a new template for the access point authentication and management frame protection (MFP) or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, select **Security > AP Authentication and MFP**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a MAC address in the AP Base Radio MAC column. The AP Authentication Policy Template appears (see Figure 11-33), and the number of controllers the template is applied to automatically populates.

Figure 11-33 AP Authentication Policy Template



Step 4 From the Protection Type drop-down menu, choose one of the following authentication policies:

- None: No access point authentication policy.
- AP Authentication: Apply authentication policy.
- MFP: Apply management frame protection.

Step 5 Check to enable AP neighbor authentication. With this feature enabled, the access points sending RRM neighbor packets with different RF network names are reported as rogues.

Step 6 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 7 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.

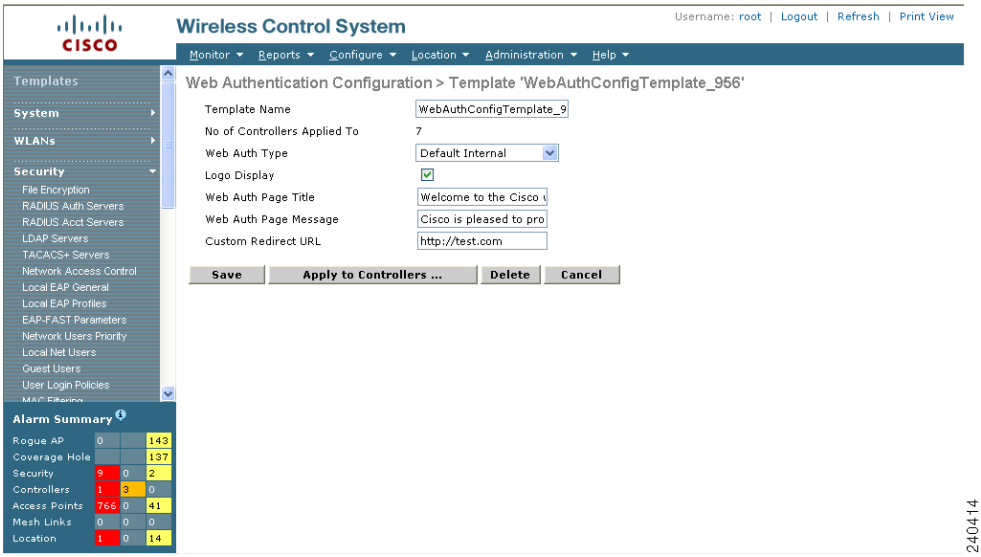
Follow these steps to add a web authentication template or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > Web Auth Configuration**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The Web Authentication Configuration Template window appears (see Figure 11-34), and the number of controllers the template is applied to automatically populates.

Figure 11-34 Web Authentication Configuration Template



Step 4 Choose the appropriate web authentication type from the drop-down menu. 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 menu 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 field is http://www.company.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 field is http://www.company.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. 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 Download the sample login.html bundle file from the server. The .html file is shown in Figure 11-35. The login page is presented to web users the first time they access the WLAN if web authentication is turned on.

Figure 11-35 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**.

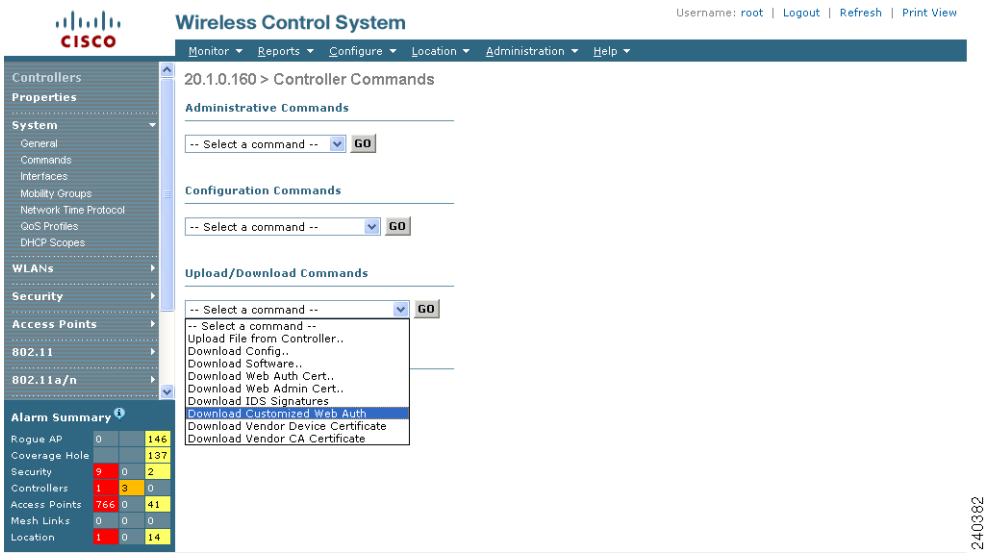
Step 7 Choose a controller by clicking the URL for the corresponding IP address. If you select more than one IP address, the customized Web authentication page is downloaded to multiple controllers.

Step 8 From the left sidebar menu, choose **System > Commands**.

Step 9 From the Upload/Download Commands drop-down menu, 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 (see Figure 11-36).

Figure 11-36 Download Customized Web Auth Bundle to Controller



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 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. 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" 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 Access Control List Templates

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 an ACL template or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 Choose **Access Control > Access Control Lists** in the left sidebar menu.

Step 3 If you want to create a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template name in the ACL Name column. The Access Control List name appears in the window.

Step 4 To create reusable grouped IP addresses and protocols, choose **Access Control > IP Groups** from the left sidebar menu.

Step 5 All the IP address groups are listed. One IP address group can have a maximum of 128 IP address and netmask combinations. To define a new IP address group, choose **Add IP Group** from the Select a command drop-down menu and click **GO**. To view or modify an existing IP address group, click the URL of the IP address group. The IP address group window opens.

Note For the IP address of any, an *any* group is predefined.

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 menu and click **GO**. To view or modify an existing protocol group, click the URL of the group. The Protocol Groups window appears.

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 In the Start Port parameter, enter a value (between 1 and 64) to determine the order of this rule in relation to any other rules defined for this ACL. The rules for each ACL are listed in contiguous sequence from 1 to 64. That is, if rules 1 through 4 are already defined and you add rule 29, it is added as rule 5.

Note If you add or change a sequence number, the operating system adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have sequence numbers 1 through 7 defined and change number 7 to 5, the operating system automatically reassigns sequence 5 to 6 and sequence 6 to 7. Any rules generated can be edited individually and resequenced in the desired order.

Step 10 From the Source Port drop-down menu, specify the source of the packets to which this ACL applies.

Step 11 For the Destination drop-down menu, specify the destination of the packets to which this ACL applies.

Step 12 In the DSCP drop-down menu, choose any or a specific IP address. DSCP is a packet header code that can be used to define the quality of service across the Internet.

Step 13 Click **Save**.

Step 14 You can now create new mappings from the defined IP address groups and protocol groups. To define a new mapping, choose the ACL template to which you want to map the new groups. All ACL mappings appear on the top of the window, and all ACL rules appear on the bottom.

Step 15 To define a new mapping, choose **Add Rule Mappings** from the Select a command drop-down menu. The Add Rule Mapping windows appears.

Step 16 Choose the desired IP address groups, protocol groups, and action and click **Add**. The new mappings will populate the bottom table.

Step 17 Click **Save**.

Step 18 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 Policy Name Template (for 802.11a/n or 802.11b/g/n)

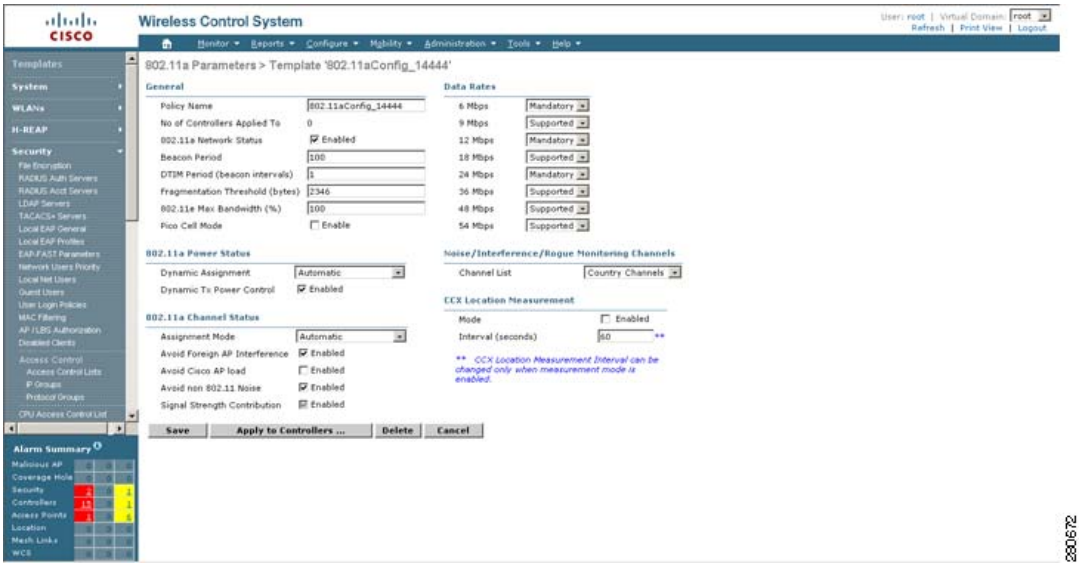
Follow these steps to add a new policy name template for 802.11a/n or 802.11b/g/n or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose either **802.11a/n > Parameters or 802.11b/g/n > Parameters**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu. To make modifications to an existing template, click to select a policy name in the Policy Name column. The 802.11a/n or b/g/n Parameters Template window appears (see Figure 11-37), and the number of controllers the template is applied to automatically populates.

Figure 11-37 802.11a/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 Enter the amount of time between beacons in kilomicroseconds. The valid range is from 100 to 600 milliseconds.

Step 6 Enter the number of beacon intervals that may elapse between transmission of beacon frames containing a traffic indicator message (TIM) element whose delivery count field is 0. This value is transmitted in the DTIM period field of beacon frames. When client devices receive a beacon that contains a DTIM, they normally wake up to check for pending packets. Longer intervals between DTIMS let clients sleep longer and preserve power. Conversely, shorter DTIM periods reduce the delay in receiving packets but use more battery power because clients wake up more often.

Step 7 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 8 Enter the percentage for 802.11e maximum bandwidth.

Step 9 Click if you want short preamble enabled.

Step 10 Click the **Pico Cell Mode** check box if you want it enabled. This feature enables automatic operating system parameter reconfiguration, allowing the operating system to function efficiently in pico cell deployments.

Step 11 Click the **Fast Roaming Mode** check box if you want to enable it. Enabling Cisco's Centralized Key Management (CCKM) authentication key management allows fast exchange when a client roams from one access point to another.

Step 12 At the Dynamic Assignment drop-down menu, 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 Use the Tx Level drop-down menu to determine the access point's transmit power level. The available options are as follows:

- 1 - Maximum power allowed per country code setting
- 2 - 50% power
- 3 - 25% power
- 4 - 6.25 to 12.5% power
- 5 - 0.195 to 6.25% power

Note 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 menu 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 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 Click the **Avoid Cisco AP Load** check box if you want it enabled. Enable this 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 Click the **Avoid non 802.11 Noise** check box if you want to enable it. Enable this 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). 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 Data rates are negotiated between the client and the controller. 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 pull-down selection 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 menu 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 High Density Templates

A method to mitigate the inter-cell contention problem in high-density networks is to adjust the access point and client station receiver sensitivity, CCA sensitivity, and transmit power parameters in a relatively cooperative manner. By adjusting these variables, the effective cell size can be reduced, not by lowering the transmit power but by increasing the necessary received power before an access point and client consider the channel sufficiently clear for packet transfer. Follow these steps to add high density on a template or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose either **802.11a/n > Parameters**.

Step 3 In the General portion of this window, you see a Pico Cell Mode parameter. Click the check box to enable pico cell.

Note In order for this check box to have validity, you must have software version 4.1 or later. If you have an earlier version, this check box value is ignored.

Step 4 Choose **802.11a/n > Pico Cell** from the left sidebar menu. Click which template in the Template Name column you want to modify or choose **Add Template** from the Select a command drop-down menu and click **GO**. The window as shown in Figure 11-38 appears.

Figure 11-38 Pico Cell Parameters Window

Note If the Pico Cell Mode parameter is set to Disabled or V1, the Pico Cell V2 parameters are grayed out.

Note For pico cell V2 to work with Intel 3945 clients, the QBSS feature also has to be enabled (i.e., WMM clients must be set to allowed), and fast roaming cannot be enabled.

Step 5 Go to **802.11a/n > Parameters** and ensure that the 802.11a/n Network Status check box is not enabled.

Step 6 From the Pico Cell Mode drop-down menu, choose **V2**. By choosing V2, the parameters for access point and clients share the same values and make communication symmetrical. This selection also allows you to put in values for Rx sensitivity, CCA sensitivity, and transmit power although the defaulted minimum and maximum values represent the Cisco recommended values for most networks.

Note You can only choose V2 if you have software version 4.1 or later.

Step 7 Set the Rx sensitivity based on the desired receiver sensitivity for 802.11a/n radios. The Current column shows what is currently set on the access point and clients, and the Min and Max columns show the range to which the access points and clients should adapt. Receiver signal strength values falling outside of this range are normally disregarded.

Step 8 Set the CCA sensitivity based on when the access point or client considers the channel clear enough for activity. The current column shows what is currently set on the access point and clients, and Min and Max columns show the range to which the access points and clients should adapt. CCA values falling outside of this range are normally disregarded.

Step 9 Click **Save** to save these values. Before choosing **Reset to Defaults** you must turn off the 802.11 network.

Configuring a Voice Parameter Template (for 802.11a/n or 802.11b/g/n)

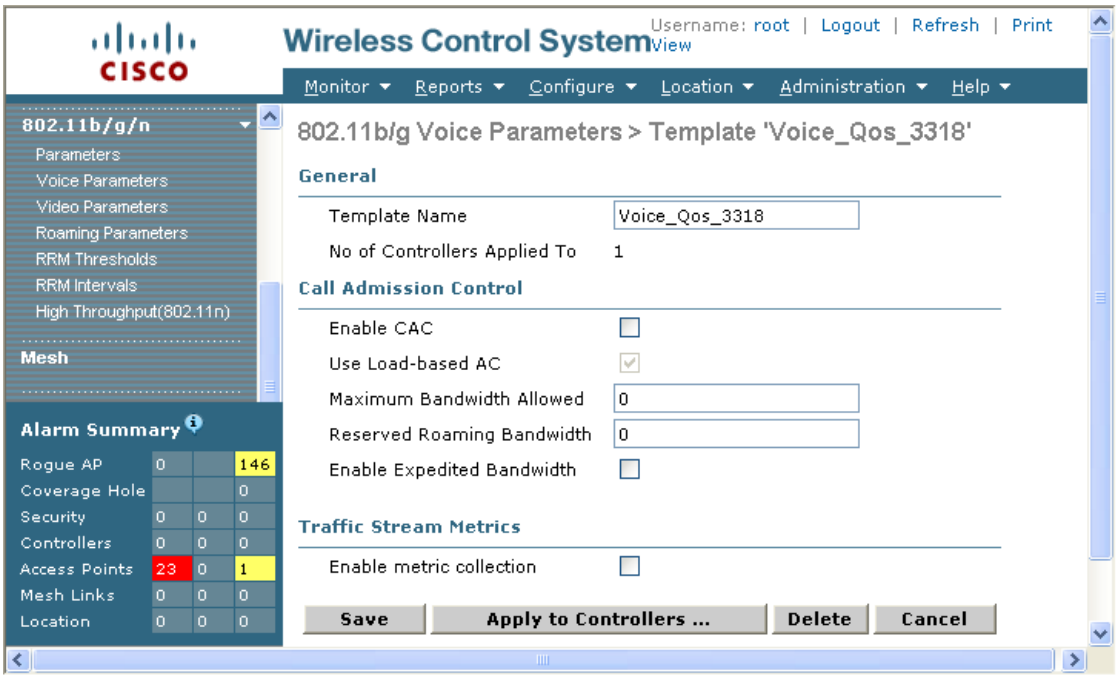
Follow these steps to add a template for either 802.11a/n or 802.11b/g/n voice parameters, such as call admission control and traffic stream metrics or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose either **802.11a/n > Voice Parameters** or **802.11b/g/n > Voice Parameters**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO.** To make modifications to an existing template, click to select a template in the Template Name column. The 802.11a/n or 802.11b/g/n Voice Parameters window appears (see Figure 11-39), and the number of controllers the template is applied to automatically populates.

Figure 11-39 802.11b/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 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. To enable load-based CAC 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 informs 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, this feature should be enabled.

Step 10 Click **Save**.

Configuring a Video Parameter Template (for 802.11a/n or 802.11b/g/n)

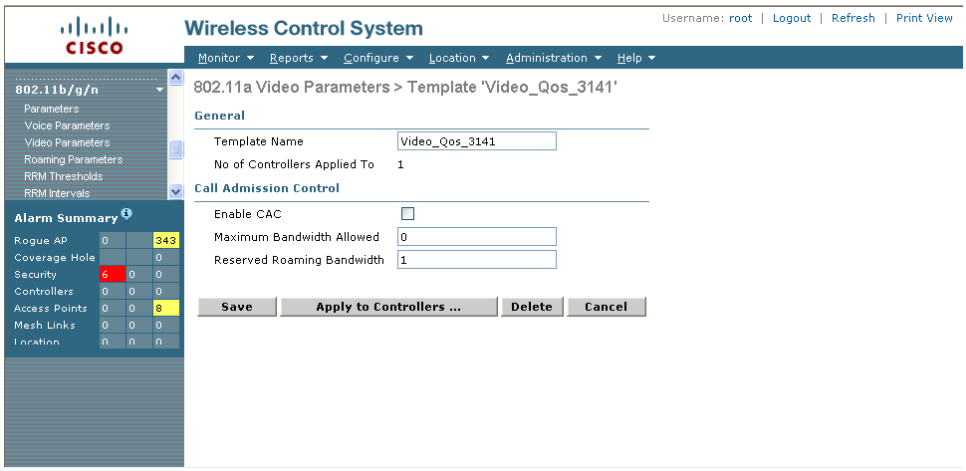
Follow these steps to add a template for either 802.11a/n or 802.11b/g/n video parameters or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose either **802.11a/n > Video Parameters** or **802.11b/g/n > Video Parameters**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO.** To make modifications to an existing template, click to select a template in the Template Name column. The 802.11a/n or 802.11b/g/n Video Parameters window appears (see Figure 11-40), and the number of controllers the template is applied to automatically populates.

Figure 11-40 802.11a/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**.

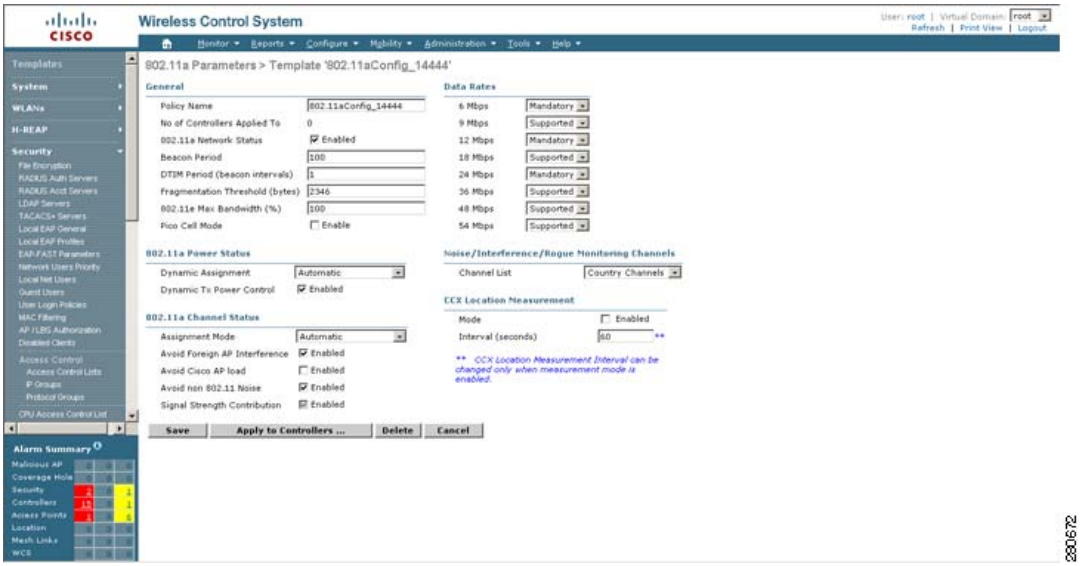
Configuring EDCA Parameters through a Controller Template

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 the instructions in this section to configure 802.11a/n or 802.11b/g/n EDCA parameters through a controller template:

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, select **802.11a/n > EDCA Parameters** or **802.11b/g/n > EDCA Parameters** to open the EDCA Parameters summary page (see Figure 11-41).

Figure 11-41 802.11a Pico Cell Parameters



Step 3 Modify or view a current template by selecting the **Template Name**
-or-
Create a new template by selecting **Add Template** from the **Select a command** drop-down menu.

Step 4 Choose one of the following options from the **EDCA Profile** drop-down menu:

- 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 **Enable Streaming MAC** checkbox to enable this feature.

Note Only enable Streaming MAC if all clients on the network are WMM compliant.

Configuring a Roaming Parameters Template (for 802.11a/n or 802.11b/g/n)

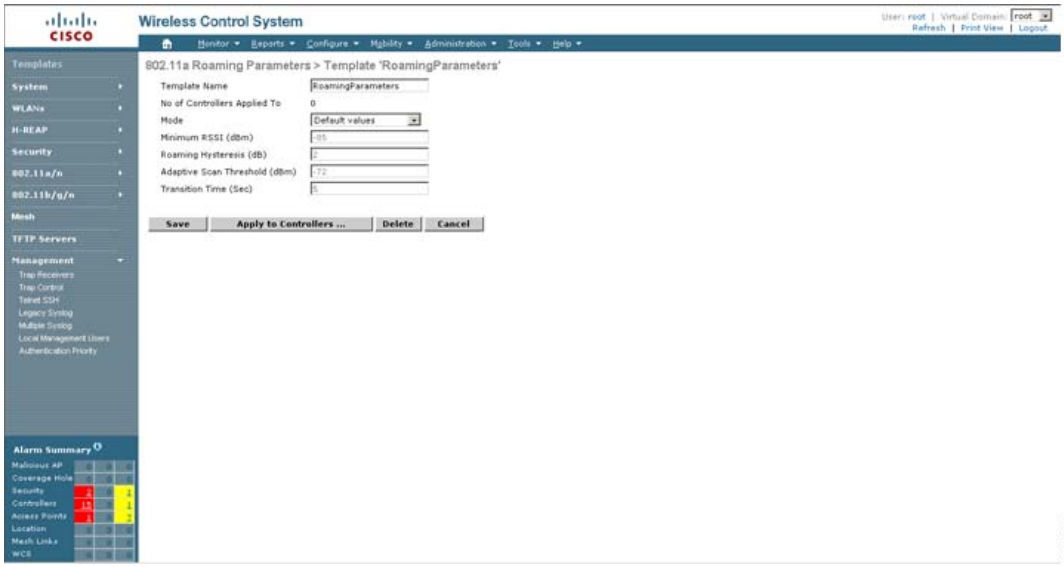
Follow these steps to add a roaming parameters template or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **802.11a/n > Roaming Parameters** or **802.11b/g/n > Roaming Parameters**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO.** To make modifications to an existing template, click to select a template name in the Template Name column. The Roaming Parameters Template appears (see Figure 11-42), and the number of controllers the template is applied to automatically populates.

Figure 11-42 802.11 Roaming Parameters Template



Step 4 Use the Mode drop-down menu 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 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: 2 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)

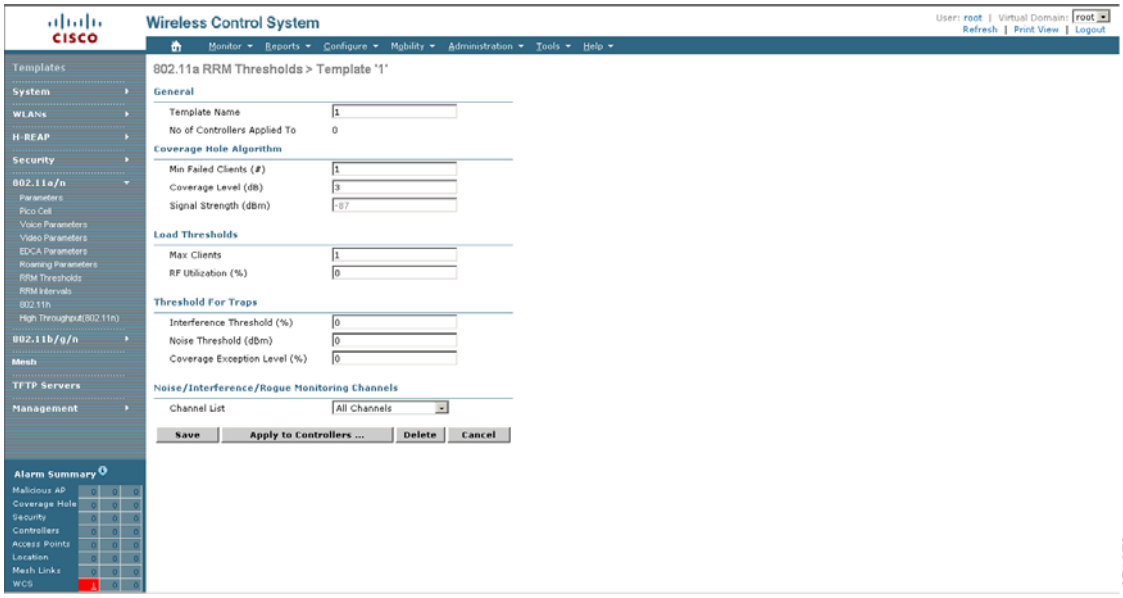
Follow these steps to add a new 802.11a/n or 802.11b/g/n RRM threshold template or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **802.11a/n > RRM Thresholds** or **802.11b/g/n > RRM Thresholds**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO.** To make modifications to an existing template, click to select a template name in the Template Name column. The 802.11a/n or 802.11b/g/n RRM Thresholds Template appears (see Figure 11-43), and the number of controllers the template is applied to automatically populates.

Figure 11-43 802.11b/g/n RRM Thresholds Template



Step 4 Enter the minimum number of failed clients that are currently associated with the controller.

Step 5 Enter the desired coverage level. When the measured coverage drops by the percentage configured in the coverage exception level, a coverage hole is generated.

Step 6 The Signal Strength (dBm) parameter shows the target range of coverage thresholds.

Step 7 Enter the maximum number of clients currently associated with the controller.

Step 8 At the RF Utilization parameter, enter the percentage of threshold for either 802.11a/n or 802.11b/g/n.

Step 9 Enter an interference threshold.

Step 10 Enter a noise threshold between -127 and 0 dBm. When outside of this threshold, the controller sends an alarm to WCS.

Step 11 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 12 At the Channel List drop-down menu 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 13 Click **Save**.

Configuring an RRM Interval Template (for 802.11a/n or 802.11b/g/n)

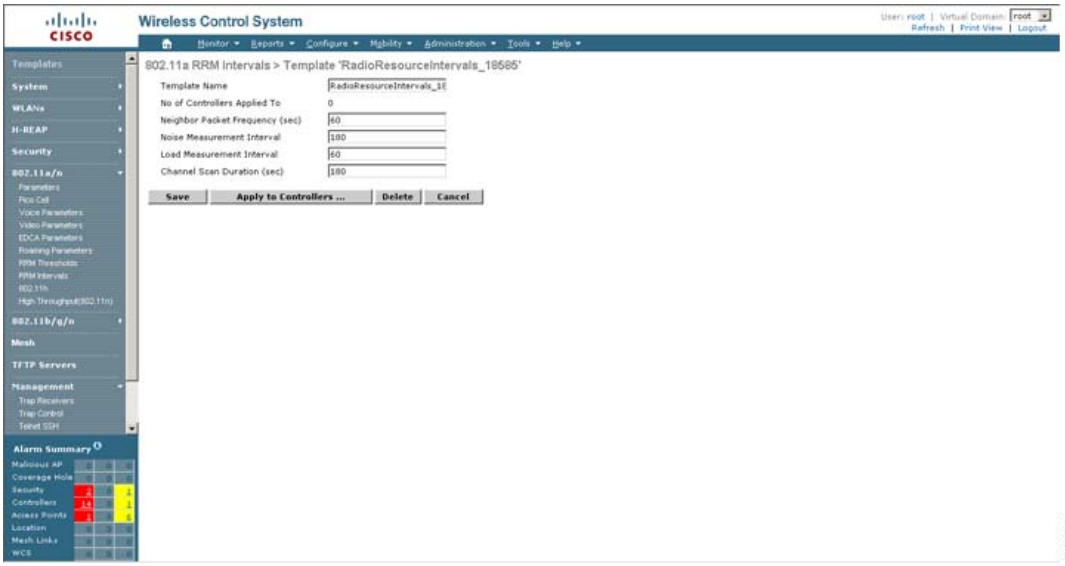
Follow these steps to add an 802.11a/n or 802.11b/g/n RRM interval template or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **802.11a/n > RRM Intervals** or **802.11b/g/n > RRM Intervals**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template name from the Template Name column. The 802.11a/n or 802.11b/g/n RRM Threshold Template appears (see Figure 11-44), and the number of controllers the template is applied to automatically populates.

Figure 11-44 802.11a/n RRM Intervals Template



Step 4 Enter at which interval you want strength measurements taken for each access point. The default is 300 seconds.

Step 5 Enter at which interval you want noise and interference measurements taken for each access point. The default is 300 seconds.

Step 6 Enter at which interval you want load measurements taken for each access point. The default is 300 seconds.

Step 7 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

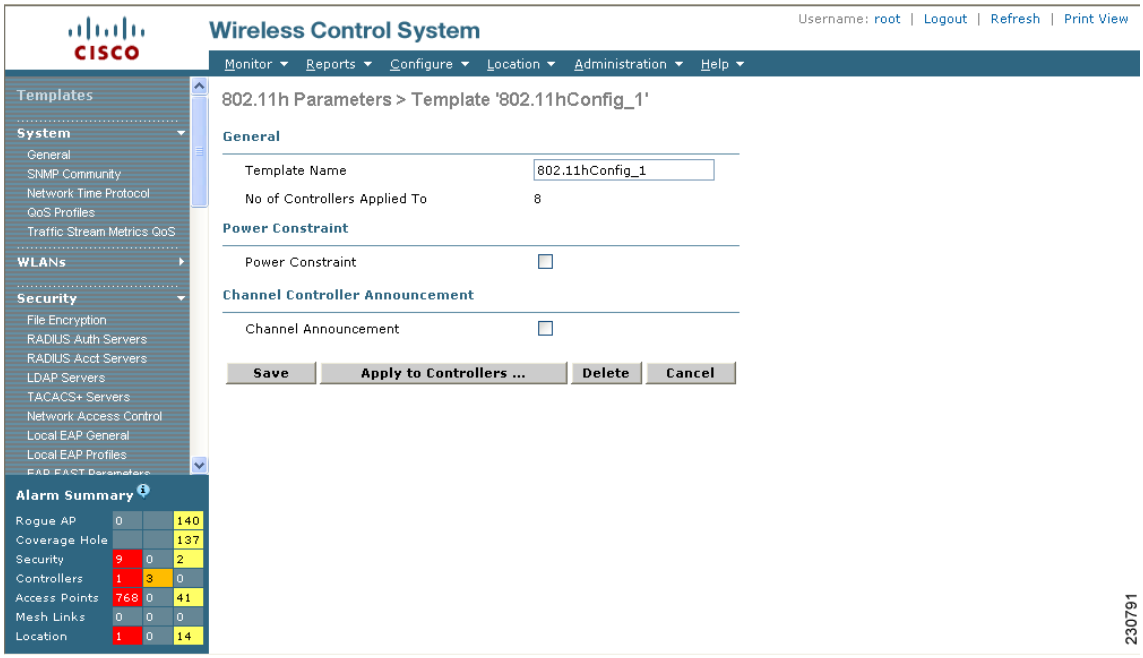
Follow these steps to add an 802.11h template or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **802.11a/n > 802.11h**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template name from the Template Name column. The 802.11h Template appears (see Figure 11-45), and the number of controllers the template is applied to automatically populates.

Figure 11-45 802.11h Template



Step 4 Check the power constraint check box to enable TPC.

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)

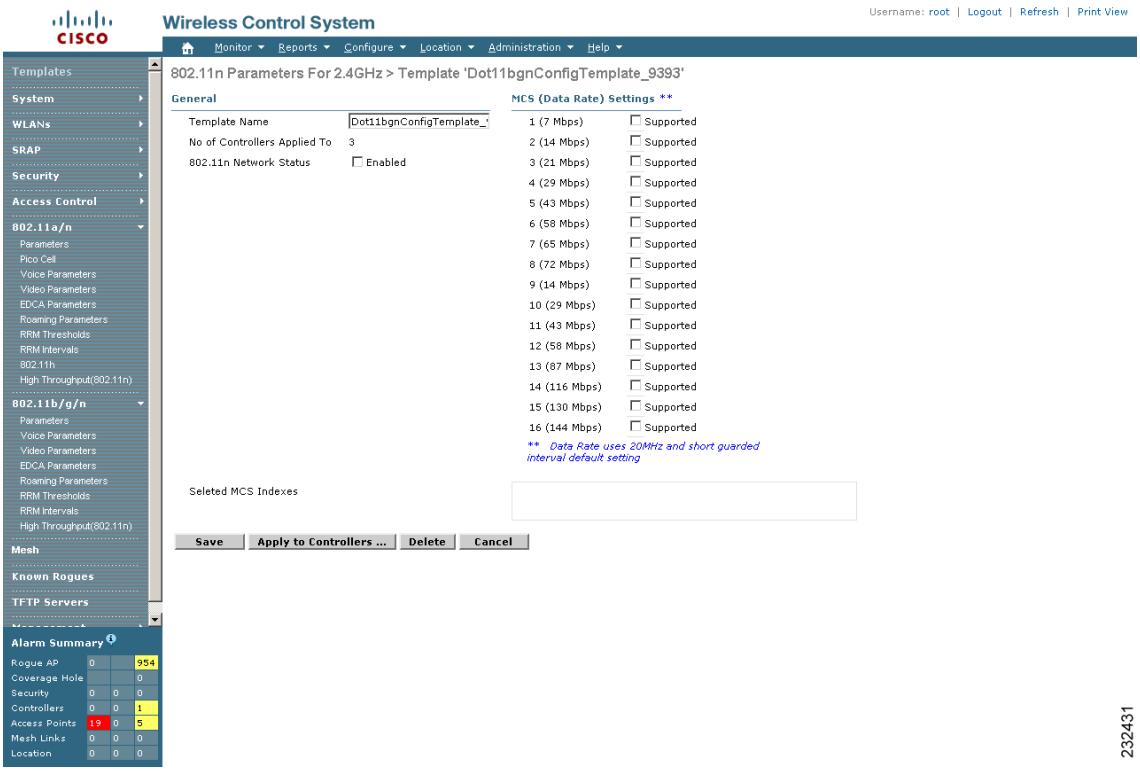
Follow these steps to add an 802.11a/n or 802.11b/g/n high throughput template or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **802.11a/n > High Throughput** or **802.11b/g/n > High Throughput**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template name from the Template Name column. The 802.11n Parameters for 2.4 GHz or 802.11n Parameters for 5 GHz template appears (see Figure 11-46), and the number of controllers the template is applied to automatically populates.

Figure 11-46 802.11n 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 click the Supported check box, the chosen numbers appear in the Selected MCS Indexes window.

Step 6 Click **Save**.

Configuring a Mesh Template

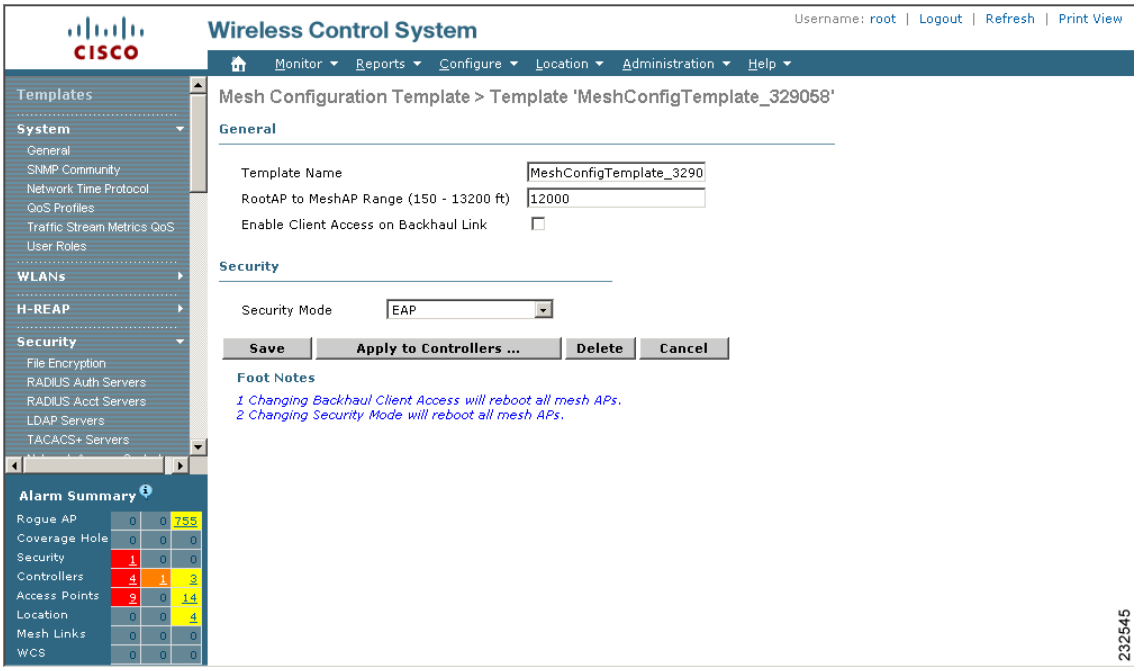
You can configure an access point to establish a connection with the controller. Follow these steps to add a mesh template or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Mesh**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click a specific template name. The Mesh Configuration Template window appears (see Figure 11-47).

