



User Guide for the CiscoWorks Wireless LAN Solution Engine

Release 2.13

Corporate 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: 408 526-4100

Text Part Number: OL-8374-01



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.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0502R)



Preface **xxiii**

Audience	xxiv
Conventions	xxiv
Product Documentation	xxiv
Obtaining Documentation	xxvi
Cisco.com	xxvi
Product Documentation DVD	xxvii
Ordering Documentation	xxvii
Documentation Feedback	xxvii
Cisco Product Security Overview	xxviii
Reporting Security Problems in Cisco Products	xxviii
Obtaining Technical Assistance	xxix
Cisco Technical Support & Documentation Website	xxix
Submitting a Service Request	xxix
Definitions of Service Request Severity	xxxi
Obtaining Additional Publications and Information	xxxi

CHAPTER 1

Getting Started **1-1**

Before You Begin	1-1
Overview of the Wireless LAN Solution Engine	1-2
Integrating the WLSE with Network Management Systems	1-3
Integrating the WLSE with a CiscoWorks Server	1-3
Understanding the Web Interface	1-4
Configuring the Web Browser	1-4
Supported Browsers	1-4
Configuring Internet Explorer	1-5
Configuring Firefox	1-6
The WLSE Dashboard	1-7
Tabs and Subtabs	1-7
Buttons	1-9
Device Identifier Display	1-10
Default Device Identifier Display	1-10
User-Defined Device Identifier	1-10

Understanding WLSE Time Displays	1-10
General Time Displays	1-11
Understanding Time Discrepancy Problems in Job Scheduling	1-11
Using the Device Selector	1-12
Using Search	1-12
Understanding the Icons	1-12
Sorting Table Data	1-13
Logging In and Out	1-13
Customizing the Web Interface	1-14
Setting the Default Tab and Subtab	1-14
Adding a Message to the Splash Screen	1-14
Finding WLSE Documentation on Cisco.com	1-15

CHAPTER 2

Using the Deployment Wizard 2-1

About the Deployment Wizard	2-1
Using the Deployment Wizard	2-2
Description	2-2
Choosing the Deployment Type	2-3
Satisfying Requirements	2-4
Checking Software Versions	2-4
Creating the Configuration Template	2-4
Setting up the WDS	2-7
Deploying the Configuration	2-9
Finishing	2-11

CHAPTER 3

Fault Monitoring 3-1

Displaying Fault Information	3-1
Understanding Fault and Security Policy Monitoring	3-2
Displaying Faults	3-4
Clearing Summary Table Faults	3-6
Acknowledging Faults	3-7
Viewing Fault Details	3-7
Managing Fault Settings	3-10
Understanding Fault Settings	3-10
Creating a Setting	3-11
Copying a Setting	3-11
Renaming a Setting	3-12
Editing a Setting	3-12

Deleting a Setting	3-13
Viewing a Summary	3-13
Assigning a Default Setting to a Device	3-14
Setting Policies and Thresholds	3-14
Viewing the Status of the VoWLAN	3-53
Viewing the Voice Fault Tables	3-53
Viewing the QoS Status Summaries	3-54
Assigning Voice QoS Fault Settings	3-54
Notification Settings	3-56
Setting Trap Notification	3-56
Setting Syslog Notification	3-60
Emailing Faults	3-61

CHAPTER 4

Device Discovery and Management 4-1

Getting Started with Device Management	4-1
Using the Deployment Wizard	4-1
Using Manual Methods	4-2
How the WLSE Communicates with Devices	4-3
Overview: Devices Tab Functions	4-3
Entering Device Credentials	4-5
Enter or Modify SNMP Community Strings for All Devices	4-6
Enter Telnet/SSH Usernames and Passwords—Access Points	4-10
Enter HTTP/HTTPS Port Settings—Access Points	4-13
Enter WLCCP Credentials for Wireless Domain Services	4-13
Monitoring AAA Servers	4-14
About AAA Servers	4-14
Adding an AAA Server	4-16
Removing an AAA Server	4-17
Modifying an AAA Server	4-17
Using Enhanced (WDS) Client Tracking	4-18
Configuring Enhanced Client Tracking	4-19
About WDS Client Tracking	4-20
Managing Device Discovery	4-23
About Discovery	4-24
Using the WLSE Discovery Methods	4-32
Pre-Discovery Checklist	4-33
About the Discovery Wizard	4-33
Using the Discovery Wizard	4-33

Running CDP Discovery	4-34
Importing Devices from a File	4-38
Importing Devices from a CiscoWorks Server	4-39
Setting Advanced Discovery Options	4-41
Using Discovery IP Address Filtering	4-47
Viewing Discovery Logs	4-48
Managing Devices	4-54
Device Management Folders and Functions	4-55
Manually Changing the State of Devices	4-56
Viewing Device Details	4-57
Entering Device Descriptions	4-59
Deleting Devices	4-60
Limitation on the Number of Managed Devices	4-60
Handling Duplicate IP Addresses on Access Points	4-61
Managing Device Inventory	4-63
About Inventories	4-63
Changing the Polling Intervals for Automatic Inventories	4-64
Deleting Inventory and Discovery Logs	4-65
Running Immediate Inventories	4-65
Managing Polling Parameters	4-66
Viewing Inventory Logs	4-69
Exporting Devices	4-71
Exporting Devices to a CiscoWorks Server	4-71
Exporting Devices to a CSV File	4-73
Managing Groups	4-74
About Groups	4-74
Using the Group Details Window	4-77
Creating a Static Group	4-80
Creating a Rule-Based Group	4-81
Creating a Static Group by Copying a Static or Rule-Based Group	4-82
Copying a Rule-Based Group	4-83
Editing a Static Group	4-84
Editing a Rule-Based Group	4-85
Deleting a Static or Rule-Based Group	4-86

CHAPTER 5

Using IOS Templates 5-1

What is a Configuration Template	5-1
Viewing the Existing Templates	5-2
Creating a Template	5-2

Copying a Template	5-3
Editing a Template	5-3
Deleting a Template	5-4
Importing a Template	5-4
Exporting a Template	5-5
Template Choices	5-6
Naming the Template	5-7
Using Basic Settings	5-8
Using Basic Security	5-12
Configuring Voice Express	5-14
Using Association	5-15
Setting Up Network Interfaces	5-18
Defining Security Settings	5-33
Defining Services	5-65
Configuring Wireless Services	5-90
Configuring the Event Log	5-94
System Config	5-96
Configuring Device Specific Settings	5-98
Configuring Custom Values	5-98
Previewing the Template	5-100
Saving the Template	5-100

CHAPTER 6

Using WLSM Templates	6-1
What is a Configuration Template?	6-1
Viewing the Existing Templates	6-2
Creating a Template	6-2
Copying a Template	6-2
Editing a Template	6-3
Deleting a Template	6-3
Importing a Template	6-4
Exporting a Template	6-5
Template Choices	6-6
Naming the Template	6-6
Using the Server Manager	6-7
Configuring Custom Values	6-10
Previewing the Template	6-11
Saving the Template	6-11

CHAPTER 7

Using Wizard Templates 7-1

- What is a Configuration Template? 7-1
- Viewing the Existing Templates 7-2
- Creating a Template 7-2
- Copying a Template 7-2
- Editing a Template 7-3
- Deleting a Template 7-3
- Exporting a Template 7-4

CHAPTER 8

Managing Device Configurations 8-1

- Managing Configuration Archives 8-1
 - Viewing Archived Configurations 8-1
 - Scheduling an Archive Collection 8-3
 - Viewing Archive Status 8-3
- Managing Jobs 8-7
 - Managing Configuration Jobs 8-7
 - Managing Archive Jobs 8-25
- Automating Configurations 8-39
 - Creating a Startup Configuration Template 8-39
 - Assigning a Startup Configuration 8-41
 - Assigning an Auto-Managed Configuration 8-43
- Managing Device Specific Configurations 8-47
 - Importing Device Specific Configurations 8-48
 - Exporting Device Specific Configurations 8-50
 - Viewing Device Specific Configurations 8-51
 - Validating a Device Specific Configuration 8-52

CHAPTER 9

Upgrading Device Firmware 9-1

- About Firmware Upgrades 9-1
 - How Firmware Upgrades Work 9-1
 - Recommendations For Running Firmware Upgrades 9-2
- Managing Firmware Images 9-3
 - Viewing Images Downloaded to the WLSE 9-3
 - Editing Image Details on the WLSE 9-4
 - Deleting Images from the WLSE 9-5
 - Importing Images to the WLSE 9-6
 - Using a Remote TFTP Server for Updating Devices 9-9
- Setting Advanced Parameters 9-9

Viewing and Updating Firmware Versions Supported by the WLSE 9-10

Managing Firmware Jobs 9-11

Creating and Running a Firmware Job 9-11

Job Creation Tasks 9-12

Using the Functions in the Main Jobs Window 9-20

CHAPTER 10

Using Reports 10-1

Using the Basic Report Features 10-1

Using the Device Selector 10-2

Sorting Table Data 10-2

Exporting a Report 10-2

Exporting URL-Based Report Data 10-2

Emailing a Report 10-3

Scheduling Email Jobs 10-5

Using the Device Center 10-7

Viewing the WDS Summary Report 10-10

Viewing the WDS Registered APs Report 10-12

Viewing the Fault Status Report 10-13

Viewing Device History 10-13

Viewing Config History 10-14

Viewing Firmware History 10-14

Viewing the Auto Config Retry Report 10-15

Displaying Radio Manager Reports 10-15

Viewing the Radio Configuration Parameters 10-16

Viewing Current Path Loss Results 10-17

Viewing Historical Path Loss Results 10-19

Viewing Current Channel Load Results 10-19

Viewing Historical Channel Load Results 10-21

Viewing Current Radar Detection Events 10-21

Viewing Historical Radar Detection Events 10-23

Displaying Voice Reports 10-24

AP Group Call Summary: Current 10-24

AP Group Metrics Summary: Current 10-25

AP Detail: Current 10-27

AP Detail: Last Hour 10-29

Voice Queuing Delay 10-30

Voice Packet Loss 10-31

Voice Roaming 10-33

Bandwidth In Use 10-34

Voice Streams In Progress	10-35
Rejected Voice Streams	10-36
Displaying Wireless Client Reports	10-37
Displaying a Client Detail Report	10-37
Displaying a Client Statistics Report	10-39
Displaying a Client Historical Association Report	10-40
Displaying a Client Access Failure Report	10-42
Voice Client Detail: Last Hour	10-43
Displaying Current Reports	10-45
Displaying a Group Client Association Report	10-48
Displaying a Group Security Report	10-50
Displaying a Group SSID Report	10-52
Displaying a Group MBSSID Report	10-53
Displaying a Group VLAN Report	10-54
Displaying a Per VLAN Client Report	10-55
Displaying a Group Client Report	10-56
Displaying a Group Identity Report	10-57
Displaying a Group Serial Number Report	10-58
Displaying a Group Security Violation Report	10-59
Displaying a Group CDP Inline Power Report	10-59
Displaying a Group Inventory Report	10-60
Displaying a Group LBS Report	10-61
Displaying a Group Mobility ID Report	10-62
Displaying a Group Version Summary Report	10-62
Displaying a Group Auto Config Retry Report	10-63
Displaying an AP Summary Report	10-65
Displaying a Detailed Report	10-67
Displaying an Associations Report	10-69
Displaying a RADIUS Authentication Report	10-69
Displaying an QoS Report	10-70
Displaying an SSID Report	10-71
Displaying an MBSSID Report	10-72
Displaying a VLAN Report	10-73
Displaying a Per VLAN Client Report	10-73
Displaying a Hot Standby Report	10-74
Displaying an EAP and MAC Failed Authentication Report	10-75
Displaying a Failed Authentication and Login Attempt per AP Report	10-76
Displaying a Switch Summary Report	10-77
Displaying an AP and Bridge Connected to Switch Report	10-78
Displaying an WLSM Modules Report	10-78