Figure 11-47 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 Mesh Mac Filter is enabled by default. When enabled, this feature secures your network against any rogue access points and does not allow access points to attach if they are not defined in the MAC filter list.

However, if you disable this feature, mesh access points can join the controller.

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.

After you check the Enable Mesh MAC Filter check box, the access points reboot and then rejoin the controller if defined in the MAC filter list. Access points that are not defined in the MAC list cannot join the controller.

Step 6 The Enable Client Access on Backhaul Link check box is not checked by default. When this option is enabled, mesh access points are able to 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 is only applicable to access points with two radios.

Step 7 Click **Save**.

Configuring a TFTP Server Template

A Trivial File Transfer Protocol (TFTP) server is often 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.

Follow these steps to add a new TFTP server template or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **TFTP Servers**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click a specific template in the TFTP Server Name column. The TFTP Server window appears.

Step 4 Enter the IP address for the TFTP server.

Step 5 Click **Save**.

Configuring a Trap Receiver Template

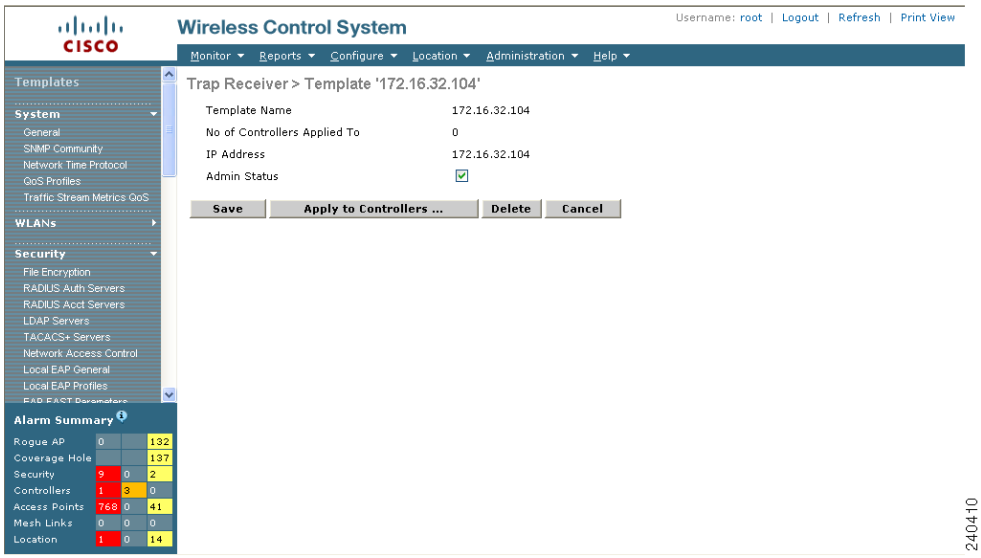
Follow these steps to add a new trap receiver template or make modifications to an existing template. If you have monitoring devices on your network that receive SNMP traps, you may want to add a trap receiver template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Management > Trap Receivers**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click a specific template in the Template Name column. The Trap Receiver Template window appears (see Figure 11-48), and the number of controllers the template is applied to automatically populates.

Figure 11-48 Trap Receiver Template



Step 4 Enter the IP address of the server.

Step 5 Click to enable the admin status if you want SNMP traps to be sent to the receiver.

Step 6 Click **Save**.

Configuring a Trap Control Template

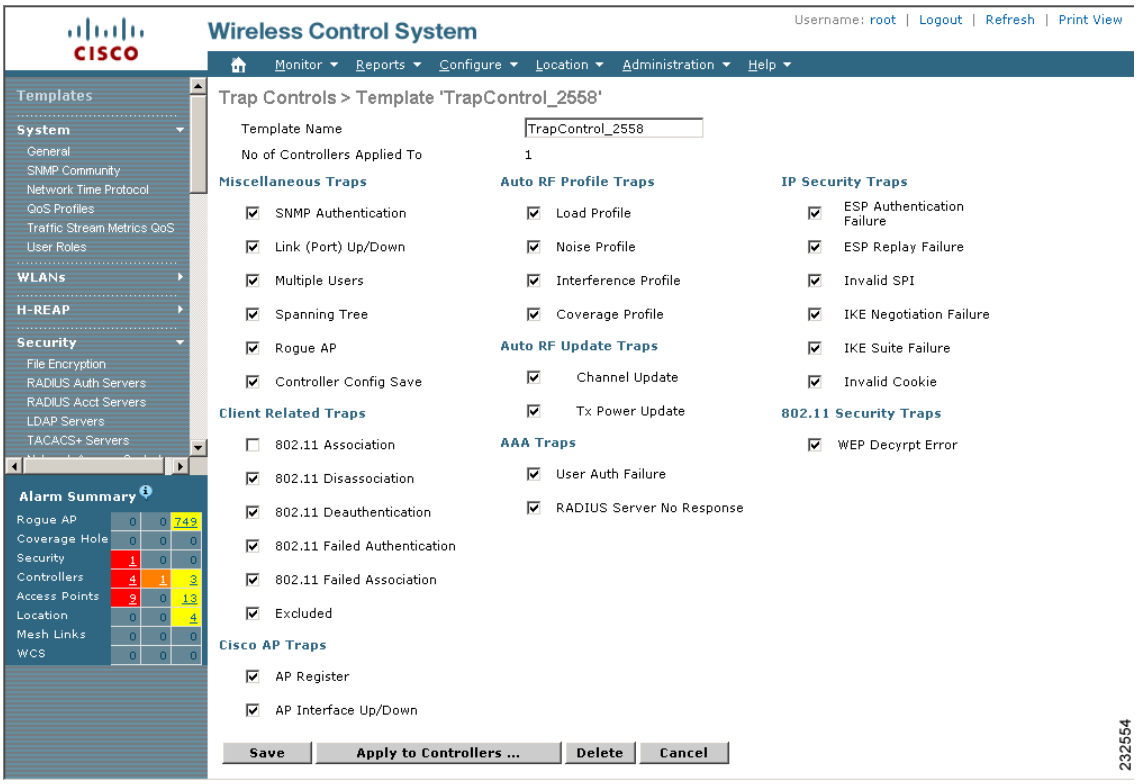
Follow these steps to add a trap control template or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Management > Trap Control**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The Trap Controls Template window appears (see Figure 11-49), and the number of controllers the template is applied to automatically populates.

Figure 11-49 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. Refer to 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 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 802.11 security trap:

- WEP Decrypt Error - Notification sent when the controller detects a WEP decrypting error.

Step 11 Check the appropriate check box to enable the following WPS trap:

- Rogue Auto Containment - Notification sent when a rogue access point is auto-contained.

Step 12 Click **Save**.

Configuring a Telnet SSH Template

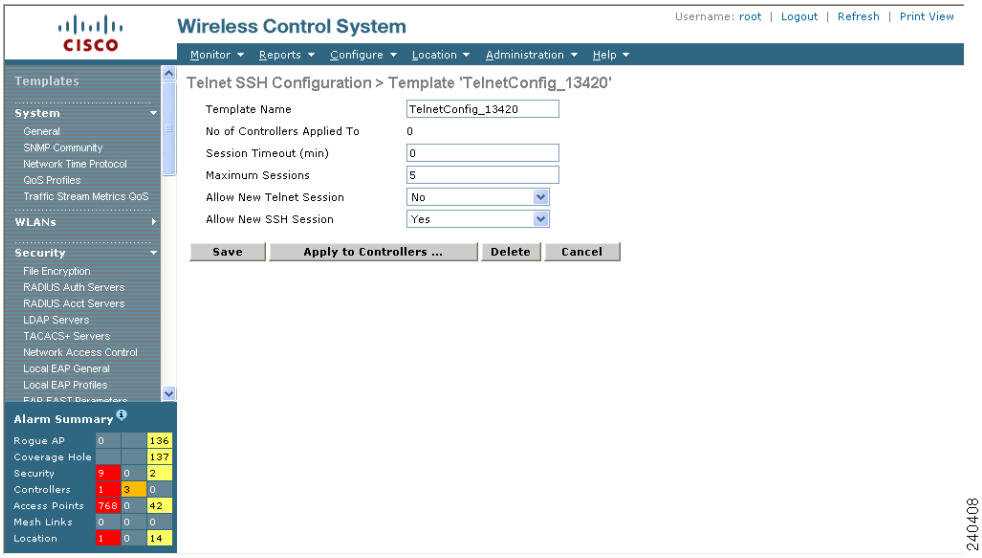
Follow these steps to add a Telnet SSH configuration template or make changes to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Management > Telnet SSH**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The Telnet SSH Configuration Template window appears (see Figure 11-50), and the number of controllers the template is applied to automatically populates.

Figure 11-50 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 menu 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 menu 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 a legacy syslog configuration template or make modifications to an existing template.

Note Legacy Syslog applies to controllers earlier than version 5.0.6.0

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Management > Legacy Syslog**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The Legacy Syslog Configuration Template window appears (see Figure 11-51), and the number of controllers the template is applied to automatically populates.

Figure 11-51 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 a multiple syslog configuration template or make modifications to an existing template.

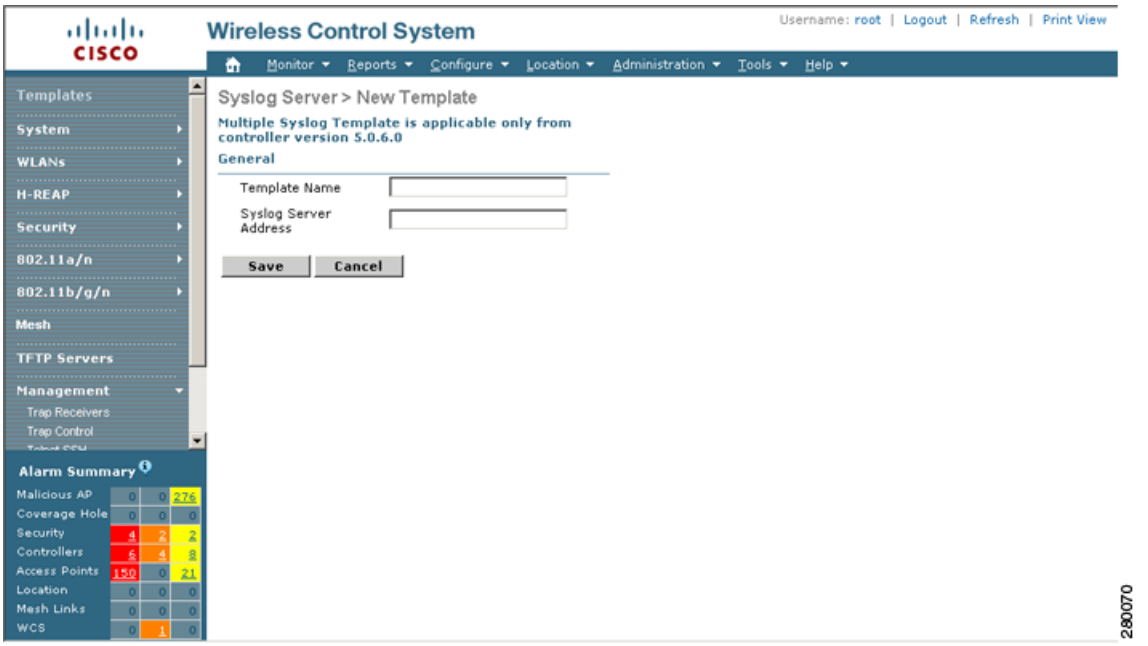
Note You can enter up to three syslog server templates.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Management > Multiple Syslog**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The Multiple Syslog Configuration Template window appears (see Figure 11-51), and the number of controllers the template is applied to automatically populates.

Figure 11-52 Syslog Server Template Window



Step 4 Enter a template name and a syslog server IP address.

Step 5 Click **Save**.

Configuring a Local Management User Template

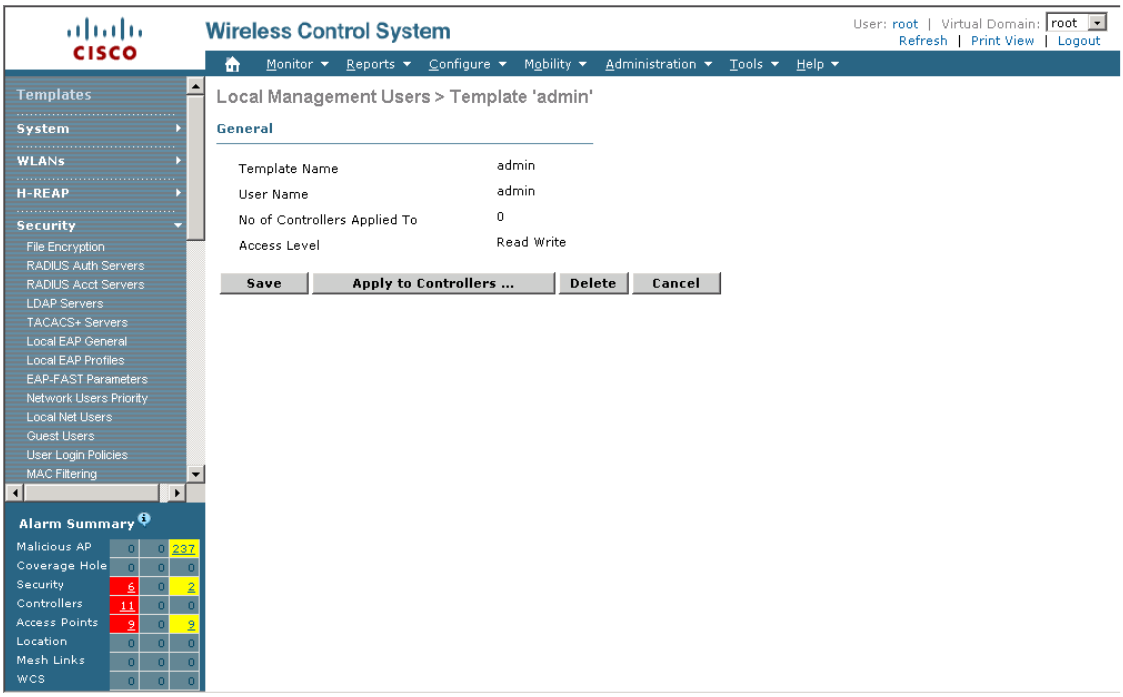
Follow these steps to add a local management user template or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Management > Local Management Users**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a username in the User Name column. The Local Management Users Template appears (see Figure 11-53).

Figure 11-53 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 menu to choose either Read Only or Read Write.

Step 9 Click **Save**.

Configuring a User Authentication Priority Template

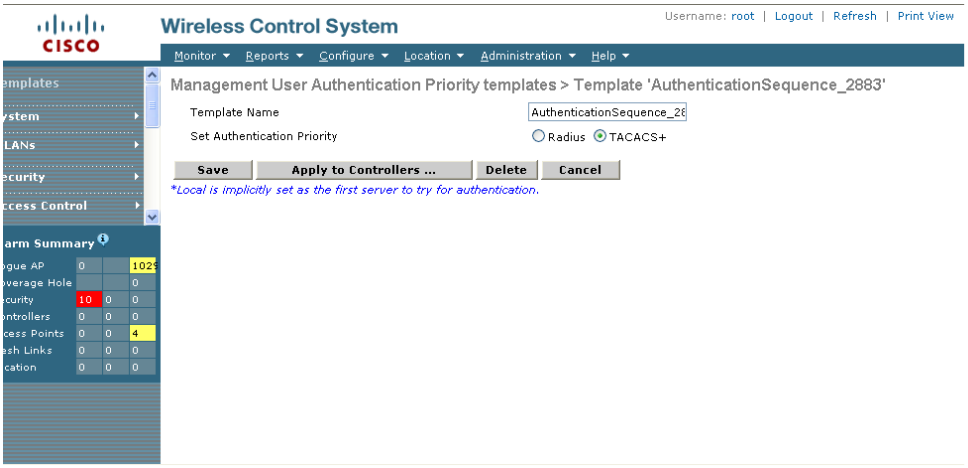
Management user authentication priority templates control the order in which authentication servers are used to authenticate a controller's management users. Follow these steps to add a user authentication priority template or make modifications to an existing template.

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Management > Authentication Priority.**

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a username in the Template Name column. The Local Management Users Template appears (Figure 11-54).

Figure 11-54 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 Controller Templates

You can apply a controller template to a controller.

Step 1 Go to **Configure > Controller Templates**.

Step 2 Using the left sidebar menu, choose the category of templates to apply.

Step 3 Click the URL from the Template Name column that you want to apply to the controller.

Step 4 Click the **Apply to Controllers** button.

Adding Access Point Templates

This page allows you to add a new access point template.

Step 1 Choose **Configure > Access Point Templates**.

Step 2 Choose **Add Template** from the Select a command drop-down menu and click **GO**.

Step 3 Enter the template name.

Step 4 Provide a description of the template.

Step 5 Click **Save**.

Configuring Access Point Templates

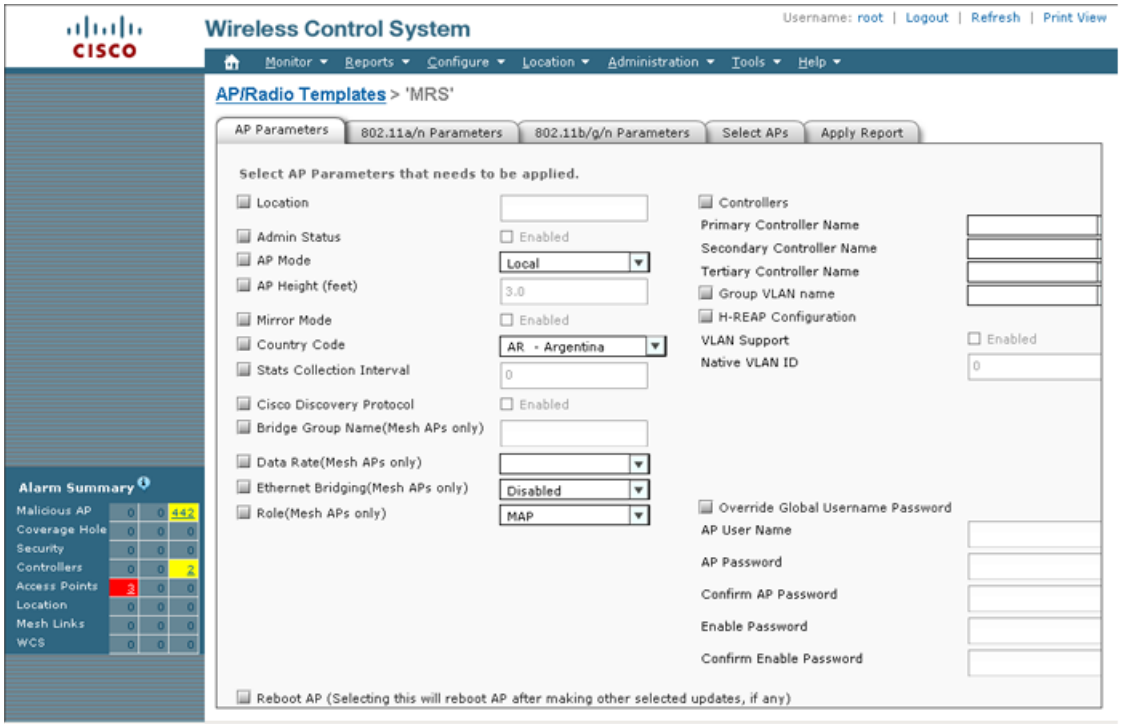
This page allows you to configure a template of access point information that you can apply to one or more access points.

Step 1 Choose **Configure > Access Point Templates**.

Step 2 From the Template Name column, click on the template name you want to configure.

Step 3 Choose the **AP Parameters** tab. The AP/Radio Templates window appears (see Figure 11-55).

Figure 11-55 AP/Radio Templates



Step 4 Click the Location check box and enter the access point location.

Step 5 Click 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. Choose the **Enabled** check box to allow access points to be turned on oroff.

Step 6 Click the **AP Mode** check box and use the drop-down menu to set the operational mode of the access point as follows:

- Local - Default
- Monitor - Monitor mode only
- REAP - Cisco 1030 remote edge lightweight access point (REAP) used for Cisco 1030 IEEE 802.11a/b/g/n remote edge lightweight access points.

- Rogue Detector - Monitors the rogue access points but does not transmit or contain rogue access points.
- Sniffer - The access point "sniffs" the air on a given channel. It captures and forwards all the packets from the client on that channel to a remote machine that runs airopeek (a packet analyzer for IEEE 802.11 wireless LANs). It includes information on timestamp, signal strength, packet size, and so on. If you choose Sniffer as an operation mode, you are required to enter a channel and server IP address on the AP/Radio Templates 802.11b/g/n or 802.11a/n parameters tab.

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.

- Bridge

Note Changing the AP mode reboots the access point.

Step 7 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 8 You must click both the **Mirror Mode** and **Enabled** check box to enable access point mirroring mode.

Step 9 Click the check box to enable the country code drop-down menu. A list of country codes is returned. For this access point, choose which 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 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.

Note Changing the country code may cause the access point to reboot.

Step 10 Click to enable **Stats Collection Interval** and then enter the collection period (in seconds) for access point statistics.

Step 11 (Mesh APs only) Choose the bridging option if you want the access point to act as a bridging access point.

Step 12 (Mesh APs only) Use the Data Rate drop-down menu to choose a data rate of 1, 2, 5.5, 6, or 9 Mbps.

Step 13 (Mesh APs only) Use the Ethernet Bridging drop-down menu to choose to enabled or disabled.

Step 14 (Mesh APs only) Use the Role drop-down menu to choose MAP or RAP.

Step 15 Click the **Cisco Discovery Protocol check box** and click **Enabled** 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 16 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 17 Click the **Controllers** check box, and then you are required to enter the Primary, Secondary, and Tertiary Controller names.

Step 18 Click the **Group VLAN Name** check box and then use the drop-down menu to select an established Group VLAN name.

Step 19 Enable local switching by checking the **H-REAP Configuration** check box. When you enable local switching, any remote access point that advertises this WLAN is able to locally switch data packets (instead of tunneling to the controller).

Step 20 Check the **VLAN Support** check box to enable it and enter the number of the native VLAN on the remote network (such as 100) in the **Native VLAN ID** field. This value cannot be zero.

Note The valid native VLAN ID range is 1-4094. If you are changing the mode to REAP and if the access point is not already in REAP mode, then all other REAP parameters are not applied on the access point.

Note By default, a VLAN is not enabled on the hybrid-REAP access point. Once hybrid REAP is enabled, the access point inherits the VLAN name (interface name) and 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 21 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 22 On the System > AP Username Password window, 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 window. If you want to override the global credentials for this particular access point, click 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 23 Save the template.

Step 24 If the updates require a reboot to be reflected, click to check the **Reboot AP** check box.

Step 25 Choose the **Select APs** tab. Use the drop-down menu 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

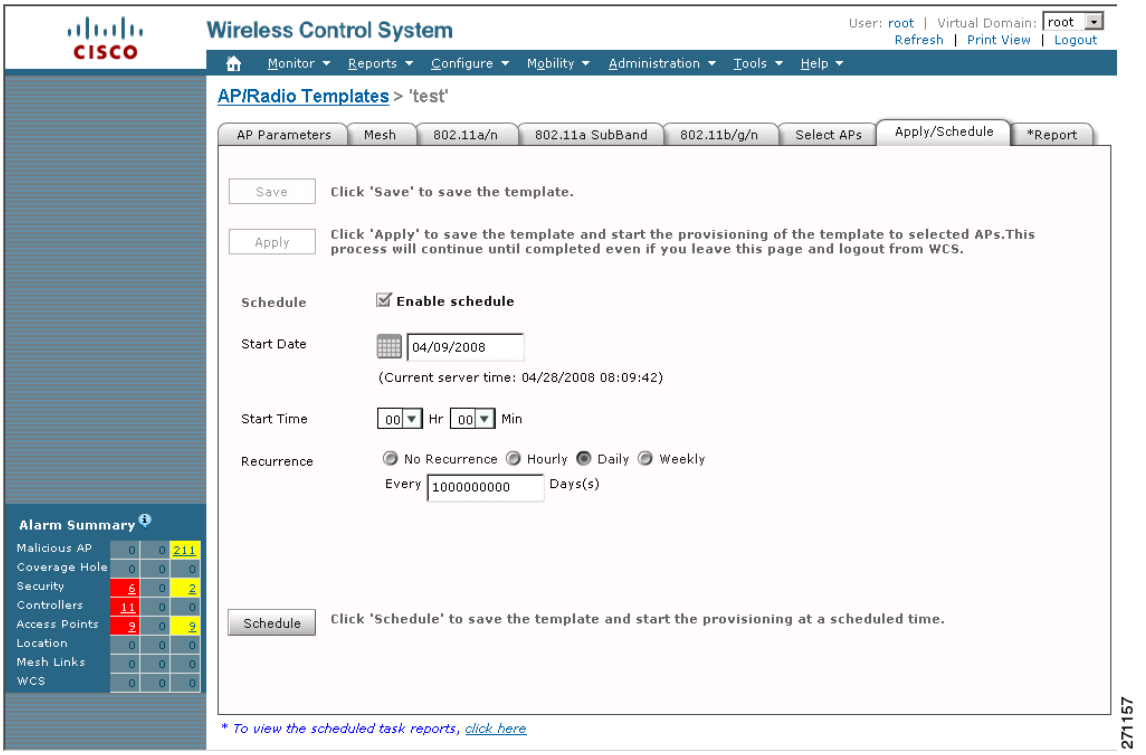
Follow these steps to apply the access point and radio templates to all the controllers in a config group.

Step 1 Choose **Configure > Access Point Templates.**

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 11-56).

Figure 11-56 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 window 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 window. It shows which templates were successfully applied to each of the controllers.

Note If you want to print the report as shown on the window, 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 menus.

Step 8 Determine how often you want the provisiong of the template to occur. The choices are no recurrence, hourly, daily, or weely. 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 window, choose **Configure > Scheduled Configuration Tasks**.

- AP Template Tasks
- Config Group Tasks

AP Template Tasks

The AP Template Tasks window allows you to view, modify, delete, enable, or disable current access point template tasks. To access the AP Template Tasks window and view current access point template tasks, choose **Configure > Scheduled Configuration Tasks**.

- Modify a Current AP Template Task, page 11-85
- View AP Status Report for the Scheduled Task, page 11-85
- Enable or Disable a Current AP Template Task, page 11-86
- View an AP Template Task History, page 11-86
- Delete a Current AP Template Task, page 11-86

Modify 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 From the AP Radio/Template window, choose the **Apply/Schedule** tab.

Step 4 Make any necessary changes to the current schedule or AP template parameters and click **Schedule**.

View 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.

Enable or Disable 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 menu, choose **Enable Schedule** or **Disable Schedule**, as applicable.

Step 4 Click **GO**.

View 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 menu, choose **View History**.

Step 4 Click **GO**.

Delete 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 menu, choose **Delete Task(s)**.

Step 4 Click **GO**.

Step 5 Click **OK** to confirm the deletion.

Config Group Tasks

The Config Group Tasks window 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 window and view current config group tasks, choose **Configure > Scheduled Configuration Tasks > ConfigGroup**.

- Modify a Current AP Template Task, page 11-85
- View Controller Status Report for the Scheduled Task, page 11-87
- Enable or Disable a Current Config Group Task, page 11-88
- View a Config Group Task History, page 11-88
- Delete a Current Config Group Task, page 11-88

Modify 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 From the Config Groups window, choose the Apply/Schedule tab.

Step 5 Make any necessary changes to the current schedule and click **Schedule**.

View 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.

Enable or Disable 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 menu, choose **Enable Schedule** or **Disable Schedule**, as applicable.

Step 5 Click **GO**.

View 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 menu, choose **View History**.

Step 5 Click **GO**.

Delete 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 menu, choose **Delete Task(s)**.

Step 5 Click **GO**.

Step 6 Click **OK** to confirm the deletion.

Configuring Radio Templates

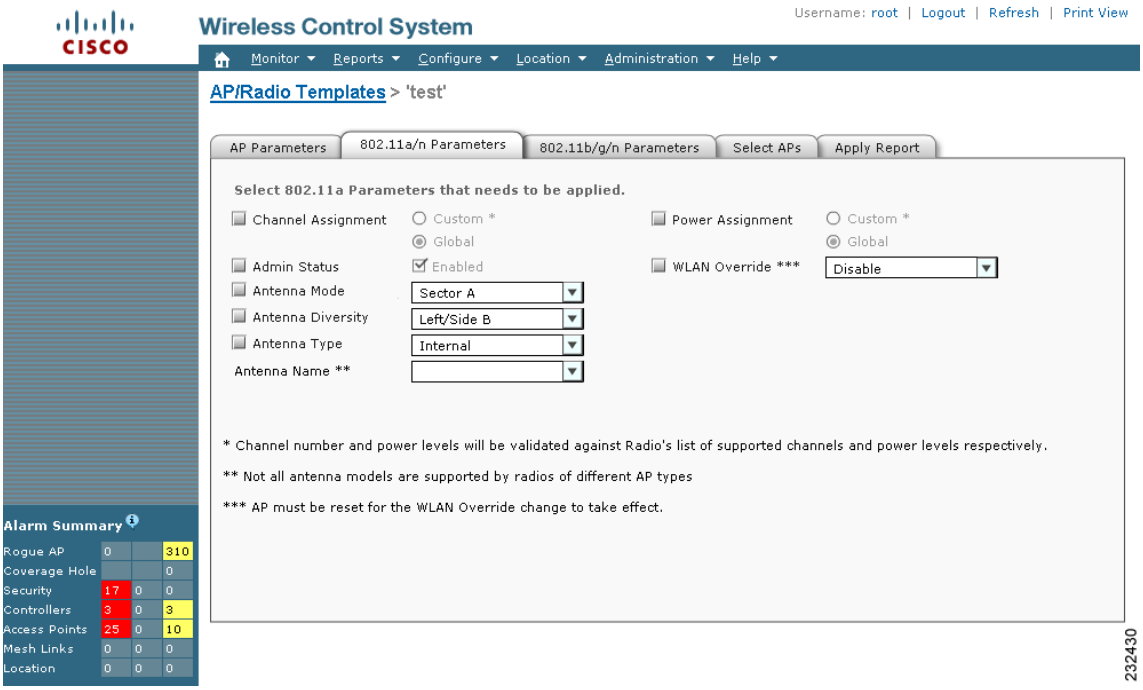
This page allows you to configure a template of radio information that you can apply to one or more access points.

Step 1 Choose **Configure > Access Point Templates**.

Step 2 From the Template Name column, click on the template name you want to configure.

Step 3 Choose the **802.11a/n Parameters or 802.11b/g/n Parameter** tab. The AP/Radio Templates window appears (see Figure 11-57).

Figure 11-57 802.11a/n Parameters



Step 4 Click the Channel Assignment checkbox to enable it. To choose a specific channel, click **Custom** and use the drop-down to designate the channel. Otherwise, click **Global**.

Note The channel assignment is validated against 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 menu 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 menu to specify if the antenna is external or internal.

Step 9 Use the Antenna Name drop-down menu to determine whether the antenna is a Kodiak directional, AIR-ANT1000, CUSH-S5157WP, etc.

Step 10 Check 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 menu. 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.

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 applied to 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 checkbox 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 12

Performing Maintenance Operations

This chapter provides routine procedures for maintaining WCS. It contains these sections:

- Checking the Status of WCS, page 12-1
- Stopping WCS, page 12-2
- Backing Up the WCS Database, page 12-3
- Restoring the WCS Database, page 12-5
- Importing and Exporting Asset Information, page 12-10
- Auto-Synchronizing Location Appliances, page 12-11
- Backing Up Location Appliance Data, page 12-12
- Importing and Exporting Asset Information, page 12-10
- Upgrading WCS, page 12-15
- Reinitializing the Database, page 12-20
- Reinitializing the Database, page 12-20
- Recovering the WCS Password, page 12-20

Checking 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\WCS4.2.47.0) 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/WCS4.2.47.0) and enter **./WCSStatus**.
- Navigate to the installation directory (such as /opt/WCS4.2.47.0) 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 Windows Start menu, click **Programs > Wireless Control System > StopWCS**.
- From the command prompt, navigate to the WCS installation directory (such as C:\Program Files\WCS4.2.47.0\bin) and enter **WCSAdmin stop**.

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 /opt/WCS4.2.47.0 directory (or the directory chosen during installation) and enter **./StopWCS**.
- Navigate to the /opt/WCS4.2.47.0/bin directory and enter **WCSAdmin stop**.

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.

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 Check the **Enabled** check box.

Step 5 Check the **Enabled** check box if you want to run a report history backup.

Step 6 In the Max Backups to Keep field, 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 field.

Step 7 In the Interval (Days) field, 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 field, 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:\WCS4.2.47.0_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:\WCS4.2.47.0_Backup\Nov11) and click **OK**.

- Follow these steps from the command prompt:

a. Navigate to the WCS installation directory (C:\Program Files\WCS4.2.47.0\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:\WCS4.2.47.0_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:\WCS4.2.47.0_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/WCS4.2 directory (or any other directory).

Step 3 Create a backup directory for the WCS database with no spaces in the name (for example, **mkdir WCS4.2.47.0_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/WCS4.2.47.0 directory (or the directory chosen during installation) and enter **./Backup**. Enter a name for the backup file when prompted (such as WCS4.2.47.0_Backup/Nov11).
- Navigate to the /opt/WCS4.2.47.0/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 WCS4.2.47.0_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 WCS4.2.47.0_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.

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:\WCS4.2.47.0_Backup\Nov11.nmsbackup) and click **OK**.

< OR >

- Follow these steps from the command prompt:

a. Navigate to the WCS installation directory (C:\Program Files\WCS4.2.47.0\bin).

b. Enter **DBAdmin restore *backup-filename***, where *backup-filename* is the full path and filename of the backup file (for example, C:\WCS4.2.47.0_Backup\Nov11.nmsbackup).

Note If you are restoring data larger than 8-GB unzipped from a WCS version prior to 4.1, 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 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.

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/WCS4.2.47.0 directory (or the directory chosen during installation) and enter **./Restore** to start the restoration process. Enter the backup filename when prompted (such as WCS4.2.47.0_Backup/Nov11.nmsbackup).
- Navigate to the /opt/WCS4.2.47.0/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 WCS4.2.47.0_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.

Importing the Location Appliance into WCS

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.

Up to 2,500 laptop clients, palmtop clients, VoIP telephone clients, active Radio Frequency Identifier (RFID) asset tags, rogue access points, and clients can be tracked.

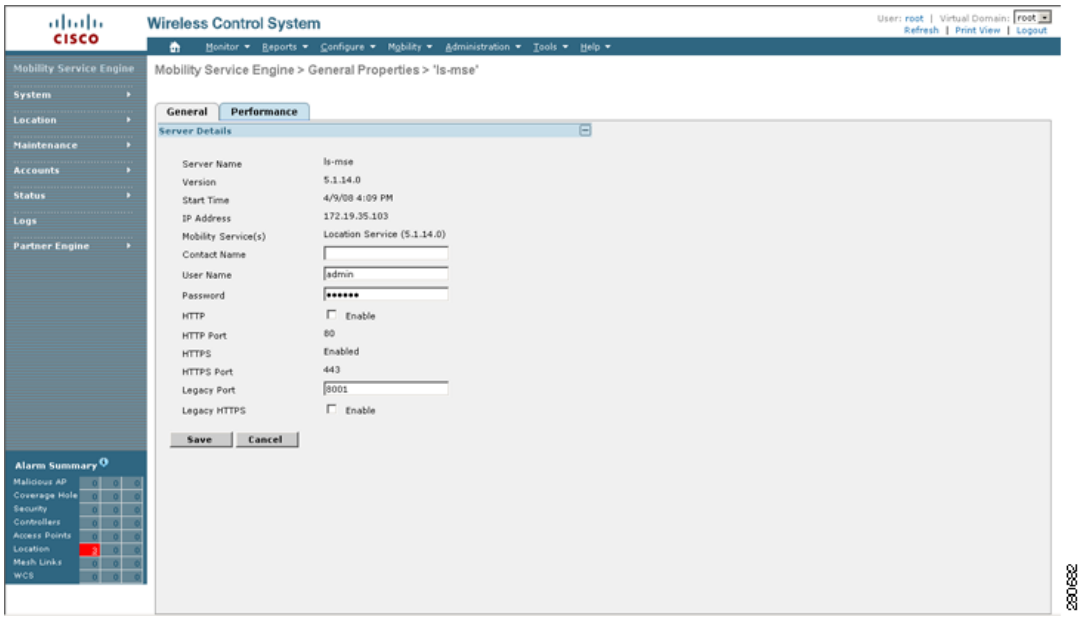
Note Even though all clients are loaded in the map, the display has a limit of 250 clients per floor to prevent overcrowding. You can do an advanced search of the map to see the items of interest.

To import a location appliance into WCS, follow the steps below.

Step 1 Navigate to **Mobility > Mobility Service Engines**. Choose **Add Location Server** from the drop-down menu and click **GO**.

Step 2 Enter any name for the appliance, its IP address, and a contact name on the Import window (see Figure 12-1). Keep the username, password, port, and HTTPS fields unaltered and click **Save**.

Figure 12-1 General Properties

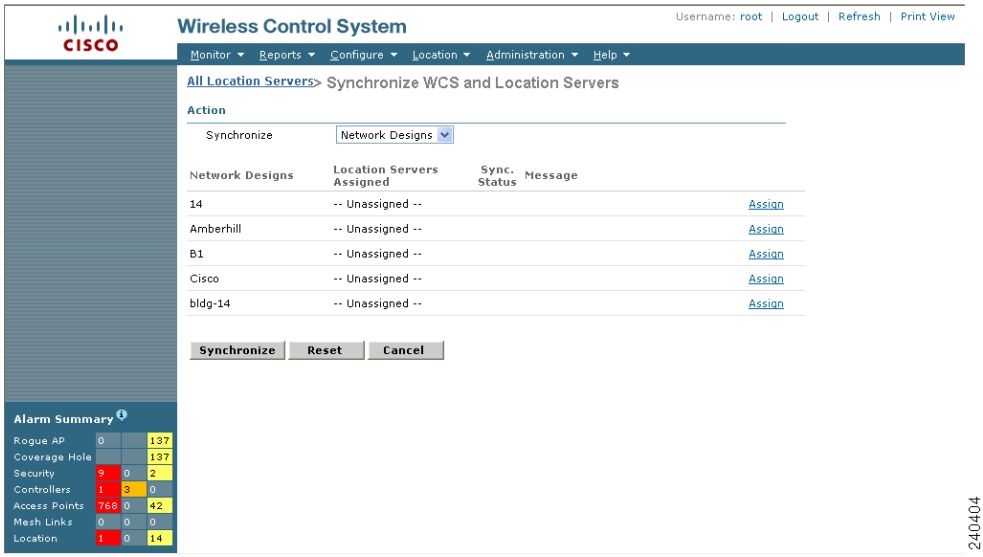


Step 3 After you import the new location appliance, a pop-up window reminds you that WCS contains data that needs to be transported to the location appliance. Those controllers and network diagrams that are available to be synchronized are listed. From the Select a command drop-down menu, choose **Synchronize Servers.**

The Synchronize WCS and Location Servers window appears (see Figure 12-2).

Note Existing network diagrams, controllers, and event groups must be synchronized with the appropriate location appliance to provide accurate location information. Synchronization is generally recommended after any network design change. You can limit areas that the location appliance tracks by synchronizing only areas that you want to actively track. Limiting synchronization to specific areas provides optimal performance of the location appliance.

Figure 12-2 Synchronizing WCS and Location Servers



Step 4 Select the **Network Designs** option from the Synchronize drop-down menu. Click the **Assign** hyperlink (far-right) of the appropriate network.

Step 5 In the **Assign to Servers** pop up window that appears, check the box next to the appropriate server (location appliance). Click **OK**.

Step 6 Click the check box next to the new location appliance and click **OK**.

Step 7 Click **Synchronize**.

Step 8 If the network diagram is properly synchronized, two green arrows appear under the Sync. Status column for each diagram. After synchronizing with the network diagram, all floor maps and access point placements associated with that diagram are copied to the location appliance; therefore, when the location appliance is set to synchronize with the diagram's controllers, it can find them.

Step 9 To set up controller synchronization, choose **Controllers** from the Synchronize drop-down menu.

Step 10 Each controller managed by WCS appears in a drop-down menu. Assign each controller to a specific location appliance by choosing the name of the location appliance with which the controllers will synchronize and click **Synchronize**.

Step 11 After the location appliance is properly synchronized with controllers, green arrows appear next to each controller under the Sync. Status column.

Note After synchronizing network designs and controllers, ensure that the location appliance polling parameters (**Location Server > Administration >Polling Parameters**) are enabled so that the location of the elements gets calculated.

Note After all relevant network designs and controllers are assigned to a new location appliance and initial synchronization is complete, you can configure the location appliance to automatically synchronize with WCS. For more details, see the "Importing and Exporting Asset Information" section on page 12-10.

Importing and Exporting Asset Information

This section describes how to import and export asset information stored in a flat text file to minimize manual entry.

Importing Asset Information

To import asset information for the location server using Cisco WCS, follow these steps:

Step 1 In Cisco WCS, choose **Mobility > Mobility Service Engines**.

The All Location Servers summary window appears.

Step 2 Click the name of the server for which you want to import asset information.

Step 3 Click **Administration** (left) to display the administrative configuration options.

Step 4 Click **Import Asset Information**.

Step 5 Enter the name of the text file or browse for the file name.

Information stored in the imported file should be in the following format:

- tag format: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname
- station format: #station, 00:00:00:00:00:00, categoryname, groupname, assetname

Step 6 Click **Import**.

Exporting Asset Information

To export asset information from the location server to a file using Cisco WCS, follow these steps:

Step 1 In Cisco WCS, choose **Mobility > Mobility Service Engines**.

The All Location Servers summary window appears.

Step 2 Click the name of the server from which you want export asset information.

Step 3 Click **Administration** (left) to display the administrative configuration options.

Step 4 Click **Export Asset Information**.

Step 5 Click **Export**.

You are prompted to **Open** (display to screen) or **Save** (to external PC or server) the asset file or to Cancel the request.

Note If you select **Save**, you are asked to select the asset file destination and name. The file is named "assets.out" by default. Click **Close** from the dialog box when download is complete.

Auto-Synchronizing Location Appliances

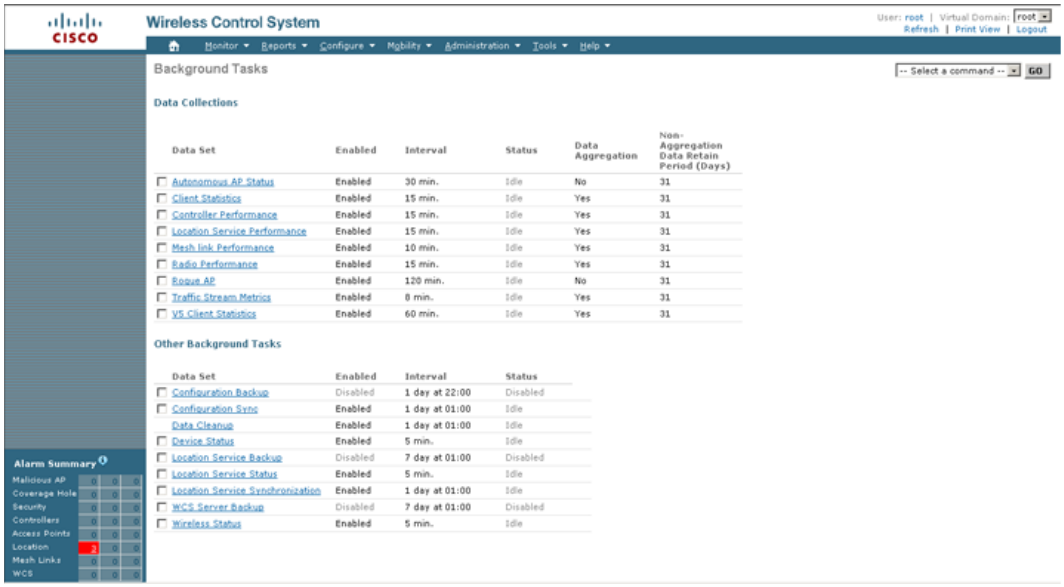
After all relevant network designs and controllers are assigned to a new location appliance and initial synchronization is complete, you can configure the location appliance to automatically synchronize with WCS by enabling the **Location Server Auto-Synchronization** feature.

Enabling auto-synchronization ensures that all future map modifications such as adding access points, changing access point positions or orientations, and any resizings are accurately reflected in the map in case a manual synchronization (Mobility > Synchronize Servers) is not performed after element changes. You can configure the frequency (minimum of 24 hours) and time of day that the automatic synchronization occurs.

Step 1 Choose **Administration > Background Tasks**.

The Background Tasks summary window appears (see Figure 12-3).

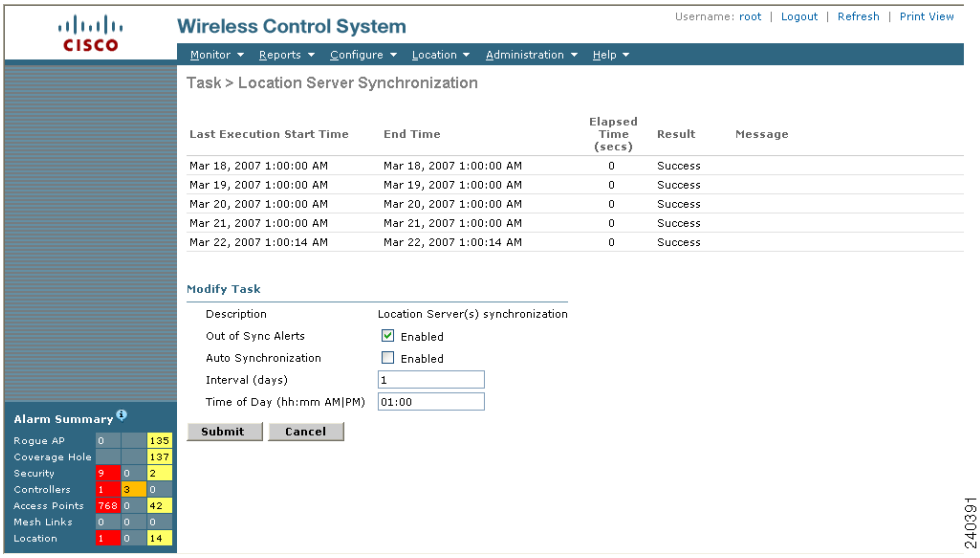
Figure 12-3 Administration > Background Tasks



Step 2 Select the **Location Server Synchronization** link.

Step 3 In the window that appears (Figure 12-4), check the **Enabled** box next to the **Auto Synchronization** option.

Figure 12-4 Location Server Synchronization Page



Step 4 Enter the frequency of the automatic synchronization in the **Interval (days)** field.

The value entered represents number of days. One day is the minimum value.

Step 5 Enter the Time of Day (hh:mm AM | PM) for the synchronization to occur.

Step 6 Click **Submit**.

You are returned to the Scheduled Tasks Summary window.

Note To disable the Auto-Synchronization, uncheck the **Enabled** box for that feature.

Note You may also want to enable the **Out of Sync Alerts** option if it is not already active. When enabled, this option generates alerts for the location appliance when elements such as network designs or controllers are not assigned to a location appliance. Modifications to elements without subsequent synchronization generate location appliance alerts as well.

Backing Up Location Appliance Data

You can configure the Cisco WCS to regularly back up the data stored on the location appliance. You can specify the frequency and the time-of-day of the backups and the number of previous backups you want to save.

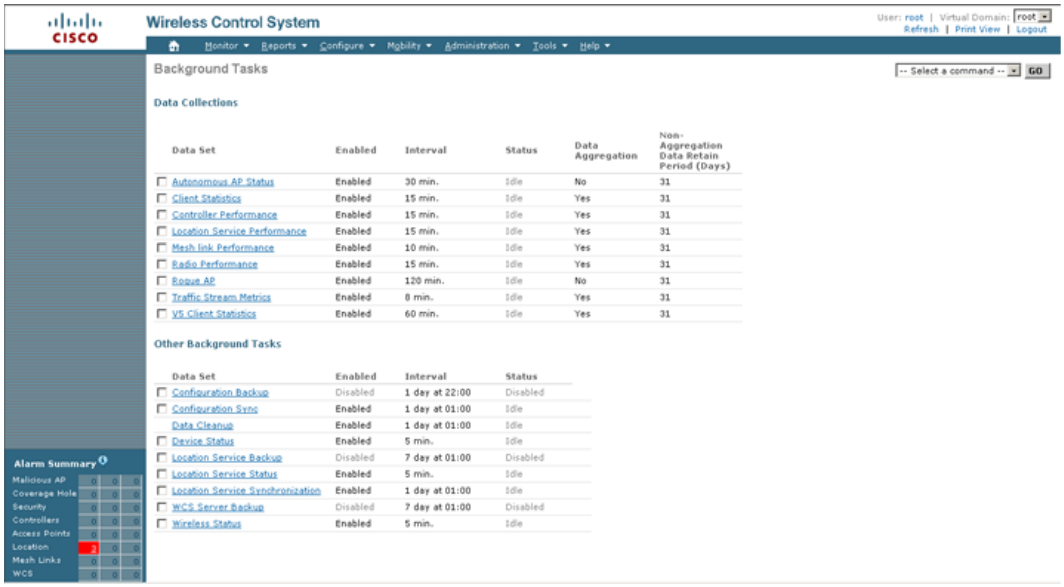
Note Back-up data is saved on the FTP server specified during WCS installation.

To back up the data stored on a location appliance, follow the steps below.

Step 1 Choose **Administration > Background Tasks**.

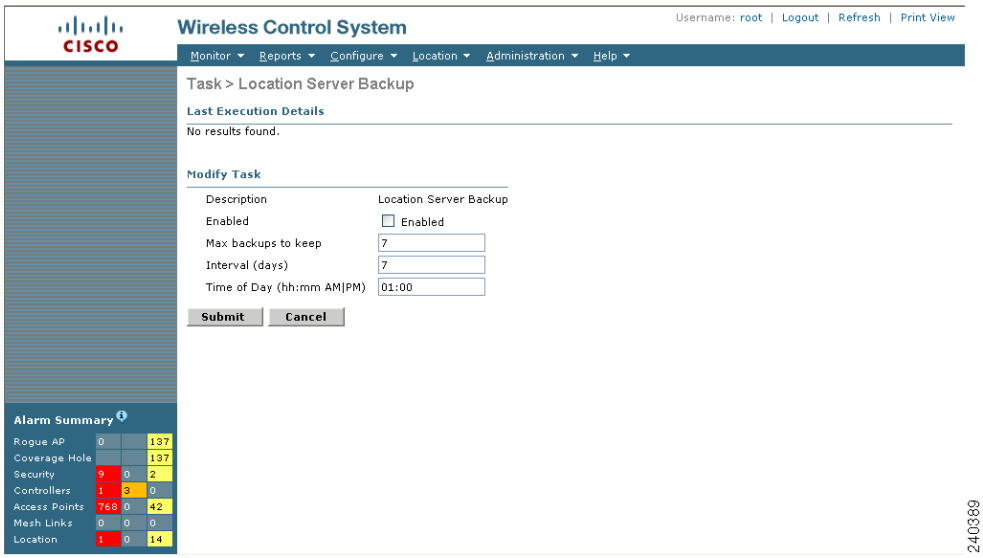
The window shown in Figure 12-5 appears.

Figure 12-5 Administration > Background Tasks



Step 2 Check the box next to the **Location Server Backup** link and then select the link. The Location Server Backup configuration window appears (see Figure 12-6).

Figure 12-6 Location Server Backup Configuration Page



Step 3 Check the **Enabled** box, if not already checked from the previous step. Generally, when you check the box at the Administration > Background Tasks window, the check box auto-populates.

Step 4 Enter the number of **Maximum Backups to Keep**.

Step 5 Enter the **Interval** (in days) between backups.

Step 6 Enter the Time of Day (hh:mm AM | PM) to run the backups.

Step 7 Click **Submit**.

The Scheduled Tasks window reappears noting the location server backup as enabled along with the interval and time-of-day settings.

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\WCS4.2.27.0 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/WCS4.2.47.0 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/WCS4.2.47.0 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.

Note You must have software release 4.1.91.0 before you can automatically upgrade to 4.2.

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.

Note Scheduled task settings are not preserved when you upgrade from WCS 4.0 or earlier releases. Make 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-K9-4.2.X.Y.exe file where 4.2.X.Y is the software build. If you downloaded the installer from Cisco.com, double click the WCS-STANDARD-WB-K9-4-2-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 12-7. If your WCS version is eligible for an automated upgrade, you receive a notification as shown in Figure 12-8.

Figure 12-7 Ineligible for Automated Upgrade

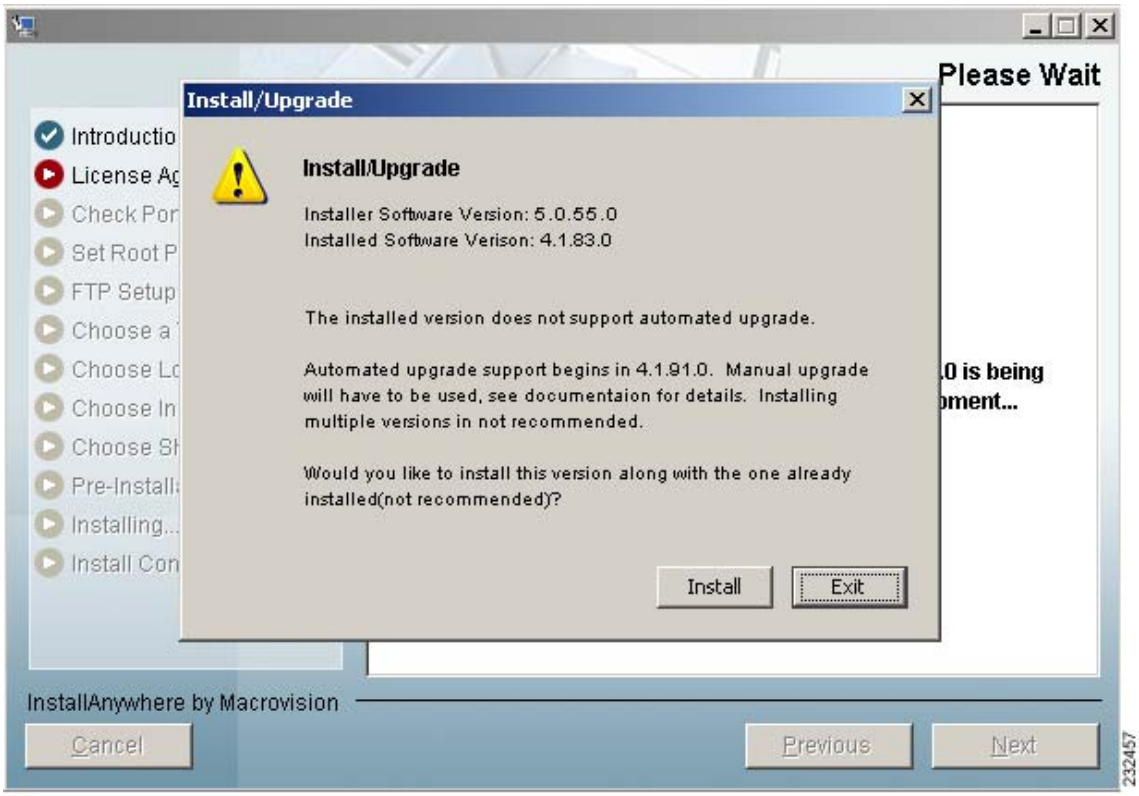
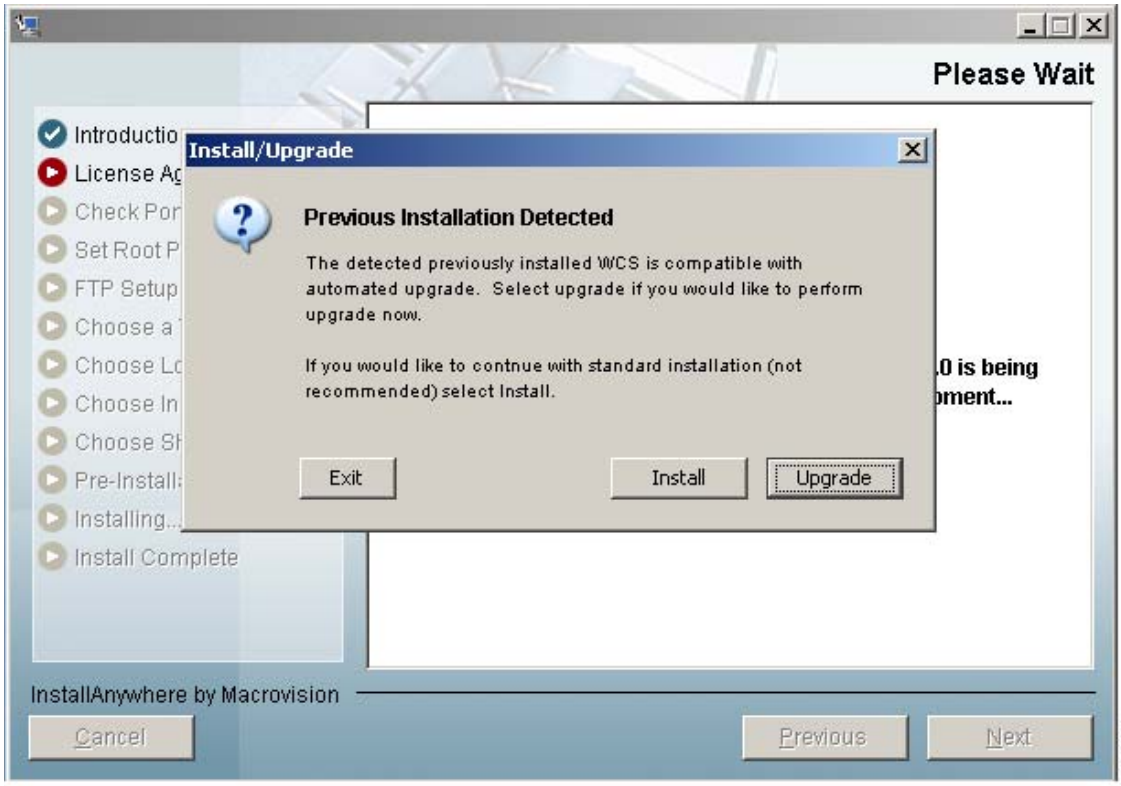


Figure 12-8 Previous Installation Detected



Step 4 If you see a window similar to the one in Figure 12-7 and choose **Install** because you cannot perform the automated upgrade, continue to the "Manually Upgrading WCS on Windows" section on page 12-19. If you see a window similar to the one in Figure 12-8 and choose **Install**, continue to the "Manually Upgrading WCS on Windows" section on page 12-19. If you see a window similar to the one in Figure 12-8 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-K9-4.2.X.Y.bin** (for CD users) or **./WCS-STANDARD-LB-K9-4-2-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 12-19. 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 12-19. 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" section on page 16-29).

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 12-4.

Step 3 Uninstall the WCS application by following the instructions in the "Uninstalling WCS on Windows" section on page 12-14.

Step 4 Install the new version of WCS by following the instructions in the "Installing WCS for Windows" section on page 2-4.

Step 5 Restore the WCS database by following the instructions in the "Restoring the WCS Database (for Windows)" section on page 12-5.

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 12-5.

Step 3 Uninstall the WCS application by following the instructions in the "Uninstalling WCS on Linux" section on page 12-14.

Step 4 Install the new version of WCS by following the instructions in the "Installing WCS for Linux" section on page 2-10.

Step 5 Restore the WCS database by following the instructions in the "Restoring the WCS Database (for Linux)" section on page 12-7.

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 13

Configuring Hybrid REAP

This chapter describes hybrid REAP and explains how to configure this feature on controllers and access points. It contains these sections:

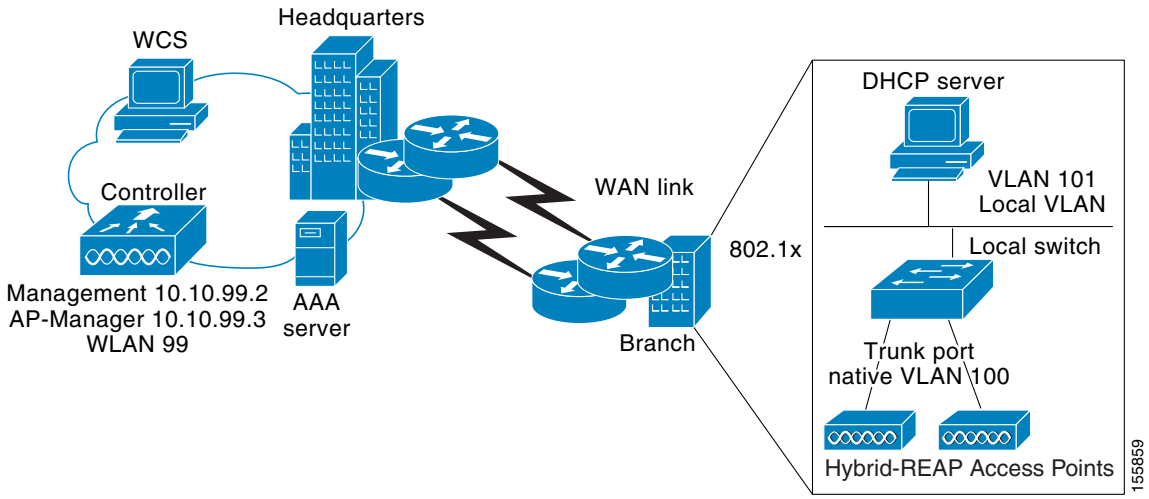
- Overview of Hybrid REAP, page 13-1
- Configuring Hybrid REAP, page 13-4
- Hybrid REAP Access Point Groups, page 13-11

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 and 1240AG 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 13-1 illustrates a typical hybrid-REAP deployment.

Figure 13-1 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 LWAPP 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 LWAPP 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 LWAPP 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. Refer to 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 LWAPP 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 13-4
- Configuring the Controller for Hybrid REAP, page 13-5
- Configuring an Access Point for Hybrid REAP, page 13-8
- Connecting Client Devices to the WLANs, page 13-10

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 Refer to 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**.

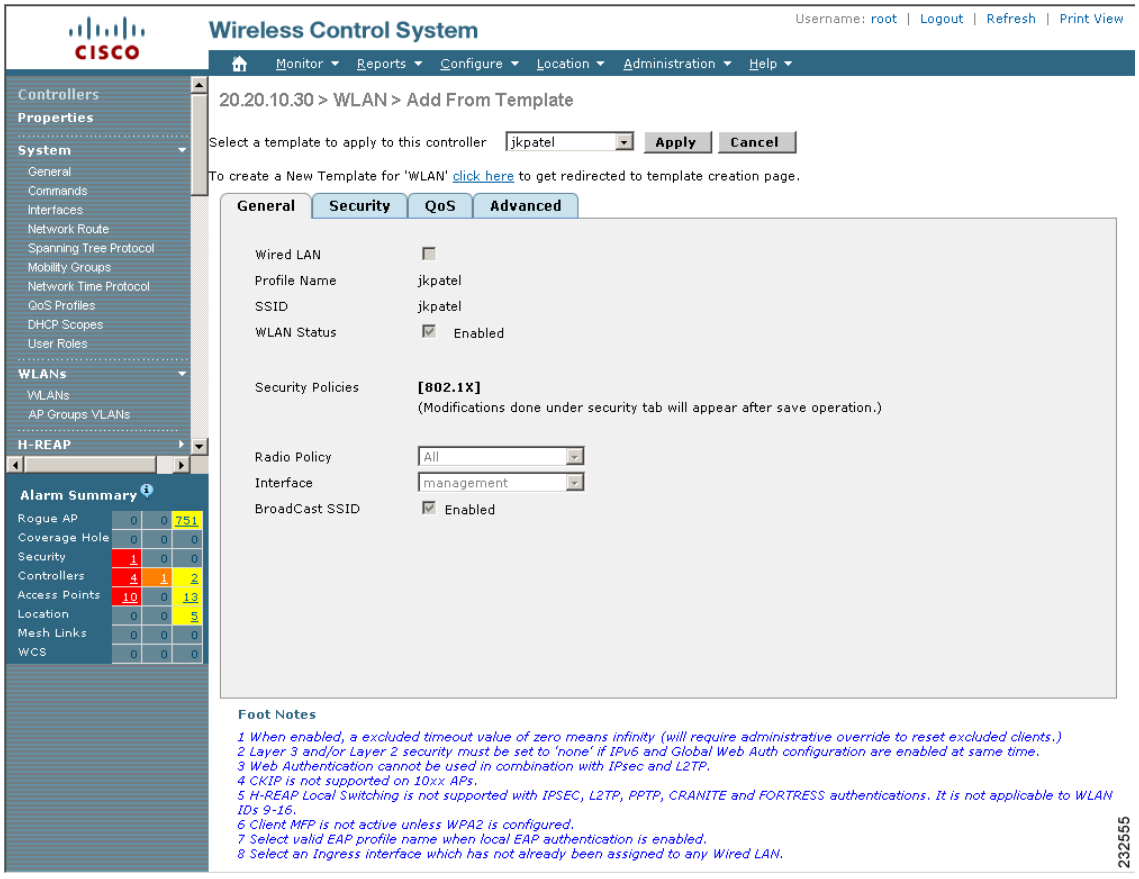
b. Click in the IP Address column for a particular controller.

c. Click **WLANs > WLANs** to access the s page.

d. Choose **Add** from the Select a command drop-down menu and click **GO** (see Figure 13-2).

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 13-2 WLANs > New Page



e. If you want to apply a template to this controller, choose a template name from the drop-down menu. 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 11-9).

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 **Admin 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, check the **Allow AAA Override** check box to ensure that the controller validates a quarantine VLAN assignment.

h. Click **Apply** 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 window 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 **Apply** 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, check 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 for the server and then choose this ACL as the WLAN preauthentication ACL.

c. Make sure to enable this by checking the **Admin Status** check box under General Policies.

d. Click **Apply** to commit your changes.

e. If you want to customize the content and appearance of the login page that guest users see the first time they access this , follow the instructions in the "Configuring a Web Authentication Template" section on page 11-51.

f. To add a local user to thisWLAN, click **Security** and then click **Local Net Users**.

g. When the Local Net Users page appears, choose **Add Local Net User** from the Select a command drop-down menu.

h. In the User Name and Password fields, enter a username and password for the local user. Click the **Generate Password** check box if you want a password automatically generated. The Password and Confirm Password parameters is automatically populated. If automatic generation is not enabled, you must supply a password twice.

i. From the SSID drop-down list, choose the SSID to which this guest user applies. Only those s for which web security is enabled are listed. The SSID must be a WLAN that has Layer 3 web authentication policy configured.

j. Enter a description of the guest user account.

k. From the Lifetime drop-down list, choose the number of days, hours, or minutes for this user account to remain active.

l. Click **Save**.

Step 4 Go to the "Configuring an Access Point for Hybrid REAP" section on page 13-8 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.

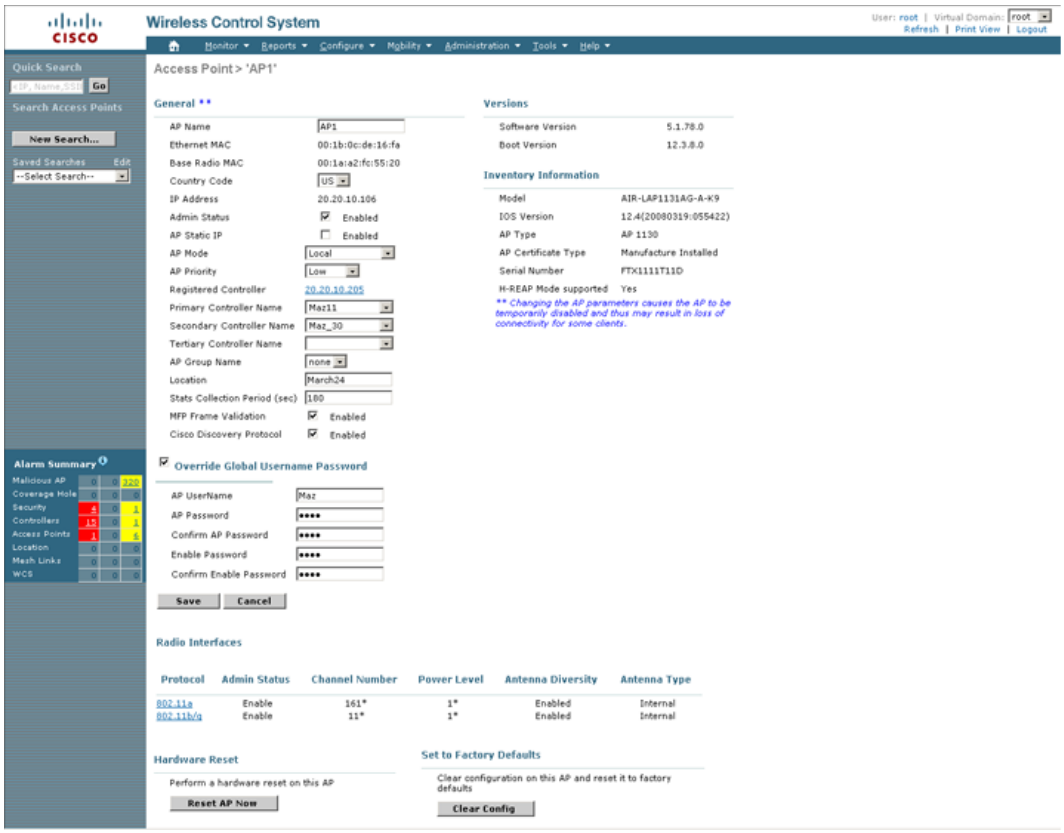
Follow these steps to configure an access point for hybrid REAP.

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 window appears (see Figure 13-3).

Figure 13-3 Detailed Access Point Window



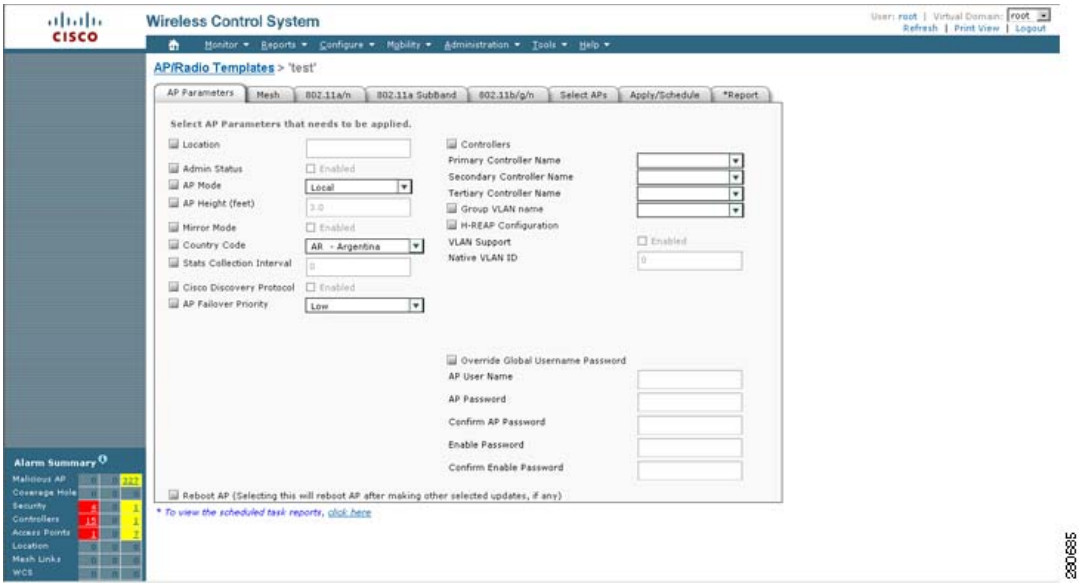
The last parameter under Inventory Information indicates whether this access point can be configured for hybrid REAP. Only the 1130AG and 1240AG access points support hybrid REAP.

Step 4 Verify that the H-REAP Mode Supported parameter displays *Yes*. If it does not, continue to Step 5. If H-REAP is showing as supported, skip to Step 7.

Step 5 Choose **Configure > Access Point Templates**.

Step 6 Choose which access point you want to configure for hybrid REAP by clicking one from the AP Name list. The AP/Radio Templates window appears (see Figure 13-4).

Figure 13-4 AP/Radio Template Window



Step 7 Check the **Enable VLAN** check box and enter the number of the native VLAN on the remote network (such as 100) in the **Native VLAN Identifier** field.

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 8 Click **Save** to save your changes.

Step 9 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 10 Click **Save** to save your changes.

Step 11 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 13-5.

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.**

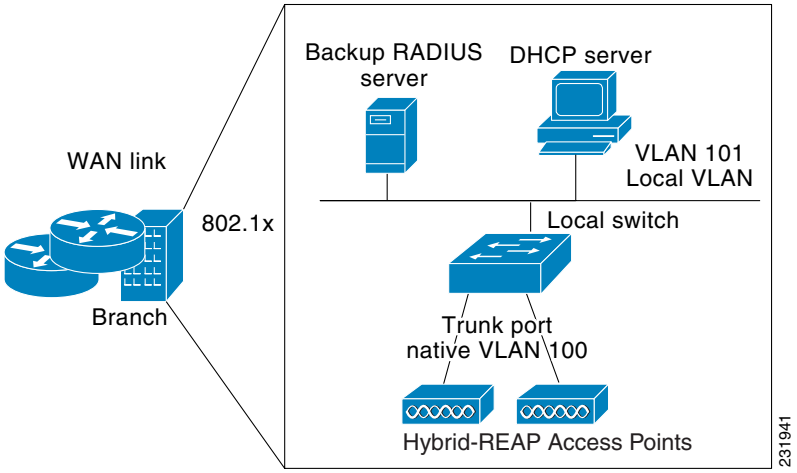
Hybrid REAP Access Point Groups

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 , 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 13-6 illustrates a typical hybrid-REAP group deployment with a backup RADIUS server in the branch office.

Figure 13-5 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 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 LWAPP 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 11-20.

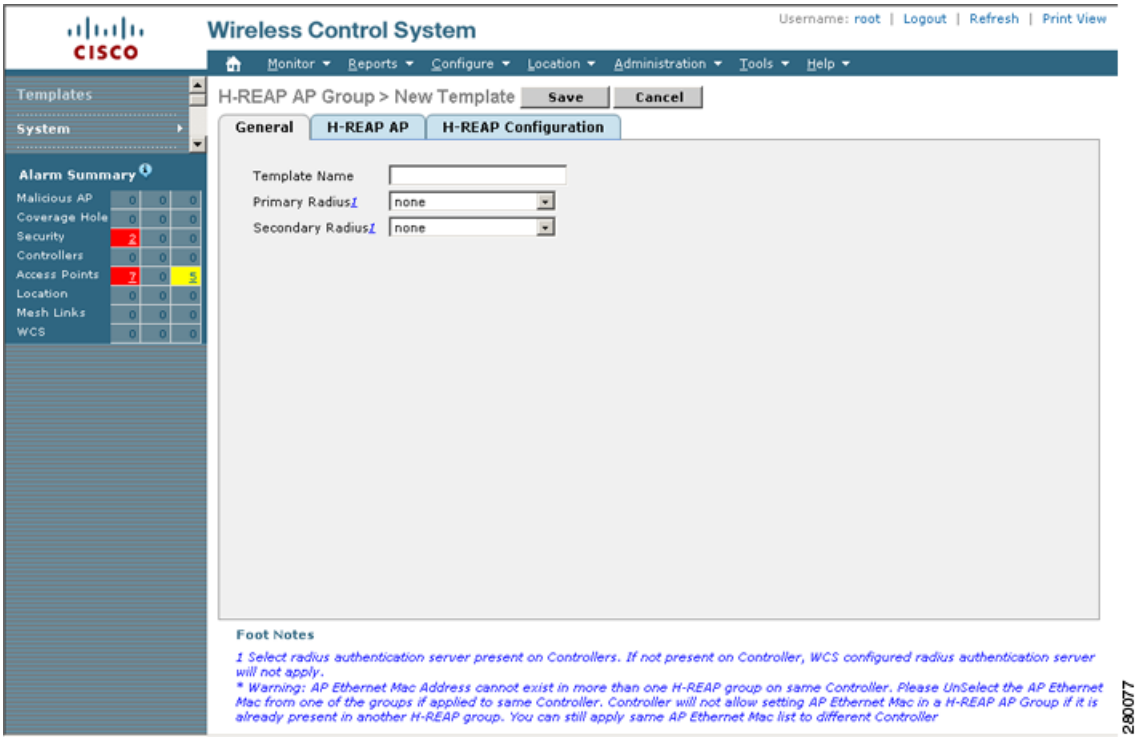
Step 1 Choose **Configure > Controllers**.