Displaying a Router Summary Report	10-79
Displaying an AP and Bridge Connected to Router Report	10-80
Displaying a Server Summary Report	10-80
Displaying an AP Usage Report	10-81
Displaying a Mobility Groups Report	10-82
Displaying a Mobility ID Report	10-82
Displaying Trends	10-83
Using Trend Reports For Capacity Planning	10-85
Displaying a Group Performance Report: RF Utilization	10-85
Displaying a Group Performance Report: Ethernet Utilization	10-86
Displaying a Top N Number of Associations: Tabular Report	10-87
Displaying a Top N Number of Associations: Graph Report	10-88
Displaying a Top N Percentage Errors Report	10-88
Displaying an RF Transmission Statistics Report	10-89
Displaying an Ethernet Transmission Statistics Report	10-91
Displaying an RF and Ethernet Utilization Graph	10-92
Displaying an RF and Ethernet Utilization: Tabular Report	10-92
Displaying Top N Busiest Clients	10-93
Displaying Top N Client MIC Error Rate	10-94
Displaying a Server Response Time Graph	10-95
Displaying a Client Roaming Statistics Report	10-96
Displaying Real-Time Reports	10-97
Viewing the Real-Time Reports	10-97
Displaying Intrusion Detection System Reports	10-103

CHAPTER 11

Configuring Your WLAN Radio Environment 11-1

WLSE Radio Management	11-1
Enabling and Disabling Radio Management Features	11-4
Using the CLI Command	11-4
Disabled Radio Management Related Faults	11-4
Configuring Your Network for Radio Management	11-5
Understanding Radio Management	11-7
What is WDS and Why Do I Need It?	11-8
Understanding Radio Performance—Coverage and Capacity	11-10
Understanding Multiple BSSIDs	11-13
Understanding Frequency and Transmit Power Planning	11-14
Collecting Radio Location Data	11-14

CHAPTER 12

Managing Your WLAN Radio Environment 12-1

- Getting Started with Radio Manager 12-1
- Using Radio Monitoring to Collect RM Data 12-1
 - Understanding Radio Monitoring 12-2
 - Guidelines for Running Radio Monitoring 12-3
 - Starting Radio Monitoring 12-4
- Evaluating AP Radio Performance 12-6
 - Understanding Auto Re-Site Survey 12-6
 - Guidelines for Running Auto Re-Site Surveys 12-7
 - Establishing Baseline Data 12-8
 - Monitoring AP Radio Performance 12-10
- Healing Your Network 12-11
 - Understanding Self Healing 12-11
 - Guidelines for Healing Your Network 12-14
 - Running Self Healing 12-15
 - Managing Self Healing Faults 12-17
- Using Frame Monitoring 12-19
 - Understanding Frame Monitoring 12-19
 - Guidelines for Using Frame Monitoring 12-19
 - Configuring Frame Monitoring 12-20
 - Displaying Frame Monitoring APs 12-23
 - Disabling Frame Monitoring on Selected APs 12-24
- Displaying Radio Manager Reports 12-25

CHAPTER 13

Managing Your WLAN Radio Environment by Sites 13-1

- Getting Started with Sites 13-2
- Using Location Manager 13-2
 - Prerequisites for Using Location Manager 13-2
 - Setting Up Location Manager 13-3
 - Using Location Manager Functions 13-16
 - Understanding the Location Manager Window 13-36
- Using AP Radio Scans to Collect RM Data 13-43
 - Understanding AP Radio Scans 13-44
 - Guidelines for Running AP Radio Scans 13-45
 - Viewing AP Radio Scan Jobs 13-46
 - Managing AP Radio Scan Jobs 13-48
 - Creating a New AP Radio Scan Job 13-50
 - Viewing AP Radio Scan Job Run Logs 13-53

Using Client Walkabouts to Collect RM Data	13-54
Understanding Client Walkabouts	13-54
Guidelines for Running a Client Walkabout	13-55
Viewing Client Walkabout Jobs	13-57
Managing Client Walkabout Jobs	13-59
Creating a New Client Walkabout	13-61
Running the Walkabout	13-64
Viewing Client Walkabout Run Logs	13-65
Generating Radio Parameters	13-66
Understanding Radio Parameter Generation	13-66
Analyzing and Comparing Radio Parameter Generation Results	13-67
Using Assisted Configuration	13-71
Managing Assisted Configuration Tasks	13-74
Creating a New Assisted Configuration Task	13-75
Managing RM Data	13-81

CHAPTER 14

Using the Intrusion Detection System 14-1

Getting Started with IDS	14-1
Understanding the IDS Subtabs	14-2
Using the Summary Subtab	14-2
Using the Faults Subtab	14-4
Using the IDS Reports Subtab	14-5
Using the Manage IDS Settings Subtab	14-6
Using the Manage Remaining IDS Settings Subtab	14-11
Using the Manage Rogues Subtab	14-11
Using the Manage Network-Wide IDS Settings Subtab	14-11
Using the Notification Settings Subtab	14-12
Detecting Rogue APs	14-12
Understanding Rogue AP Detection	14-12
Guidelines for Detecting Rogue APs	14-14
Setting the Rogue AP Detection Policy	14-16
Setting the Friendly AP to Rogue AP Reclassification Policy	14-18
Displaying Rogue AP Faults	14-19
Managing Rogue APs	14-24
Viewing Rogue AP Reports	14-26
Viewing Friendly AP Reports	14-28
Detecting Switch Port Locations and Suppressing Ports	14-30
Understanding Switch Port Tracing and Suppression	14-30
Guidelines for Detecting and Suppressing Switch Ports	14-31

Setting the Automatic Rogue AP Suppression Policy	14-32
Tracing Switch Ports and Monitoring Automatic Rogue AP Suppression	14-34
Detecting Ad-Hoc Networks	14-37
Understanding Ad-Hoc Network Detection	14-37
Guidelines for Detecting Ad-Hoc Networks	14-37
Setting the Ad-Hoc Network Detection Policy	14-38
Displaying Ad-Hoc Network Faults	14-39
Viewing Ad-Hoc Network Reports	14-41
Detecting Interference	14-43
Understanding Interference Detection	14-43
Guidelines for Detecting Interference	14-44
Setting the Interference Detection Policy	14-45
Displaying Interference Faults	14-46
Detecting Excessive Management Frame Transmissions	14-47
Understanding Excessive Management Frame Detection	14-47
Guidelines for Using Excessive Management Frame Detection	14-48
Setting the Excessive Management Frame Detection Policy	14-48
Displaying EMF Detection Faults	14-49
Viewing EMF Detection Reports	14-50
Detecting Management Frame Protection Faults	14-52
Understanding Management Frame Protection	14-52
Guidelines for Using Management Frame Protection	14-53
Setting the Management Frame Protection Policy	14-53
Displaying Management Frame Protection Faults	14-54
Viewing MFP Capabilities Reports	14-55
Viewing MFP Events Reports	14-56
Detecting Unregistered Clients	14-58
Understanding Unregistered Client Detection	14-58
Guidelines for Using Unregistered Client Detection	14-59
Enabling Unregistered Client Detection	14-59
Displaying Unregistered Client Faults	14-60
Viewing Unregistered Client Reports	14-61
Detecting Authentication and Protection Attacks	14-63
Understanding Authentication and Protection Attack Detection	14-63
Guidelines for Using Authentication and Protection Detection	14-64
Enabling Authentication and Protection Attack Detection	14-65
Displaying Authentication and Protection Attack Faults	14-79

CHAPTER 15**Managing Your Voice Network 15-1**

- Understanding Radio Management for VoWLAN 15-1
 - Understanding Call Admission Control 15-1
 - Understanding Roaming 15-3
 - Understanding Voice Packet Latency, Jitter, and Loss 15-3
 - Voice Capacity Planning 15-5
- Guidelines for Using Voice 15-5
- Enabling VoWLAN 15-6
- Monitoring Your Voice Network 15-7
- Generating Voice Reports 15-8

CHAPTER 16**Managing the WLSE System 16-1**

- Ports and Protocols 16-1
- Overview of the Admin Tab 16-2
- Managing the Appliance 16-2
 - Using WLSE Log Files 16-4
 - About Log Files 16-5
 - Restarting the WLSE 16-7
 - Managing WLSE System Software 16-7
 - Managing Security 16-15
 - Using an Authentication Module 16-16
 - Managing SSL (HTTPS) 16-18
 - Enabling Telnet and Selecting SSH Type 16-19
 - Viewing the Last 10 Logged-On Users 16-19
 - Backing Up and Restoring Data 16-20
 - Managing WLSE Master Configuration Files (WLSE Express Only) 16-26
 - Managing WLSE Redundancy 16-28
 - Using WLSE Diagnostics Options 16-39
 - Specifying a Splash Screen Message 16-43
 - Setting Time, Time Servers, Name Servers, and Web Session Timeout 16-43
 - Configuring the Mail Route 16-45
 - Managing Files for the WLSE TFTP Server (WLSE Express Only) 16-45
 - Using Connectivity Tools 16-47
- Managing Firmware Version Support 16-49
- Managing GUI Users 16-49
 - Managing Roles 16-49
 - Managing User Accounts 16-51
- Modifying Your Profile 16-55

Changing Your Password	16-56
Changing Your Email Address	16-56
Changing the Default Tab and Subtab	16-56
Creating Links	16-57
Creating a Link to Another System	16-57
Configuring the ACS Failed Login Report Link	16-58
Running the ACS Failed Login Report	16-60

CHAPTER 17

Managing the WLSE System via the CLI 17-1

Using CLI Commands	17-1
Using a Console with the WLSE	17-2
Logging In and Out via CLI	17-2
Logging In	17-2
Logging Out	17-3
User Management via CLI	17-3
Managing User Accounts	17-3
Setting Up TACACS+ or RADIUS Authentication for CLI Login	17-4
Backing Up and Restoring via CLI	17-5
Setting Up the Backup Location	17-5
Backing Up the WLSE	17-6
Restoring WLSE Configuration	17-7
Installing a Replacement WLSE	17-8
Removing the Old WLSE	17-8
Installing the Replacement WLSE	17-8
Copying Configuration Data to another WLSE via CLI	17-9
Upgrading WLSE Software via CLI	17-10
Rebooting the WLSE via CLI	17-10
Shutting Down and Powering Off the WLSE	17-10
Setting WLSE System Date and Time via CLI	17-11
Setting the System Clock Using NTP via CLI	17-11
Setting the System Clock Manually via CLI	17-12
Configuring Ethernet Interfaces	17-12
WLSE 1130 Series Interfaces	17-13
WLSE 1030 Interface	17-13
Configuring Protocols on Ethernet Interfaces	17-13
Configuring Interface Parameters	17-14
Changing the WLSE's IP Address	17-14
Using Both Interfaces on the WLSE 1130 Series	17-14

Configuring the Mail Route via CLI	17-15
Administering Management Services via CLI	17-15
Viewing System Information via CLI	17-15
Managing Disk Space	17-17
Recovery Management	17-17
Erasing System Configuration and Resetting to Factory Defaults	17-18
Using the Maintenance Image	17-18
Using the Recovery CD	17-19
Recovering from the Loss of All Administrator Passwords	17-21

CHAPTER 18

Using the Internal AAA Server (WLSE Express Only) 18-1

About the AAA Server	18-1
Basic Authentication and Authorization	18-2
RADIUS Attributes of the AAA Server	18-2
Supported Services	18-3
Methods of Storing User Information	18-3
Extensible Authentication Services	18-4
Methods of Configuring the AAA Server	18-4
Backup/Restore and Software Upgrades	18-5
Ports Used by the AAA Server	18-5
Fault Monitoring and Trend Reports	18-5
Certificates and RSA Keys	18-5
Configuring the AAA Server—Overview	18-6
Naming Guidelines	18-6
Configuration Methods	18-6
Configuration Tasks	18-6
Reconfiguration Tasks	18-7
Using AAA Server Screens	18-7
AAA Server Administration Subtab Functions	18-8
Displaying AAA Server Status	18-9
Setting AAA Server Trace Level and Viewing Trace Logs	18-10
Trace Levels and Information Logged	18-10
Managing the LDAP Central Server	18-11
Managing the LDAP Local Server	18-12
About LDAP Parameters	18-13
Configuring Windows Domain Authentication	18-15
Configuring LEAP Settings	18-18
Configuring Cisco-PEAP Settings	18-18
Configuring MS-PEAP Settings	18-19

Configuring EAP-TLS Settings	18-21
Configuring EAP-FAST Settings	18-21
Managing AAA Clients	18-23
Managing AAA Users	18-24
Managing Groups	18-26
Viewing and Releasing Sessions	18-27
Using AAA Server Log Files	18-28
Monitoring the AAA Server	18-28
Using AAA Server CLI Commands	18-30
aaa-server cisco-peap	18-32
aaa-server client	18-33
aaa-server domain-auth	18-34
aaa-server eap-fast	18-35
aaa-server eap-tls	18-37
aaa-server ldap	18-37
aaa-server leap	18-39
aaa-server logging	18-40
aaa-server ms-peap	18-41
aaa-server reinit	18-42
aaa-server session	18-43
aaa-server start	18-43
aaa-server status	18-44
aaa-server trace	18-44
aaa-server user	18-45
aaa-server usergroup	18-45
RADIUS Attributes for the AAA Server	18-46
Setting Tunnel Attributes	18-50