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 menu.
- or -
To make modifications to an existing template, click to select a template in the Template Name column. The General tab of the HREAP AP Groups template appears (see Figure 13-6).

Figure 13-6 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 menu.

Step 5 The Group Name parameter shows the group name assigned to the HREAP access point group.

Step 6 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 7 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 8 Click **Save**.

Step 9 If you want to add an access point to the group, click the **H-REAP AP** tab.

Step 10 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 11 Click **Add AP**. The H-REAP AP Group window appears. Choose the access point Ethernet MAC from the WCS list of H-REAP MAC addresses and apply it.

Step 12 Click **Save**.

Step 13 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 14 Check the **H-REAP Local Authentication Enabled** check box to enable local authentication for this hybrid-REAP group. The default value is unchecked.

Note When you attempt to use this feature, a warning message indicates that it is a licensed feature.

Step 15 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 16 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 field. 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 **Ignore Server Key** check box.

Step 17 In the EAP-FAST Authority ID field, enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.

Step 18 In the EAP-FAST Authority Info field, enter the authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.

Step 19 In the EAP-FAST Pac Timeout field, 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 14

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 Dashboard, page 14-1
- Monitoring Alarms, page 14-4
- Alarm and Event Dictionary, page 14-15

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 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.).

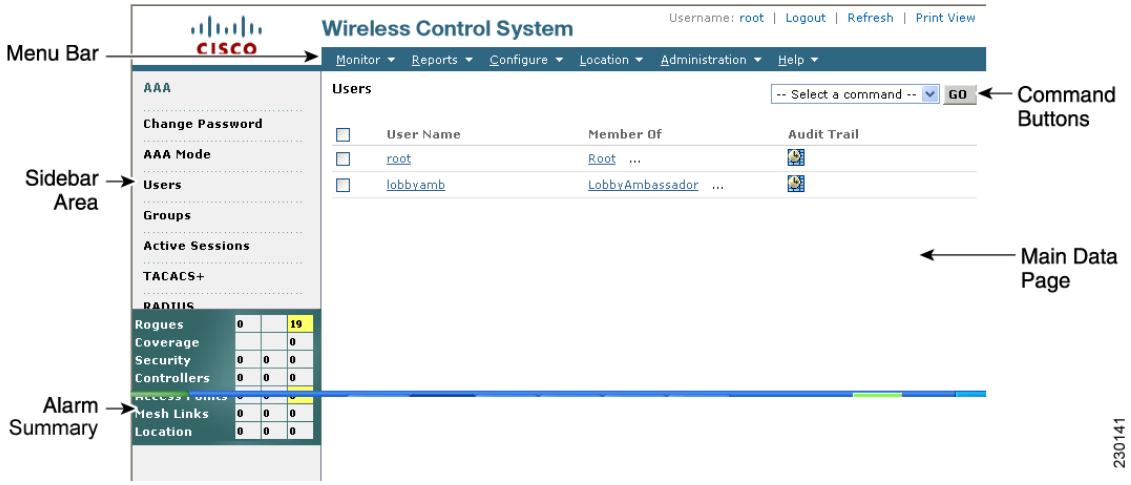
Using the Alarm Dashboard

The number of active alarms for controllers, access points, location, and rogue elements as well as alarms associated with entities such as coverage, mesh, and severity are actively displayed on the left-side of most WCS windows (see Figure 14-1).

Note The Administration > Settings > Alarms page has a Hide Acknowledged Alarms check box. You must uncheck the preference of hiding acknowledged alarms if you want acknowledged alarms to show on the WCS Alarm Summary and alarms lists window. 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 14-1 Alarm Summary Block



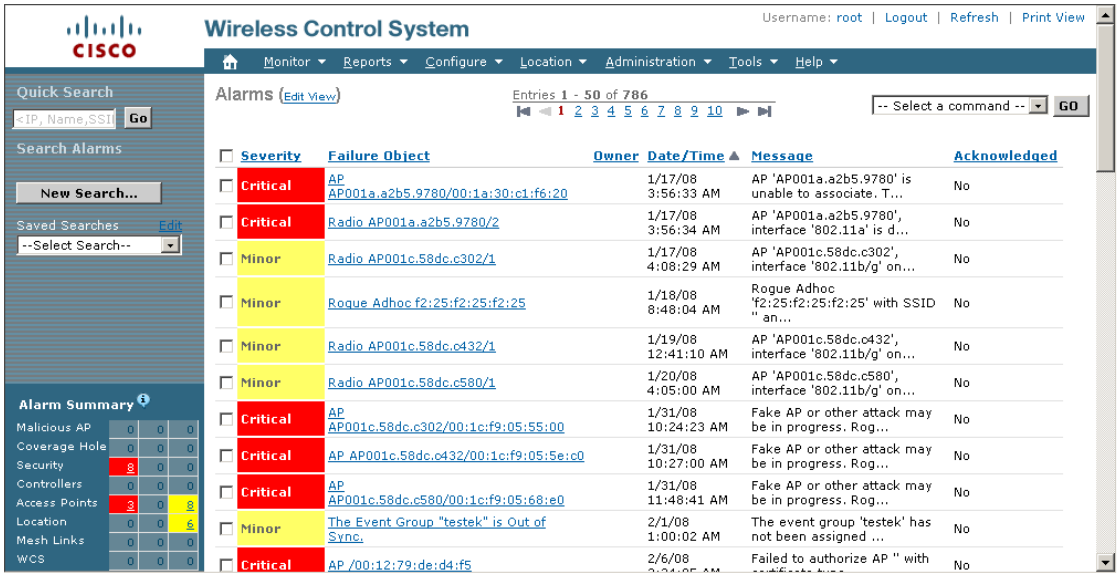
To view a listing of a specific type of alarm (critical, major, or minor) for a specific product or entity (such as coverage), click on the appropriate box within the alarm dashboard and a window displaying details for that alarm type and severity appears (see Figure 14-2).

Note You can also view alarm details for a specific product or entity by choosing **Monitor > Alarms** and then selecting the desired alarm level from the **Severity** drop-down menu and the product or entity type from the **Alarm Category** drop-down menu.

Note To search for additional alarms, click **New Search...** on the left panel of the page.

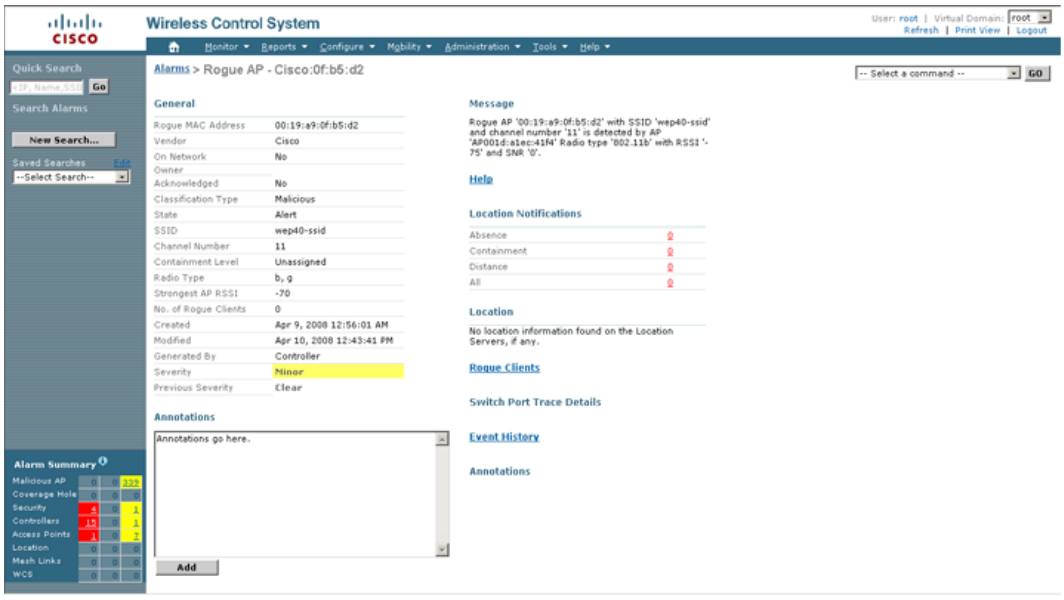
Note You can also configure a username and password login for access points from the controller.

Figure 14-2 Alarm Summary Page for WCS



Note You can click a box in the alarm dashboard to display alarm events for the entity and alarm type selected. For example, if you click on the minor alarms box for location, the Alarms page for that specific item appears (see Figure 14-2). For more details on a specific alarm listed on the Alarms page, click on the **Failure Object** link (see Figure 14-3).

Figure 14-3 Details for a Specific Failure Object (Alarm)



Note You can use the drop-down menu at the upper-right of the Alarms page to assign, unassign, delete, acknowledge, or clear the alarm. The event history of the alarm is also accessible from this menu.

Alarm Acknowledgement

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 window or any alarms list. In this scenario, you can find the alarm for the 802.11g interface in the Alarms list, click the checkbox, 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 window 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 window 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 **Adminstration > Settings > Alarms** window and disable the **Hide Acknowledged Alarms** perference.

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 Alarms

Choose **Monitor > Alarms** to access the Alarms window. This window provides a summary of the controller alarms.

This section provides information on the following information.

- Using Edit View, page 14-5
- Using Search, page 14-6
- Monitoring Failed Objects, page 14-7
- Monitoring Rogue Access Point Alarms, page 14-8
- Monitoring Rogue Access Point Details, page 14-9
- Monitoring Rogue Adhoc Alarms, page 14-10
- Monitoring Rogue Adhoc Details, page 14-11
- Detecting Access Points, page 14-12
- Monitoring Events, page 14-13
- Monitoring Rogue Clients, page 14-13
- Monitoring E-mail Notifications, page 14-14
- Monitoring Severity Configurations, page 14-14

Table 14-1 displays a table of logged alarms.

Table 14-1

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 menu.
Severity	Displays an alarm's level of security (color coded): Critical, Major, Minor, Warning, Clear, Info.
Failure Object	Displays the name and IP or MAC address of the object for which the alarm was generated.
Owner	Displays the name of the person to whom this alarm is assigned, if one is entered.
Date/Time	Displays the date and time that the alarm occurred.
Message	Displays a message explaining why the alarm occurred.
Acknowledged	Verifies whether an alarm has been acknowledged or not.

When there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use these scroll arrows to view additional alarms.

To add, remove, or reorder columns in the table, click the **Edit View** link to go to the Edit View window.

Using Edit View

The Edit View window allows you to add, remove, or reorder columns in the Alarms table.

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

Step 1 Choose **Monitor > Alarms**.

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

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. All items in the left column are not displayed 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.

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

Using Search

Use the controls in the left sidebar to create and save custom searches. To use a saved search, choose it from the Saved Searches drop-down list to open the Search Alarms window.

Note You can change the saved search criteria before intiating the search.

To delete a saved search, click **Edit** to open the Edit Saved Searches window. Check the check box for the saved searched that you want to cancel, then click **Submit**.

To create a new search, click **New Search...** to open a Search Alarms window and set search criteria.

Search criteria windows have the following commands:

- New Search drop-down menu—Opens the Search Alarms window. Use the Search Alarms window to configure, run, and save searches.
  - **Severity** (drop-down list)—All Severities, Critical, Major, Minor, Warning, Clear, Info.
  - **Alarm Category**—All Types, Access Points, Controllers, Coverage Hole, Config Audit, Location Services, Location Notifications, Interference, Mesh Links, Rogue APs, Rogue Adhocs, Security, and WCS.
  - **Time Period**—Specify whether you want the results to be returned for the last 5 minutes, last 15 minutes, last 30 minutes, last hour, last 8 hours, last 24 hours, last 7 days, or any time.
  - **Acknowledged State**—Specify if you want the alarms in the Acknowledged state to appear in the search results.
  - **Assigned State**—Specify if you want the alarms in the Assigned state to appear in the search results.
  - **Rogue State** (only shown when Rogue AP Alarm Category is selected)—All States, Alert, Known, Acknowledged, Contained, Threat, Contained Pending, Removed.
  - **Search for Rogue APs by** (only shown when Rogue AP Alarm Category is selected)—All APs, AP Name, Floor Area, Outdoor Area.
  - **Enter AP Name** (only shown when Rogue AP Alarm Category and Search for Rogue APs by AP Name are selected)—Enter the desired rogue access point name.
  - **Select Radio Type** (only shown when Floor Area Alarm Category, or Rogue AP Alarm Category and Search for Rogue APs by AP Name are selected)—All Radios, 802.11a, 802.11b/g.
  - **Campus** (only shown when Rogue AP Alarm Category and Search for Rogue APs by Floor Area/Outdoor Area are selected)—Root Area, <Campus Name>.
  - **Outdoor Area** (only shown when Rogue AP Alarm Category and Search for Rogue APs by Outdoor Area are selected)—Outdoor Area, <Outdoor Area Name>.
  - **Building** (only shown when Rogue AP Alarm Category and Search for Rogue APs by Floor Area are is selected)—All Buildings, <Building Name>.
  - **Floor Area** (only shown when Rogue AP Alarm Category and Search for Rogue APs by Floor Area are selected)—All Floors, <Floor Area Name>.
  - **Access Point** (only shown when Rogue AP Alarm Category and Search for Rogue APs by Floor Area/Outdoor Area are selected)—All Access Points, <Access Point Name>.
  - **Save Search**—To save a search, check the check box and enter the name of the search. The new search can later be accessed from the Saved Searches drop-down list on the left sidebar menu.

  - **Items per page**—The number of alarms to list per page.
- **Saved Searches** drop-down menu—Lists the saved custom searches. To open a saved search, choose it from the Saved Searches list.
- **Edit link**—Opens the Edit Saved Searches window. You can delete saved searches in the Edit Saved Searches window.

Monitoring Failed Objects

Choose **Monitor > Alarms** to access the Alarms page. Click an item under Failure Object to access this page.

This page provides the alarm details and messages regarding any anomalies with the controllers and access points.

The General Parameters descriptions are shown in Table 14-2.

Table 14-2 General Parameters

Parameter	Description
Failure Object	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.
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 severity: Critical, Major, Minor, Warning, Clear, Info. Color coded.
Previous Severity	Critical, Major, Minor, Warning, Clear, Info. Color coded.

- Annotations—Enter any new notes in this box and click **Add** to update the alarm. Notes are displayed in the Annotations display area.
- Messages—Displays information about the alarm.
- Audit Report—Click to view config audit 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.

- Help—Displays the latest information about the alarm.

- Rogue Clients—If the failure object is a rogue access point, information about rogue clients is displayed.
- Event History—Takes you to the Monitor Alarms > Events page to view events for Rogue Alarms.

Monitoring Rogue Access Point Alarms

Rogue access point radios are unauthorized access points detected by one or more Cisco lightweight access points. This page displays rogue access point alarms based on the severity you clicked in the Alarm Monitor.

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

- Choose **Monitor > Alarms**. From the left sidebar, click **New Search** and choose **Rogue AP from the Alarm Category drop-down menu.** Click **GO** to display the matching alarms.
- Choose **Monitor > Security**. From the left sidebar, click **Rogue APs**.
- Click the **Malicious AP** number link in the Alarm Summary box at the bottom of the left sidebar.

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 the scroll arrows to view additional alarms.

The Rogue AP Alarms page contains the following parameters:

Table 14-3 Rogue Access Point Alarms

Parameter	Description
Check box	Select the alarms on which you want to take action.
Severity	The severity of the alarm: Critical, Major, Minor, Clear. Color coded.
Rogue MAC Address	Media Access Control 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 strongest received signal strength indicator in dBm.
No. of Rogue Clients	Indicates the number of rogue clients associated to this access point.
Owner	Indicates the ‘owner’ of the rogue access point.
Date/Time	Date and time the alarm occurred.
State	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.)
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.

The other sections on the Rogue AP Alarms page include the following:

- Unacknowledge—Unacknowledge an already acknowledged alarm.
- E-mail Notification—Takes you to the **All Alarms > E-mail Notification** page to view and configure e-mail notifications. See Monitor Alarms > E-mail Notification for more information.
- Severity Configuration—Change the severity level for newly-generated alarms. See Monitor Alarms > Severity Configuration for more information.
- Detecting APs—View the Cisco lightweight access points that are currently detecting the rogue access point.
- Map (High Resolution)—Click to display a high-resolution map of the rogue access point location.
- Rogue Clients—Click to view a list of rogue clients associated with this rogue access point. The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the rogue access point.
- Set State to 'Unclassified - Alert'—Choose this command to tag the rogue access point as the lowest threat, continue monitoring the rogue access point, and to turn off containment.
- Set State to 'Malicious - Alert'—Choose this command to tag the rogue access point as *Malicious*.
- Set State to 'Friendly - Internal'—Choose this command to tag the rogue access point as internal, add it to the Known Rogue APs list, and to turn off containment.
- 1 AP Containment—Target the rogue access point for containment by one access point. (Lowest containment level.)
- 2 AP Containment—Target the rogue access point for containment by two Cisco lightweight access points.
- 3 AP Containment—Target the rogue access point for containment by three Cisco lightweight access points.
- 4 AP Containment—Target the rogue access point for containment by four Cisco lightweight access points. (Highest containment level.)

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.

Monitoring 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 From 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 Cisco lightweight access points. The following information is available:

- General—
  - Rogue MAC Address—Media Access Control address of the rogue access points.
  - Vendor—Rogue access point vendor name or Unknown.
  - On Network—Indicates whether or not the rogue access point 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 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.
- **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.

Monitoring Rogue Adhoc Alarms

The Rogue Adhoc Alarms page displays alarm events for rogue adhocs.

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

- Choose **Monitor > Alarms**. From the left sidebar, click **New Search** and choose **Rogue Adhoc from the Alarm Category drop-down menu.** Click **GO** to display the matching alarms.
- Choose **Monitor > Security**. From the left sidebar, click **Rogue Adhocs**.

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 this to view additional alarms.

The Rogue Adhoc Alarms page contains the following parameters:

Table 14-4 Rogue Adhoc Alarms

Parameter	Description
Check box	Choose the alarms on which you want to take action.
Severity	The severity of the alarm: Critical, Major, Minor, Clear. Color coded.
Rogue Adhoc MAC Address	Media Access Control address of the rogue adhoc.
Vendor	Rogue adhoc vendor name or Unknown.
Classification Type	Malicious, Friendly, or Unclassified.
Radio Type	Indicates the radio type for this rogue adhoc.
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 rogue adhoc.
Owner	Indicates the owner of the rogue adhoc.
Date/Time	Date and time the alarm occurred.
State	State of the alarm: Alert, Known, or Removed.
SSID	Service Set Identifier being broadcast by the rogue adhoc radio. (Blank if SSID is not broadcast.)
Map Location	Indicates the map location for this rogue adhoc.
Acknowledged	Displays whether or not the alarm is acknowledged by the user.

Monitoring Rogue Adhoc Details

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

Follow these steps to view the alarm events for a rogue adhoc radio.

Step 1 From the Rogue Adhoc 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 rogue adhoc.
  - Vendor—Rogue adhoc vendor name or Unknown.
  - On Network—Indicates whether or not the rogue adhoc 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 rogue adhoc radio. (Blank if SSID is not broadcast.)
  - Channel Number—Indicates the channel of the rogue adhoc.
  - Containment Level—Indicates the containment level of the rogue adhoc or Unassigned.
  - Radio Type—Indicates the radio type for this rogue adhoc.
  - 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 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—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.

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 Events

Click a **Rogues** alarm square in the **Alarm Monitor** (lower left-hand side of the screen), click a list item under **Rogue MAC Addresses**, from the Select a command drop-down list choose **Event History**, and click **GO** to access this page.

Choose **Monitor > Alarms** and then click **New Search** in the left sidebar. Choose **Severity > All Severities** and **Alarm Category > Rogue AP**, and click **Go** to access the Monitor Alarms > <failure object> page. Click an item under the Rogue MAC Address to display the Monitor Alarms > Rogue AP Details page. From the Select a command drop-down list choose **Event History**, and click **GO** to access this page.

This page enables you to review information about rogue alarm events. Events list the sequence of occurrences for an element(s) over a period of time.

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 Rogue Clients

Choose **Monitor > Alarms** and then click **New Search** in the left sidebar. Choose **Severity > All Severities** and **Alarm Category > Rogue AP**, and click **GO** to access the Monitor Alarms > <failure object> page. Click an item under the Rogue MAC Address to display the Monitor Alarms > Rogue AP Details page. From the Select a command drop-down list, choose **Rogue Clients** to access this page.

This page enables you to view information about clients that have associated with the rogue access point.

- Client MAC Address—Media Access Control address of the rogue access point client.
- Last Heard—The last time a Cisco access point detected the rogue access point client.
- Status—Status of the rogue access point client.

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 menu, 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 a comma.

Step 6 Click **OK**.

Step 7 Click the **Enabled** check box for applicable 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 menu, 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.

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.

Notification Format

For each alarm and event notification, the following information is provided:

Table 14-5 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.
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 on 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 rogue adhoc "{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 rogue adhoc "{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 rogue adhoc "{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 adhoc rogue and automatically contained it.
WCS Severity	Major.
Probable Causes	The system detected an adhoc rogue and automatically contained it as configured in the system's wireless prevention policy.
Recommended Actions	Identify the adhoc 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 adhoc rogue that the system has detected earlier is now clear.
WCS Severity	Informational.
Probable Causes	The system no longer detects an adhoc 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 adhoc 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 theWLAN 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 rogue adhoc "{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.

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 15

Running Reports

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 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 If you want the report to print as it appears on the window display, you must choose landscape mode.

From the Reports menu, you can access any of the following types:

- 802.11n Scaling Reports, page 15-5
- Access Point Reports, page 15-7
- Audit Reports, page 15-9
- Client Reports, page 15-10
- Compliance Reports, page 15-12
- Mesh Reports, page 15-15
- Performance Reports, page 15-17
- Security Reports, page 15-19

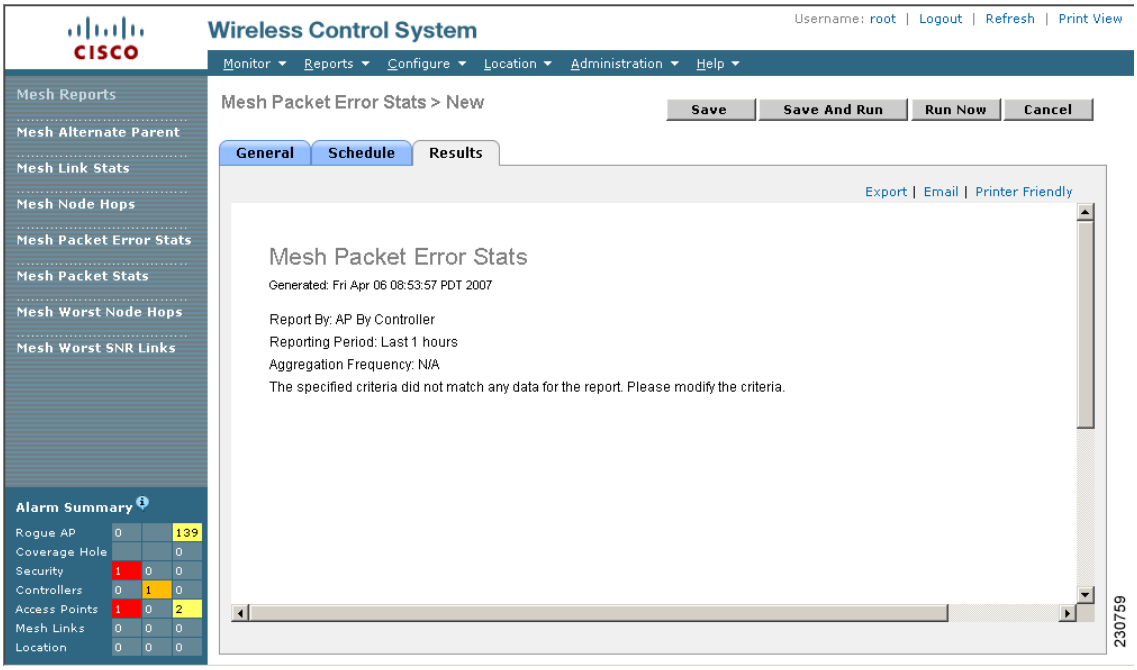
Choosing a Report

If you choose one of the above options from the Reports menu, a window with a list of created report tasks appears. Perform one of the following operations:

- If you want to enable or disable a report schedule, refer to the "Enabling or Disabling a Schedule" section on page 15-2.
- If you want to delete a report, refer to the "Deleting a Report" section on page 15-3.
- If no reports are defined, you can create a report by selecting **New** from the Select a command menu. After clicking **GO**, two new panels appear: General and Schedule. The General panel allows you to configure data gathering parameters. The Schedule panel allows you to control when and how often the report runs, based on what you specify. Refer to the "Accessing the Schedule Panel" section on page 15-4.

  After running the report, a Results tab shows the report data (see Figure 15-1).

Figure 15-1 Results Tab



A History Tab appears after some scheduled executions have occurred.

Enabling or Disabling a Schedule

To enable a defined report, check the check box next to the report and select **Enable Schedule** from the Select a command menu. Click **GO**. If the scheduled time period for the report has passed, then *Expired* appears in the Schedule column. To remedy, click the report title and enter new time parameters in the window that appears.

To disable a defined report, check the check box next to the report and select **Disable Schedule** from the Select a command menu. Click **GO**. The disabled state appears in the Schedule column.

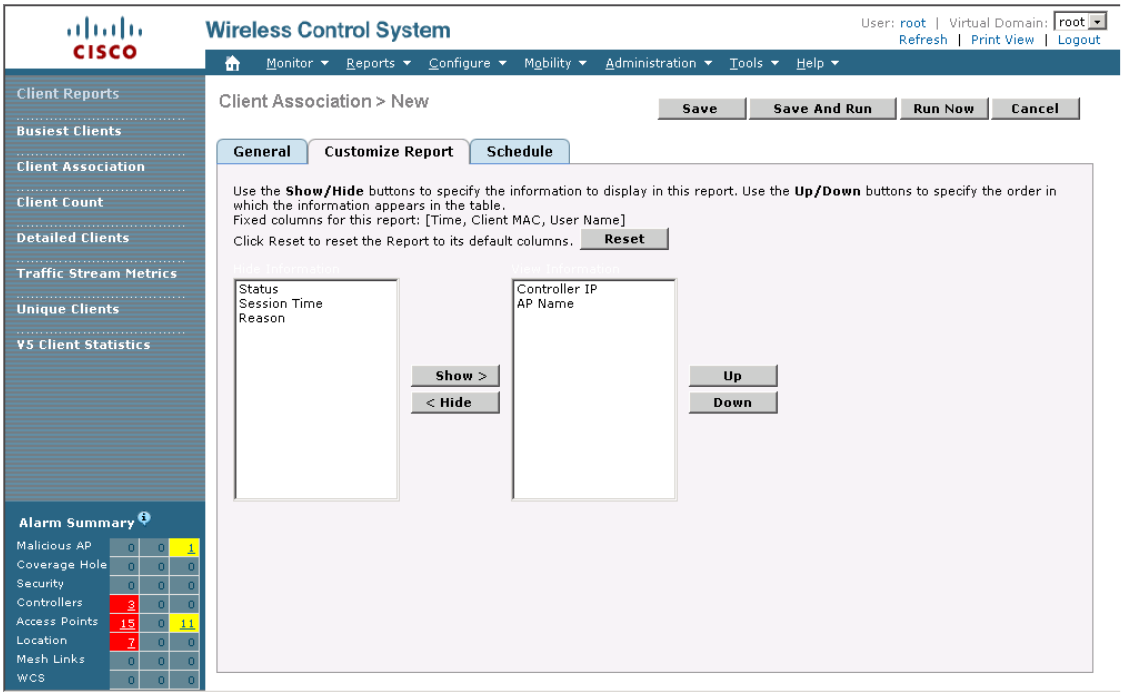
Deleting a Report

To delete a defined report, check the check box next to the report and select **Delete** from the Select a command menu and click **GO**. The report is deleted from the listing.

Customizing a Report

Several reports have a Customize Report tab (see Figure 15-2). Within this tab, you can use the Show and Hide buttons to specify which information you want displayed in the report. After you have column headings appearing in the Show window, you can use the Up and Down buttons to specify the order that you want the information to appear. Some columns may be fixed and vary per report.

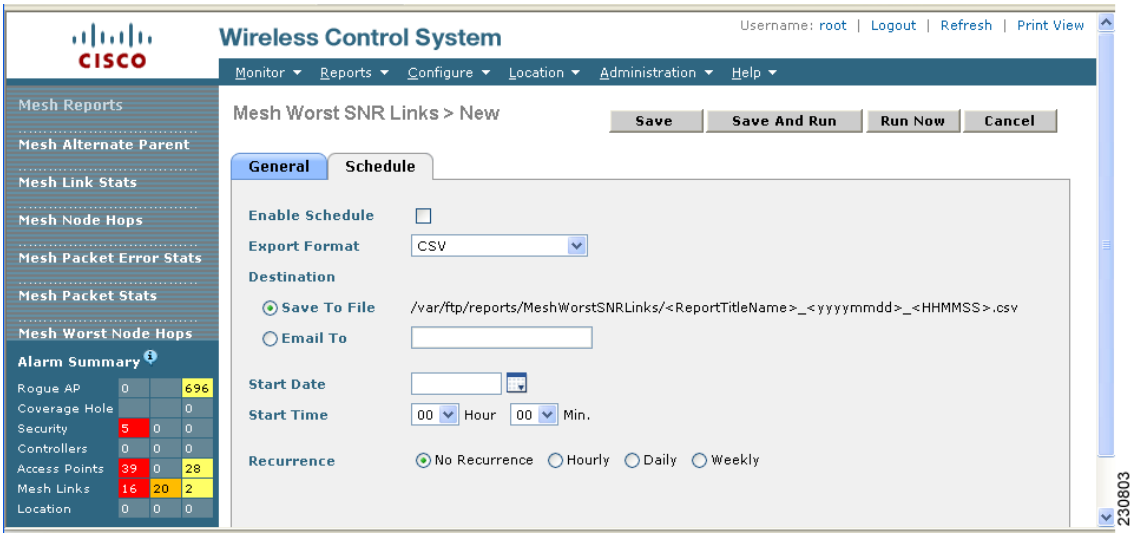
Figure 15-2 Customize Report Tab



Accessing the Schedule Panel

The schedule panel is the same for any report. After choosing the Schedule tab, the Schedule window appears (see Figure 15-3).

Figure 15-3 Schedule Tab



Follow these steps after choosing the **Schedule** tab within any report type.

Step 1 Check the **Enable Schedule** check box.

Step 2 Specify if you want the export format to be .csv (a file containing the MAC addresses of access points) or .pdf from the Export Format drop-down menu.

Step 3 Choose either the **Save to File** or **E-mail To** option as the destination type.

- If you select the Save to File option, a destination path must first be defined at the **Administration > Settings** > *Report* page. Enter the destination path for the files in the Repository Path field.
- If you select the E-mail to option, an SMTP Mail Server must be defined prior to entry of the target e-mail address. Choose **Administrator > Settings** > *Mail Server* to enter the appropriate information.

Step 4 Enter a start date (MM:DD:YYYY format) in the provided field or click the calendar icon to select a date. The report begins running on this date.

Step 5 Specify a start time using the hour and minute drop-down menus.

Step 6 Click on one of the recurrence buttons to select how often the report is run.

Step 7 When entry is complete, do one of the following:

- Click **Save** to save the entry.
- Click **Save and Run** to save the changes and run the report now. The report is run, and the results are either e-mailed or saved to a designated file as defined in the Schedule tab. The report runs again at the scheduled time.

- Click **Run Now** if you want to run the report immediately and review the results in the WCS window. The report runs regardless of any scheduled time associated with the report.

Note You can use the Run command to check a report scenario before saving it or to run ad hoc reports as necessary.

802.11n Scaling Reports

The 802.11n Scaling reports can help you to find out the client mix in your network and respective utilization of the infrastructure. These reports can also help you discover how the current controller deployment scales up to the given client mix and how you can scale to add more controllers and access points.

802.11n Scaling reports include:

- Client Count
- Throughput

Note The 802.11n Scaling reports do not include clients connected to Autonomous IOS access points.

Client Count

The Client Count is a graph report which displays the associated clients and authenticated clients. The clients can be filtered by controller, floor area, SSID, access point, and client protocol.

Note The Client Count report does not include clients connected to Autonomous IOS access points.

To access this report, follow these steps:

Step 1 Choose **Reports > 802.11n Scaling**.

Step 2 From the left sidebar menu, click **Client Count**.

In the report window, saved reports are displayed in a table.

Creating a New Client Count Report

To create a new Client Count report, follow these steps:

Step 1 From the Reports > 802,11n Scaling > Client Count report page, choose *New* from the Select a command drop-down menu.

Step 2 Click **GO**.

Step 3 Enter applicable report parameters.

- Report Title

- Report By:

  Note The parameters change depending upon the Report By selection.

  - Controller—Choose the controller from the drop-down menu.
  - Floor Area—Choose the campus, building, and floor from the drop-down menus.
  - Outdoor Area—Choose the campus and outdoor area from the drop-down menus.
  - AP by Floor Area—Choose the campus, building, floor, and access point from the drop-down menus.
  - AP by Outdoor Area—Choose Campus, Outdoor Area, and Access Point from the drop-down menus.
  - SSID —Choose All SSIDs or other applicable SSID from the drop-down menu.
- Protocol—All Clients, 802.11a/n, 802.11b/g/n, 802.11a. 802.11b, 802.11g, 802.11n_5GHz, and 802.11n_2.4GHz.
- Reporting Period.

Step 4 Configure the report schedule. See the "Enabling or Disabling a Schedule" section on page 15-2.

Step 5 Click **Save**, **Save and Run**, **Run Now**, or **Cancel**.

You can manage saved reports using the Select a command drop-down list.

Throughput

The 802.11n Throughput report is a graph report which displays the total throughput of a selected device or service domain along with the selected clients below it. These selected clients are differentiated by protocol types.

Note The Throughput report does not include clients connected to Autonomous IOS access points.

To access this report, follow these steps:

Step 1 Choose **Reports > 802.11n Scaling**.

Step 2 From the left sidebar menu, click **Throughput**.

Step 3 In the report window, saved reports are displayed in a table.

Creating a New Throughput Report

To create a new Throughput report, follow these steps:

Step 1 From the Reports > 802.11n Scaling > Throughput report page, choose **New** from the Select a command drop-down menu.

Step 2 Click **GO**.

Step 3 Enter applicable report parameters.

- Report Title
- Report By:

Note The parameters change depending upon the Report By selection.

  - Controller—Choose the controller from the drop-down menu.
  - Floor Area—Choose the campus, building, and floor from the drop-down menus.
  - Outdoor Area—Choose the campus and outdoor area from the drop-down menus.
  - AP by Controller—Choose the controller and access point from the drop-down menus.
  - AP by Floor Area—Choose the campus, building, floor, and access point from the drop-down menus.
  - AP by Outdoor Area—Choose campus, outdoor area, and access point from the drop-down menus.
- Protocol—All clients, 802.11a/n, 802.11b/g/n, 802.11a, 802.11b, 802.11g, 802.11n_5GHz, 802.11n_2.4GHz.
- Reporting Period

Step 4 Configure the report schedule. See the "Accessing the Schedule Panel" section on page 15-4 for more information.

Step 5 Click **Save**, **Save and Run**, **Run Now**, or **Cancel**.

You can manage saved reports using the Select a command drop-down list.

Access Point Reports

In the left sidebar menu, all of the access point report options are listed.

Note The access point reports do not show the status of autonomous access points.

The choices are as follows:

- AP List by Location and SSID Report—Displays information on access points located in specific physical areas and specific SSIDs.
- AP Profile Status Report—Displays information on access points located in specific physical areas and with specific SSIDs.
- AP Up Times—This report displays information related to the uptime of various devices on your network. You can choose between AP up time, LWAPP up time, and LWAPP join time and then sort the report from lowest-to-highest up times or from highest-to-lowest up times. The graphical trending identifies the availability of services to the client with a quick summary of overall network availability over a given period of time. The report also displays the access point and map location if applicable.

- Busiest APs Report—Allows you to view information on the busiest access points in terms of total utilization. The total utilization is the sum of transmitting, receiving, and channel utilization.
- Traffic Stream Metrics Report—Shows voice traffic stream metrics and high density related reports. This report is useful in determing the current and historical quality of service (QoS) for given client(s) at the radio level. The controller keeps multiple records of the voice metrics data for each client. The access points update the controller with traffic stream metric information every 90 seconds, and 10 minutes of data is stored at one time to generate an on-demand report. WCS polls the data from the controllers and aggregates it as hourly, daily, and weekly. The generated data that is returned includes but is not limited to the following: uplink and downlink statistics such as packet loss rate, average queuing delay, distribution of delayed packets, and roaming delays.
- Graphical Traffic Stream Metrics Report—The Traffic Streams Metrics (Graphs) report is equivalent to the Traffic Streams Report, but the information is displayed in graph form.

Viewing or Modifying Access Point Reports

Follow these steps to view or modify existing access point reports.

Step 1 Choose **Reports > Access Point Reports**. The Access Point Report page appears.

Step 2 Choose the Access Point Report type from the left panel.

Step 3 Define (or modify) the conditions for the report in the General panel.

Step 4 Refer to the "Accessing the Schedule Panel" section on page 15-4 to complete the scheduling process.

Step 5 Click the **History** tab if you want to review details of the current and past runs of the report.

Creating a New Access Point Report

Follow these steps to create a new access point report.

Note Some of these steps or options are not required for every report.

Step 1 Choose **Reports > Access Point Reports**. The Access Point Reports page appears.

Step 2 Click on one of the report types summarized under Access Points Reports (left-side).

Step 3 Choose **New** from the Select a command drop-down menu and click **GO**.

Step 4 Specify a report title.

Step 5 Use the Report By drop-down menu to choose of which physical area to report. The following options are available:

- AP By Outdoor Area—Generates the report of the outdoor area on a per-access point basis.
- AP by Floor Area—Generates the report of the floor area on a per-access point basis.

Step 6 Perform one of the following:

If you chose outdoor, you need to specify in which campus and outdoor area it is located.
If you chose floor area, you need to choose in which campus, building, and floor the area is located.

Step 7 Determine which access points you want to include in the report.

Step 8 Specify if you want to include 802.11a/n or 802.11b/g/n radios in the report.

Step 9 Click the **Schedule** tab to complete the scheduling process. Refer to the "Accessing the Schedule Panel" section on page 15-4.

Audit Reports

Network configuration audit reports give configuration differences between WCS and the controllers managed by it. Such audits can be performed based on the controllers' current configuration or the templates that have been applied to them. Data for this report is collected by the Network Audit Configuration task which is enabled by default on a newly installed WCS system and is scheduled to run once every 7 days. To change the frequency of the background task, refer to the "Running Background Tasks" section on page 16-1. The report shows the audit status for each controller and shows the attribute differences in the configurations. Even controllers which are not reachable during the network audit configuration task are listed. The authorization for the audit reports is tied into the security framework so that only certain users can have access. By default, the admin, configManagers, system monitoring, superusers, and root users have access.

Note The Audit Reports do not show the status of autonomous access points.

Viewing or Modifying Audit Reports

Follow these steps to view or modify existing audit reports.

Step 1 Choose **Reports > Audit Reports**. The Audit Report page appears.

Step 2 Choose the Audit Report type from the left panel.

Step 3 Define (or modify) the conditions for the report in the General panel.

Note Even controllers that are not audited or not reachable are listed on the report.

Step 4 Refer to the "Accessing the Schedule Panel" section on page 15-4 to complete the scheduling process.

Step 5 Click the **History** tab if you want to review details of the current and past runs of the report.

Creating a New Network Configuration Audit Report

Follow these steps to create a new audit report.

Note Some of these steps or options are not required for every report.

Step 1 Choose **Reports > Audit Reports**. The Audit Reports page appears.

Step 2 Click on one of the report types summarized under Audit Reports (left-side). Currently only one network configuration audit report is available.

Note With a clean install, Background Tasks > Network Audit is enabled.

Step 3 Select **New** from the Select a command menu. Click **GO**. The two-tabbed entry panel appears.

Step 4 Specify a report title.

Step 5 Specify if you want the report to include all controllers or a selected controller.

Step 6 From the Audit Time drop-down menu, determine if you want to view the latest report or choose from a network audit time. Audit time is the time when the network audit background task was excluded. *Latest* is the default selection.

Step 7 Click the **Schedule** tab to complete the scheduling process. Refer to the "Accessing the Schedule Panel" section on page 15-4.

Note You can also choose Run Now to run the report. The report shows the data collected by the network audit task. You must set the network audit schedule appropriately.

Client Reports

You can run reports of all unique clients that have accessed the network for a specified duration. For example, you may want to show all clients that were on a certain floor in the last three days and see detailed information network activity.

Note The Client Count report is the only client reports that shows the status of autonomous access points.

The client report options are as follows:

Busiest Clients Report—Displays information on the busiest clients in terms of total throughput of clients during a given period of time. WCS polls Tx and Rx bytes from controllers and reports them on a per client basis. Within a 15 minute minute polling cycle (the default), the number of actual Tx and Rx bytes between this and previous polling cycles is calculated.The throughput is the Kb/s between this cycle and previous polling cycles. Utilization is the percentage of bandwidth used during the polling cycle (the throughput multiplied by 1000, divided by the bandwidth based on the radio, and then multiplied by 100). The bandwidth is the maximum speed for the radio (54 Mb/s for 802.11a/g, 11 Mb/s for 802.11b, 100 Mb/s for wired guest clients, and 200 Mb/s for 802.11n).

- Client Association Report—Shows a detailed association history of the clients as collected from the controller. The generated data that is returned includes but is not limited to the following: the username and MAC address of the client, which access point it is associated with, and a status.

Note The client association history only goes back 7 days. You cannot retrieve any history prior to that.

- Client Count Report—Displays data on the numbers of clients that connected to the network through a specific device, in a specific geographical region, or through a specific SSID.
- Detailed Clients Report—Consolidates client-related information currently present in other client reports in WCS. It includes network information (such as access point name, MAC and IP addresses, the controller name and IP address, and SSID information), client information (such as client name, MAC and IP addresses, brief configuration information such as client OUI, CCX rev, and client type voice/data/location), client statistics (such as RSSI, SNR, throughput, and session length), client location, and ACS information (whether the authentication succeeded or failed). The report can be generated multiple ways.
- Traffic Stream Metrics Report—Shows voice traffic stream metrics and high density related reports for clients. The controller keeps multiple records of the voice metrics data for each client. The traffic stream metrics report is used to determine the current and history quality of service (QoS) for given client(s) at the radio level. The generated data that is returned includes but is not limited to the following: uplink and downlink statistics such as packet loss rate, average queuing delay, distribution of delayed packets, and roaming delays.
- Unique Client Report—Shows which unique clients have accessed the network within a specified duration. For example, you could show all clients on a particular floor in the last three days and view detailed information about their network activity. The generated data that is returned includes but is not limited to the following: the vendor and MAC address of the client, which access point it is associated to, and the Cisco Compatible Extensions version supported by the client.
- V5 Client Statistics Report—Collects client statistics for V5 clients and above that are in an associated and authenticated state. The report contains counters for a Dot11 statistics measurement and a security statistics measurement. If V5 clients exist, a request is initiated for Dot11 measurement; and if the request is successful, the database is populated with the Dot11 response for the client. Then the security request is initiated and if successful, the database is populated with the security response for the client.

Viewing or Modifying Client Reports

Follow these steps to view or modify existing client reports.

Step 1 Choose **Reports > Client Reports**. The Client Report page appears.

Step 2 Choose the Client Report type from the left panel.

Step 3 Define (or modify) the conditions for the report in the General panel.

Step 4 Refer to the "Accessing the Schedule Panel" section on page 15-4 to complete the scheduling process.

Step 5 Click the **History** tab if you want to review details of the current and past runs of the report.

Creating a New Client Report

Follow these steps to create a new client report.

Note Some of these steps or options are not required for every report.

Step 1 Choose **Reports > Client Reports**. The Client Reports page appears.

Step 2 Click on one of the report types summarized under Client Reports (left-side).

Step 3 Choose **New** from the Select a command drop-down menu and click **GO**. The two-tabbed entry panel appears.

Step 4 Specify a report title.

Step 5 Enter the number of clients you want displayed in the report.

Step 6 Choose ALL SSIDs or choose a specific SSID to restrict the report to access points using that SSID.

Step 7 Enter a specific client MAC address. If no MAC address is specified, then all the clients per specified SSID would be reviewed.

Step 8 Specify if you want the report listed by controller, floor area, outdoor area, AP by floor, AP by outdoor area, or SSID. The floor area and outdoor area report generates the report on an area basis while the AP by floor or AP by outdoor area generates the report on a per-access point basis.

Step 9 If you chose controller, you need to enter a controller IP address.
If you chose floor area or AP by floor area, you need to enter the campus, building, and floor location.
If you chose outdoor area or AP by outdoor area, you need to enter the campus and outdoor area.

Step 10 Determine which access points you want to include in the report.

Step 11 Specify if you want to include 802.11a/n or 802.11b/g/n radios in the report.

Step 12 In the Reporting Period section, choose **Last** to determine the timeframe the report should encompass or choose **Between** and use the calendar icon to choose a date and set the hour and minutes.

Step 13 Click the **Schedule** tab to complete the scheduling process. Refer to the "Accessing the Schedule Panel" section on page 15-4.

Compliance Reports

The PCI DSS Compliance report provides a summary of 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. PCI DSS standards can be located at https://www.pcisecuritystandards.org.

To see the information a PCI Compliance Report provides, see the "Compliance Reports Results" section on page 15-13.

Viewing or Modifying Compliance Reports

This report identifies the device and network configuration in light of PCI requirements and provides PCI auditors with information about the level of compliance on your network. With the PCI requirements, the contents of this detailed report can serve as guidance to the auditors while they perform PCI audit of the network. To access this report, follow these steps:

Step 1 Choose **Reports > Compliance Reports**.

Step 2 From the left sidebar menu, click **PCI Compliance Reports**.

In the report window, saved reports are displayed in a table.

Creating a New Compliance Report

To create a new PCI Compliance report, follow these steps:

Step 1 From the Reports > Compliance Reports > PCI Compliance report page, choose **New** from the Select a command drop-down menu.

Step 2 Click **GO**.

Step 3 Enter the applicable report parameters:

- Report Title
- Reporting Period

Step 4 Configure the report schedule. Refer to the "Enabling or Disabling a Schedule" section on page 15-2 for more information.

Step 5 Click **Save**, **Save and Run**, **Run Now**, or **Cancel**.

Compliance Reports Results

Note Do not consider this report as a replacement for a formal PCI compliance audit. This report only addresses various aspects of the PCI standards as applicable to Cisco Unified Wireless Network (CUWN).

This report addresses the following PCI requirements and resulting issues:

- Install and maintain a firewall configuration to protect cardholder data—Includes the following information:
  - New rogue access points (most recent alarms for rogue access points) and rogue adhocs (rogue adhoc alarms) detected on your wireless LAN network—Lists all threats associated with rogue access points and rogue adhocs.
- Do not use vendor-supplied defaults for system passwords and other security parameters.

  - Lists all devices with default configuration scuh as default username/password, default SNMP community string, and SSID broadcast.

Note A configuration sync background task must be run at least once to get appropriate results.

- Encrypt transmission of cardholder data across open, public networks.
  - Lists all encryption and authentication violations.
- Track and monitor all access to network resources and cardholder data.
  - Lists detailed association history for clients that connect to your wireless LAN network.

Note A configuration sync background task must be run at least once to get appropriate results.

- Annually test security controls, limitations, network connections, and restrictions to assure the ability to adequately identify and to stop any unauthorized access attempts. User a wireless analyzer at least quarterly to identify all wireless devices in use.
  - Lists all wireless devices in the network (controllers, access points, and location servers).
  - Lists all intrusion attempts including signature attacks, MFP attacks, access point threats and attacks, client security events, and Cisco wired IPS events (only criticial and major alarms are included).

Inventory Reports

In the left sidebar menu, all of the inventory report options are listed. These reports generate inventory-related information of controllers, access points, and mobility service engines managed by WCS. The information provided can be grouped and includes but is not limited to the following: hardware type and distribution, software distribution, CDP information, and so on. These reports are generated based on the data already stored in the WCS database. Because inventory reports are not on-demand reports, some configuration changes may have occurred since the storage and may not duplicate the attributes of the controller that are reflected in the stored data.

Note The inventory reports do not show the status of autonomous access points.

The choices are as follows:

- Access Point Inventory Report—Provides data on deployed access points. The data that is returned includes but is not limited to the following: the access points' MAC address, base radio MAC, 802.11a/n or b/g/n radio MAC, model, location, and radio status.
- Combined Inventory Report—Provides data on all deployed controllers, access points, and location appliances. The data that is returned includes but is not limited to the following: base radio MAC and 802.11a/n or b/g/n radio MAC.
- Controller Report—Provides data on deployed controllers. The data that is returned includes but is not limited to the following: the model, IP address, and serial number of the controller, what software version it is running, and where it is located.

- Mobility Service Engines Report—Provides data on deployed location appliances. The data that is returned includes but is not limited to the following: the IP address and version of the location appliance, which port is being used, and the time the appliance starts up.

Viewing or Modifying Inventory Reports

Follow these steps to view or modify existing inventory reports.

Step 1 Choose **Reports > Inventory Reports**. The Inventory Reports page appears.

Step 2 Choose the Inventory Report type from the left panel.

Step 3 Define (or modify) the conditions for the report in the General panel.

Step 4 Refer to the "Accessing the Schedule Panel" section on page 15-4 to complete the scheduling process.

Step 5 Click the **History** tab if you want to review details of the current and past runs of the report.

Creating a New Inventory Report

Follow these steps to create a new inventory report.

Note Some of these steps or options are not required for every report.

Step 1 Choose **Reports > Inventory Reports**. The Inventory Reports page appears.

Step 2 Click on one of the report types summarized under Inventory Reports (left-side).

Step 3 Choose **New** from the Select a command drop-down menu and click **GO**. The two-tabbed entry panel appears.

Step 4 Specify a report title.

Step 5 Click the **Schedule** tab to complete the scheduling process. Refer to the "Accessing the Schedule Panel" section on page 15-4.

Mesh Reports

Mesh reports are used to analyze and diagnose mesh networks. In the left sidebar menu, all of the mesh report options are listed.

Note The mesh reports do not show the status of autonomous access points.

The following reports can be generated for 1510 mesh access points.

- Mesh Alternate Parent–Lists the number of alternate parents available for a mesh access point. A value of zero (0) indicates the mesh access point has no alternate parents.

- Mesh Link Stats–Lists link statistics for a mesh access point such as packets transmitted, packet error rate, parent changes, SNR, and hops from the root access point.
- Mesh Node Hops–Lists the number of hops between a mesh access point and its root access point.
- Mesh Packet Error Statistics–Notes the percentage of packet errors for packets transmitted by the neighbor mesh access point. Packet error rate percentage = 1- (number of successfully transmitted packets/number of total packets transmitted).
- Mesh Packet Queue Statistics–Generates a graph of packet queue statistics for each access point selected and for each report type selected. The report types are Packet Queue Average, Packets Dropped Per Minute, and Packet Dropped Count. The Packet Queue Average report shows the average number of packets for each queue when the MIB was polled. The Packets Dropped Per Minute report shows the number of packets dropped since the last sample divided by the number of minutes since the sample. The Packet Dropped Count contains the counter for the number of packets dropped.
- Mesh Packet Statistics—Generates a graph of the total number of packets transmitted and the total number of packets successfully transmitted by the neighbor mesh access point.
- Mesh Stranded APs—Displays any potentially stranded access points. A stranded access point is one listed as a mesh neighbor but not currently joined with a controller or one joined with a controller known by WCS but no longer seen by a mesh neighbor. The report displays all current access points believed to be stranded and lists the current detecting access points (the last set of access points detecting the device when the access point is not seen by any mesh neighbor). The report also displays the state of the stranded access point. As determined by WCS, the three states are:
  - Detected and Never Associated: An access point which has never joined a controller and is being detected as a neighbor.
  - Not Detected and Previously Associated: An access point which has associated to a controller at one time but is no longer associated. No mesh access points are detecting this access point as a neighbor.
  - Detected and Not Associated: An access point which has associated to a controller at one time but is no longer associated. A neighbor access point is detecting this access point.
- Mesh Worst Node Hops–Lists mesh access points by name and MAC address and notes those that are 10 hops (default) away from the root access point. Number of hops can be modified.
- Mesh Worst SNR Links–Lists the10 (default) mesh access point-to-neighbor links that exhibit the worst signal-to-noise ratio (SNR). You can change the number of links to display.

Viewing or Modifying Mesh Reports

Follow these steps to view or modify existing inventory reports.

Step 1 Choose **Reports > Mesh Reports**. The Mesh Reports page appears.

Step 2 Choose the Mesh Report type from the left panel.

Step 3 Define (or modify) the conditions for the report in the General panel.

Step 4 Refer to the "Accessing the Schedule Panel" section on page 15-4 to complete the scheduling process.

Creating a New Mesh Report

Follow these steps to create a new mesh report.

Note Some of these steps or options are not required for every report.

Step 1 Choose **Reports > Mesh Reports**. The Mesh Reports page appears.

Step 2 Click on one of the report types summarized under Mesh Reports (left-side).

Step 3 Select **New** from the Select a command menu. Click **GO**. The two-tabbed entry panel appears.

Step 4 Specify a report title.

Step 5 If you want to report more items than the default setting, enter a new value. For example, you could enter a new value at the Mesh Worst SNR Links field which is currently configured by default to report the 10 worst links.

Step 6 Specify if you want the report listed by controller, floor area, outdoor area, AP by floor, AP by outdoor area, or SSID. The floor area and outdoor area report generates the report on an area basis while the AP by floor or AP by outdoor area generates the report on a per-access point basis.

Step 7 If you chose controller, you need to enter a controller IP address.
If you chose floor area or AP by floor area, you need to enter the campus, building, and floor location.
If you chose outdoor area or AP by outdoor area, you need to enter the campus and outdoor area.

Step 8 If necessary, enter which access points to include in the report.

Step 9 Select the neighbor type and display option (table or graph).

Step 10 At the Graph Type parameter, choose either packet count or packets per minute.

Step 11 Enter the reporting period for the report. You can define the report to collect data for an hourly or weekly period or select a specific date and time range for reporting.

Note Hours are defined on a 24-hour basis rather than a 12-hour basis with AM and PM. For example, select hour 13 for 1 PM.

Step 12 Click the **Schedule** tab to complete the scheduling process. Refer to the "Accessing the Schedule Panel" section on page 15-4.

Performance Reports

In the left sidebar menu, all of the performance report options are listed.

Note Performance reports do not show the status of autonomous access points.

The choices are as follows:

- 802.11 Counters Report—Shows counters for the access points at the MAC layer such as error frames, fragment counts, RTS/CTS frame count, and retried frames which can help interpret performance at the MAC layer.

- Controller Utilization Report— Shows utilization based on metrics such as but not limited to CPU usage, memory usage, link utilization, radio utilization, and overall network utilization of the devices (controllers, access points, mobility service engines) on your network based upon filtering criteria selected at the time of report generation. These statistics help identify current network performance and assist with capacity planning for scalability needs.
- Coverage Hole Summary Report—Identifies where the potential coverage holes occur in your network. If a certain spot recurs more than others, you can tweak the RRM settings or place additional access points. The data that is returned includes but is not limited to the following: the base radio MAC address of the alarming access point, the radio type, and the coverage threshold.
- Location Server Utilization—Shows utilization based on metrics such as but not limited to CPU usage, memory usage, link utilization, radio utilization, and overall network utilization of the devices (controllers, access points, mobility service engines) on your network based upon filtering criteria selected at the time of report generation. These statistics help identify current network performance and assist with capacity planning for scalability needs..
- Radio Utilization Report—Shows utilization based on metrics such as but not limited to CPU usage, memory usage, link utilization, radio utilization, and overall network utilization of the devices (controllers, access points, mobility service engines) on your network based upon filtering criteria selected at the time of report generation. These statistics help identify current network performance and assist with capacity planning for scalability needs.
- Tx Power Level and Channel Report—Shows the channel plan assignment and transmit power level trends of the devices based on the filtering criteria used at the time of report generation. The trending of power levels and channel plan assignments help identify abnormal behavior and provide an outlook into how the wireless network has been performing. The data that is returned includes but is not limited to the following: the transmit power level for 802.11a/n and 802.11b/g/n interfaces, the channel number used for 802.11a/n and 802.11b/g/n interfaces, and the grouping types.
- Voice Statistics Report—Helps analyze the wireless network usage from a voice perspective. It presents details such as percentage of bandwidth used by voice clients, voice calls, roaming calls, and rejected calls per radio on the network. Voice client need CAC support to gather useful data from this report.

Viewing or Modifying Performance Reports

Follow these steps to view or modify existing performance reports.

Step 1 Choose **Reports > Performance Reports**. The Performance Reports page appears.

Step 2 Choose the Performance Report type from the left panel.

Step 3 Define (or modify) the conditions for the report in the General panel.

Step 4 Refer to the "Accessing the Schedule Panel" section on page 15-4 to complete the scheduling process.

Step 5 Click the **History** tab if you want to review details of the current and past runs of the report.

Creating a New Performance Report

Follow these steps to create a new performance report.

Note Some of these steps or options are not required for every report.

Step 1 Choose **Reports > Performance Reports**. The Performance Reports page appears.

Step 2 Click on one of the report types summarized under Performance Reports (left-side).

Step 3 Choose **New** from the Select a command drop-down menu and click **GO**. The two-tabbed entry panel appears.

Step 4 Specify a report title.

Step 5 Specify if you want the report listed by controller, floor area, outdoor area, AP by floor, AP by outdoor area, or SSID. The floor area and outdoor area report generates the report on an area basis while the AP by floor or AP by outdoor area generates the report on a per-access point basis.

Step 6 If you chose controller, you need to enter a controller IP address.
If you chose floor area or AP by floor area, you need to enter the campus, building, and floor location.
If you chose outdoor area or AP by outdoor area, you need to enter the campus and outdoor area.

Step 7 If necessary, enter which access points or location server to include in the report.

Step 8 Specify if you want to include 802.11a/n or 802.11b/g/n radios.

Step 9 Enter the reporting period for the report. You can define the report to collect data for an hourly or weekly period or choose a specific date and time range for reporting.

Step 10 Click the **Schedule** tab to complete the scheduling process. Refer to the "Accessing the Schedule Panel" section on page 15-4.

Security Reports

In the left sidebar menu, all of the security report options are listed. The security reports display information about the security of the wireless network.

Note Security reports do not show the status of autonomous access points.

The choices are as follows:

- New Rogue APs—Displays, in tabular form, all rogues detected in a selected timeframe. It provides which new rogues were detected within a selected time. The created time indicates the time at which the rogue was first detected.
- New Rogue AP Count—Displays, in graphical form, all rogues detected in a selected timeframe.
- Rogue APs—Displays all rogues that are active in your network and have been updated in the selected timeframe. WCS receives updated events for rogues that are detected
- Rogue APs Event—Displays all the events received by WCS. The controller sends updates of detected rogues if any of the attributes change or new rogues are detected.

Note This report was formally called the Rogue Detected by AP.

- Rogue Adhocs—Displays all adhocs that have been updated in the selected timeframe.
- Rogue Adhocs Event—Displays all adhoc events that WCS has received in the selected timeframe.
- Security Summary Report— Shows the number of association failures, rogues access points, ad hocs, and access point connections or disconnections over one month.

Viewing or Modifying Security Reports

Follow these steps to view or modify existing security reports.

Step 1 Choose **Reports > Security Reports**. The Security Reports page appears.

Step 2 Choose the Security Report type from the left panel.

Step 3 Define (or modify) the conditions for the report in the General panel.

Step 4 Refer to the "Accessing the Schedule Panel" section on page 15-4 to complete the scheduling process.

Step 5 Click the **History** tab if you want to review details of the current and past runs of the report.

Creating a New Security Report

Follow these steps to create a new security report.

Note Some of these steps or options are not required for every report.

Step 1 Choose **Reports > Security Reports**. The Security Reports page appears.

Step 2 Click on one of the report types summarized under Security Reports (left-side).

Step 3 Choose **New** from the Select a command drop-down menu and click **GO**. The two-tabbed entry panel appears.

Step 4 Specify a report title.

Step 5 Specify if you want the report listed by controller, floor area, outdoor area, AP by floor, AP by outdoor area, or SSID. The floor area and outdoor area report generates the report on an area basis while the AP by floor or AP by outdoor area generates the report on a per-access point basis.

Step 6 If you chose controller, you need to enter a controller IP address.
If you chose floor area or AP by floor area, you need to enter the campus, building, and floor location.
If you chose outdoor area or AP by outdoor area, you need to enter the campus and outdoor area.

Step 7 If necessary, enter which access points or location server to include in the report.

Step 8 Enter the reporting period for the report. You can define the report to collect data for an hourly or weekly period or choose a specific date and time range for reporting.

Step 9 Click the **Schedule** tab to complete the scheduling process. Refer to the "Accessing the Schedule Panel" section on page 15-4.

CHAPTER 16

Administrative Tasks

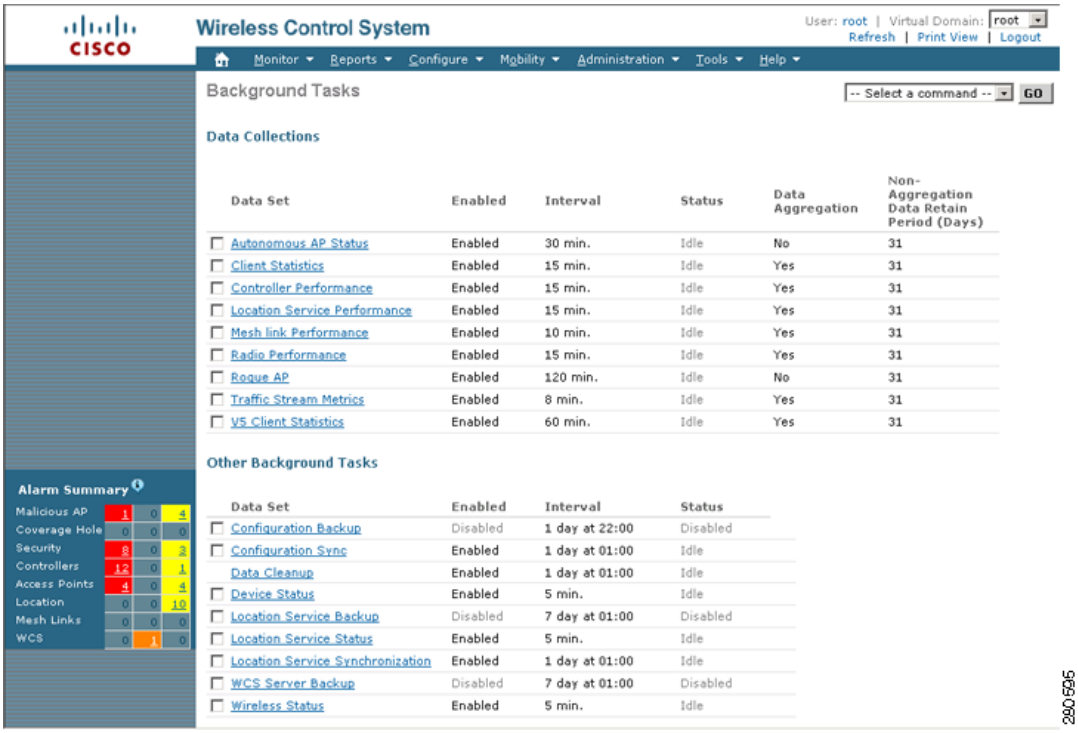
This chapter describes administrative tasks to perform with WCS. These tasks include the following:

- Running Background Tasks, page 16-1 (such as database cleanup, location server synchronization, network audit, server backup)
- Performing a Task, page 16-2
- Importing Tasks Into ACS, page 16-5
- Setting AAA Mode, page 16-16
- Auto Provisioning, page 16-17
- Turning Password Rules On or Off, page 16-23
- Configuring TACACS+ Servers, page 16-23
- Configuring RADIUS Servers, page 16-24
- Establishing Logging Options, page 16-26
- Performing Data Management Tasks, page 16-27
- Establishing Logging Options, page 16-26

Running Background Tasks

Choose **Administration > Background Tasks** to view several scheduled tasks. The Background Tasks window appears (see Figure 16-1).

Figure 16-1 Background Tasks Window



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 menu. 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).

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 16-1).

Step 2 On this window, 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 menu, 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 menu, choose **Enable Collection** and click **GO**. The task converts from grayed out 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 menu, choose **Disable Collection** and click **GO**. The task is grayed out after the disabling is complete.

- View details of a task.

  Click a URL in the Data Set column to view a specific task. The details on that task appear (see the figure in Figure 16-2).

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 what task you choose.

Figure 16-2 Detailed Background Task Window

Step 3 Check the **Admin Status** check box to enable it.

Step 4 In the Max Backups to Keep field, enter the maximum number of backup files to be saved 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 field.

Step 5 In the Interval (Days) field, 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 6 In the Time of Day field, enter the back-up start time. 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 (such as, in the middle of the night).

Step 7 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 16-1).

Step 2 On this window, 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 menu, choose **Execute Now** and click **GO**. You see the status change in the Enabled column.

  <OR>

- Enable the task.

  Click the check box of the task you want to enable. From the Select a command drop-down menu, choose **Enable Task** and click **GO**. The task converts from grayed out to active in the Enabled column.

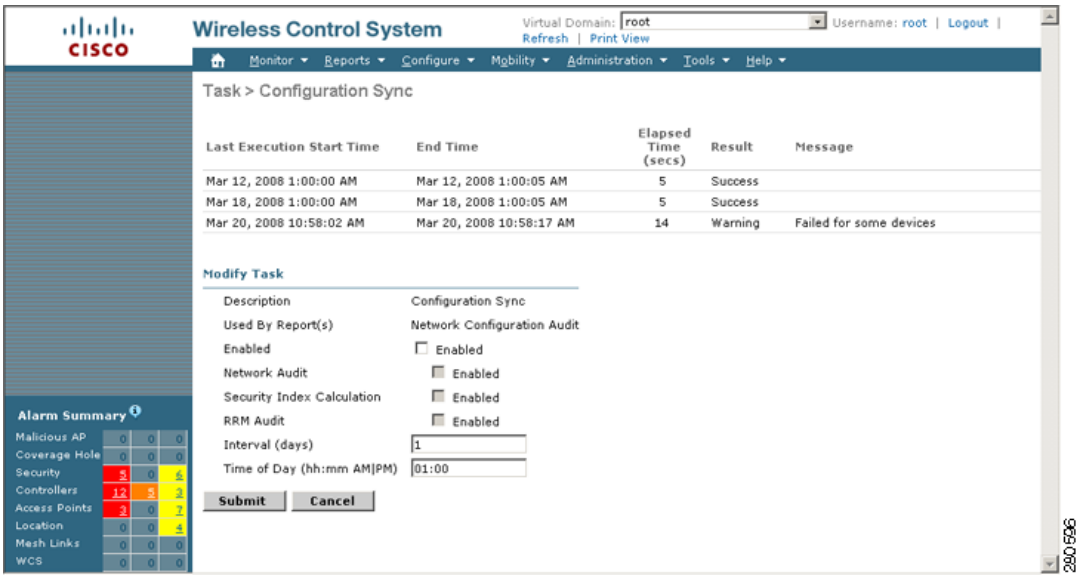
  <OR>

- Disable the task.

  Click the check box of the task you want to disable. From the Select a command drop-down menu, 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 window appears (see Figure 16-3).

Figure 16-3 Task > Configuration Sync



Step 4 In this window 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.**

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).

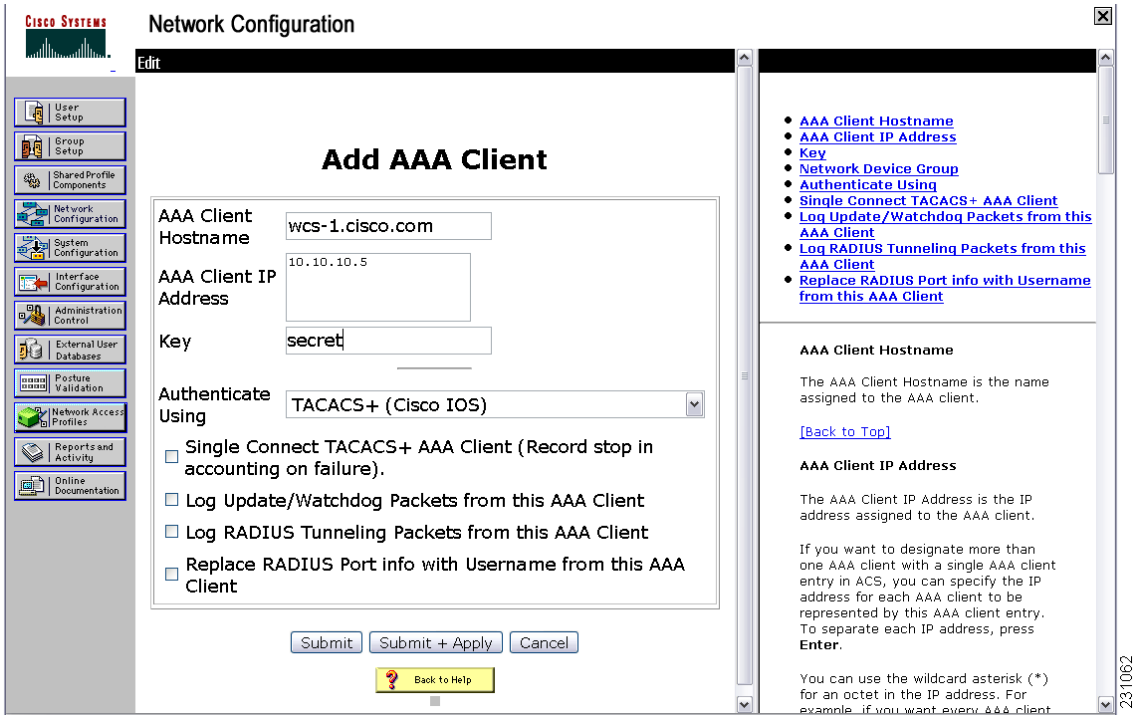
Adding WCS to an ACS Server

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. Refer to the CiscoSecure ACS documentation or the documentation for the vendor you are using.

Step 1 Click **Add Entry** on the Network Configuration window of the ACS server (see Figure 16-4).

Figure 16-4 ACS Server Network Configuration Window



Step 2 In the AAA Client Hostname field, enter the WCS hostname.

Step 3 Enter the WCS IP address into the AAA Client IP Address field.

Step 4 In the Key field, 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 menu.

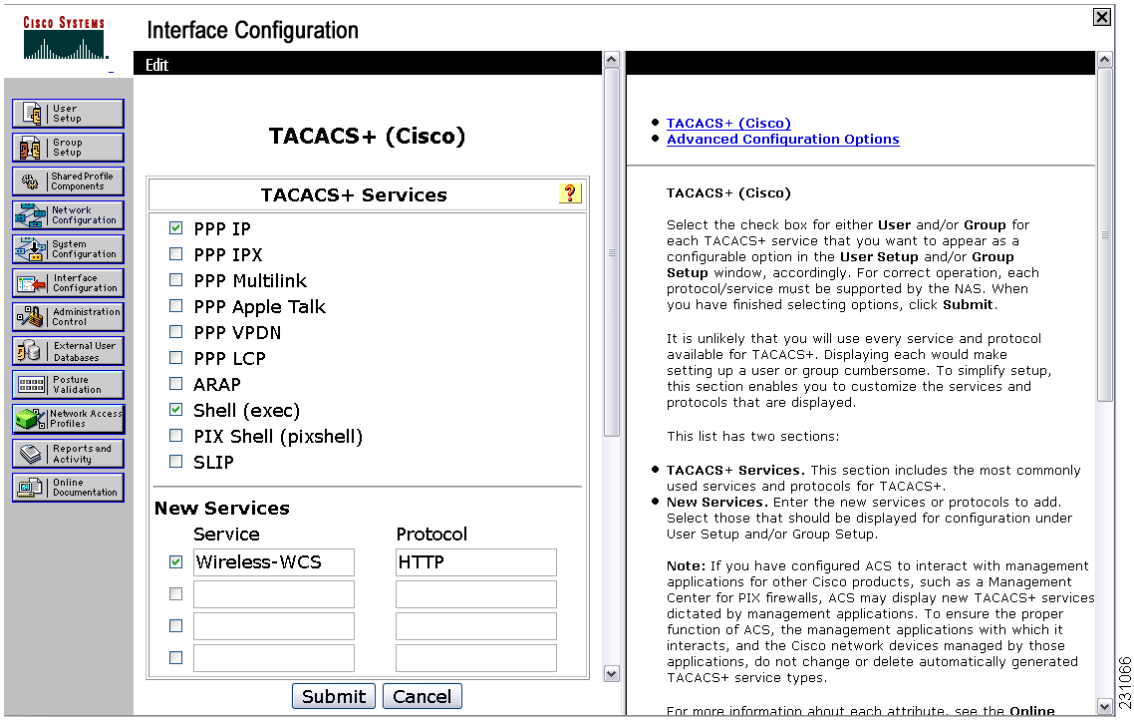
Step 6 Click **Submit + Apply.**

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 window (see Figure 16-5).

Figure 16-5 TACACS+ Cisco IOS Interface Configuration Window



Step 2 In the New Services portion of the window, 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**.

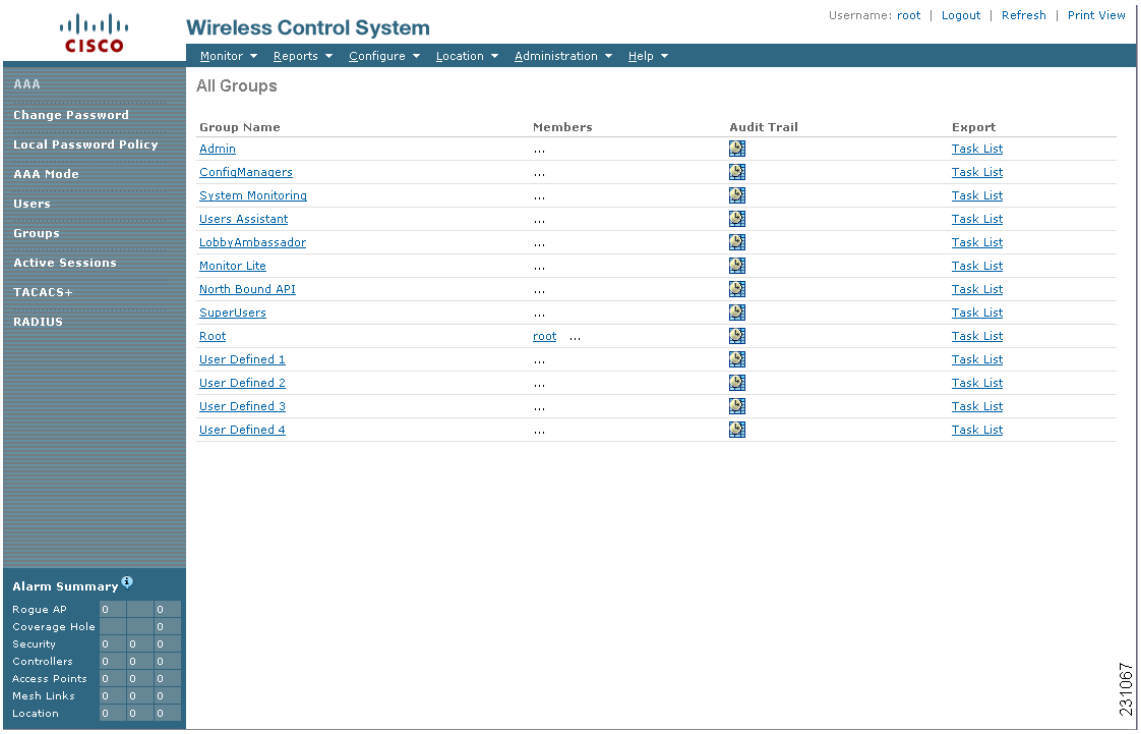
Adding WCS UserGroups into ACS for TACACS+

Follow these steps to add WCS UserGroups into an ACS Server for use with TACACS+ servers.