APPENDIX A

Command Line Interface (CLI) Commands A-1

Using the CLI	A-1
CLI Conventions	A-2
Command Privileges	A-2
Checking Command Syntax	A-2
Command History Feature	A-2
Help for CLI Commands	A-2
Command Description Conventions	A-3
Command Summary	A-3
CLI Command Details	A-7

aaa-server	A-7
apptyp	A-7
auth	A-7
backup	A-8
backupconfig	A-9
cdp	A-10
clear	A-11
clearbackuphosts	A-11
clearvar	A-12
clock set	A-12
debug	A-13
df	A-14
diagnostic-info	A-15
dumpcores	A-15
dumptcp	A-16
dumptech	A-17
erase config	A-17
exit	A-18
firewall	A-19
gethostbyname	A-20
help	A-20
hostname	A-21
http-server	A-21
import	A-22
install	A-23
interface	A-25
ip domain-name	A-26
ip name-server	A-27
listbackup	A-28
mail	A-28
mailcntrl	A-30
mailroute	A-30
mkcert	A-31
nslookup	A-32
ntp server	A-32
ping	A-34
ps	A-35
radiomanager	A-35
redundancy	A-36
reinitdb	A-37

reload	A-38
repository	A-38
reset device-snmp	A-40
restore	A-41
route	A-42
services	A-42
setup	A-43
show auth-cli	A-44
show auth-http	A-44
show backupconfig	A-44
show backuplog	A-45
show bootlog	A-45
show cdp neighbor	A-46
show cdp run	A-47
show clock	A-47
show config	A-48
show daemonslog	A-48
show dmgtldlog	A-49
show domain-name	A-50
show hosts	A-50
show http-server	A-51
show import hosts	A-51
show install	A-51
show interfaces	A-53
show ipchains	A-53
show maillog	A-54
show mailroute	A-55
show proc[ess]	A-55
show redundancy	A-56
show repository	A-57
show route	A-57
show securitylog	A-58
show snmp-server	A-59
show ssh-server	A-59
show ssh-version	A-59
show syslog	A-60
show tech	A-61
show telnetenable	A-61
show time	A-62
show tomcatlog	A-62

show version	A-63
show webaccesslog	A-63
show weberrorlog	A-64
show websslaccesslog	A-65
shutdown	A-65
snmp-server	A-66
ssh host	A-67
ssh-server accept	A-67
ssh-version	A-68
tarlog	A-68
telnet	A-68
telnetenable	A-69
tftpserver	A-70
traceroute	A-70
username	A-71
webtimeout	A-72
Maintenance Image Commands	A-73
erase config	A-73
fsck	A-73
reload	A-73

APPENDIX B
Naming Guidelines B-1

Naming Rules for Users and Roles	B-1
Naming Rules for Hostnames and Device Names	B-2
Naming Rules for Other Names and Descriptions	B-2
Naming Rules for Domain Names	B-3
Naming Rules for the Built-In AAA Server (WLSE Express Only)	B-3
Naming Rules for Authentication Modules	B-4

APPENDIX C
Ports and Protocols C-1

Ports Used by the WLSE	C-1
Ports Hosted by the WLSE	C-2
Transport Protocols and Authentication Methods Used by the WLSE	C-2

GLOSSARY

INDEX



Preface

Revised: June 5, 2006, OL-8374-01

This guide describes the features of the CiscoWorks Wireless LAN Solution Engine (WLSE) and the WLSE Express and provides instructions for using them. This guide consists of the following chapters and appendixes and a glossary of terms:

- [Preface](#)
- [Getting Started](#)
- [Fault Monitoring](#)
- [Device Discovery and Management](#)
- [Using IOS Templates](#)
- [Using WLSM Templates](#)
- [Managing Device Configurations](#)
- [Upgrading Device Firmware](#)
- [Using Reports](#)
- [Managing Your WLAN Radio Environment by Sites](#)
- [Using the Intrusion Detection System](#)
- [Managing the WLSE System](#)
- [Managing the WLSE System via the CLI](#)
- [Using the Internal AAA Server \(WLSE Express Only\)](#)
- [Naming Guidelines](#)
- [Command Line Interface \(CLI\) Commands](#)
- [Ports and Protocols](#)

Audience

This document is for system administrators and network administrators who are responsible for managing a wireless network and are familiar with the concepts and terminology of Ethernet and wireless local area networking.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	boldface font
Variables for which you supply values	<i>italic</i> font
Displayed session and system information	screen font
Information you enter	boldface screen font
Variables you enter	<i>italic screen</i> font
Menu items and button names	boldface font
Selecting a menu item in paragraphs	Option > Network Preferences
Selecting a menu item in tables	Option > Network Preferences

**Note**

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

**Caution**

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

Product Documentation

**Note**

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

[Table 1](#) describes the available product documentation for WLSE 2.13. Unless otherwise indicated, all documentation applies to both the WLSE and WLSE Express platforms.

Table 1 **Product Documentation**

Document Title	Available Formats
<i>Release Notes for the CiscoWorks Wireless LAN Solution Engine</i>	On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_release_notes_list.html
<i>Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine</i>	On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html
<i>Installation and Configuration Guide for the 1130-19 CiscoWorks Wireless LAN Solution Engine</i>	- Printed document included with the product. - PDF on the WLSE Recovery CD-ROM. - On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html
<i>Installation and Configuration Guide for the 1030 CiscoWorks Wireless LAN Solution Engine Express</i>	- Printed document included with the product. - PDF on the WLSE Recovery CD-ROM. - On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html
<i>Installation and Configuration Guide for the 1133 CiscoWorks Wireless LAN Solution Engine</i>	- Printed document included with the product. - PDF on the WLSE Recovery CD-ROM. - Online: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_13/index.htm
<i>Regulatory Compliance and Safety Information for the 1130-19 CiscoWorks Wireless LAN Solution Engine</i>	- Printed document included with the product. - PDF on the WLSE Recovery CD-ROM. - On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html
<i>Regulatory Compliance and Safety Information for the 1030 CiscoWorks Wireless LAN Solution Engine Express</i>	- Printed document included with the product. - PDF on the WLSE Recovery CD-ROM. - On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html
<i>Regulatory Compliance and Safety Information for the CiscoWorks 1133 Wireless LAN Solution Engine</i>	- Printed document included with the product. - PDF on the WLSE Recovery CD-ROM. - Online: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_13/index.htm

Table 1 **Product Documentation (continued)**

Document Title	Available Formats
<i>User Guide for the CiscoWorks Wireless LAN Solution Engine</i>	- From the WLSE online help. - PDF on the WLSE Recovery CD-ROM. - On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html
<i>Upgrading CiscoWorks Wireless LAN Solution Engine Software</i>	- From the WLSE online help. - On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html
<i>Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine</i>	On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_device_support_tables_list.html
Context-sensitive online help	Select an option from the WLSE navigation tree, then click Help .
<i>FAQ and Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine</i>	- From the WLSE online help. - On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_troubleshooting_guides_list.html
<i>Developer Guide for the CiscoWorks Wireless LAN Solution Engine</i>	Development information for the WLSE's XML application programming interface. On Cisco.com in the Software Center: http://www.cisco.com/cgi-bin/tablebuild.pl/wlan-sol-eng
<i>Configuring the CiscoWorks Wireless LAN Solution Engine TACACS+/RADIUS Authentication Using CiscoSecure ACS</i>	On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>



Getting Started

The following topics provide an overview of the Wireless LAN Solution Engine (WLSE), information about WLSE displays, and assistance with getting started:

- [Before You Begin, page 1-1](#)
- [Overview of the Wireless LAN Solution Engine, page 1-2](#)
- [Integrating the WLSE with Network Management Systems, page 1-3](#)
- [Understanding the Web Interface, page 1-4](#)
- [Configuring the Web Browser, page 1-4](#)
- [The WLSE Dashboard, page 1-7](#)
- [Device Identifier Display, page 1-10](#)
- [Understanding WLSE Time Displays, page 1-10](#)
- [Using the Device Selector, page 1-12](#)
- [Using Search, page 1-12](#)
- [Understanding the Icons, page 1-12](#)
- [Sorting Table Data, page 1-13](#)
- [Logging In and Out, page 1-13](#)
- [Customizing the Web Interface, page 1-14](#)
- [Finding WLSE Documentation on Cisco.com, page 1-15](#)



Caution

The WLSE does not support Network Address Translation (NAT).

Before You Begin

Before using the WLSE for monitoring, reporting, and other tasks, you should:

- Install and configure the WLSE or WLSE Express, as described in the relevant installation and configuration guide:
 - *Installation and Configuration Guide for the CiscoWorks 1130-19 Wireless LAN Solution Engine, Release 2.13.*
 - *Installation and Configuration Guide for the CiscoWorks 1030 Wireless LAN Solution Engine Express, Release 2.13.*

- Set up devices and device management by either:
 - Using the Deployment Wizard (for deploying access points and [WDS](#) devices in a Cisco [SWAN](#) framework), as described in the online help and [Chapter 2, “Using the Deployment Wizard.”](#)
 - Using the procedures in *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine* and [Chapter 4, “Device Discovery and Management.”](#)

For information on locating these documents on Cisco.com, see [Finding WLSE Documentation on Cisco.com, page 1-15.](#)

Overview of the Wireless LAN Solution Engine

The WLSE is a hardware and software solution for managing Cisco wireless devices. The WLSE has the following major features:

- Configuration and Firmware

The configuration feature allows you to apply a set of configuration changes to access points and bridges and to archive configurations. Using the firmware feature, you can upgrade the firmware on access points and bridges.
- Reporting

Allows you to display reports for tracking device, client, and security information. Reports can be emailed, printed, and exported.
- Fault and Policy Monitoring

Provides device monitoring for fault and performance conditions, monitoring of authentication server responses, and monitoring of policy misconfigurations.
- Radio Management

Helps you manage your WLAN radio environment. All the device information shown under this tab is polled from the managed devices in your network. Radio Manager features simplify the deployment, expansion, and day-to-day management of the WLAN.
- Site Management

Displays a graphical view of the WLAN environment.
- Intrusion Detection System (IDS)

Displays intrusion detection information for devices in your network and allows you to manage IDS settings and set up IDS notifications.
- Voice Management

Allows you to display voice call information for devices in your network, manage voice settings, and set up voice notifications.

The WLSE works by gathering fault, performance, and configuration information about Cisco devices that it discovers in your network. The devices must be properly configured for discovery. After devices are discovered, you decide which devices to manage with the WLSE.

Integrating the WLSE with Network Management Systems

You can integrate the WLSE with other network management systems as follows:

- Add a link to a WLSE from a CiscoWorks server, using CiscoWorks Management Connection—See [Integrating the WLSE with a CiscoWorks Server, page 1-3](#).
- Launch a CiscoWorks server's desktop from the WLSE—See [Creating Links, page 16-57](#).
- Use the WLSE's fault notification interface to forward WLSE faults as SNMP traps and syslog messages—See [Notification Settings, page 3-56](#).



Note For information about the SNMP trap version that is supported by the WLSE, see [Setting Trap Notification, page 3-56](#).

- Forward intrusion detection system (IDS) events to network management systems.
- Share inventory by exporting devices to and importing devices from Resource Manager Essentials (RME) running on a CiscoWorks server—See the following:
 - [Exporting Devices to a CiscoWorks Server, page 4-71](#)
 - [Importing Devices from a CiscoWorks Server, page 4-39](#)

Integrating the WLSE with a CiscoWorks Server

You can use CiscoWorks Management Connection to add external application links to a CiscoWorks server's navigation tree. Such links allow you to access the applications directly from the navigation tree.

Adding links to a WLSE involves installing a connection to the WLSE's URL, as outlined in the following procedure.

Procedure

-
- Step 1** Enter the CiscoWorks server's URL in the browser (for example, <http://my-cwserver:1741/>).
- Step 2** Select **Management Connection > Administration > Create**.
- Step 3** Follow the directions in the CiscoWorks online help.



Note In the screen titled Enter Item Information, enter any name for the connection in the Item Name field. Enter `main.html` in the URL field.

- Step 4** When you finish, the connection to the WLSE appears under **Management Connection > Connections**.
-

Understanding the Web Interface

When you log into the WLSE through the World Wide Web, the set of features (tabs and subtabs) displayed in the UI depends on the roles assigned to your user login. A user with system administrator privileges can access the features in all of the tabs and subtabs, while other users may see only a subset of features. For more information about user roles, see [Managing Roles, page 16-49](#).