Step 1 Log into WCS.

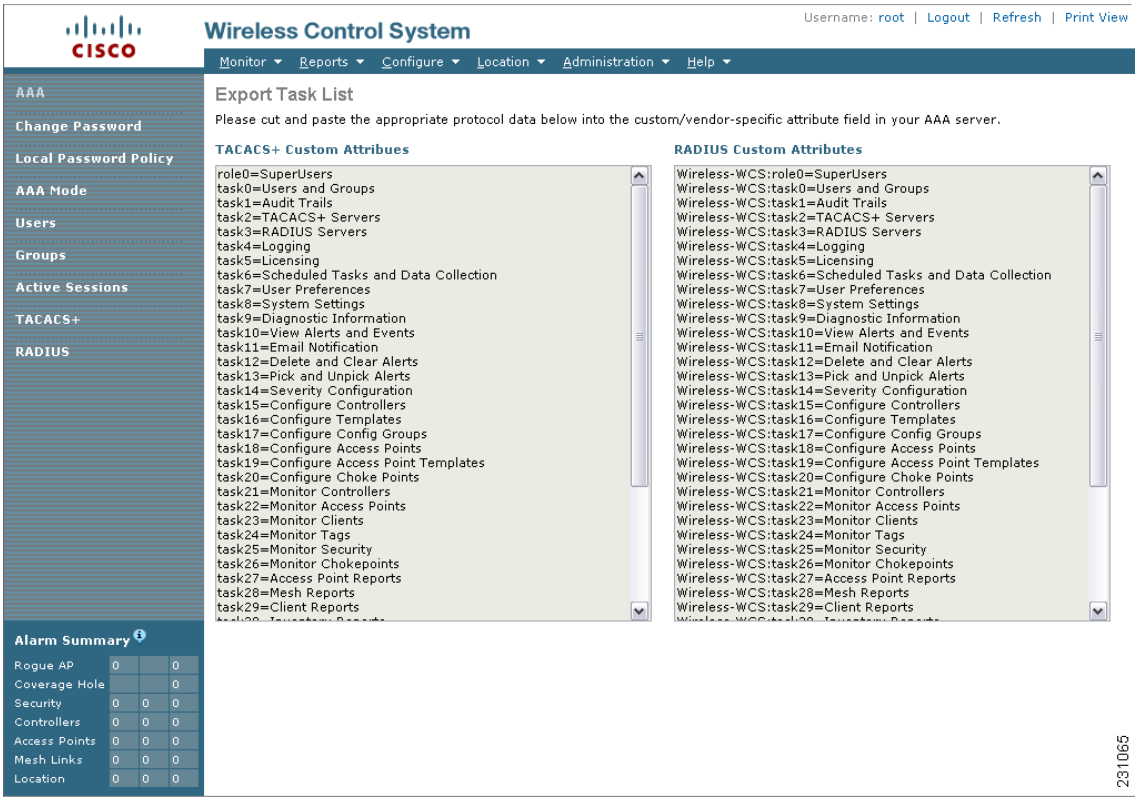
Step 2 Navigate to Administration > AAA > Groups. The All Groups window appears (see Figure 16-6).

Figure 16-6 All Groups Window



Step 3 Click on the Task List URL (the Export right-most column) of the User Group that you wish to add to ACS. The Export Task List window appears (see Figure 16-7).

Figure 16-7 Export Task List Window

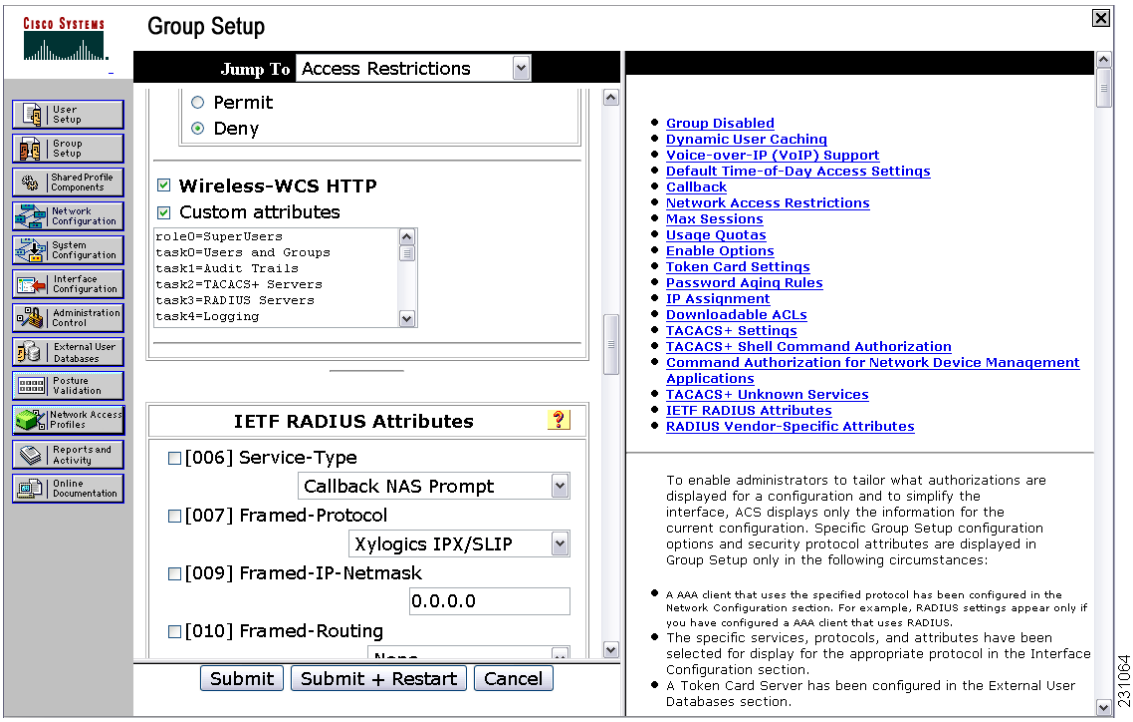


Step 4 Highlight the text inside of the TACACS+ Custom Attributes, go to your browser's menu, and choose Edit > Copy.

Step 5 Log in to ACS.

Step 6 Go to Group Setup. The Group Setup window appears (see Figure 16-8).

Figure 16-8 Group Setup Window 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 field.

Step 9 Click the checkboxes to enable these attributes.

Step 10 Click **Submit + Restart**.

You can now associate ACS users with this ACS group.

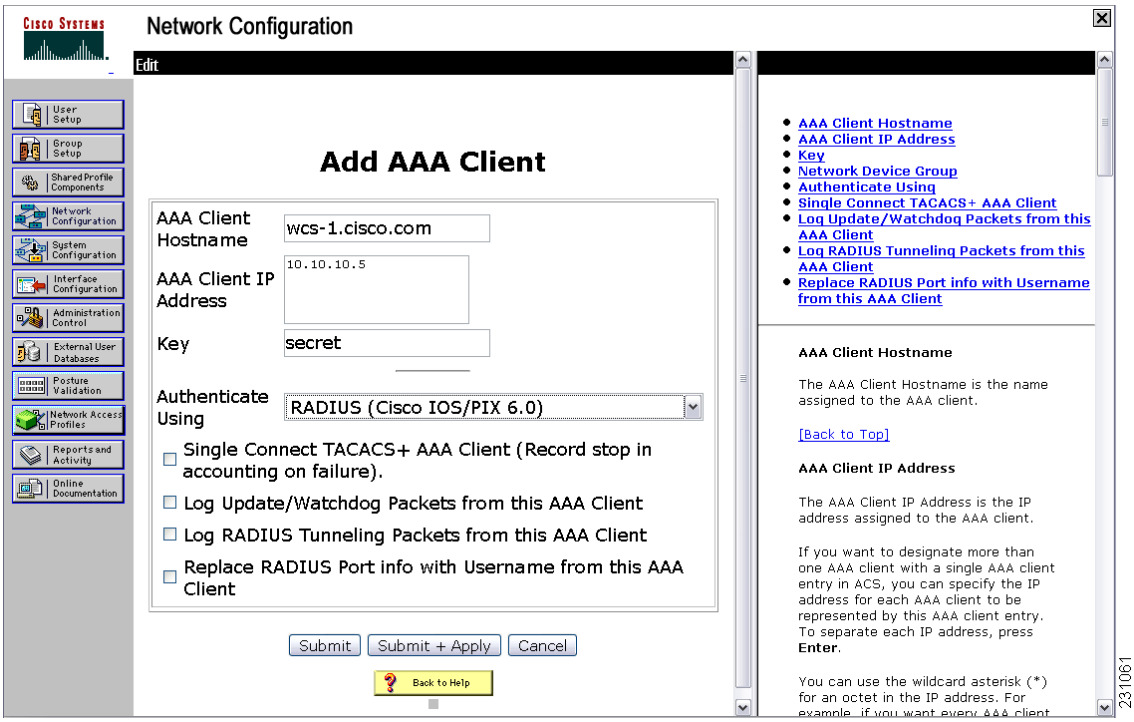
Note To enable TACACS+ in WCS, refer to the "Configuring TACACS+ Servers" section on page 16-23.

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 16-14.

Step 1 Go to Network Configuration on the ACS server (see Figure 16-9).

Figure 16-9 Network Configuration Window on ACS Server



Step 2 Click **Add Entry**.

Step 3 In the AAA Client Hostname field, enter the WCS hostname.

Step 4 In the AAA Client IP Address field, enter the WCS IP address.

Step 5 In the Key field, 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 menu.

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 16-24.

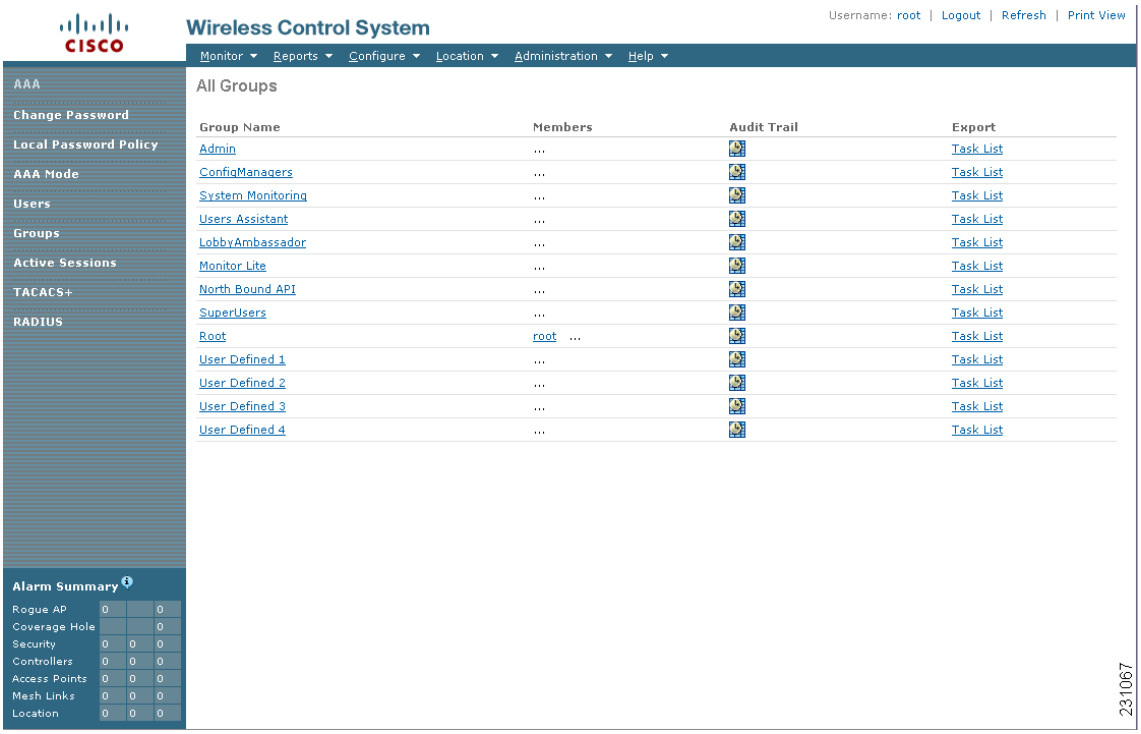
Adding WCS UserGroups into ACS for RADIUS

Follow these steps to add WCS UserGroups into an ACS Server for use with RADIUS servers.

Step 1 Log into WCS.

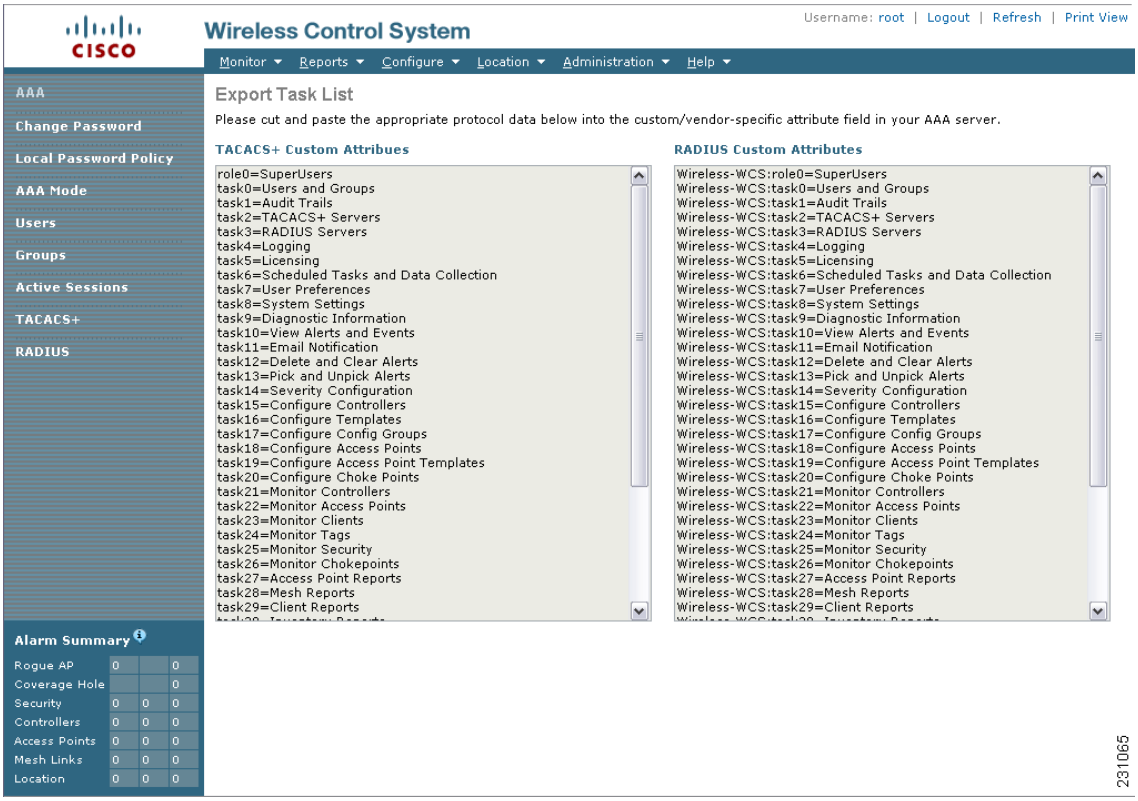
Step 2 Navigate to Administration > AAA > Groups. The All Groups window appears (see Figure 16-10).

Figure 16-10 All Groups Window



Step 3 Click on the Task List URL (the Export right-most column) of the User Group that you wish to add to ACS. The Export Task List window appears (see Figure 16-11).

Figure 16-11 Export Task List Window

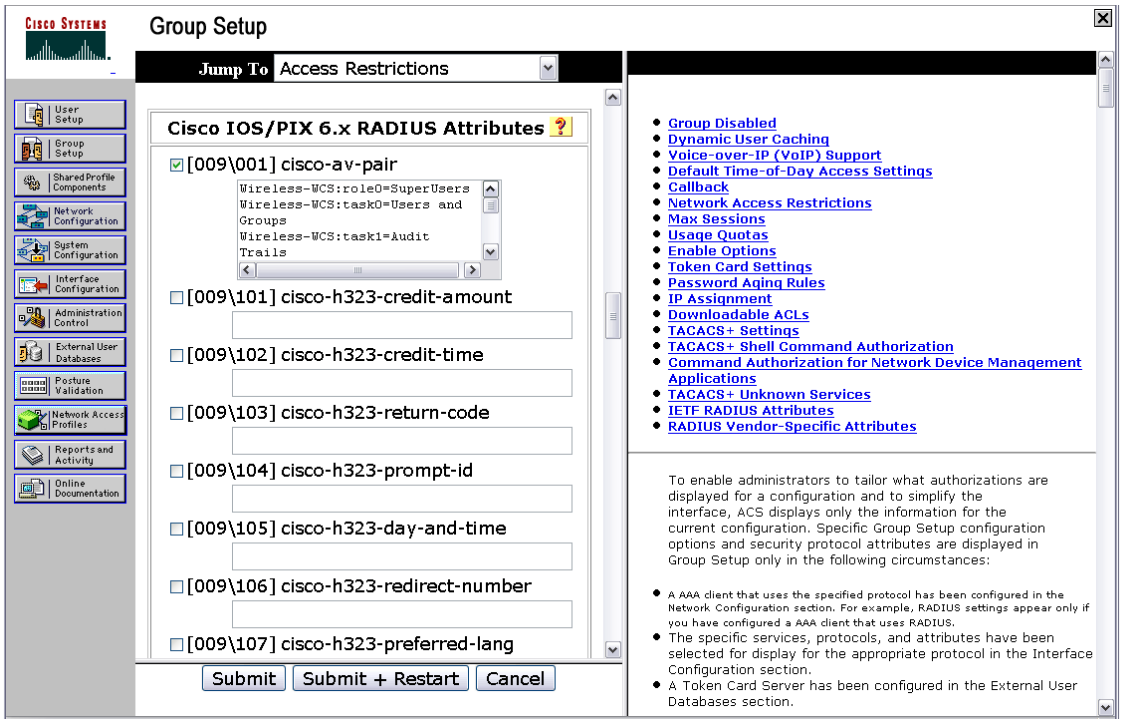


Step 4 Highlight the text inside of the RADIUS Custom Attributes, go to your browser's menu, and choose **Edit > Copy**.

Step 5 Log in to ACS.

Step 6 Go to Group Setup. The Group Setup window appears (see Figure 16-12).

Figure 16-12 Group Setup Window 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 field.

Step 9 Click the checkboxes to enable these attributes.

Step 10 Click **Submit + Restart**.

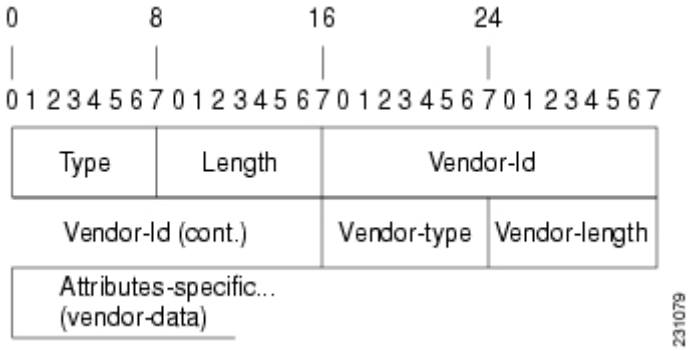
You can now associate ACS users with this ACS group.

Note To enable RADIUS in WCS, refer to the "Configuring RADIUS Servers" section on page 16-24.

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 16-13).

Figure 16-13 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 16-1 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 16-1 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)

Table 16-1 Access=Access Packet Example (continued)

Attribute	Description
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.

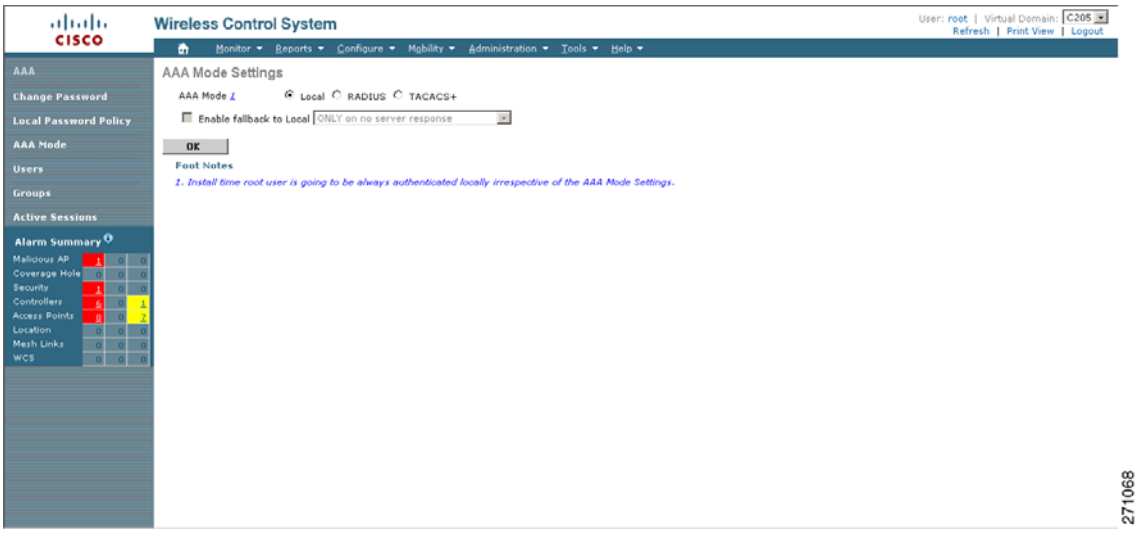
Setting AAA Mode

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 window appears (see Figure 16-14).

Figure 16-14 AAA Mode Settings Window



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 Click the **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. 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 auto provisioning privileges to a user, edit the permitted tasks using the Administration > AAA > Groups > <group name> List of Tasks Permitted section of WCS. Select or deselect the check box to allow or disallow these privileges.

Follow these steps to configure auto provisioning.

Step 1 Choose **Configure > Auto Provisioning**. The Auto Provisioning Filter List window appears (see Figure 16-15).

Figure 16-15 Auto Provisioning Filter List

Step 2 Choose **Auto Provisioning Device Management** from the left sidebar menu. This 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.

Note Auto provisioning startup files generated by WCS are kept in the TFTP root directory. This directory is not backed up as part of the WCS backup; therefore, if data is restored on to another machine, the startup files will not get restored. You must manually backup the TFTP folder to preserve the auto provisioning startup files.

You cannot use a template to replicate the configuration on a second controller during auto provisioning. The dynamic interfaces must be created separately so that any WLAN or AP groups (or any other key format values) that are mapped to dynamic interfaces function as expected. Regardless of which format (ASCII or hexadecimal) you choose, for security reasons, only ASCII is visible on WLC.

Step 3 The Auto Provisioning Filter List window displays the following information:

- Filter Name: 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.

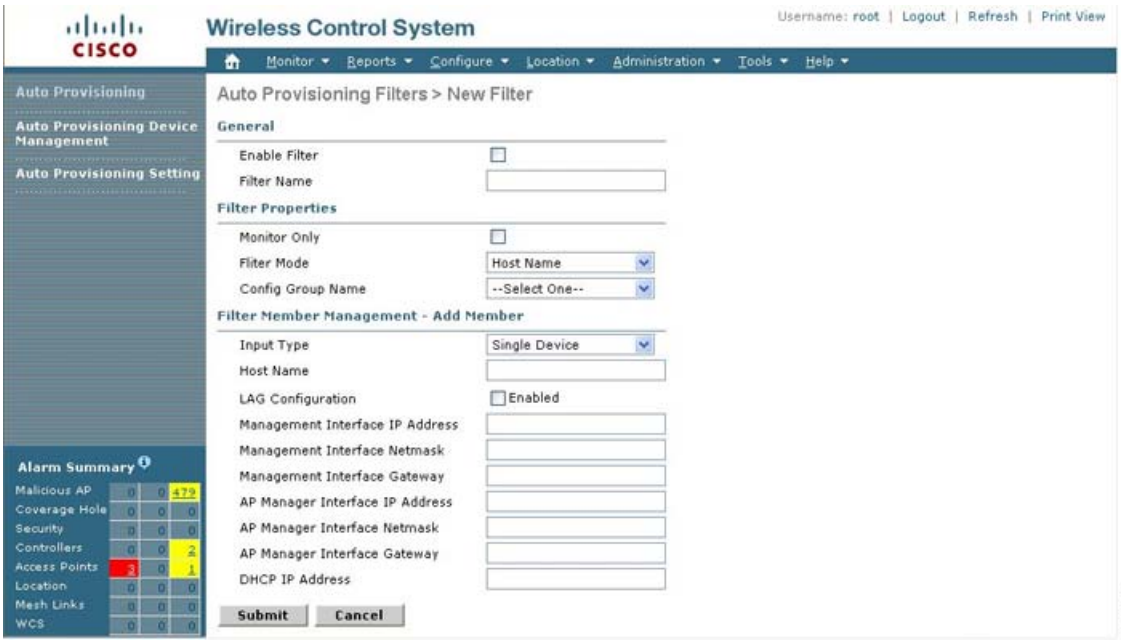
- Filter Mode: Indicates the search mode for this filter (host name, MAC address, or serial number).
- Config Group Name: Indicates the configuration group name.

Step 4 From the Select a command drop-down menu, you can choose to add or delete a filter or list some or all filter device information. If you choose to add a new filter, continue to Step 5.

Step 5 From the Select a command drop-down menu, choose **Add Filter**.

Step 6 Click **GO**. The Auto Provisioning Filters > New Filter window appears (see Figure 16-16).

Figure 16-16 Auto Provisioning Filters > New Filter



Step 7 Configure the following information:

- General
  - Enable Filter: Click the 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: When contacted by WCS during the auto provisioning process, the WLC defined in this filter is managed, but not configured, by WCS.
  - Filter Mode: From the drop-down menu, choose **Host Name**, **MAC Address**, and **Serial Number** to indicate the search mode for this filter.
  - Config Group Name: From the drop-down menu, choose a **Config Group Name**.

Note An empty config group with no controllers defined must be created so that all config groups appear in the drop-down list.

- Filter Member Management - Add Member
  - Input Type: From the drop-down menu, choose **Single Device** or **CSV file**.

    If Single Device is selected, enter the Host Name, Management Interface IP Address, Management Interface Netmask, Management Interface Gateway, LAG, AP manager interface IP address, AP manager interface network mask, AP manager interface gateway IP address, and DHCP information.

If CSV File is chosen, enter the CSV file or use the **Browse** button to navigate to the applicable CSV File. An example of a valid CSV file (with MAC address filter mode) is as follows:

```
deviceId, LAG, managementIP, managementNetmask, managementGateway, apManagerIP,
apManagerNetmask, apManagerGateway, dhcpServerIP
00:0B:85:46:F2:60, true, 1.9.116.39, 255.255.255.0, 1.9.116.1, 2.9.116.39,
255.255.255.0, 2.9.116.1, 2.9.116.250
00:0B:85:46:F2:61, true, 1.9.116.40, 255.255.255.0, 1.9.116.1, 2.9.116.40,
255.255.255.0, 2.9.116.1, 2.9.116.250
00:0B:85:46:F2:62, false, 1.9.116.41, 255.255.255.0, 1.9.116.1, 2.9.116.41,
255.255.255.0, 2.9.116.1, 2.9.116.250
00:0B:85:46:F2:63, false, 1.9.116.42, 255.255.255.0, 1.9.116.1, 2.9.116.42,
255.255.255.0, 2.9.116.1, 2.9.116.250
00:0B:85:46:F2:64, false, 1.9.116.43, 255.255.255.0, 1.9.116.1, 2.9.116.43,
255.255.255.0, 2.9.116.1, 2.9.116.250
```

The first line in the CSV file must be keyword “deviceId, LAG, managementIP, managementNetmask, managementGateway, apManagerIP, apManagerNetmask, apManagerGateway, dhcpServerIp.”

Each of the following lines should contain nine tokens as follows, separated by commas:

1st token can be host name, MAC address, or serial number depending on the selected filter mode.

2nd token is the controller’s LAG configuration (true/false).

3rd token is the controller’s management interface IP address.

4th token is the controller’s management interface network mask.

5th token is the controller’s management interface gateway IP.

6th token is the controller’s AP Manager interface IP address.

7th token is the controller’s AP Manager interface network mask.

8th token is the controller’s AP Manager interface Gateway IP.

9th token is the controller’s DHCP IP address.

- 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 8 Click **Submit**.

Viewing Detailed Auto Provisioning Device Information

To view detailed information about auto provisioning devices, choose **List Filters Device Info** or **List All Filters Device Info** from the Select a command drop-down menu. The Detailed Auto Provisioning Device window appears (see Figure 16-17). The filter name, its device ID, and the IP address, netmask, and gateway address are provided.

The status displays as idle, trap received, failed in trap processing, failed in applying templates, failed in discovery switch, managed, managed partially applied templates, or unknown error.

Figure 16-17 Detailed Auto Provisioning Device Information

Editing a Current Auto Provisioning Filter

Follow these steps to edit a current auto provisioning filter.

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.

Step 4 Click **Submit**.

Deleting an Auto Provisioning Filter

Follow these steps to delete an auto provisioning filter.

Step 1 Choose **Configure > Auto Provisioning**.

Step 2 Choose the check box of the file you want to delete.

Step 3 From the Select a command drop-down menu, choose **Delete Filter(s)**.

Step 4 Click **GO**.

Step 5 Click **OK** to confirm the deletion.

Viewing Details of an Auto Provisioned Filter

To view details for an individual auto provisioning filter, follow these steps:

Step 1 Choose **Configure > Auto Provisioning**.

Step 2 Choose the check box of the filter you want to view.

Step 3 From the Select a command drop-down menu, choose **List Filter(s) Device Info**.

Step 4 Click **GO**.

The following information is provided for the selected filter.

Table 16-2 List Filter(s) Device Information

Parameter	Description
Filter Name	Indicates the filter name.
Device ID	Indicates the device ID.
Interface IP	Indicates the management interface IP address of the controller.
Interface Netmask	Indicates the netmask mask of the management interface of the controller.
Interface Gateway	Indicates the netmask gateway of the management interface of the controller.
Status	
Timestamp	

Setting Auto Provisioning

The Primary Search Key Setting provides the ability 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**. The Auto Provisioning Primary Search Key Setting appears.

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

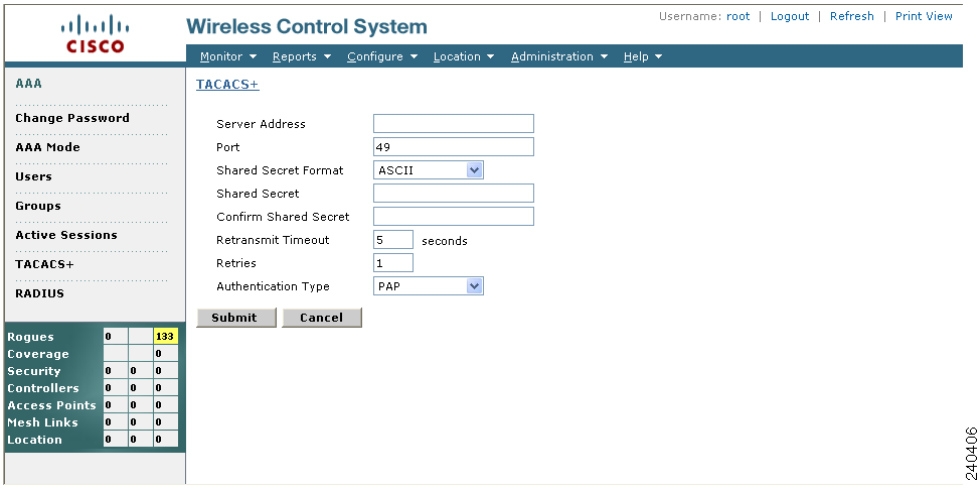
This section describes how to add and delete TACACS+ servers. TACACS+ servers provide an effective and secure management framework with built-in failover mechanisms. If you want to make configuration changes, you must be authenticated.

Note In order to activate TACACS+ servers, you must enable them as described in the "Importing Tasks Into ACS" section on page 16-5.

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **TACACS+**. The TACACS+ window appears (see Figure 16-18).

Figure 16-18 TACACS+ Window



Step 3 The TACACS+ window 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 menu in the upper right-hand corner to add or delete TACACS+ servers. You can click on 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 menu 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 field.

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 menu, choose a protocol: PAP or CHAP.

Step 11 Click **Submit**.

Configuring RADIUS Servers

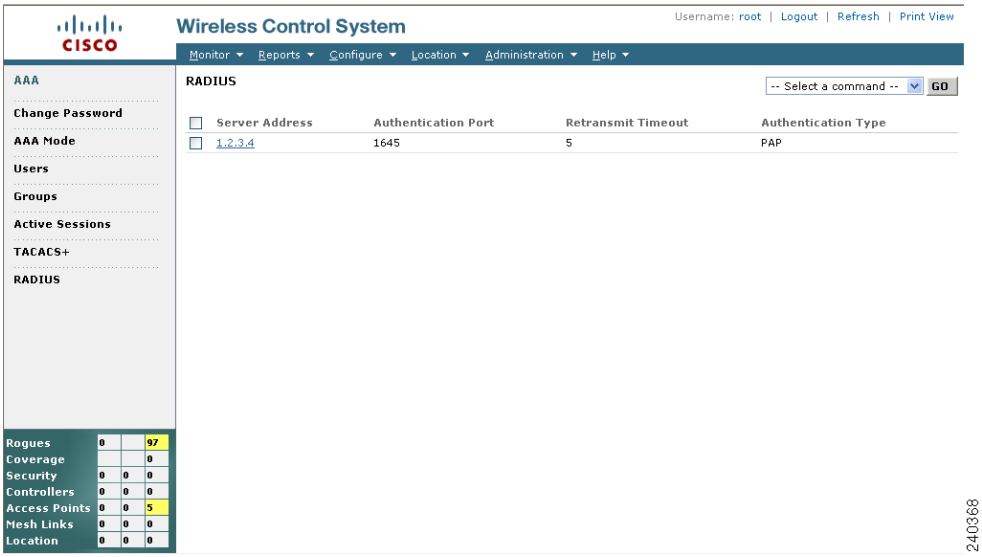
This section describes how to add and delete RADIUS servers. You must enable RADIUS servers and have a template set up for them in order to make configuration changes.

Note In order to activate RADIUS servers, you must enable them as described in the "Importing Tasks Into ACS" section on page 16-5.

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **RADIUS**. The RADIUS window appears (see Figure 16-19).

Figure 16-19 RADIUS Window

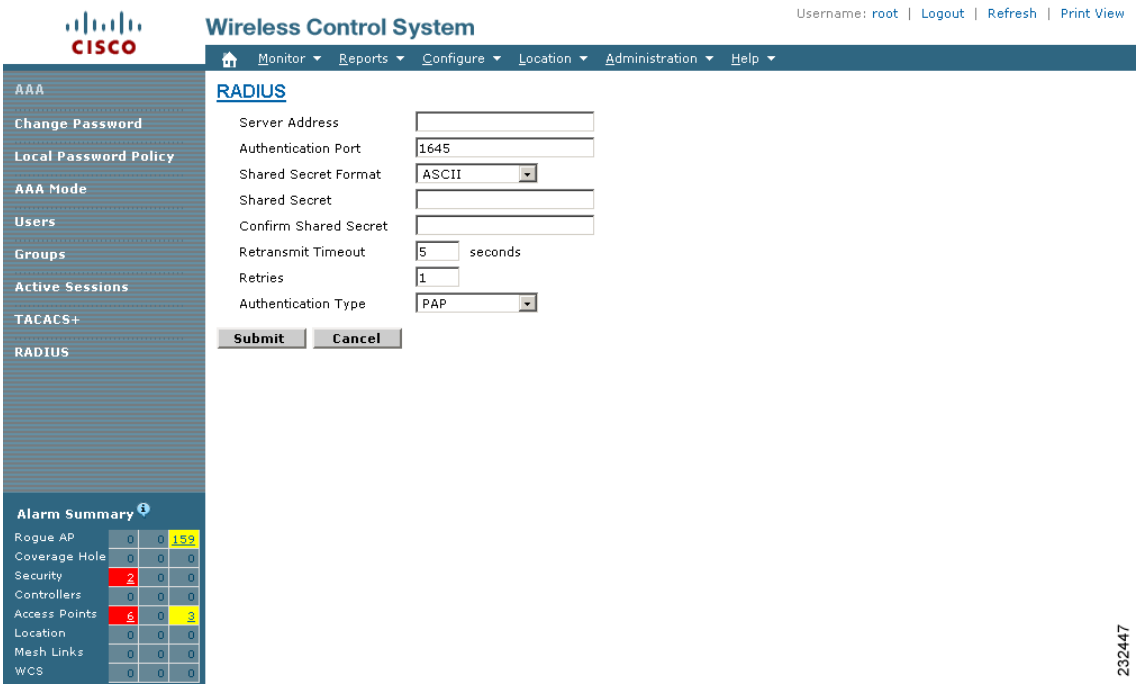


Step 3 The RADIUS window shows the server address, authentication port, retransmit timeout value, and authentication type for each RADIUS server that is configured. The RADIUS servers are tried based on how they were configured.

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 menu in the upper right-hand corner to add or delete RADIUS servers. You can click on an IP address if you want to make changes to the information. When you click on a particular IP address, the window shown in Figure 16-20 appears.

Figure 16-20 RADIUS Server Detailed Window



Step 5 The current authentication port is displayed. Use the drop-down menu 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 field.

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 menu, choose a protocol: PAP or CHAP.

Step 11 Click **Submit**.

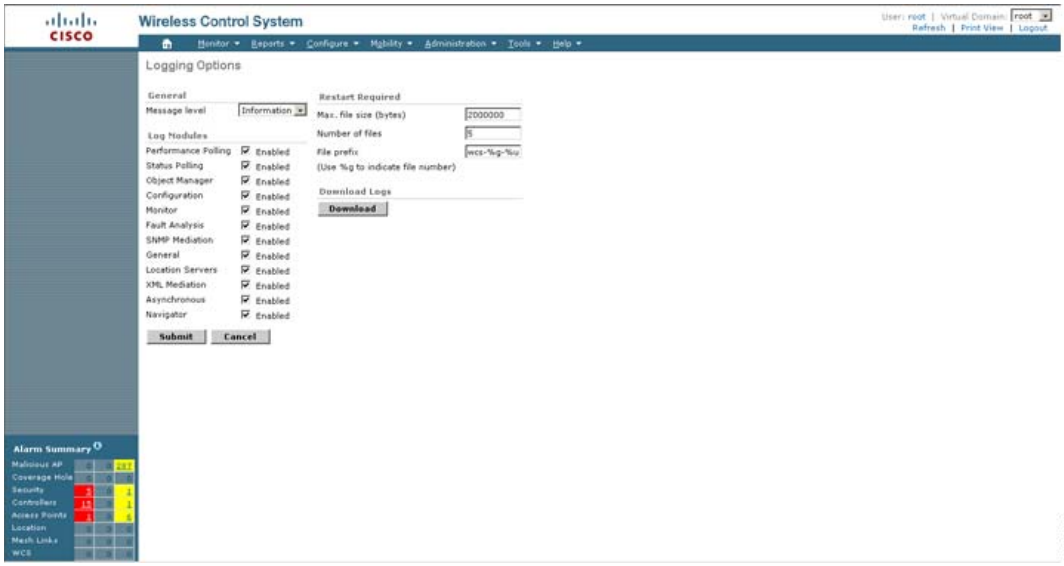
Establishing Logging Options

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 window.

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 16-21).

Figure 16-21 Logging Options Window



Step 2 Choose a message level option of Trace, Information, or Error in the General portion of the window.

Step 3 Click the check boxes within the Log Modules portion of the window to enable various administration modules (such as performance, status, object, configuration, monitor, fault analysis, SNMP mediation, general, location servers, XML mediation, asynchronous, and portal).

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.

Performing Data Management Tasks

Within the Settings window, you can determine what data to generate for reports and e-mails. Choose **Administration > Settings** in the left sidebar menu. Three choices appear.

- Refer to the "Data Management" section on page 16-28 to establish trends for hourly, daily, and weekly data periods.
- Refer to the "Report" section on page 16-29 to designate where the scheduled reports will reside and for how long.
- Refer to the "Mail Server" section on page 16-29 to set the primary and secondary SMTP server host and port.
- Refer to the "Login Disclaimer" section on page 16-31 to enter disclaimer information.
- Refer to the "Alarms" section on page 16-31 to specify how to handle old alarms and how to display assigned and acknowledged alarms in the Alarm Summary window.
- Refer to the "Client" section on page 16-32 to enable client troubleshooting on a diagnostic channel.
- Refer to the "Severity Configurations" section on page 16-32 to configure the severity level for newly-generated alarms.

- Refer to the "Notification Receiver" section on page 16-32 to configure parameters for notification support of guest access functionality.
- Refer to the "SNMP Settings" section on page 16-33 to configure global SNMP settings from WCS.
- Refer to "Audit" section on page 16-34 to configure audit information.
- Refer to the "Auto Refresh" section on page 16-34 for information on controller upgrade settings.

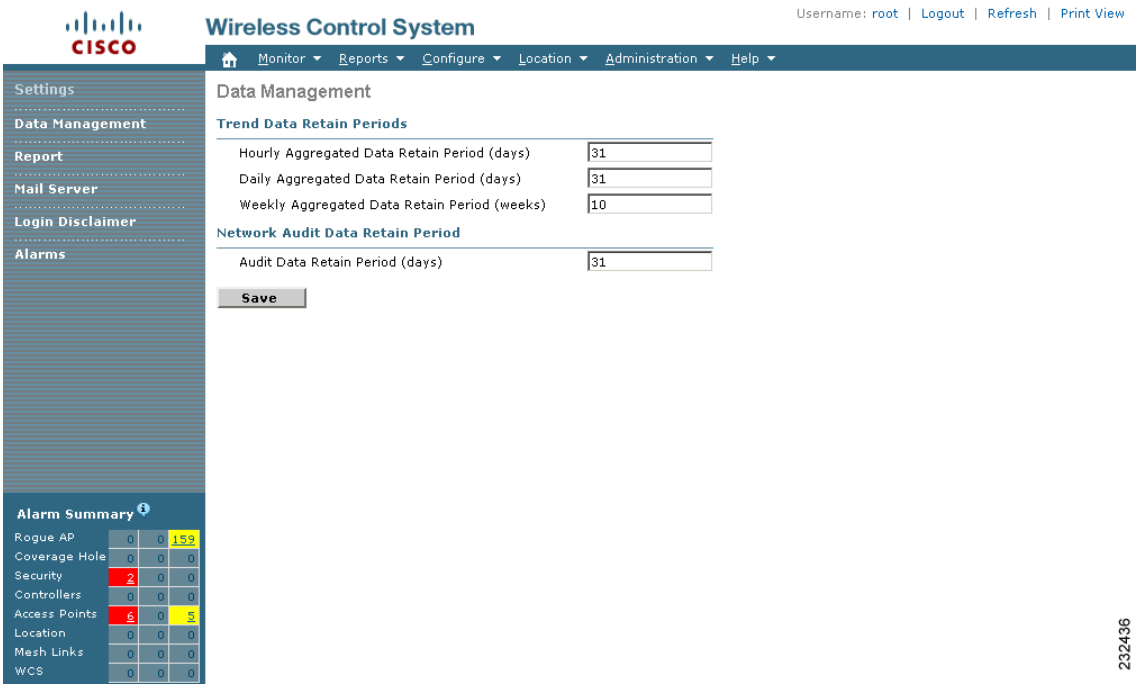
Data Management

Follow the steps below to manage data aggregation 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 window appears (see Figure 16-22).

Figure 16-22 Data Management Window



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 31.

Step 5 Specify the number of weeks to keep the weekly data. The valid range is 2 to 10.

Step 6 Specify the number of days to retain the audit data 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**.

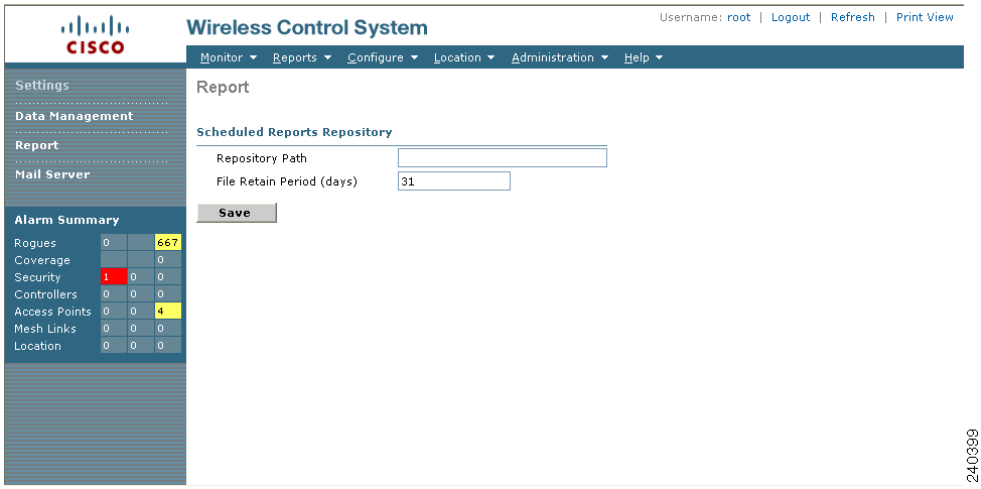
Report

Follow the steps below 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 window appears (see Figure 16-23).

Figure 16-23 Report Window



Step 3 Enter the location on the WCS server where you want the scheduled reports to reside on the server.

Step 4 Specify the number of days the file will stay in the repository.

Step 5 Click **Save**.

Mail Server

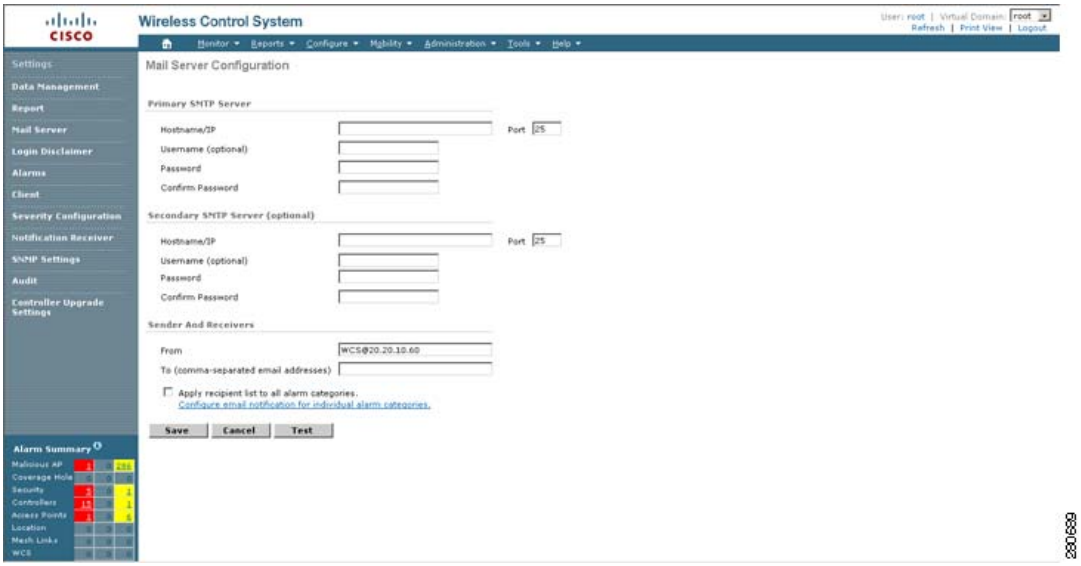
You can configure global e-mail parameters to use when sending e-mails from WCS reports, alarm notifications, and so on. This mail server page allows you to configure e-mail parameters at a single place to avoid re-entering the information each time you need it. The Mail Server window allows you to set the primary and secondary SMTP server host and port, the sender's e-mail address, and the recipient's e-mail address(es). 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**.

From the left sidebar menu, choose **Mail Server**. The window in Figure 16-24 appears.

Figure 16-24 Mail Server Configuration Window



The Mail Server window allows you to set the primary and secondary SMTP server host and port, the sender's e-mail address, and the recipient's e-mail address. From this window, you can configure e-mail parameters without having to visit multiple places.

You must designate the primary mail server, and the secondary one is used only if the primary fails. SMTP authorization is also supported for both primary and secondary mail servers. Follow the steps below to configure the mail server.

Step 1 Enter the host name of the primary SMTP server.

Step 2 The SMTP port is set to 25 by default, but you can change it if your mail server is using a non-default port.

Step 3 Enter the designated username if SMTP authorization is turned on for this mail server.

Step 4 Provide a password for logging on to the SMTP server and enter it for the Password and Confirm Password parameter.

Step 5 Provide the same information for the secondary SMTP server (only if a secondary mail server is available). The secondary server is used only if the primary fails.

Step 6 The From field in the Sender and Receivers portion of the window is populated with *WCS@<WCS server IP address>*. You can change it to a different sender.

Step 7 Enter the recipient's e-mail address(es) in the To field. The e-mail address you provide serves as the default values for other functional areas, such as alarms or reports. Multiple e-mail addresses can be added and should be separated by a comma.

Note If you make global changes to the recipient e-mail address(es) in Step 7, they are disregarded if e-mail notifications were set.

You are required to set the primary SMTP mail server and the From address fields.

Step 8 Click the **Test** button to send a test e-mail using the parameters you configured. The results of the test operation are shown 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 9 If the test results were satisfactory, 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**.

Step 3 Type your Login Disclaimer text in the available text box.

Step 4 Click **Save**.

Alarms

This Alarms page allows you to manage the following:

- The handling of old alarms.
- The display of assigned and acknowledged alarms in the Alarm Summary window.

To access this window, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Alarms**.

Step 3 In the Cleanup of Old Alarms section, check the check box to enable the deletion of old alarms.

Step 4 Enter the number of days after which old alarms are deleted.

Step 5 In the Alarm Summary Window section, check the check box to hide acknowledged and assigned alarms on the Alarm Summary window. This preference applies only to the Alarm Summary window. A quick search or alarms for any entity show alarms regardless of the acknowledged or assigned state specified here. The default is to hide acknowledged alarms.

Client

From the Settings > Client window, you can enable automatic client troubleshooting on a diagnostic channel. Refer to the "WLAN Client Troubleshooting" section on page 6-20 for further information on client troubleshooting. Follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Client**.

Step 3 Choose the **Automatically troubleshoot client on diagnostic channel** check box.

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.

Step 4 Click **Save**.

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 menu, 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.

Notification Receiver

The Notification Receiver page allows you to configure parameters for notification support of guest access functionality.

Follow these steps to configure notification receiver parameters:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Notification Receiver**.

Step 3 Enter the Notification Type parameter including Port Number and Community.

Note The Notification Type automatically defaults to SNMP.

Step 4 Click **Submit** to confirm the Notification Receiver information.

SNMP Settings

The SNMP Settings window allows you to configure global SNMP settings from WCS.

Note Any changes made on this screen take effect globally for WCS and 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**.

Step 3 If Trace Display Values is selected, mediation trace-level logging shows data values fetched from the controller using SNMP. If unchecked, the values do not display.

Note The default is unchecked for security reasons.

Step 4 For the Backoff Algorithm, choose either **Exponential** or **Constant Timeout** from the drop-down menu. 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 unchecked, WCS always uses the timeout and retries specified per-controller or per-IOS access point. The default is checked.

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.

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.

Audit

The Controller Audit Report displays the following information depending on the type of audit selected in Administration > Settings > Audit:

- Applied template discrepancies (Template Based Audit only)
- Config group template discrepancies (Template Based Audit only)
- Total enforcements for config groups with background audit enabled (Template based Audit only)
  - If the total enforcement count is greater than zero, this number appears as a link. Click the link to view a list of the enforcements made from WCS.
- Failed for config groups with background audit enabled (Template Based Audit only)
  - If the failed enforcement count is greater than zero, this number appears as a link. Click the link to view the failures returned from the device.
- Other WCS discrepancies

A current Controller Audit Report can be accessed from the Configure > Controllers window 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 menu in the Configure > Controllers window or by clicking **Audit Now** directly from the Controller Audit report. See the "Viewing Audit Status (for Controllers)" section on page 10-5.

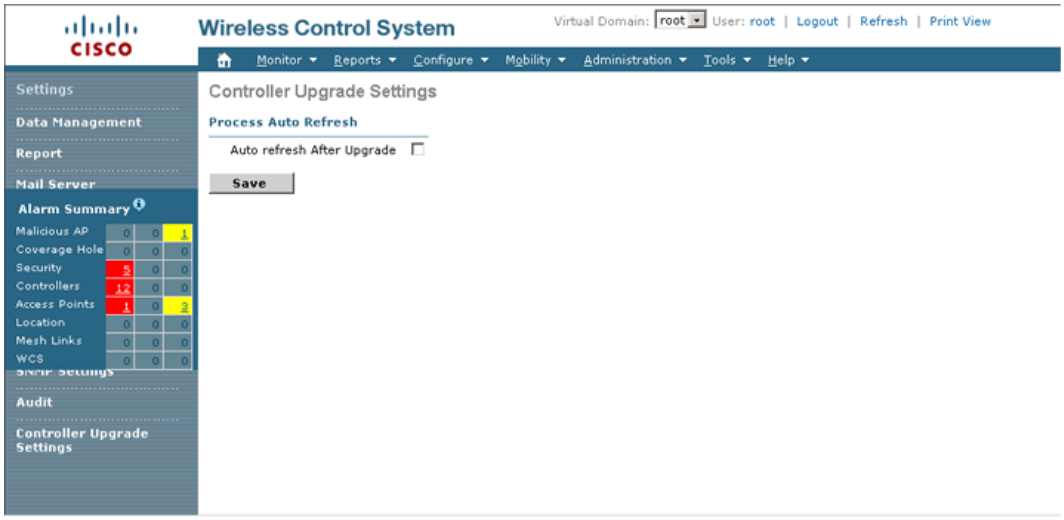
Auto Refresh

The Auto Refresh page allows you to automatically upgrade the controller. Follow these steps to perform an automatic refresh.

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Controller Upgrade Settings** (see Figure 16-25).

Figure 16-25 Controller Upgrade Settings



Step 3 Check the Auto refresh After Upgrade check box to automatically restore the config whenever there is a change in the WLC image.

Step 4 Click **Save**.

Setting User Preferences

This page contains user-specific settings you may want to adjust.

Step 1 Choose **Administration > User Preferences**. The User Preferences Window appears (see Figure 16-26).

Figure 16-26 User Preferences Window

Step 2 Use the Items Per List Page drop-down menu to configure the number of entries shown on a given list window (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 window.

Step 4 Use the drop-down menu to indicate how often you want the alarm count refreshed in the Alarm summary window on the left panel.

Step 5 Click **Save**.

CHAPTER 17

Virtual Domains

A 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 menu 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 Domain 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.

- 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:

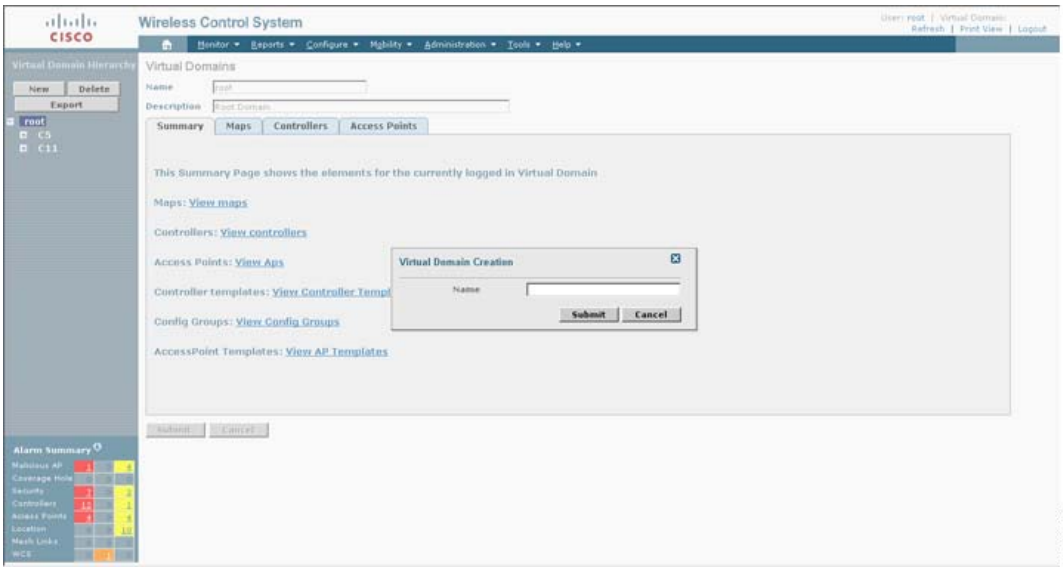
Step 1 Choose **Administration > Virtual Domains**.

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 17-1).

Figure 17-1 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 window 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 **Alarm Email Notifications**—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 adminstrator 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:

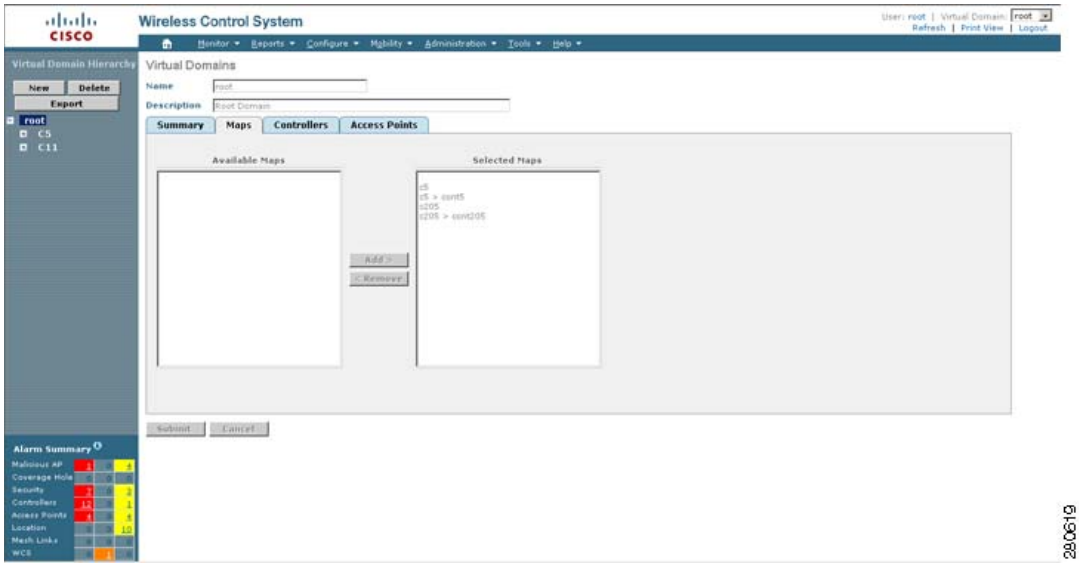
Step 1 Choose **Administration > Virtual Domains**.

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 seconds to load.

Step 3 Choose the applicable Maps, Controller, or Access Points tab (see Figure 17-2).

Figure 17-2 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 window 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 (i.e., tasks, roles, virutal 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 field.

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 16-7 or the "Adding WCS UserGroups into ACS for RADIUS" section on page 16-11.

Understanding Virtual Domains as a User

When you log in, you can access any of the virtual domains that the adminstrator assigned to you.

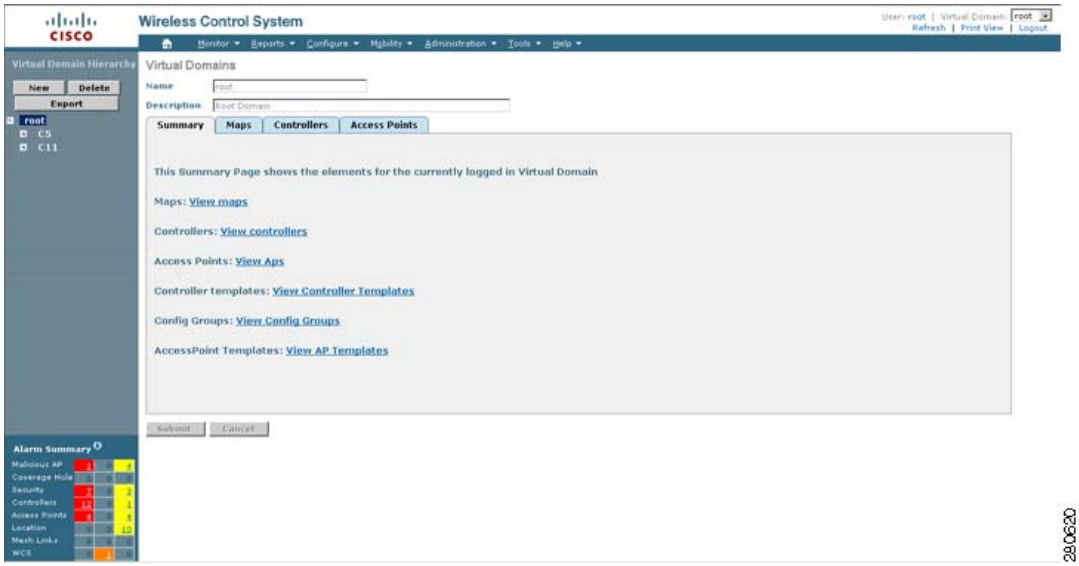
Only one virtual domain can be active at login. You can change the current virtual domain by using the Virtual Domain drop-down menu at the top of the screen. Only virtual domains that have been assigned to you are available in the drop-down menu.

When you select a different virtual domain from the drop-down menu, 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 17-3). Click a link in the Summary tab window to view the assigned components for your virtual domain.

Figure 17-3 Virtual Domains Summary Tab



Limited Menu Access

Non-root virtual domain users do not have access to the following WCS menus:

- Monitor > RRM
- Configure > Auto Provisioning
- Configure > ACS View Servers
- Mobility > Mobility Service Engines
- Mobility > Synchronize Servers
- Administration > Background Tasks
- Administration > Settings
- Administration > User Preferences
- Tools > Voice Audit
- Tools > Config Audit

CHAPTER 18

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
- Google Earth Settings

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:

- 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 panel on the left sidebar, select **My Places** or **Temporary Places**.

Step 3 Right-click Temporary Places and select **Add > Folder** from the drop-down menus.

Note Folders can be created hierarchically to n level depths. When creating KMLs, you can create placemarks and organize them hierarchically according to the zone, 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 panel to create Placemarks.

To create Placemarks, follow these steps:

Step 1 Launch Google Earth.

Step 2 In the Places panel 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 menus.

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 "<CrossRef>Understanding Geographical Coordinates for Google Earth" 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 on 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 on the folder, select **Save as** from the drop-down menu, 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 18-1 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 18-1.

Table 18-1 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
"FolderLatitude"	"Value Optional"	Range: 0 to ±90
"FolderAltitude"	"Value Optional"	Range: 0 to 99999
"FolderRange"	"Value Optional"	Range: 0 to 99999

Table 18-1 (continued)Potential Fields for the CSV File

"FolderName"	"Value Optional"	Max Length: 32
"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 menu, 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 longitude, latitude, tilt, heading, range, and other geographical coordinates fields.
- If provided, longitude and latitude coordinates are validated.

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 window 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 window 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 web site.

Viewing Google Earth Map Details

To view details for a Google Earth Map folder, follow these steps:

Step 1 From the Google Earth Map window, click the folder name to open the details window 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 window.

Google Earth Settings

Access point related settings can be defined from the Google Earth Settings window. To configure access point settings for the Google Earth Maps feature, follow these steps:

Step 1 Choose **Monitor > Google Earth Maps**.

Step 2 From the Select a command drop-down menu, choose **Settings**.

Step 3 Click **GO**.

Step 4 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 window.

Note These settings apply when Google Earth sends the request for the next refresh.

  - Access Points—From the drop-down menu, 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 menu, 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 menu (- 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 menu. Choose **Link SNR** or **Packet Error Rate** from the Link Color drop-down menu.

Note When the AP Mesh Info check box is chosen, Mesh Links are also automatically shown.

Step 5 Click **Save** to confirm these changes or **Cancel** to close the window without saving the changes.

APPENDIX A

Troubleshooting and Best Practices

This document identifies and explains any additional troubleshooting or best practices you may find necessary as you implement a particular function.

The following features are included in this document:

- Troubleshooting Cisco Compatible Extensions Version 5 Client Devices, page A-1
- Web Auth Security on WLANs, page A-2

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 on an IP address to choose a specific controller.

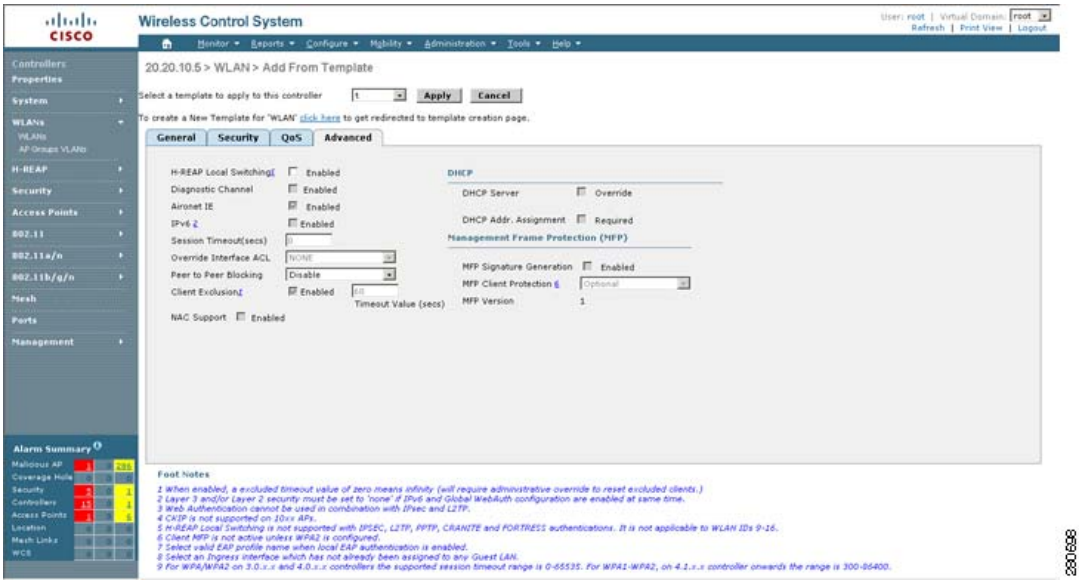
Step 3 Choose **WLAN> WLANs** from the left sidebar menu.

Step 4 Choose **Add 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, check the **Diagnostic Channel** check box. Otherwise, leave this check box unchecked, 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 window.

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 Enable 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 **show client detail <client-mac-address>**.

```
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=0xddffffff,
prev_trd_index=0xddffffff
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 Wireless Control System (WCS). It contains these sections:

- WCS Licenses, page B-1
- OpenSSL/Open SSL Project, page B-6
- End User License Agreement, page B-8

WCS Licenses

Before you purchase a Cisco Wireless Control System (WCS) license, determine if you will need a Base or Location license and how many access points will need to be supported and licensed.

The two types of 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 Location** includes all the features present in the Cisco WCS Base, plus the ability to track a single Wi-Fi device on demand or expand location capabilities by adding a Cisco Wireless Location Appliance to simultaneously track up to 2500 Wi-Fi devices.

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-STANDARD-K9 — For customer buying new or expansion Cisco WCS licenses running Cisco Unified Wireless Network Software Release 4.1.82.0. It is available as Cisco WCS Base or Cisco WCS Location increments of 50, 100, 500, 1000, or 2500 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 "Conversion of a WLSE Autonomous Deployment to a WCS Controller Deployment" in Appendix B for steps to migrate from CiscoWorks WLSE to the Cisco Unified Wireless Network architecture.

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-LOC-UPG-K9 — For customers upgrading from their existing Cisco WCS base licenses to equivalent Cisco WCS Location licenses. It is available as Cisco WCS Location in increments of 50, 100, 500, 1000, or 2500 lightweight access points.
- WCS-ADV-SI-SE-10—A feature license that enables the integration of up to 10 spectrum experts. This license requires a valid base or location license.
- AIR-WCS-DEMO-K9 — For customers wishing to download the new full featured, location-enabled Cisco WCS 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-LOC-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 location 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 location to location. Unequal option levels (base and location) cannot be mixed. Only one type of license can be used on the WCS at one time. For example, if your computer has a location 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 location license with an access point count of 50 and in a year you need to add more access points, you can buy another location license with an access point count of 100, apply it to the WCS, and have a WCS with location 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 location, you will need to purchase a location upgrade license. You need to purchase a location 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 a single location upgrade license 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 version of the Internet Explorer browser.

Step 3 In the Location or Address field, 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 From the Help menu, select **Licensing**.

Step 6 On the Licensing page, from the Select a command drop-down menu, choose **Add License**.

Step 7 On the Add License page, click **Browse** to navigate to the location where you saved the .lic file.

Step 8 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 "Location Feature." For example, Base or Location.
- The "Location Feature" (Base or Location) 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.

Managing Licenses

Choose **Help > Licensing** to access the Licenses page.

This page enables you to view a list of the current licenses installed, add a license, and delete a license.

The license information displays the following:

- Host name
- Type
- AP count (for specified number of access points)
- Percentage of what is licensed
- Capacity of licenses currently used

The license list displays the following:

- A summary of each individual license.
- ID: Unique identifier for the license.
- Host: License applies to this host machine.
- Type: Location or base.
- AP Count: Number of access points for listed license. Should correspond with AP Count in License Information column.
- Expires: When license expires.

Adding a License

Follow these steps to add a license.

Step 1 From the Select a command drop-down list, choose **Add License** and click **GO**.

Step 2 Click **Browse** to search for the license file you are adding.

Step 3 Click **Upload**.

Deleting a License

Follow these steps to delete a license.

Step 1 From the License List portion of the Licenses window, click the check box of the license you want to delete.

Step 2 From the Select a command drop-down list, choose **Delete License** and click **GO**.

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 location license, during the reinstall, you need to first install the base license, then install the location license. To backup and restore the WCS database, refer to the "Backing Up the WCS Database" section on page 12-3 and the "Restoring the WCS Database" section on page 12-5.

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, i.e. 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].

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.

REVIEW DRAFT—CISCO CONFIDENTIAL

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.

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.

- **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
- Configuring the Converted Appliance, page C-4
- Licensing, page C-7

REVIEW DRAFT—CISCO CONFIDENTIAL

Supported Hardware

Supported 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.

REVIEW DRAFT—CISCO CONFIDENTIAL

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. Refer to "Installing WCS for Linux" procedure on page 2-13 if you need further assistance.

Note If you cannot execute the installation file, enter **chmod +x WCS-install-file.bin**.

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.

REVIEW DRAFT—CISCO CONFIDENTIAL

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 go through a series of prompts over the console connection that are addressed below.

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 password *setup*.

```
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]:
```

REVIEW DRAFT—CISCO CONFIDENTIAL

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.

REVIEW DRAFT—CISCO CONFIDENTIAL

```
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.