This section describes the following aspects of the UI:

- The supported browsers and versions and browser configuration—See [Configuring the Web Browser, page 1-4](#).
- The dashboard, including tabs and subtabs, buttons and messages in the upper right corner; and Deployment Wizard—See [The WLSE Dashboard, page 1-7](#).
- How device names and IP addresses are displayed in the WLSE GUI—See [Device Identifier Display, page 1-10](#).
- How the WLSE displays time—See [Understanding WLSE Time Displays, page 1-10](#).
- How to use the device selector and Search—See [Using the Device Selector, page 1-12](#).
- How to sort table data—See [Sorting Table Data, page 1-13](#).

Configuring the Web Browser

Normally, all WLSE tasks are performed in the Web interface. Before you connect to the Web interface, make sure you are using a supported browser and that the browser is properly configured.

- [Supported Browsers, page 1-4](#)
- [Configuring Internet Explorer, page 1-5](#)
- [Configuring Firefox, page 1-6](#)
- [The WLSE Dashboard, page 1-7](#)

**Note**

While using the WLSE's Web interface, you should disable popup-blocking software or add the WLSE to the "allow" list.

Supported Browsers

Before connecting to the WLSE web interface, make sure you are using a supported browser and the browser is properly configured. The supported browsers for WLSE 2.13 are listed in [Table 1-1 on page 1-5](#). Use the procedures in [Configuring Internet Explorer, page 1-5](#), [Configuring Firefox, page 1-6](#), or [The WLSE Dashboard, page 1-7](#) to configure your browser.

**Note**

Using earlier, unsupported versions of Internet Explorer compromises the security of the WLSE.

Table 1-1 Supported Browsers

Client Operating System	Supported Browsers
Windows 2000, Windows NT, and Windows XP	Microsoft Internet Explorer 6.0 with Service Pack 1 Firefox 1.0.6
Japanese Windows 2000, Windows NT, and Windows XP	Japanese Microsoft Internet Explorer 6.0 with Service Pack 1 Firefox 1.0.6
Solaris 8 and 9	Firefox 1.0.6
Japanese Solaris 8 and 9	Japanese Firefox 1.0.6
Java plug-in	1.5 Note The Java Plug-in is required for some WLSE functions, such as Location Manager.

Configuring Internet Explorer



Note

While using the WLSE's Web interface, you should disable popup-blocking software or add the WLSE to the "allow" list.

To configure Internet Explorer 6.0, perform the following steps:

-
- Step 1** Select **Tools > Internet Options**.
- Step 2** Enable JavaScript:
- Select **Security**.
 - Make sure that the Internet icon is selected, and click **Custom Level**.
 - Scroll to Scripting and select the following:
 - Select Enable for Active scripting.
 - Select Enable for Allow paste operations via script.
 - Select Enable for **Scripting of Java applets**.
 - Click **OK**.
- Step 3** Configure the browser to accept all cookies:
- Select **Privacy**.
 - Move the slider down to until "Accept all Cookies" appears.
 - Click **OK**.
- Step 4** Change the default font to improve readability:
- Select **General**. Then elect **Fonts**.
 - Select a sans-serif font (for example, Arial) from the **Web page font** and **Plain text font** lists.
 - Click **OK**, then click **OK** again.

The text in the browser window is redrawn using the new fonts. Not all of the fonts will change after this user-defined font option is set.

Step 5 Disable caching:

- a. Select **General**. Then select **Settings**.
- b. Under “Check for newer versions of stored pages,” select **Every visit to the page**.

Step 6 Click **OK**.

Step 7 Windows XP does not come with the Java Plugin installed on Internet Explorer 6.0. This causes problems when updating the software on a WLSE. If you plan to use a Windows XP client or server to update WLSE software, see the following references:

- Using a Windows XP client and Internet Explorer 6.0—See [Installing the Software Upgrade, page 16-12](#).
 - Using a Windows XP server and Internet Explorer 6.0—See [Creating a Repository on a Windows Server, page 16-11](#).
-

Configuring Firefox



Note

While using the WLSE's Web interface, you should disable popup-blocking software or add the WLSE to the “allow” list.

To configure Firefox 1.0.6, perform the following steps:

Procedure

Step 1 Select **Tools > Options**.

Step 2 Configure the browser to accept cookies:

- a. Select **Privacy > Cookies**.
- b. Select **Allow sites to set cookies**.
- c. Select **until they expire**.

Step 3 Enable Java:

- a. Select the **Web Features** panel.
- b. Select **Enable Java** and **Enable Javascript**.

Step 4 Click **OK**.

The WLSE Dashboard

The WLSE dashboard consists of:

- Tabs and subtabs that provide access to WLSE functions (see [Tabs and Subtabs, page 1-7](#)).
- Buttons in the upper right corner that provide general functions (see [Buttons, page 1-9](#)) and provide access to the Deployment Wizard. For information on the Deployment Wizard, see [Chapter 2, “Using the Deployment Wizard.”](#)
- Messages, in red, in the upper right corner indicate failed processes. For more information on processes, see [Managing Processes, page 16-40](#).

Tabs and Subtabs

The dashboard contains the following tabs and subtabs:

Table 1-2 **Tabs and Subtabs**

Main Tab	Subtabs	For information, see...
IDS	Intrusion Detection System: • Setup—create thresholds and policies for Intrusion Detection monitoring. • Summary—view summaries of all intrusions. • Faults—display intrusion detection fault information for the devices in your network. • Reports—view intrusion detection reports on recently polled device information. • Unknown AP Setting—view and change Rogue AP to Friendly AP.	Using the Intrusion Detection System, page 14-1
Faults	• Display Faults—display device faults. • Manage Fault Settings—use profiles to set thresholds and policies. • Voice Summary—view a summary of the current Voice status of the WLAN. • Voice QoS Settings—assign voice quality of service configuration settings. • Notification Settings—send fault information (traps, syslog messages, and emails).	Fault Monitoring, page 3-1
Devices	• Discover—enable discovery options and run discoveries, reset polling intervals, enter device credentials, manage devices, run inventories, view inventory and discovery logs, import and export devices, monitor AAA servers, and enable enhanced (WDS) client tracking. • Group Management—use system-defined groups and manage device grouping by setting up static and dynamic groups.	Device Discovery and Management, page 4-1

Table 1-2 **Tabs and Subtabs (continued)**

Main Tab	Subtabs	For information, see...
Configure	• Templates—create IOS access point templates and WLSM configuration templates, and modify Wizard templates.	• Using IOS Templates, page 5-1 • Using WLSM Templates, page 6-1 • Using Wizard Templates, page 7-1
	• Archives—view and manage archived configurations. • Jobs—apply configuration templates to access points and retrieve configurations for archiving. • Auto Update—automate initial configuration of access points. • Device Specific—Import and export device specific settings.	Managing Device Configurations, page 8-1
Firmware	• Images—import firmware for access points and bridges from the desktop or from Cisco.com to the WLSE. • Jobs—upload firmware to access points. • Advanced Parameters—set timing parameters for firmware upgrades.	Upgrading Device Firmware, page 9-1
Reports	• Device Center—view device reports. • Radio Manager—view radio management reports. • Voice—view voice reports containing recently polled device information. • Wireless Clients—view reports about client associations with access points. • Current—view, export, and email reports. • Trends—view, export, and email reports about current trends. • Realtime—view current reports. • Scheduled Email Jobs—manage email jobs.	Using Reports, page 10-1
Radio Mgr	• Radio Monitoring—monitor WLAN and collect channel measurements for radio configuration, rogue AP discovery, and interference detection. • Self Healing—adjust radio parameters of APs using the generated radio measurements to eliminate coverage holes in the face of network failure. • Auto Re-Site Survey—evaluate current AP radio performance on a per-floor basis against baselined performance data. • Frame Monitoring—capture frames of scanning AP and forward to an external frame analysis and monitoring tool.	Configuring Your WLAN Radio Environment, page 11-1 Managing Your WLAN Radio Environment, page 12-1

Table 1-2 **Tabs and Subtabs (continued)**

Main Tab	Subtabs	For information, see...
Sites	- Location Manager—Display graphical view of WLAN environment, including AP locations, radio configurations, and estimated location of unknown APs. - AP Radio Scan—collect rogue location estimates, radio parameter generation (RPG) data, and coverage data. - Client Walkabout—collect radio measurements and report them to the serving AP as you walk a client station throughout the coverage area. - Assisted Configuration—configure APs using measurement data collected from client walkabouts and AP radio scans. - Manage Data—manage collected Radio Measurements.	Managing Your WLAN Radio Environment by Sites, page 13-1
Admin	- Appliance—manage the WLSE system (view diagnostics, manage WLSE software, manage WLSE security, backup and restore data, configure WLSE redundancy, configure the login screen, set current time, specify NTP servers and name servers, set up routing for email jobs, use connectivity tools and the SNMP query tool, manage files for the built-in TFTP server (WLSE express only), and create WLSE configuration files (WLSE Express only). - System—view information about supported device firmware versions, and import information about newly supported firmware versions. - AAA Administration—(WLSE Express only) use built-in RADIUS server for authentication, and authorization. - User Admin—manage users and user profiles. - My Profile—reset your password and email address and configure your login environment. - Links—set up and activate links to other systems (such as other WLSEs and CiscoWorks servers) and run ACS failed login reports.	Managing the WLSE System, page 16-1

Buttons

The buttons in the upper right corner of the user interface have the following functions:

- Wizard—Displays the Deployment Wizard. See [Chapter 2, “Using the Deployment Wizard”](#) for more information.

The Deployment Wizard configures devices and the WLSE and deploys devices in a WDS (Wireless Domain Service) WLAN.

- Overview—Displays an overview of the tabs and their functions.
- Help—Displays an online help topic for the option you are using and the help table of contents and index.

In the online help screens, you can also display the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13* by clicking **View PDF**.

You can also display the *FAQ and Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine* by clicking **Troubleshooting**.

- About—Displays information about the WLSE software and hardware versions.
- Logout—Logs you out of the WLSE and displays the login screen.

Device Identifier Display

Many WLSE displays include a field for the device identifier:

- By default, the identifier is the device's hostname—See [Default Device Identifier Display, page 1-10](#).
- You can select whether devices will be identified by their DNS name, hostname, IP address, device type, user-defined description, Ethernet MAC address, radio MAC address, or a combination of these identifier types—See [User-Defined Device Identifier, page 1-10](#).

Default Device Identifier Display

By default, the device identifier type is the device hostname. In some displays there are separate fields for device name, sysName, and IP address.

User-Defined Device Identifier

To specify how to identify devices in WLSE displays, select **Devices > Discover > DISCOVER > Advanced Options**. Then enter the desired identifier type in the Name Format field.

If you select the description option, you specify a name for each type in the device detail screen under **Devices > Discover > Managed Devices**.

For more information on using this option, see the online help or [Selecting the Device Name Format, page 4-41](#).

Understanding WLSE Time Displays

It is recommended that you check the current local time on the WLSE the first time you log in. If you need to reset the time, see [Set the Current Local and UTC Time, page 16-43](#). To use NTP to set the time, see [Setting Time, Time Servers, Name Servers, and Web Session Timeout, page 16-43](#).

This section contains information on:

- How time appears in WLSE displays—See [General Time Displays, page 1-11](#).
- A warning message that may appear when you are running WLSE jobs—See [Understanding Time Discrepancy Problems in Job Scheduling, page 1-11](#).

General Time Displays

The WLSE uses browser (client) time in most of its displays. The current WLSE server time, in your local timezone, is displayed in the upper right corner of the screen.

In Internet Explorer, the timestamp usually consists of the browser time (hours:minutes:seconds) and date; for example:

14:17:16 10/12/2005

In some displays the timestamp is the day of the week, month and day, browser time, timezone, and year; for example:

Sat Oct 12 11:15:01 PDT 2005

The WLSE's internal system time is Universal Coordinated Time (UTC), and UTC is displayed in certain logs, such as the discovery run log.

Understanding Time Discrepancy Problems in Job Scheduling

When you schedule a job based on your local time, the scheduled time that you select in the job wizard is converted to the appropriate WLSE server time by using the timezone in which the client system is located.

If a significant time difference is discovered (more than 5 minutes), a warning message is displayed in the final step of the job scheduling wizard. The message displays the offset and whether the WLSE is ahead of or behind your local time.

**Note**

The WLSE server time, in your local timezone, is always displayed in the upper right corner of the screen, so you can compare your local time with the server time.