REVIEW DRAFT—CISCO CONFIDENTIAL

```
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 10-15
802.11a policy name 11-55
802.11b/g RRM interval template 11-66, 11-67
802.11b/g RRM threshold templates 11-64
802.11b/g voice templates 11-60
802.11 counters report 15-17, 15-18
802.11h template
  configuring 11-66
802.11 security trap 11-73
802.11 tags layer 5-48
802.1n scaling reports 15-5
802.1X association 6-35
802.1X authentication 6-35
802.3 bridging
  configuring 10-14
880 series ISRs 1-7

A

AAA override 11-16
AAA servers 11-15
AAA traps 11-73
absolute 18-2
access control list templates 11-40, 11-54
accessing the schedule panel 15-3
access point
  configuring 11-39
  configuring for hybrid REAP 13-9
  credentials 9-2
  friendly 11-46
access point/radio templates 11-79
access point authentication and MFP templates 11-49
access point authorization template 11-39
access point inventory report 15-14
access point layer 5-45
access point load
  avoiding 11-57
access point placement 5-25
access point positions
  changing with import or export of file 5-34
access point reports 15-5
  modifying 15-8
  viewing 15-8
access points
  adding 5-24
  adding to maps 5-24 to 5-25
  configuring 9-8
  configuring for LOMM 9-15
  converting to LWAPP C-2
  detecting 14-12
  embedded 1-7
  searching 9-17
  selecting 11-88
access point security statistics
  for mesh 6-47
access point templates
  adding 11-78
access point threats 6-7
access point traps 11-73
accuracy tool 5-68
ACL template 11-40
  configuring 11-40
ACS server
  adding WCS to 16-5

ACS View Server credentials 6-31
active interferer count per channel 9-20
active interferers 9-19
active sessions
  monitoring 7-5
adaptive scan threshold 11-64
add config groups 8-18
add group members 8-10
adding access points 5-23
adding access point templates 11-78
adding a license B-5
adding a migration template 9-7
adding a spectrum expert 9-18
adding autonomous access points
  by CSV file 9-5
adding auto-provisioning filter 16-18
adding chokepoints 5-35
adding controllers 10-2
adding controllers from config group 8-20
adding guest user account 7-16
adding IOS access points 9-4
  by device information 9-5
adding templates from config group 8-20
adding WCS as TACACS+ server 16-6
adding WCS to ACS server 16-5
  for use with RADIUS 16-10
adding WCS to a non-Cisco ACS server 16-14
adding WCS usergroups
  into ACS for RADIUS 16-11
  into ACS for TACACS+ 16-7
add known rogue 11-69
adjusted link metric 6-38
administration menu 2-26
advanced debug 5-34, 5-64, 5-69
Advanced Options
  definition 5-21
advanced options 5-19
Advanced tab
  on WLAN template 11-17
Aironet IE 11-18
alarm 14-1
alarm dashboard 2-27, 14-1
alarm monitor 2-27, 6-13
alarms 14-1
  config audit 8-25
  monitoring 14-4
  rogue access point 14-8
  rogue adhoc 14-11
alarm trigger threshold 11-50
all groups window 16-8
alternate parent
  for mesh 15-15
altitude 18-2
anonymous provisioning 11-33
antenna gain 6-30
antenna type 6-29
AP attack details 2-16
AP failover priority
  setting 9-2, 10-8
AP list by location 15-8
AP list by location report 15-8
AP list by SSID 15-8
AP mesh layer info 5-46
applying calibration models 5-59
applying config groups 8-21
applying controller templates 11-77
AP policies 3-7
AP policies template 11-42
AP profile status report 15-8
APs not assigned to maps 2-15
AP status report
  viewing for scheduled task 11-83
AP template task history
  viewing 11-84
AP template tasks 11-83
AP up time 6-43
assigned virtual domain components 17-8
assigning location presence 5-3

assigning virtual domains 7-23
association request failures 6-50
association request success 6-50
association request timeouts 6-50
attacks
  access points 6-7
audience of document 21
AUDIT_STATUS_DIFFERENCE 14-60
auditing config groups 8-22
auditing H-REAP groups 13-16
audit report 15-9, 16-34
  configuring 9-16, 10-5
audit status 6-46
  viewing 10-5
  viewing for access points 9-16
  viewing for controllers 10-5
audit trail
  enabling for guest user activities 7-12
  viewing 7-10
authentication order
  managing 10-5
authentication priority 10-5
authentication process
  Hybrid REAP 13-2
authentication request failures 6-50
authentication request success 6-50
authentication request timeout 6-50
auto key generation 11-22
automated upgrade 12-16
automatic backups, scheduling 12-4, 16-2
automatic client exclusion 11-19
automatic client troubleshooting 16-32
autonomous access points
  adding by CSV file 9-5
  viewing 9-6
autonomous to LWAPP migration support 9-4
auto provisioning 16-17
  setting 16-22
auto provisioning device information
  detailed 16-20
auto provisioning filter
  deleting 16-21
  editing 16-21
auto refresh 16-34
auto-synchronizing location appliances 12-11
avoid access point load 11-57
avoid Cisco AP load 11-57
avoid foreign AP interference 11-57
avoid non-802.11 noise 11-57

B

background tasks 12-14
  running 16-2
backhaul interface 6-49
backing up location appliance data 12-13
backing up the WCS database
  on Linux 12-5 to 12-6
  on Windows 12-5
backup and restore license B-6
bandwidth
  making expedited 11-61
basic auditing 8-23
best practices A-1
bridge group name 6-49
bridging link information 6-53
bridging mesh statistics 6-49
broadcast deauthentication frame signatures 3-10
bronze 11-17
bronze queue 6-50
buildings
  adding to a campus map 5-3
  adding to WCS database 5-4
busiest APs report 15-8
busiest clients report 15-10

C

CAC
- enabling 10-9

CA certificates 4-5

CAD files 5-2

calculating access point requirements 5-17

calibration models 5-59

calibration status bar 5-62

call admission control 11-60

campus map, adding to WCS database 5-2

cascade reboot 8-26

caution, defined 23

CCA sensitivity 11-59

certificate signing request 3-22

changing access point positions 5-34
- by importing or exporting a file 5-34

channel bonding
- configuring 10-15

channel change notifications 6-68

channels
- monitoring on a floor map 5-51

channel width
- monitoring 6-55

checking the status of WCS
- on Linux 12-2
- on Windows 12-2

chokepoints 5-35
- adding 5-35
- monitoring 5-43
- removing 5-42
- using to enhance tag location 5-35

Cisco AP load
- avoiding 11-57

Cisco Discovery Protocol 9-11

Cisco UDI 5-20

Cisco Unified Wireless Network Solution 5-64

Cisco WCS base B-2

Cisco WCS location B-2

Cisco Wireless LAN Solution
- overview 1-2
- security solutions 3-2 to 3-5

civic address 5-4

clamped to ground 18-2

classification rule 11-43

clear config 9-13

client alarms
- most recent 2-16

client association report 15-10

client authentication provision 11-33

client count 2-15, 2-20

client count graph report 15-5

client count report 15-11

client devices
- connecting to WLANs 13-11

client exclusion 11-19
- happening automatically 11-19

client exclusion policies template 11-47

client MFP 3-7

client properties 6-22

client related traps 11-72

client reports
- creating new 15-11
- modifying 15-9, 15-11
- viewing 15-9, 15-11

clients
- finding 6-31
- manually disabled 2-16
- map 6-34
- monitoring on a floor map 5-53
- parameters 5-53

clients detected by location server 2-20

client security component 2-19

clients layer 5-47

client statistics 6-34

client tab
- home page 2-15

client traffic 2-16, 2-20

client troubleshooting
automatic 16-32
combined inventory report 15-14
command buttons 2-27
components
of virtual domain 17-8
conducting accuracy testing 5-68
config audit 8-24
config audit alarms 8-25
config groups
adding controllers 8-20
adding templates 8-20
applying 8-21
auditing 8-22
configuring 8-19
creating 8-17
deleting 11-86
downloading customized webauth 8-28
downloading IDS signatures 8-27
downloading sw to controllers 8-26
rebooting 8-25
removing controllers 8-20
removing templates 8-20
reporting 8-2
config group task history
viewing 11-86
config group tasks 11-84
configuration audit summary 8-24
configuration mismatch 6-71
configuration sync 16-4
configure menu 2-25
configuring 40 MHz channel bonding 10-15
configuring an 802.11h template 11-66
configuring 802.3 bridging 10-14
configuring access control lists 11-54
configuring an access point 9-8, 10-14, 11-39
configuring an access point for hybrid REAP 13-9
configuring alarm severity 14-64
configuring audit reports 10-5
configuring a client exclusion policy template 11-44
configuring config group 8-18
configuring the controller for hybrid REAP 13-6
configuring a CPU ACL template 11-40
configuring an EAP-FAST template 11-31
configuring EDCA parameters
for individual controllers 10-16
through a template 11-62
configuring firewall for WCS 3-6
configuring general templates 11-4
configuring global credentials 9-2
configuring global email parameters 16-30
configuring high density templates 11-58
configuring a high throughput template 11-67
configuring H-REAP AP groups 11-20
configuring Hybrid REAP 13-1
configuring hybrid REAP access point groups 13-12
configuring Hybrid-REAP groups 13-13
configuring IDS 3-9
configuring IDS signatures 3-9
configuring intrusion detection systems 3-9
configuring a local EAP general template 11-28
configuring a local EAP profile template 11-30
configuring a manually disabled client template 11-39
configuring a mesh template 11-67, 11-68
configuring multiple country codes 8-15
configuring NAC out-of-band 10-18
configuring a policy name template 11-55
configuring radio templates 11-86
configuring RADIUS servers 16-24
configuring a roaming parameters template 11-62
configuring a rogue policies template 11-41
configuring an RRM interval template 11-66
configuring an RRM threshold template 11-64
configuring scheduled configuration tasks 11-83
configuring SNMPv3 10-17
configuring spectrum experts 9-18
configuring the switch
for hybrid REAP 13-4

configuring TACACS+ servers 16-17
configuring a TACACS+ server template 11-26
configuring templates
802.11a policy name 11-54
802.11b/g RRM interval 11-66
802.11b/g RRM threshold 11-61
802.11b/g voice 11-60
access point/radio 11-79
access point authentication and MFP 11-42
access point authorization 11-39
ACL 11-39
file encryption 11-22
guest users 11-35
known rogue access point 11-66
local management user 11-76
MAC filter 11-37
QoS 11-6
RADIUS accounting 11-25
RADIUS authentication 11-23
for rogue AP rule groups 11-44
syslog 11-74
Telnet SSH 11-73
traffic stream metrics QoS 11-8
trap control 11-71
trap receiver 11-70
web authentication 11-50
WLAN 11-9
configuring a TFTP server template 11-70
configuring a trusted AP policies template 11-42
configuring a user authentication priority template 11-77
configuring a user login policies template 11-37
configuring a video parameter template 11-61
configuring a voice parameter template 11-60
configuring wired guest access 10-23
connecting client devices
to WLANs 13-11
connecting to the Guest WLAN 3-21
containment
of rogue access points 6-12
content
customizing 2-19
controllers
adding 10-2
adding to WCS database 4-2
configuring for hybrid REAP 13-6
pinging network devices 10-9
searching 10-4
specified 1-2
controller audit report 16-34
controller CPU utilization 2-19
controller inventory report 15-14
controller inventory status 2-20
controller memory utilization 2-20
controller status report
viewing 11-85
controller templates
applying 11-78
controller upgrade settings 16-34
controller utilization report 15-17
controller values
refreshing 10-7
conventions of document 23
converting WLSE autonomous to WCS controller C-1
counters report
for 802.11 15-17
country codes
multiple 8-15, 10-3
setting 10-3
coverage areas 2-20
coverage holes 2-15, 6-64, 6-71
finding 5-10
monitoring on a floor map 5-52 to 5-53
summary report 15-17
creating calibration models 5-46
creating guest user accounts 7-12
creating a lobby ambassador account 7-13
creating a network configuration audit 15-10
creating a network design 5-28

creating a new access point report 15-8
creating a new client report 15-11
creating a new inventory report 15-15
creating a new mesh report 15-10, 15-16
creating a new performance report 15-18
creating placemarks 18-3
creating a new security report 15-19
creating a virtual domain 17-1
CSR 3-22
CSV file 9-5, 16-19, 18-4
CSV file format 11-35
current AP template task
  deleting 11-84
  disabling 11-84
  enabling 11-84
  modifying 11-83
current config group task
  disabling 11-85
  enabling 11-85
  modifying 11-85
current templates
  viewing 10-17
customized web auth 3-18, 10-26
  downloading 8-28, 11-52
customizing content on WCS Home page 2-19
customizing tabs on WCS Home page 2-18
custom signature 3-15

D

dashboard
  RRM 6-67
data/coverage 5-20
data management tasks
  performing 16-27
data point collection 5-59
debug commands A-4
debug strategy A-4
default lobby ambassdor credentials
  editing 7-10
deleting a current AP template task 11-84
deleting a current config group task 11-86
deleting a guest user 3-21
deleting guest user templates 7-18
deleting a license B-6
deleting a report 15-3
deleting WCS user accounts 7-4
designing a network 5-28
detailed auto provisioning device information 16-20
detecting access points 14-12
detecting rogue access points 6-13
device certificates 4-5
device information 9-5
DHCP 6-35
DHCP server
  overriding 11-19
DHCP statistics 6-66
diagnostic channel A-2
disable report schedule 15-2
disabling current AP template task 11-84
disabling a current config group task 11-85
disabling IDS signatures 3-14
DNS ping 6-35
DNS resolution 6-35
document
  audience ii-21
  conventions 23
  organization 22
download logs 5-71
downloading a customized web auth 3-18, 8-28, 11-52
downloading IDS signatures 3-13
  from your config group 8-27
downloading sw to controllers
  after adding config group 8-26
downloading vendor CA certificates 4-5
downloading vendor device certificates 4-5
downstream delay 11-9

downstream packet loss rate 11-9
drawing polygon areas
using map editor 5-14
DTIM 11-56

E

EAP-FAST template 11-31
EAPOL flood signature 3-11
EDCA parameters
configuring for individual controllers 10-16
configuring through a template 11-62
editing the default lobby ambassador credentials 7-10
editing guest users 7-17
editing signature parameters 3-16
edit link 5-9
home page 2-18
edit location presence information 5-3
edit view 14-5
email
configuring parameters 16-29
email notifications
monitoring 14-14
embedded access points 1-7
enable background audit 8-18
enable enforcement 8-18
enable report schedule 15-2
enabling audit trails
for guest user activities 7-12
enabling current AP template task 11-84
enabling a current config group task 11-85
enabling high density 10-11
enabling IDS signatures 3-14
enabling load-based CAC 10-8
enabling location presence 5-7
enabling Web login 3-17
end user license agreement B-8
entry chokepoint 5-43
establishing logging options 16-26
event history 6-18
event notification 1-5
events 14-1
monitoring 14-13
excluded packets 6-49
exit chokepoint 5-43
expedited 11-61
expedited bandwidth 11-61
export task list 16-8
exporting asset information 12-11
exporting a file
to change access point position 5-34
exporting WLSE map data 5-55
extend to ground 18-2
external web auth 10-26
extracting task list 16-15

F

failed objects
monitoring 14-7
feature license B-3
file encryption template 11-22
filter
deleting auto provisiioning 16-21
editing current auto provisioning 16-21
using to modify maps 6-53
filter member management 16-19
filter mode 16-18
filter properties 16-19
finding clients 6-31
finding coverage holes 5-10
firewall, configuring for WCS 3-6
floor plans
adding to a campus building 5-11 to 5-12
adding to a standalone building 5-12 to 5-13
enhancing with map editor 5-13
foreign access point interference
avoiding 11-57

foreign AP interference
avoiding 11-57
frame type 3-15
friendly access point template 11-46
friendly rogue 11-43
friendly rogue access points 6-6

G

general tab
client properties 6-22
home page 2-15
RF properties 6-24
security 6-25
general templates
configuring 11-4
generate password 11-36
GEO check box 5-8
geographical coordinates 18-1
global credentials
configuring 9-2
global settings
for standard and custom signatures 3-16
global username and password
overriding 9-12
gold 11-17
gold queue 6-50
Google Earth coordinates 18-2
Google Earth maps 18-1
viewing 6-56
Google KML or CSV
importing into WCS 18-5
GPS markers 5-4
grid of plus marks 5-60
groups
for hybrid-REAP 13-13
for rogue access point rules 11-44
group setup window on ACS server 16-10
GUEST_USER_ADDED 14-58
GUEST_USER_AUTHENTICATED 14-58
Guest user
deleting 3-21
guest user account
adding 7-16
creating 7-12
managing 7-15
scheduling 7-19
guest user activities 7-12
guest user credentials 7-17
guest user details
emailing 7-20
print 7-20
guest users
viewing and editing 7-17
guest user templates 11-35
deleting 7-18
guest WLAN
connecting 3-21
guidelines
for NAC out-of-band integration 10-19
for using the map editor 5-13

H

heater status 6-43
heat map
described 5-25
graphic 5-25
help menu 2-26
hierarchy
of mesh network 6-52
hierarchy of mesh parent to child 6-54
high density
enabling 10-11
high density requirements 10-11
high density templates 11-58
high throughput template
configuring 11-67

historical report type 15-1
home page
customizing content 2-19
customizing tabs 2-18
H-REAP AP groups
configuring 11-20
H-REAP configuration tab 11-21
H-REAP groups 13-13
auditing 13-16
Hybrid REAP
configuring 9-1, 10-1, 13-1
hybrid REAP access point groups 13-12
Hybrid REAP local switching 11-18
hysteresis 11-64

I

identical audit status 6-46
IDS 3-9
configuring 3-9
IDS sensors 3-9
IDS signature events
viewing 3-17
IDS signatures 3-9
disabling 3-14
downloading 3-13
downloading from config group 8-27
enabling 3-14
uploading 3-12
importing a file
to change access point position 5-34
importing asset information 12-11
importing coordinates
as CSV file 18-4
into Google Earth 18-2
importing Google KML or CSV into WCS 18-5
importing WLSE map data 5-55
indicator of alarms 2-27
information elements
Aironet 11-18
infrastructure MFP 3-7
input type 16-19
inspect location readiness 5-22
inspect VoWLAN readiness 5-23
installer
using to upgrade 12-16
installing a license B-4
installing WCS
for WLSE conversion C-2
insufficient memory 6-49
integrating NAC out-of-band 10-18
interferers
summary 9-19
internal web auth 10-26
inter-subnet roaming 8-4
intrusion detection systems 3-9
invalid association request 6-51
invalid reassociation request 6-51
invalid reauthentication request 6-51
inventory detail status 2-15
inventory reports 15-12
creating 15-15
modifying 15-14
viewing 15-14
inventory status 2-20
IOS access points
adding 9-4
adding by device information 9-5
IOSAP_DOWN 14-59
IOSAP_LINK_DOWN 14-59
IOSAP_LINK_UP 14-59
IOSAP_UP 14-59
IP connectivity 6-35
IPSEC failures 6-8

K

KEK
key encryption key 11-24
key wrap 11-24
KML file 18-2

L

laptop icon 6-33
latest network audit report 10-8
latitude 18-1
Layer 1 security solutions 3-2
Layer 2 11-11
Layer 2 security solutions 3-2
Layer 3 11-14
Layer 3 security solutions 3-2
Layer 3 to Layer 2 mode, converting Cisco Wireless LAN Solution 3-5
LBS authorization 11-39
LEAP authentication
requirements 8-8
legacy syslog template 11-74
license
adding B-5
backup and restore B-6
deleting B-6
license agreement B-8
license installation B-4
license management B-5
licenses B-2
license types B-2
licensing
on WLSE network management C-3
lifetime 7-18
linear point collection 5-59
link aggregation 11-5
link aggregation (LAG)
guidelines 13-4
link metric
adjusted 6-38
unadjusted 6-38
link SNR 6-38
link stats
for mesh 15-15
Link test
running 6-59
link test
running 6-59
Link test result 6-60
link test results 6-38
list all filters 16-20
list filters 16-20
load 5-43
load-based CAC 11-60
enabling 10-9
lobby ambassador 7-12
logging activites 7-20
lobby ambassador account
creating 7-13
editing 7-14
lobby ambassador defaults
setting 7-8
local authentication
for hybrid-REAP groups 13-13
local EAP check box 11-16
local EAP general template 11-28
local EAP profile template 11-30
local management user template 11-76, 11-77
local net users template 11-34
local password policy 16-23
local switching
Hybrid REAP 11-18
locating rogue access points 6-13
location
of rogue access points 6-12
location accuracy
analyzing 5-64

using testpoints 5-64
location appliance
adding to WCS database 4-2
auto-synchronizing 12-12
functionality 4-3
importing 12-8
relationship with WCS Location 1-5
location appliance data
backing up 12-13
location inventory status 2-20
location menu 2-26
location optimized monitor mode 9-10
location presence
assigning 5-3
on a location server 5-7
location readiness
inspecting 5-22
location server inventory report 15-14
location server utilization 15-17
location tab 6-28
location upgrade B-2
log analysis 6-17
logging 16-4
logging in
to the WCS user interface 2-13 to 2-15, 7-14
logging options 16-26
logging the lobby ambassador activities 7-20
login.html 3-18
LOMM 9-10
configuring access point radios 9-15
longitude 18-3
long preambles, enabling for SpectraLink NetLink phones 4-6
LWAPP migration 9-4

M

MAC filtering 11-13
MAC filter template 11-38
MAC frequency 3-15
MAC information 3-15
MACK
message authenticator code keys 11-24
maintain image aspect ratio 5-54
maintaining WCS 12-1 to 12-20
malformed neighbor packets 6-49
malicious rogue 11-43
malicious rogue access points 6-3
managed network
security index 6-3
management frame flood signatures 3-10
management frame protection 3-7, 11-49
management queue 6-50
managing guest user accounts 7-15
managing licenses B-5
managing multiple WCSs 1-8
managing user authentication order 10-5
managing virtual domains 17-6
manually disabled client 2-16
template for 11-39
manufacturer information 6-29
maps
adding chokepoints 5-35
creating 5-2 to 5-25
monitoring 5-43, 5-43 to 5-54
removing chokepoints 5-42
searching 5-9
using to monitor link stats 6-36
using to monitor mesh AP neighbors 6-41
map editor
enhancing floor plans 5-13
general notes 5-13
guidelines for using 5-13
using to draw polygon areas 5-14
map view
updating 6-54
menu bar 2-25

mesh access point neighbors
monitoring 6-41
mesh access points
monitoring 6-39
mesh alarms
most recent 2-17
mesh alternate parent 15-15
mesh health 6-43
monitoring 6-43
mesh link statistics 6-36
monitoring 6-36
mesh link stats 15-15
mesh neighbors 6-42
mesh network
monitoring using maps 6-36
mesh network hierarchy 6-52
mesh node hops 15-15
mesh packet error statistics 15-15
mesh packet statistics 15-15
mesh parent-child hierarchical view 5-46
mesh reports
creating 15-10, 15-16
modifying 15-16
viewing 15-16
mesh security statistics
for an AP 6-43
mesh statistics
for an access point 6-47
mesh stranded APs 15-16
mesh tab
home page 2-17
mesh template
configuring 11-68
mesh tree
viewing 6-52
mesh worst node hops 15-16
mesh worst SNR links 15-16
message integrity check information element 11-49
metrics
in QoS 11-8
MFP 3-7
for clients 3-7
MFP client protection 11-19
MFP signature generation 11-19
MFP templates 11-49
MIC IE 11-49
minimum RSSI 11-64
mirror mode 9-11
mismatched audit status 6-46
mobile announce messages 8-8
mobility 8-2
mobility anchors 8-12
mobility groups 8-7
configuring 8-8
prerequisites 13-4
mobility scalability 8-11
modifying access point reports 15-8
modifying audit reports 15-9
modifying client reports 15-9, 15-11
modifying a current AP template task 11-83
modifying a current config group task 11-85
modifying inventory reports 15-14
modifying map displays 6-53
using filters 6-53
modifying mesh reports 15-16
modifying a migration template 9-7
modifying performance reports 15-18
modifying security reports 15-19
monitoring active sessions 7-6
monitoring alarms 14-4
monitoring channels
on a floor map 5-51
monitoring channel width 6-55
monitoring chokepoints 5-43
monitoring clients
on a floormap 5-53

monitoring coverage holes
on a floormap 5-52
monitoring email notifications 14-14
monitoring events 14-13
monitoring failed objects 14-7
monitoring maps 5-43
monitoring mesh access point neighbors 6-41
using maps 6-41
monitoring mesh health 6-38, 6-43, 6-55
monitoring mesh link statistics
using maps 6-36
monitoring mesh networks
using maps 6-36
monitoring outdoor areas 5-46, 5-54
monitoring pre-coverage holes 6-64
monitoring predicted coverage 5-44
monitoring rogue access point alarms 14-8
monitoring rogue access point details 14-9
monitoring rogue access points 6-8
monitoring rogue adhoc alarms 14-10
monitoring rogue adhocs 6-10
monitoring rogue clients 6-10, 14-13
monitoring security configurations 14-14, 16-32
monitoring shunned clients 6-11
monitoring spectrum experts 9-19
monitoring transmit power levels 5-46
on a floormap 5-51
monitor menu 2-25
monitor mode
location optimized 9-10
most recent AP alarms 2-19
most recent audit alarms 8-25
most recent client alarms 2-16
most recent mesh alarms 2-17
most recent rogue adhocs 3-3
most recent security alarms 2-17
multicast mobility mode 8-12
multiple country codes
configuring 8-15
setting 10-3
multiple syslog template 11-75

N

N+1 redundancy 8-5
NAC out-of-band
configuring 10-18
NAT 8-11
Navigator 1-8
NetStumbler signature 3-11
network address translation 8-11
network audit report
viewing latest 10-8
network design 5-28
network protection 3-9
Network Summary page 2-14
new rogue AP count report 15-19
new rogue APs report 15-19
new search 5-9
node hop count
worst 2-17
node hops 6-49
for mesh 15-15
noise
avoiding non-802.11 types 11-57
non-802.11 noise
avoiding 11-57
non-Cisco ACS server
for use with RADIUS 16-14
note, defined 23
notifications
of channel change 6-68
of RF grouping 6-69
of transmission power change 6-69
NTP server template 11-3
null probe response signatures 3-10

O

on-demand accuracy testing 5-68
optimizing the controller for high density 10-12
organizationally unique identifier 6-29
organization of document 22
outdoor areas
  adding to a campus map 5-6
  monitoring 5-54
outdoor location
  creating with Google Earth 18-1
override global username password 9-12
overview
  Cisco Wireless LAN Solution 1-2
  WCS 1-3

P

packet error rate
  worse 2-17
packet error rate link color 6-54
packet error statistics
  for mesh 15-15
packet jitter 11-8
packet latency 11-8
packet loss 11-8
packet loss rate 11-9
packets received 6-51
packet statistics
  for mesh 15-15
packets transmitted 6-51
parent changes 6-49
parent TSF 6-35
passthrough 11-14
password rules
  turning on or off 16-22
PEAP 11-31
peer-to-peer blocking 11-19
  guidelines 10-19
performance reports 15-17
  creating 15-18
  modifying 15-18
  viewing 15-18
performing data management tasks 16-27
pico cell mode 11-56
pinging network devices from a controller 10-9
placemarks
  creating 18-3
placement of access points 5-26
planning mode 5-18
  to calculate access point requirements 5-17
platinum 11-17
platinum queue 6-50
PLR 11-9
POE status 6-46
policy manager solutions 3-3
policy name template
  configuring 11-55
polygon areas
  drawing with map editor 5-14
poor neighbor SNR 6-49
position testpoints 5-69
power-over-ethernet status 6-46
pre-coverage holes
  monitoring 6-64
predicted coverage, monitoring 5-44
predictive tool
  distance based 5-22
prerequisites 2-2
presence parameters 5-7
present map 6-33
print guest user details 7-20
protection type 11-50
purpose of document 21

Q

QoS 11-17

QoS templates 11-6
quarantine 10-21
queues 15-15
    silver, gold, platinum, bronze, management 6-50
quiet time 3-15

R

radio inventory status 2-20
radio measurements
    receiving 6-35
radio receiver sensitivity 6-30
radio resource management 11-57
radio resource management statistics 6-68
radio status
    scheduling 9-15
radio templates
    configuring 11-86
radio utilization report 15-17
RADIUS accounting template 11-25
RADIUS and TACACS+ attributes
    for virtual domain 7-24, 17-7
RADIUS authentication template 11-23
RADIUS servers
    configuring 16-24
reachability status 9-18
reassociation request failures 6-51
reassociation request success 6-51
reassociation request timeouts 6-51
reauthentication request failures 6-51
reauthentication request success 6-51
reauthentication request timeout 6-51
rebooting config groups 8-23
receiving radio measurements 6-35
recent alarms 2-19
recent coverage holes 2-15, 2-20
recent map 6-33
recent rogue adhoc alarm 2-17
recent rogue AP alarms 2-17
recovering the WCS password 12-21
refresh
    automatically 16-34
refresh browser 5-43
refresh controller values 10-7
refresh from network 5-43
refresh heatmap 5-43
related publications 23
relative to ground 18-2
removing chokepoints 5-42
removing controllers from config group 8-20
removing switches 10-29
removing templates from config group 8-20
report
    802.11 counters 15-17
    access point inventory 15-14
    busiest APs 15-8
    busiest clients 15-10
    client association 15-10
    client count 15-11
    combined inventory 15-14
    controller inventory 15-14
    controller utilization 15-17
    coverage hole summary 15-17
    deleting 15-3
    location server inventory 15-14
    location server utilization 15-17
    mesh alternate parent 15-15
    mesh worst node hops 15-16
    radio utilization 15-17
    security summary 15-19
    traffics stream metrics 15-8, 15-11
    Tx power level and channel 15-17
    unique client 15-11
    voice statistics 15-17
reporting tag location 5-35
reports
    802.11n scaling 15-5
    access point type 15-7

disable schedule 15-2
enable schedule 15-2
mesh link stats 15-15
mesh node hops 15-15
mesh packet error statistics 15-15
mesh packet statistics 15-15
mesh worst SNR links 15-16
running 15-1
reset AP now 9-13
restore WCS values 10-7
restoring WCS database on Linux 12-7
retain WCS value 8-23
retention expiration 5-9
retransmission rule enable 5-8
retrieving UDI 6-60
RF calibration model, creating 4-7
RF calibration tool 1-8
RF grouping notifications 6-69
RF prediction heat map 5-25
RF profile traps 11-73
RF properties 6-24
RF update traps 11-73
RLDP 11-42
roaming 8-2
roaming parameters template
configuring 11-63
roaming time 11-8, 11-9
rogue access point alarms
monitoring 14-8
rogue access point details 14-9
rogue access point location 6-12
rogue access point rule groups 11-44
rogue access point rules
configuring a template 11-42
viewing or editing 9-18
rogue access points
alarm monitor 6-13
detecting 6-13
detecting and locating 6-13 to 6-14
friendly 6-6
locating 6-13
malicious 6-5
monitoring 6-2 , 6-8
solutions for 3-3
unclassified 6-6
rogue adhoc alarm 2-17
monitoring 14-10
rogue adhocs
monitoring 6-10
most recent 3-3
rogue adhocs event report 15-19
rogue AP alarms 2-17
rogue AP detail summary 2-20
rogue APs event report 15-19
rogue APs layer 5-49
rogue APs report 15-19
rogue clients
monitoring 6-10, 14-13
rogue clients layer 5-50
rogue detector 9-10
rogue location discovery protocol 11-42
rogue management 3-3
rogue policies
template for 11-41
rogues detected by APs 15-19
routing state 6-49
RRM dashboard 6-67
RRM DCA 10-15
RRM intervals 11-66, 11-67
RRM interval template
configuring 11-66, 11-67
RRM thresholds 11-64
RRM threshold template
configuring 11-64
rules
for rogue access point 11-42
viewing or editing for rogue access points 9-18
Running 6-59

running a link test 6-58, 6-59
running background tasks 16-2
running report 15-1
RX neighbor requests 6-49
RX neighbor responses 6-49
Rx sensitivity 11-59

S

saved searches 5-9
scalability parameters 8-11
scaling reports
  802.11n 15-5
scan threshold 11-64
scheduled accuracy testing 5-68
scheduled configuration tasks
  configuring 11-83
scheduled tasks
  viewing 9-16
schedule panel
  accessing 15-3
scheduling guest user account 7-19
scheduling radio status 9-15
search
  using for alarms 14-5
search clients 6-32
searching controllers 10-4
searching maps 5-7
security alarms
  most recent 2-17
security color range 6-3
security configurations
  monitoring 14-14, 16-32
security index 6-3
security index detailed report 6-4
security mesh statistics 6-50
security reports 15-18
  creating 15-19
  modifying 15-19
  viewing 15-19
security solutions 3-2 to 3-5
security statistics
  for mesh 6-47
security summary report 15-19
security summary window 6-2
security tab
  home page 2-16
selecting access points 11-88
sending mobile announce messages 8-8
sensors
  viewing IDS types 3-9
sequence parameter 11-55
serial number 6-29
servers
  synchronizing WCS and location servers 12-9
service options 5-20
setting AP failover 9-2
setting AP failover priority 10-8
setting lobby ambassodor defaults 7-8
setting multiple country codes 10-3
shunned clients
  monitoring 6-11
shutting switch port 10-29
sidebar area 2-26
signature attacks 6-7
signature attacks summary 2-16
silver 11-17
silver queue 6-50
single device 16-19
skull-and-crossbones indicator 6-14
sniffer 11-80
sniffer mode 9-11
SNMP authentication 11-72
SNMPv3
  configuring 10-17
SNR definition 6-54
SNR down 6-38

SNR link
worst 2-17
SNR UP 6-38
software
downloading config groups to controllers 8-26
software, updating 4-4
SpectraLink NetLink phones, enabling long preambles 4-6
spectrum experts
adding 9-18
configuring 9-18
monitoring 9-19
summary 9-19
spectrum expert details 9-20
standard signature 3-9, 3-15
starting WCS
on Linux 2-12
on Windows 2-12
statistics
DHCP 6-66
statistics tab 6-26
status, checking 12-2
status report
AP profile 15-8
stopping WCS
on Linux 12-3
on Windows 12-3
supported Cisco WLSE management stations C-2
switches
configuring for hybrid REAP 13-4
removing 10-29
switch port
shutting 10-29
switch port tracing
using 10-27
symmetric mobility tunneling 11-5
symmetric tunneling 8-5
synchornization
of configuration 16-4
synchronize servers 12-9
syslog templates 11-74, 11-75
system requirements 2-2

T

TACACS+ server
configuring 16-23
configuring a template for 11-27
tagging
of rogue access points 6-12
tag location reporting 5-35
target 6-35
target TSF 6-35
tasks
importing into ACS 16-5
Telnet SSH templates 11-73
temperature 6-43
template
for configuring network user credentials 11-33
for configuring rogue AP rules 11-42
template-based auditing 8-23
templates
using 11-1
test analysis 6-35
testing
accuracy 5-68
testpoints 5-64
TFTP server 3-12
TFTP server template
configuring 11-70
thermometer color range 6-3
threats
access points 6-7
throughput report 15-6
tilt 18-2
tool to conduct accuracy testing 5-68
top APs by client count 2-15
top security issues 6-3

total APs not assigned to maps 2-15
total interferer count 9-20
total mismatched controllers 8-25
trace switch port 10-27
traffic indicator message 11-56
traffic stream metrics 11-61
traffic stream metrics QoS status 11-8
traffic stream metrics QoS template 11-8
traffic stream metrics report 15-8, 15-11
  graphical 15-8
transition time 11-64
transmission power change notifications 6-69
transmit power level 5-52, 11-57
  monitoring on a floor map 5-51
  monitoring on a floormap 5-51
  values 5-52
trap
  802.11 security 11-73
trap control templates 11-71
trap receiver template 11-70
traps
  AAA 11-73
  access point 11-73
  client related 11-72
  RF profile 11-73
  RF update 11-73
  unsupported 14-63
  WPS 11-73
traps added in 2.1 14-33
traps added in 2.2 14-37
traps added in 3.0 14-39
traps added in 3.1 14-41
traps added in 3.2 14-44
traps added in 4.0 14-45
traps added in 4.0.96.0 14-49
traps added in 4.1 14-51, 14-58
trend report type 15-1
troubleshooting A-1
troubleshooting voice RF coverage 5-23
trusted AP policies
  template for 11-42
trusted AP policies template 11-42
tunneling 8-5
turning password rules on or off 16-17
Tx channel report 15-17
TX neighbor requests 6-49
TX neighbor responses 6-49
Tx power level report 15-17

U

UDI
  retrieving on controllers and access points 6-61
unadjusted link metric 6-38
unclassified rogue 11-43
understanding virtual domains 7-25, 17-8
uninstalling WCS
  on Linux 12-15
  on Windows 12-15
unique client report 15-11
unique device identifier 6-61
unknown association requests 6-51
unknown reassociation request 6-52
unknown reauthentication request 6-52
update map view 6-54
updating system software 4-4
upgrading the network 12-21
upgrading to Linux 4
  during WLSE conversion C-3
upgrading WCS
  on Linux 12-20
  on Windows 12-20
uploading IDS signatures 3-12
upstream delay 11-8
upstream packet loss rate 11-9
user accounts
  for guest 7-12

user authentication order
managing 10-5
user authentication priority template
configuring 11-77
user credential retrieval priority 11-33
user details
emailing 7-20
printing 7-20
user groups 7-2
user interface 2-24
user login policies
configuring a template 11-37
user preferences 16-35
using chokepoints 5-34
to enhance tag location reporting 5-34
using edit view 14-5
using filtering 6-53
using maps
to monitor mesh AP neighbors 6-41
to monitor mesh link statistics 6-36
using maps to monitor mesh networks 6-36
using planning mode 5-14
using search 14-5
using switch port tracing 10-27
using template
ACL 11-40
for friendly access point 11-46
using templates 11-1
802.11a policy name 11-55
802.11b/g RRM interval 11-66, 11-67
802.11b/g RRM threshold 11-64
802.11b/g voice 11-60
access point/radio 11-79
access point authentication & MFP 11-49
access point authorization 11-39
file encryption 11-22
for legacy syslog 11-74
for multiple syslog 11-75
guest users 11-35
local management user 11-76, 11-77
local net users 11-34
MAC filter 11-38
NTP server 11-3
QoS 11-6
RADIUS accounting 11-25
RADIUS authentication 11-23
syslog 11-74, 11-75
Telnet SSH 11-73
traffic stream metrics QoS 11-8
trap control 11-71
trap receiver 11-70
web authentication 11-50
WLAN 11-9
using testpoints
to analyze element location accuracy 5-64
using the installer to upgrade 12-16
utilization report
for controllers 15-17

V

V5 client statistics report 15-11
vendor CA certificates
downloading 4-5
vendor device certificates
downloading 4-5
video parameter template
configuring 11-61
view audit reports 10-6
view filters icon 5-45, 5-51, 5-52, 5-53
viewing access point reports 15-8
viewing all current templates 10-17
viewing an AP template task history 11-84
viewing AP status report
for scheduled task 11-83
viewing audit reports 15-9
viewing audit status 10-5
for access points 9-16

viewing the audit trail 7-10
viewing autonomous access points 9-6
viewing client reports 15-11
viewing clients
identified as WGBs 6-58
viewing controller status report
for the scheduled task 11-85
viewing DHCP statistics 6-66
viewing Google Earth maps 6-55, 18-6
viewing guest users 7-17
viewing IDS signature events 3-17
viewing inventory reports 15-14
viewing mesh reports 15-16
viewing mesh tree 6-44, 6-47
viewing MFP events 14-3
viewing performance reports 15-18
view in grid 2-19
viewing security reports 15-19
viewing shunned clients 3-9
viewing the RRM dashboard 6-69
virtual domain hierarchy 17-3
virtual domains 17-1
assigning 7-23
attributes 7-24, 17-7
creating 17-1
hierarchy 17-3
managing 17-6
understanding 7-25, 17-8
voice parameter template
configuring 11-60
voice RF coverage
troubleshooting 5-23
voice statistics report 15-17
voice traffic 5-20
VoWLAN readiness
inspecting 5-23

W

WCS
checking status
on Linux 12-2
on Windows 12-2
installing 2-4
maintaining 12-1 to 12-20
overview 1-3
servers supported 1-3
starting
on Linux 2-12
on Windows 2-12
stopping
on Linux 12-3
on Windows 12-3
uninstalling
on Linux 12-15
on Windows 12-15
upgrading
on Linux 12-20
on Windows 12-20
versions 1-4 to 1-6
WCS_EMAIL_FAILURE 14-60
WCS-ADV-SI-SE-10 B-3
WCS Base, described 1-4, 1-6
WCS controller deployment
from WLSE autonomous C-1
WCS database
adding chokepoints 5-35
adding controllers 4-2
adding location appliances 4-2
backing up
on Linux 12-5 to 12-6
on Windows 12-5
removing chokepoints 5-42
restoring
on Linux 12-7
on Windows 12-6

scheduling automatic backups 12-4, 16-2
WCS home 2-13
customizing content 2-19
customizing tabs 2-18
WCS licenses B-2
WCS location
described 1-5 to 1-6
relationship with Cisco location appliances 1-5
WCS navigator 1-8
WCS on WLSE
licensing C-7
WCS password
recovering 12-21
WCS user accounts
adding 7-2
changing passwords 7-5
deleting 7-4
WCS user interface 7-15
described 1-3, 1-7
logging into 2-13 to 2-15
WCS values
restoring 10-7
web authentication template 11-50
web authentication types 3-18
web auth security A-3
web auth types 10-26
web login
enabling 3-17
Wellenreiter signature 3-11
WGBs 9-6
viewing those clients 6-58
wired guest access
configuring 10-23
Wireless Control System (WCS)
See WCS
WLANs
web auth security A-3
WLAN templates 11-9
WLSE autonomous deployment conversion C-1
WLSE management stations C-2
WLSE map data
exporting 5-55
importing 5-55
WLSE upgrade B-2
WLSE upgrade license C-7
WMM policy 11-17
work group bridge mode 9-6
worst node hop count 2-17
worst node hops
for mesh 15-16
worst packet error rate 2-17
worst SNR link 2-17
for mesh 15-16
WPS traps 11-73