Procedure

If a time offset warning message appears:

Step 1

Select an action:

- If you click **Cancel**, the job is not saved. The wizard remains at the scheduling screen so you can reschedule the job, if desired.
- If you click **OK**, the wizard will finish and the job will be scheduled. The actual time that the job is run will be ahead of or behind the scheduled time.

Step 2

To synchronize your local time with WLSE server time, see [Set the Current Local and UTC Time, page 16-43](#).

**Note**

Resetting the local time also resets the server time.

Using the Device Selector

To select a group of devices or individual device for which you want to run a report, use the device selector in the left pane of some displays.

Procedure

-
- Step 1** Click to expand the desired folder.
- Step 2** Click to select a group of devices or an individual device.
-

Using Search

To search for a device, use the dialog box in the left pane above the device selector.



Note

Not all of the following search methods are available on all of the screens.

Procedure

-
- Step 1** From the list, select the method you want to use to search for the device, then enter the search information.
- Device Name—The name of the device.
 - IP Address—The IP address of the device.
 - AP MAC Address—The Ethernet and radio MAC addresses of the device.
 - Device Description—The description of the device.
 - Serial Number—The top assembly serial number of the access point.
 - APs Based on Client MAC—The MAC address of a known client.
 - APs Based on Client Name—The name of a known client.
 - APs Based on Client IP—The IP address of a known client.
 - Use an asterisk (*) as a wildcard to denote numbers and letters.
- Step 2** Click **Search**. The requested device appears in the Search Results folder.
-

Understanding the Icons

Search results and folders in the device selector display the following icons indicating the alarm status of the devices:

- Red X—Indicates a P1 or P2 fault or the device is unreachable.
- Yellow exclamation—Indicates a P3, P4, or P5 fault and the device is reachable.
- Green check—Indicates the device has no faults and is reachable.

The icons on the folders reflect the status of the highest severity fault for any of the devices or folders within that folder.

Sorting Table Data

To sort table data, click on the column heading by which you want to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Logging In and Out

After initial setup, only the admin user can log into the WLSE, using the reserved username **admin** and the password specified during initial setup. When you use the Web interface to create other logins, you assign one or more roles to each user. Roles define which tabs and subtabs are visible to the user and, therefore, which features users can access. There are predefined roles, which can be edited but not removed; and you can create new roles. You can also assign CLI privileges.

To set up access for other users, see [Managing User Accounts, page 16-51](#) and [Managing Roles, page 16-49](#). The WLSE supports up to 10 simultaneous users.

To log in via the CLI, see [Logging In and Out via CLI, page 17-2](#). Some users may not have access to the CLI.

**Note**

The WLSE Web interface times out after 30 minutes of inactivity. You will be logged out after that time. To change the timeout period, see [Set the Web Timeout Period, page 16-44](#).

Procedure

To log into the Web interface:

Step 1

Access the WLSE through a browser by entering the WLSE's IP address or hostname, followed by **:1741** (for example: <http://209.165.128:1741>).

**Note**

The default HTTP port is 1741, but the administrator can configure the WLSE to use port 80 instead. In that case, use the WLSE's IP address or hostname followed by **:80**.

If you using [HTTPS](#) to log in, do not append a port number to the IP address or hostname.

**Tip**

For information on supported browsers, see [Supported Browsers, page 1-4](#).

Step 2

Enter your username and password and click **Login**.

If you do not see the features you need to use, log out and log back in as a user with those privileges. Contact the system administrator for information about the features you can access.

To log out, click **Logout** in the upper right corner of the window.

Related Topics

[Logging In and Out via CLI, page 17-2](#)

Customizing the Web Interface

You can customize the Web interface by:

- [Setting the Default Tab and Subtab, page 1-14](#)
- [Adding a Message to the Splash Screen, page 1-14](#)

Setting the Default Tab and Subtab

By default the overview screen appears when you log in and provides a brief description of each of the main tabs. When you select a tab, the overview changes to describe each of the subtabs.

Use the following procedure to customize the initial display.

Procedure

-
Step 1	Select Set Tab Defaults in the upper right corner of the overview screen, or select Administration > My Profile > Set Tab Defaults .
Step 2	Select a tab from the list.
Step 3	Select a subtab or the Overview from the pulldown list.
Step 4	Click Save .

Result: The next time you log in, your home page will be the tab and subtab that you selected.

Adding a Message to the Splash Screen

Use the following procedure to add a message to the splash screen that appears just before the login prompt.

Procedure

-
Step 1	Select Administration > Appliance > Splash Screen .
Step 2	Enter your message.
Step 3	Select Enable .

Result: Your message appears before users log in. Users must click **Agree** in the splash screen.

Finding WLSE Documentation on Cisco.com

You can find WLSE 2.13 documentation on Cisco.com by using one of the following methods.

- Use the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_13/index.htm
- On the Cisco.com home page, select **Technical Support and Documentation > Product Support > Network Management > Wireless Access Management**, then select either **CiscoWorks Wireless LAN Solution Engine** or **CiscoWorks Wireless LAN Solution Engine Express**.



Using the Deployment Wizard

The Deployment Wizard enables you to configure a wireless LAN (WLAN) using the Cisco Structured Wireless-Aware Network (SWAN) framework.

Using the wizard, you can deploy your network using the Wireless Domain Services ([WDS](#)) provided by the following:

- Wireless LAN Services Modules (WLSM)
- WDS access points

About the Deployment Wizard

The Deployment Wizard replaces many of the manual configuration procedures that are normally required to configure infrastructure access points and WDS devices and to configure the WLSE to discover and manage those devices.

Specifically, the Deployment Wizard helps you configure a Wireless LAN (WLAN) using the Cisco Structured Wireless-Aware Network (SWAN) framework. (For additional information on SWAN, see the *Cisco Structured Wireless-Aware Implementation Guide* on Cisco.com.) The wizard creates basic configurations for access points (APs) that can be deployed to existing devices managed by WLSE or deployed to devices that are added later. The wizard also configures WDS devices.

Besides configuring the devices to be managed by the WLSE, the Wizard enters the necessary device credentials on the WLSE and places devices in the managed state.

Newly-installed devices require basic configuration in order to be managed by the WLSE. The basic configurations created by the Wizard can be applied only to devices that are supported by the WLSE. Configurations are downloaded to devices when the devices power up and are deployed according to criteria that you set in the Wizard.

The SWAN framework for WLANs relies on the presence of Wireless Domain Services (WDS). WDS can be supplied by access points or a Wireless LAN Services Module ([WLSM](#)).

The Wizard configures WDS devices as follows:

- WDS-WLSM—If you use a WLSM, you must manually configure some parameters on the WLSM. Details on how to configure the WLSM are displayed in the Wizard's Requirements screen. Other parameters are configured by the Wizard.
- WDS-AP—If you use access points for WDS, you can chose manual or automatic configuration.

For configuring the access points, you configure a DHCP server to upload the initial configuration provided by the WLSE to newly-installed devices. Details on how to configure DHCP are displayed in the Deployment Wizard's Requirements screen.

Finally, a RADIUS server is required. You can use a separate AAA server or configure a WDS access point as a RADIUS server.

Related Topics

[Using the Deployment Wizard, page 2-2](#)

Using the Deployment Wizard



Note

The roles and privileges assigned to your login determine whether you can use the Deployment Wizard. Select **Admin > User Admin > Manage Roles**, and make sure that both the **Wizard > WLSE Wizard** and **Configure > Auto Update** options are checked.



Note

If you do not want the wizard to launch at login, deselect the **Launch at login** checkbox. Then, when you want to launch the Wizard, click **Wizard** in the upper right corner of the screen.

The wizard steps you through the following screens:

1. **Description**—See [Description, page 2-2](#).
2. **Deployment Type**—See [Choosing the Deployment Type, page 2-3](#).
3. **Requirements**—See [Satisfying Requirements, page 2-4](#).
4. **Software**—See [Checking Software Versions, page 2-4](#).
5. **Configuration**—See [Creating the Configuration Template, page 2-4](#).
6. **WDS Setup**—See [Setting up the WDS, page 2-7](#).
7. **Deploy**—See [Deploying the Configuration, page 2-9](#).
8. **Finish**—See [Finishing, page 2-11](#).



Note

In all of the screens, click **Next** to move to the next screen, and click **Back** to modify a previous screen.

Related Topics

[About the Deployment Wizard, page 2-1](#)

Description

The Description screen displays general information about the Wizard and allows you to disable automatic launch of the Wizard after login.

Before completing a deployment using the Wizard, you will need to set up a DHCP server with boot file options that specify the IP address of the WLSE and the initial configuration file name (wlsestartup.ini). Details on DHCP requirements are explained in the Requirements screen.

When you finish going through the steps in the Wizard and install a new device in the network, the following occur:

1. The newly powered on device contacts the DHCP server to provide an IP address.
2. The device downloads the `wlsestartup.ini` file, which contains only minimal credentials and a command to Telnet to the WLSE.
3. The WLSE then discovers the device, adds it to inventory, manages it, and downloads a configuration template to it via SSH.

This template contains user-specified credentials (entered in the Wizard Configuration step), which overwrite the existing minimal credentials that were uploaded in the `wlsestartup.ini` file. The template also contains security information.

The Deployment Wizard launches right after you log in. To change this default behavior, so the Wizard does not automatically launch, deselect **Launch at Login** in this screen. To launch the Wizard, click **Wizard** in the upper right corner of any screen.

Related Topics

- [About the Deployment Wizard, page 2-1](#)
- [Using the Deployment Wizard, page 2-2](#)

Choosing the Deployment Type

Use this option to specify the type of deployment:

- **AP**—[infrastructure access points](#) with wireless domain services (**WDS**) provided by WDS access points (APs).

The WDS provides control path technologies that must be active on an AP in each AP subnet. For more information, see [Understanding WDS Access Points, page 11-8](#).

- **WLSM**—[infrastructure access points](#) with wireless domain services (**WDS**) provided by a wireless LAN service module (**WLSM**).

The WLSM is a module for the Cisco Catalyst 6500 series switches that provides WDS to the wireless network. For additional information, see [Understanding WLSM WDS Devices, page 11-9](#).

Procedure

-
Step 1	Select either WLSM or AP , depending on the type of WDS deployment you are using.
Step 2	The screen refreshes and the next screen appears. See Satisfying Requirements, page 2-4 .
-

Related Topics

- [What is WDS and Why Do I Need It?, page 11-8](#)
- [About the Deployment Wizard, page 2-1](#)

Satisfying Requirements

The Requirements screen provides information about configuration that must be completed outside the Wizard. The displayed requirements provide all the necessary details and are based on the deployment type you chose—WDS-AP or WDS-WLSM.

For either AP or WLSM WDS, you must configure DHCP. Optionally, you can configure [AAA](#) server settings. For WLSM WDS, there are further requirements.

Click **Next** to continue. See [Checking Software Versions](#), page 2-4.

Checking Software Versions

This screen lists the minimum and recommended image versions for different device types. Devices must meet or exceed the minimum image versions in order to be deployed by the Wizard.

- Click **Import Image** to import a new image from the desktop or from Cisco.com—See [Importing Images to the WLSE](#), page 9-6.
- Click **Firmware Upgrade** to schedule a firmware upgrade for managed devices—See [Managing Firmware Jobs](#), page 9-11.
- Click **Compare Known Devices Version** to check the firmware installed on devices that have already been discovered and inventoried. A table of devices is displayed showing:
 - Devices with firmware that does not meet the minimum version (displayed in red). These devices are not supported by the Wizard.
 - Devices that meet the minimum version requirement but do not have the recommended firmware installed (displayed in yellow). These devices are supported by the Wizard.
 - Devices that have the recommended firmware (displayed in green). These devices are supported by the Wizard.

Click **Back** to return to the display of images for all devices.

Click **Next** to continue. See [Creating a General Configuration](#), page 2-4

Creating the Configuration Template

The Wizard uses two screens to create a configuration template:

- General configuration (credentials)—see [Creating a General Configuration](#), page 2-4.
- Security configuration—see [Creating a Security Configuration](#), page 2-6.

The template created by the Wizard is saved and is listed under **Configuration > Templates** as template type WIZARD. You can use the normal WLSE configuration template features to copy, edit, and delete templates; export templates to your local drive; and import templates from a file or from devices. For more information on managing Wizard templates, see [Chapter 7, “Using Wizard Templates.”](#)

Creating a General Configuration

This option creates a general configuration (set of AP credentials) to be applied to APs and added to the WLSE's database. You can add as many sets of credentials as you need. The credentials that you enter here are:

- Telnet or SSH username and password and enable password—Required for applying configuration templates and upgrading firmware on APs.
- SNMP community strings—Required for discovering devices and enabling other WLSE options, such as firmware upgrades, applying configuration templates, and radio management.

Procedure

Step 1 Complete the following:

Table 2-1 General Configuration

Field	Description
Name	Name for the configuration. Note You will use this name in the Wizard's Deploy step to assign the General Configuration to one or more access points.
Protocol	Select Telnet or SSH, and enter the following device credentials. Note Usernames and passwords must match the login sequence on the access points. For more information see Supported Telnet/SSH Login Sequences for APs, page 4-11 .
User Name	Telnet or SSH user name. The following characters are not supported and cannot be entered in this field: double quote, single quote, and angle brackets (< >).
Password	Telnet or SSH user password.
Password Confirm	
Enable Secret	Telnet or SSH secret password.
Enable Secret Confirm	
SNMP RO Community	Read/write and read-only community strings.
SNMP RW Community	Both read/write and read-only community strings are required in order to enable all WLSE management functions. For more information on community strings (including characters that are not supported or not recommended), see Recommendations For Configuring SNMP Credentials, page 4-8 .

Step 2 Click **Add**. The General Configuration is added to the table at the bottom of the screen.



Note The General Configuration template name that you create with the Wizard also appears in the template listings under **Configure > Templates**.

- Step 3** Repeat steps 1 and 2 to add more configurations.
- Step 4** To remove a configuration, click **Delete** next to the name of the configuration in the table.
- Step 5** Click **Next** to continue. See [Creating a Security Configuration, page 2-6](#).

Creating a Security Configuration

This option sets up simple security configurations. This will allow you to enter all the access points' essential settings for basic security.

Procedure

- Step 1** Complete the following:

Table 2-2 Security Configuration

Field	Description
SSID Configuration	
Apply to	Select one or both of the following: - Radio B/G—Select this option for radio 802.11b/g. - Radio A—Select this option for radio 802.11a.
SSID	Select one of the following: - Enter any alphanumeric, case-sensitive string, from 1 to 32 characters long. - Select Broadcast SSID in Beacon to allow devices without a specified SSID to associate with this access point. Click Broadcast SSID in Beacon for additional information.
VLAN	Note For AP-WDS deployments only. Select one of the following: - No VLAN—Use this setting if there is no VLAN. - Enable VLAN ID—Use this setting to indicate there is a VLAN and enter the VLAN identification number. - Native VLAN—Select if this is a Native VLAN. - Bridge Group ID—Enter the bridge group identification number.
Mobility	Note For WLSM-WDS deployments only. Select one of the following: - No Mobility Network ID—Select this if a mobility network ID is not required. - Enable Mobility Network ID—Use this option to require the use of a mobility network ID, then enter the ID number.

Table 2-2 Security Configuration (continued)

Field	Description
Security	Select one of the following: • No Security—Use this setting if you do not want to specify security options. Click No Security for additional information. • Static WEP Key—Use this setting to specify WEP encryption. Click Static WEP Key for additional information. – For 40-bit WEP keys, enter 10 hexadecimal digits (0-9, a-f, A-F). – For 128-bit WEP keys, enter 26 hexadecimal digits (0-9, a-f, A-F). • EAP Authentication—Use this setting to specify mandatory WEP, encryption open authentication + EAP, network EAP authentication, and no key management, RADIUS server authentication on port 1645. Click EAP Authentication for additional information. – RADIUS Server—Enter the hostname or IP address of the RADIUS server you are either adding or deleting. – RADIUS Server Secret—Enter the server's shared secret.

- Step 2** Click **Add** to add the security configuration to the SSID table at the bottom of the screen.
- Step 3** Repeat steps 1 and 2 to add more security configurations.
- Step 4** To remove a configuration, click **Delete** next to the name of the configuration you want to remove from the table.
- Step 5** Click **Next** to continue. See [Setting up the WDS, page 2-7](#).

Setting up the WDS

WDS must be set up for WLSE radio management features to work. There are two ways to set up the WDS: automatically and manually. For an explanation of each see: [WDS on an Access Point, page 2-7](#) and [WDS on WLSM, page 2-8](#).

WDS can be provided by either access points or a Wireless LAN Services Module (WLSM). The WDS setup for each is different:

- **AP WDS Setup**—See [Setting up WDS on Access Points, page 2-8](#).
- **WLSM WDS Setup**—See [Setting up WDS on WLSMs, page 2-9](#).

WDS on an Access Point

When an access point is discovered and inventoried:

- If the *automatic* configuration option is selected and if this is the first access point discovered in a subnet, the AP-WDS template is pushed to this access point. This access point then becomes the active WDS of the subnet, and the second and third access points discovered in the same subnet become the backup WDS devices.
- If the *manual* configuration option is selected, the MAC address of the AP is compared to the configured MAC address for the subnet. If both match, the AP-WDS template is uploaded to the access point.

If the configuration is manual but the MAC address does not match the configured WDS MAC address for the given subnet, the template, which contains the WLCCP credentials, is uploaded to the access point.

WDS on WLSM

When a WLSM is discovered and inventoried, the WLSM template is uploaded to the WLSM. When a new access point joins the network, the corresponding access point template, which contains the WLCCP credentials, is uploaded to the access point based on the subnet that it is in.

Setting up WDS on Access Points

Use this option to set up WDS on access points.

Procedure

-
- Step 1** To automatically configure WDS:
- Select **Automatic WDS Configuration**.
 - Click **Save**.
 - Click **Next** to continue. See [Deploying the Configuration, page 2-9](#).
- Step 2** To manually configure WDS:
- Select **Manual WDS Configuration**.
 - Click **Insert New Row** to add information about a WDS access point. You can enter an active and backup WDS access points for each subnet.

Complete the following:

Table 2-3 AP-WDS Setup

Field	Description
WDS MAC Address	Enter the MAC address of the WDS access point. Use this format: aaaa.bbbb.cccc
Subnet	Enter the IP address and subnet mask separated by a backslash. For example: 172.10.10.0/24
Active/Backup	Select Active or Backup to indicate if this is an active or a backup WDS.

- To add another row, click **Insert New Row**.

- To delete a row, select it, then click **Delete**.
 - To save the setup, click **Save All**.
- c. Click **Next** to continue. See [Deploying the Configuration, page 2-9](#).

Setting up WDS on WLSMs

Use this option to set up WDS on WLSMs.

Procedure

- Step 1** If you selected WLSM in the Deployment Type screen, complete the following:

Table 2-4 WLSM WDS Configuration

Field	Description
WLSM IP	Enter the IP address of the WLSM. For example: 172.10.10.100
Subnet Details	The subnets the WLSM manages. For each subnet, enter the IP address and subnet mask separated by a backslash. For example: 172.10.10.0/24 Because each WLSM can support more than one subnet, you can enter multiple subnets.

- To add another row, click **Insert New Row**.
- To delete a row, select it, then click **Delete**.
- To save the setup, click **Save All**.

- Step 2** Click **Next** to continue. See [Deploying the Configuration, page 2-9](#).

Deploying the Configuration

The Deployment Wizard automatically discovers all deployed access points, uploads configurations, and manages all access points. You can create deployment specifications which include an auto-configuration and a configuration template. The auto-configuration and the configuration template are saved and can be accessed later from the Configuration tab (**Configure > Auto Update > Automanaged Configuration** and **Configure > Templates**).

You can add as many different deployment specifications as you need.

Procedure

- Step 1** Complete the following:

Table 2-5 **Deploy Configuration**

Field	Description
Enable Timer for Deploying Configurations	Select to deploy this configuration during a specified time interval. This sets the timer for all configurations. - This option has the same effect as enabling filtering for auto-manage devices in Devices > Discover > Discover > Advanced Options > Enable Filtering for Auto-Managed Devices. If you set Enable Timer in the Wizard, these settings will be changed correspondingly under Advanced Options. - If you set the timer under Advanced Options, the settings in the Wizard will be changed correspondingly. Note If you want to enable the timer for certain MAC addresses, you can do so under Devices > Discover > Discover > Advanced Options.
From/To	Specify the time period for deploying this configuration.
Assign Name to the Auto-Managed Configuration	
Name	Enter a name for the auto-configuration.
Assign matching criteria to the Auto-Managed Configuration	
Description	Enter a description for the auto-managed configuration.
Matching Criteria	
Subnet	Specify the subnets to which this configuration will be deployed by selecting a subnet, then clicking >>. To remove a subnet from the list, select it and then click Remove.
Save Configurations to NVRAM	Select the checkbox to save the configuration to the access points' NVRAM (IOS access points only).
Assign Configuration to the Associated Configuration Template	
General Config	From the list, select one previously-defined general configuration to associate to the configuration template.

Table 2-5 *Deploy Configuration (continued)*

Field	Description
Security Config	From the list, select one or more previously-defined security configurations to associate to the configuration template. Then click >> to add the general and security configurations to the list. To remove a configuration from the list, select it and click Remove.

- To add the auto-managed configuration and the associated configuration template to the table at the bottom of the screen, click **Add**.

Result: The name of the auto-managed configuration and the configuration template are added to the table.

- To change an auto-managed configuration and its associated configuration template, select it, then click **Modify**.



Note The name cannot be modified; only the criteria and deployment timer can be modified.

- To remove an auto-managed configuration and its associated configuration template from the table, select it, then click **Delete**.
- To preview the configuration template, click the icon under Preview Configuration Template.

Result: The CLI commands that will be applied are displayed.

Step 2 Click **Next** to finish. See [Finishing, page 2-11](#).

Related Topics

- [Assigning an Auto-Managed Configuration, page 8-43](#)
- [Managing Device Configurations, page 8-1](#)

Finishing

After you have deployed the access points in your network:

- The devices will automatically be managed by the WLSE.
- You can use the options listed in the Finish screen to monitor access points and use other WLSE features.



Fault Monitoring

The Faults tab displays information to help you monitor your devices. All the device information shown under this tab is polled from the devices in your network.

Following are the subtabs under Faults:



Note

Some of the subtabs may not be visible to some users.

- **Display Faults**—See [Displaying Fault Information](#), page 3-1
- **Manage Fault Settings**—See [Managing Fault Settings](#), page 3-10
- **Voice Summary**—See [Viewing the Status of the VoWLAN](#), page 3-53
- **Voice QoS Settings**—See [Assigning Voice QoS Fault Settings](#), page 3-54
- **Notification Settings**—See [Notification Settings](#), page 3-56



Note

In this release, the Rogue, Ad-Hoc, and Interference network-wide settings have been moved from Faults > Manage Network-Wide Settings to IDS > Manage Network-Wide IDS Settings (see [Using the Manage IDS Settings Subtab](#), page 14-6).

Displaying Fault Information



Note

For an explanation of the faults, in the online help click **Troubleshooting**, or on Cisco.com see the Fault Description Table in the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.13*.

The topics covered in this section are:

- [Understanding Fault and Security Policy Monitoring](#), page 3-2
- [Displaying Faults](#), page 3-4
- [Clearing Summary Table Faults](#), page 3-6
- [Acknowledging Faults](#), page 3-7
- [Viewing Fault Details](#), page 3-7

Related Topics

- [Setting Policies and Thresholds, page 3-14](#)

Understanding Fault and Security Policy Monitoring

The fault monitoring feature interrogates managed devices for specific data, compares these data against thresholds, and declares faults when the thresholds have been crossed.

You can configure the WLSE to generate a notification as an SNMP trap and/or a syslog message after a fault has been declared. The data interrogated by the fault monitoring feature includes security configuration parameters (security policy monitoring) and SNMP parameters used for performance related faults.

The following topics are included in this section:

- [Understanding How Faults Are Generated, page 3-2](#)
- [Understanding Fault States, page 3-2](#)
- [Understanding Security Policy Monitoring Faults, page 3-3](#)
- [Understanding Threshold-Related Faults, page 3-3](#)

Understanding How Faults Are Generated

The WLSE declares a fault condition for a managed device when an abnormal condition is detected. An abnormal condition for a managed device occurs when a system component is not configured or functioning properly, or when processed data related to system components exceed performance thresholds.

Related Topics

- [Understanding Fault States, page 3-2](#)

Understanding Fault States

Faults can be in any of the following states:

- **Active**—This is a state in which at least one of the conditions contributing to the fault is broken.
For example, the CPU utilization threshold has three states: OK, Degraded and Overloaded. In this case, OK is the ‘best’ state and Overloaded and Degraded are ‘broken’ states. Similarly, a port threshold might have an Up and a Down state, where Up is the ‘best’ state and Down is the ‘broken’ state.
- **Acknowledged**—This is a state in which you have selected an Active fault from the Fault Summary, and acknowledged it. The fault is removed from the Active list, but the conditions contributing to the fault still exist.

Faults can be acknowledged from the Summary Page. See [Acknowledging Faults, page 3-7](#)

- **Cleared**—This is a state in which all the conditions contributing to the fault no longer exist or when the administrator selects a fault and clears it.

Faults generated by polling are automatically cleared based on polled data. When the fault has not been generated by polling, or when polling has been disabled, the fault can be manually cleared from the following places:

- Summary Page—See [Clearing Summary Table Faults, page 3-6](#).

- Fault Details Window—See [Viewing Fault Details, page 3-7](#).
- Thresholds and Policies—See [Viewing Current Faults, page 3-51](#).

Related Topics

- [Managing Fault Settings, page 3-10](#)
- [Understanding Fault and Security Policy Monitoring, page 3-2](#)

Understanding Security Policy Monitoring Faults

Many WLAN security vulnerabilities can be mitigated by correctly configuring the WLAN. You can use the WLSE to validate a critical set of configuration parameters and generate faults if improper configurations are detected.

The WLSE uses SNMP to periodically interrogate the configuration parameters of managed devices. If the configuration parameter is not correctly configured, a fault is generated. For example, you can use the WLSE to periodically verify that Publicly Secure Packet Forwarding (PSPF) is configured and enforced on wireless devices. If the WLSE determines that PSPF has been turned off on a wireless device, it will generate a fault for the security misconfiguration.

After you have established security policies in your network, you can use this feature to validate that the security policies are enforced on managed access points.

Related Topics

- [Setting Policies and Thresholds, page 3-14](#)
- [Understanding Fault and Security Policy Monitoring, page 3-2](#)

Understanding Threshold-Related Faults

The WLSE compares data retrieved from managed devices against thresholds and can generate faults when the thresholds are exceeded. You can configure the priority of the fault condition and the threshold conditions for the fault (see [Setting Policies and Thresholds, page 3-14](#)).

Each WLSE fault is described by a finite state machine (FSM). A WLSE fault is described by either a two-state FSM or a three-state FSM. In each fault FSM, state transitions occur when polled and processed data exceed a configured threshold. These thresholds are defined by two parameters—a configured state transition condition and a number of polling intervals.

Two-State Finite State Machines

The RF Port Status for managed wireless bridges and/or access points is an example of a two-state fault FSM:

- The clear state for the RF port status FSM corresponds to when the RF port status is administratively and operationally up.
- The fault state for the RF port status FSM corresponds to when the RF port status is administratively up but operationally down.

Therefore, when the WLSE polls a managed wireless bridge or access point and determines that its RF port is administratively up but operationally down, and this condition has existed for the configured number of polling intervals, the WLSE will generate a fault for the device, indicating that RF port status is down. If during subsequent polling, the WLSE determines the RF port status is both administratively and operationally up for the required number of polling intervals, the WLSE will clear the RF port status down fault for the device.

Three-State Finite State Machines

The RF port utilization for managed wireless bridges and access points is an example of the three-state fault FSM. RF port utilization is measured as a percent of available bandwidth on the wireless device's RF port. For this example, we will make the following assumptions:

- The threshold for the degraded state for RF port utilization is fifty percent utilization for three polling cycles.
- The threshold for the overloaded state is eighty percent utilization for three polling cycles.
- The RF port utilization for each managed device is considered in the OK state when the utilization is below fifty percent for any two consecutive polling cycles.

Using these threshold values, the WLSE will generate faults for:

- The degraded state if the RF port utilization is between fifty and eighty percent for three consecutive polling intervals.
- The overloaded state if the RF port utilization moves above 80% for three consecutive polling intervals.

In both cases, if subsequent polling indicates the RF port utilization has moved below fifty percent for two consecutive polling cycles, the fault condition will clear.

Related Topics

- [Setting Policies and Thresholds, page 3-14.](#)
- [Understanding Fault and Security Policy Monitoring, page 3-2.](#)

Displaying Faults



Note

For an explanation of the faults, in the online help click **Troubleshooting**, or on Cisco.com see the Fault Description Table in the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.13*.

This window displays device fault information.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Faults > Display Faults**. The Fault window appears.
- Step 2** Use the Filter: bar to display the faults you want to view:

Table 3-1 Display Faults Filter Bar

Field	Description
Products	From the list, select the device type whose fault summary you want to display. Note If you select APs, bridges will also be displayed. If you want to display bridges only, select them from the list specifically.

Table 3-1 *Display Faults Filter Bar (continued)*

Field	Description
Severity	From the list, select the severity from P1, which is the highest severity level to P5, which is the lowest severity level, to display: • P1—Severity P1 faults. • P1-P2—Severity P1 and P2 faults. • P1-P3—Severity P1 through P3 faults. • P1-P4—Severity P1 through P4 faults. • P1-P5—Severity P1 through P5 faults. • All—Severity P1 through P5 faults, and faults that have been cleared. Note When more than one fault is reported against a device, the fault priorities are aggregated, and the maximum priority of all the active faults for that device is displayed. For example, if the device has a P1, a P2, and a P3 fault against it, only the P1 is displayed in the Severity column. However, when you click on the Description for that fault, all three priorities are displayed with an explanation for each.
State	From the list, select a state to display. See Understanding Fault States, page 3-2 for a description of each state.
Name/IP	Enter a complete or partial device name or IP address.
Refresh (Sec)	Enter the number of seconds (30 seconds or higher) to indicate how often you want the screen to refresh. The default is 300 seconds (5 minutes). You cannot enter a value under 30 seconds.

Step 3 Click **Apply**. The following table appears:



Note If no data is displayed in the table, there are no faults for your filtering selection to report.

Table 3-2 *Display Faults Table*

Column	Description
Address	The device address. Click to see various reports about the device. For information on the reports, see Using the Device Center, page 10-7.
Name	The device for which the fault is reported. Click to see various reports about the device. For information on the reports, see Using the Device Center, page 10-7.
Family	The product family.
Product	The product name.
Type	The device or the sub-device component.

Table 3-2 **Display Faults Table (continued)**

Column	Description
Description	A description of the fault. Click to see fault details. See Viewing Fault Details, page 3-7. Note For an explanation of the faults, in the online help click Troubleshooting, or on Cisco.com see the Fault Description Table in the <i>FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.13</i>.
Severity	The fault severity level.
State	The operational state of the device.
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed. See Understanding WLSE Time Displays, page 1-10. Click to see fault details. See Viewing Fault Details, page 3-7.

- To sort table data, click on the column heading you want to use to sort the data:
 - A triangle indicates ascending order.
 - An upside-down triangle indicates descending order.
 - No triangle indicates that the data is not sorted.

Clearing Summary Table Faults

There are two ways in which you can clear faults:

- Select **Faults > Display Faults**. The Summary Table appears with the faults that meet the filtering criteria you selected.
 - To clear an individual fault, select it, then click **Clear**.
 - To clear more than one fault, select them, then click **Clear**.
 - To clear all the faults, click **Select All**, then click **Clear**.
- Click the Description or Timestamp fields in the Summary Table for a particular fault, and the Fault Details page appears. Click the Clear button in the Conditions table.



Note

It may be a few seconds before the faults clear.

Related Topics

- [Viewing Fault Details, page 3-7](#)
- [Understanding Fault States, page 3-2](#)

Acknowledging Faults

When you select **Faults > Display Faults** the Summary Table appears with the faults that meet the filtering criteria you selected.

- To acknowledge an individual fault, select it, then click **Acknowledge**.
- To acknowledge more than one fault, select them, then click **Acknowledge**.
- To acknowledge all the faults, click **Select All**, then click **Acknowledge**.

Related Topics

[Understanding Fault States, page 3-2](#)

Viewing Fault Details

There are several types of fault detail windows:

- [Device Fault Details, page 3-7](#)—Displays details about the device, its fault conditions and history.
- Rogue Access Point Details (see [Table 14-1 on page 14-20](#))—Displays details about the unknown access point, beacon and location information, switch port tracing, reporting access points, and fault history.
- Auto Re-Site Survey Details (see [Table 12-2 on page 12-11](#))—Displays details about performance degradations.
- Self Healing Fault Details (see [Table 12-3 on page 12-18](#))—Displays details about self healing faults.



Note

For an explanation of the faults, in the online help click **Troubleshooting**, or on Cisco.com see the Fault Description Table in the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.13*.

Device Fault Details

When you click the link in the Description or Timestamp fields in the Fault Summary Table for an device, the following tables are displayed in the Fault Details window:

- [Fault details](#)
- [Conditions](#)
- [Fault History](#)



Note

You can clear one or more faults from the Conditions table by selecting them, then clicking **Clear**. It may be a few seconds before the faults clear.

Fault details**Table 3-3** *Fault Details Table*

Column	Description
IP	The device IP address.
Name	The device hostname.
Family	The device family.
Product	The product name.
Type	The device or the device sub-entity (which could include a logical entity, such as software or a service) in which the fault is found. Note If the Type is a sub-entity, additional columns appear with keys and values to help identify the precise sub-entity. These additional keys and values are MIB variables.
ifIndex	A unique number that identifies the interface. Note This value only displays when you are viewing fault details for ports.

Conditions**Table 3-4** *Conditions Table*

Column	Description
Name	The fault condition.
State	The state of the device. See Understanding Fault States for a description of the states.
Severity	The fault severity level.
Description	A description of the fault. Note For an explanation of the faults, in the online help click Troubleshooting , or on Cisco.com see the Fault Description Table in the <i>FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.13</i> .
Product	The product name for the device.
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed. See Understanding WLSE Time Displays, page 1-10 .
Clear	Click Clear , then refresh your browser window to view the updated fault display. Note It may be a few seconds before the fault clears.

Fault History**Table 3-5** **Fault History Table**

Column	Description
State	The state of the device. See Understanding Fault States, page 3-2 for a description of the states.
Severity	The fault severity level.
Description	A description of the fault. Note For an explanation of the faults, in the online help click Troubleshooting, or on Cisco.com see the Fault Description Table in the <i>FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.13</i>.
Change	A description of the state change.
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed. See Understanding WLSE Time Displays, page 1-10.
By	Displays the username of the person who changed the fault state. If the fault state has not been cleared or acknowledged, nothing is displayed in this column.

Managing Fault Settings

Every device managed by the WLSE has a fault setting (also called a fault policy profile) assigned to it. Fault settings include threshold values and security policies.

If you have not assigned a specific setting to a device, it uses the system Default setting. Default settings can be edited, but cannot be deleted.

The topics covered in this section are:

- [Understanding Fault Settings, page 3-10](#)
- [Creating a Setting, page 3-11](#)
- [Copying a Setting, page 3-11](#)
- [Renaming a Setting, page 3-12](#)
- [Editing a Setting, page 3-12](#)
- [Deleting a Setting, page 3-13](#)
- [Viewing a Summary, page 3-13](#)
- [Assigning a Default Setting to a Device, page 3-14](#)
- [Setting Policies and Thresholds, page 3-14](#)

Understanding Fault Settings

A fault policy profile (or fault setting) is a set of security policy settings and fault thresholds that is assigned to one or more managed devices. Multiple profiles can be created for devices, but a managed device can only be assigned one profile at a time. If a device is not explicitly assigned a profile, it will be assigned the default profile.

Fault policy profiles allows you to engineer security policies and fault polling to the needs of their network(s). You can create a profile to customize:

- Thresholds and security configurations that generate fault events
- Fault priority
- Polling interval frequency

Note that the WLSE is also able to receive some link up and link down SNMP traps related to interface port status and admin status from access points. (For more detailed information, see [Setting RF Port Status Threshold, page 3-34](#) and [Setting RF Port AdminStatus Threshold, page 3-35](#).) This means that the polling interval for these policies can be increased, which reduces the load on the WLSE, and allows faster processing of the faults when they do occur. In this instance, traps are sent immediately to set or clear a fault, compared with waiting for the polling interval to see if a fault has changed state.

For example, Site A is connected via high-speed LAN connections, and remote Sites Band C are connected via slow WAN links. It might be appropriate to configure a fault policy profile for each site, where many of the parameters are checked more frequently for Site A than for Sites B and C.

Here is another example. Suppose access points in Site A with IP addresses 10.1.5.5 and 10.1.5.6 are intended to provide public network access, but the other Site A access points are for private use. In this case, there are different security misconfiguration policies appropriate for the public access points than for the private access points. This means that the fault policy profile for the public access points will check for different SSIDs than the profile for the private access points:

- The public profile may check that PSPF is enforced on the access points, which is usually not appropriate for private networks where all clients are trusted.
- The private profile may confirm that EAP is enforced on the private access points, but the public profile will probably not check for EAP enforcement.

Related Topics

- [Setting Policies and Thresholds, page 3-14](#)

Creating a Setting

Use this option to create a setting.

**Tip**

If some managed access points are enabled to send traps to the WLSE and some are not, it is recommended that you create two separate groups: one for enabled traps, which can have higher polling intervals, and the other using shorter polling intervals. For information about enabling traps sent to the WLSE, see **Configure > Templates > IOS > Services > SNMP**.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Faults > Manage Fault Settings**. The Fault Settings dialog box appears.
- Step 2** Enter a unique name. See [Naming Guidelines, page B-1](#) for details.
- Step 3** Click **Create New**. The new name appears in the Existing Fault Settings list and the The Editing Profile window appears. See [Editing a Setting, page 3-12](#).

**Note**

The new setting is a copy of the Default setting.

Related Topics

[Understanding Fault Settings, page 3-10](#)

Copying a Setting

Use this option to copy an existing setting to use as a base for a new setting.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Faults > Manage Fault Settings**. The Fault Settings dialog box appears.

- Step 2** Select the setting you want to copy from the Existing Fault Settings box, then click **Create Copy**. A dialog box appears asking you to enter a name for the copy.
- Step 3** Enter a unique name. See [Naming Guidelines, page B-1](#) for details.
- Step 4** Click **OK**. The new name appears in the Existing Fault Settings list.
- Step 5** Select the name, then click **Edit**. The Editing Profile window appears. See [Editing a Setting, page 3-12](#).
-

Related Topics

[Understanding Fault Settings, page 3-10](#)

Renaming a Setting

Use this option to rename a setting.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Faults > Manage Fault Settings**. The Fault Settings dialog box appears.
- Step 2** Select the profile you want to rename from the Existing Fault Settings box, then click **Rename**. A dialog box appears asking you to enter a new name.
- Step 3** Enter a unique name. See [Naming Guidelines, page B-1](#) for details.
- Step 4** Click **OK**. The new name appears in the Existing Fault Settings list.
-

Related Topics

[Understanding Fault Settings, page 3-10](#)

Editing a Setting

Use this option to edit a setting.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Faults > Manage Fault Settings**. The Fault Settings dialog box appears.
- Step 2** Select the setting you want to edit from the Existing Fault Settings box, then click **Edit**. The Editing Settings window appears.

- Step 3** Select the policies and thresholds in the left pane that you want to assign to the setting. For a description, see [Setting Policies and Thresholds, page 3-14](#).
-

Related Topics

[Understanding Fault Settings, page 3-10](#)

Deleting a Setting

Use this option to delete a setting.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Faults > Manage Fault Settings**. The Fault Settings dialog box appears.
- Step 2** Select the profile you want to delete from the Existing Fault Settings box, then click **Delete**. A window appears asking if you want to delete the setting.



Note

Any devices that were assigned the deleted setting will be automatically assigned the Default setting.

- Step 3** Click **OK** to delete it.
-

Viewing a Summary

Use this option to view a summary of the current selections for a particular fault setting.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Faults > Manage Fault Settings**. The Fault Settings dialog box appears.
- Step 2** Select the setting you want to view from the Existing Fault Settings box, then click **View Summary**. A window displays the current fault settings.
- Step 3** Click **OK** to close the window.
-

Assigning a Default Setting to a Device

Use this option to assign a setting to a single device or a group of devices. Devices can only have one setting assigned to them at a time.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Faults > Manage Fault Settings**.
- Step 2** Assign a setting to devices either of the following ways:
- From the Editing Settings window, click **Assign Devices**.
 - From the Fault Settings window, select a setting from the **Existing Fault Settings** list, then click **Assign Devices**.
- Step 3** If you want to search for devices, use the dialog box in the left pane above the device selector. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 4** If you know which device you want, use the device selector to select the devices. They are added to the list of Available Devices.
- Step 5** From the list of Available Devices, select the device to which you want to apply the profile and click >>. The devices are moved to the Selected Devices list.
- Step 6** Click **Continue**. A confirmation dialog box appears for the device assignment.
- Step 7** Click **OK** to accept the device assignment or **Cancel** to cancel the device assignment.
-

Related Topics

[Understanding Fault Settings, page 3-10](#)

Setting Policies and Thresholds

Use the policy settings to activate or deactivate a set of predefined policies for access points and radio interfaces.

Use the threshold settings to set polling and [exception](#) threshold values collected from the devices you are monitoring.

The policies and threshold values you set in this window will determine how the faults are displayed in the **Faults > Display Faults** subtab.

This section includes procedures for setting the following:

- **Access Point/Bridge Policies**—[Setting Access Point/Bridge Policies, page 3-15](#).
- **Radio-802.11x Policies**—[Setting Radio-802.11x Policies, page 3-24](#)
- **Access Point/Bridge Thresholds**—See [Setting Access Point/Bridge Thresholds, page 3-30](#).
- **Radio-802.11x Thresholds**—See [Setting Radio-802.11x Thresholds, page 3-34](#)
- **Switch Settings**—See [Setting Switch Fault Thresholds, page 3-42](#).

- **WLSM**—See [Setting WLSM Fault Thresholds](#), page 3-46
- **Router Settings**—See [Setting Router Fault Thresholds](#), page 3-48.
- **AAA Server**—See [Setting AAA Server Response Time](#), page 3-49.
- **WLSE**—See [Setting WLSE Policies](#), page 3-49.
- **WDS**—See [Setting WDS Thresholds](#), page 3-50.

**Note**

Policies are disabled by default unless otherwise noted.

You can also view the current faults for each setting. See [Viewing Current Faults](#), page 3-51.

Setting Access Point/Bridge Policies

When you set access point policies, the policies are applicable to the access point; they are not set per radio interface type and are not reported by interface type on the faults page.

Following are the access point policies:

- **HTTP Disabled**—See [Setting the HTTP Disabled Policy](#), page 3-15.
- **Telnet Disabled**— See [Setting the Telnet Disabled Policy](#), page 3-16.
- **Firmware Version**—See [Setting the Firmware Version Policy](#), page 3-17.
- **HotStandBy Status**—See [Setting the HotStandBy Status Policy](#), page 3-17.
- **Registration Error**—See [Setting the Registration Error Policy](#), page 3-18.
- **EAP Per SSID Enforced for Cisco-Supplicant**—See [Setting EAP Per SSID Enforced for Cisco-Supplicant Policy](#), page 3-18.
- **EAP Per SSID Enforced for Non-Cisco-Supplicant**—See [Setting EAP Per SSID Enforced for Non-Cisco-Supplicant Policy](#), page 3-19.
- **EAP Per SSID Enforced for Mixed-Cisco-Supplicant**—See [Setting EAP Per SSID Enforced for Mixed-Cisco-Supplicant Policy](#), page 3-20.
- **MIC per VLAN**—See [Setting the MIC per VLAN Policy](#), page 3-20.
- **WEP per VLAN**—See [Setting the WEP per VLAN Policy](#), page 3-21.
- **Key Rotation per VLAN**—See [Setting Key Rotation per VLAN Policy](#), page 3-22.
- **WEP Encryption per VLAN**—See [Setting WEP Encryption per VLAN Policy](#), page 3-23.
- **PSPF per VLAN**—See [Setting PSPF per VLAN Policy](#), page 3-23.

Related Topics

[Understanding Security Policy Monitoring Faults](#), page 3-3

Setting the HTTP Disabled Policy

When HTTP is enabled on the access point, a fault is generated.

This setting is disabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.

Setting the Telnet Disabled Policy

When Telnet is enabled on the access point, a fault is generated.

This setting is disabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.

Setting the Firmware Version Policy

Use this setting to verify that the access point is running the correct and authorized firmware version. This policy is disabled by default.

Procedure

- Step 1** To activate the policy, do the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
Firmware Version	Enter the firmware version.

- Step 2** Click >> to add the firmware version to the list.
- Step 3** To remove a firmware version from the list, select it, then click <<.
- Step 4** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 5** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 6** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.

Setting the HotStandBy Status Policy

Use this setting to indicate when the access point that is configured for hot standby has become active. This policy is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.

Setting the Registration Error Policy

Use this setting to verify that the managed access point is registered with a WDS.



Note For Radio Manager functionality to work, all access points must register with a WDS. If an access point is not registered, it will be excluded from all the Radio Manager procedures, which will provide incorrect results.

This policy is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Down	From the list, select the severity level and the number of polling cycles before the status is Down.
Up	From the list, select the number of polling cycles before the fault is cleared and the status is Up.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.

Setting EAP Per SSID Enforced for Cisco-Supplicant Policy

Use this setting to check for the Network EAP setting on the access point. If the Network EAP is disabled, then this policy generates a fault.

You should not add an SSID to this policy that is already being used in another EAP per SSID policy.

This policy is disabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
Available SSID	Lists the SSIDs that are available. To move an SSID to the Selected SSID list, select it, then click >>.
Selected SSID	Lists the SSIDs to which this policy is applied. To remove an SSID from the Selected list, select it, then click <<.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.

Setting EAP Per SSID Enforced for Non-Cisco-Supplicant Policy

Use this setting to check for the Open with EAP setting on the access point. If this setting is not enabled, then this policy generates a fault.

You should not add an SSID to this policy that is already being used in another EAP per SSID policy.

This policy is disabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
Available SSID	Lists the SSIDs that are available. To move an SSID to the Selected SSID list, select it, then click >>.
Selected SSID	Lists the SSIDs to which this policy is applied. To remove an SSID from the Selected list, select it, then click <<.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.
-

Setting EAP Per SSID Enforced for Mixed-Cisco-Supplicant Policy

Use this setting to check for both the Network EAP and the Open with EAP settings on the access point. You should not add an SSID to this policy that is already being used in another EAP per SSID policy. This policy is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
Available SSID	Lists the SSIDs that are available. To move an SSID to the Selected SSID list, select it, then click >>.
Selected SSID	Lists the SSIDs to which this policy is applied. To remove an SSID from the Selected list, select it, then click <<.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.
-

Setting the MIC per VLAN Policy

Use this setting when a VLAN is defined on the access point to verify that MIC is enabled on the selected VLAN. If it is disabled, it will generate a fault.

This policy is disabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
Available Vlans	Lists all the VLAN ID numbers that are available. To apply the policy to one of the available VLANs, select it, then click >> to move it to the Selected VLANs list.
Selected Vlans	Lists the VLAN identification numbers to which this policy is applied. To remove a VLAN ID from the list, select it, then click << to move it to the Available VLANs list.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.

Setting the WEP per VLAN Policy

Use this setting when a VLAN is defined on the access point to verify that WEP for the selected VLAN is enabled. If it is disabled, it will generate a fault.

This policy is disabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
Available Vlans	Lists all the VLAN ID numbers that are available. To apply the policy to one of the available VLANs, select it, then click >> to move it to the Selected VLANs list.
Selected Vlans	Lists the VLAN identification numbers to which this policy is applied. To remove a VLAN ID from the list, select it, then click << to move it to the Available VLANs list.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.
-

Setting Key Rotation per VLAN Policy

Use this setting when a VLAN is defined on the access point to verify that the key broadcast rotation is enabled on the selected VLAN. If it is not enabled, it will generate a fault.

When broadcast key rotations is enabled, only wireless client devices using 802.11x authentication (such as LEAP, EAP-TLS, or PEAP) can use the access point.

This policy is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
Available Vlans	Lists all the VLAN ID numbers that are available. To apply the policy to one of the available VLANs, select it, then click >> to move it to the Selected VLANs list.
Selected Vlans	Lists the VLAN identification numbers to which this policy is applied. To remove a VLAN ID from the list, select it, then click << to move it to the Available VLANs list.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.
-

Setting WEP Encryption per VLAN Policy

Use this setting when a VLAN is defined on the access point to verify that WEP key length for the selected VLAN, which is used by the clients to associate to the access point, is correct.

This policy is disabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
WEP Key Length	Select to indicate the bit length.
Available Vlans	Lists all the VLAN ID numbers that are available. To apply the policy to one of the available VLANs, select it, then click >> to move it to the Selected VLANs list.
Selected Vlans	Lists the VLAN identification numbers to which this policy is applied. To remove a VLAN ID from the list, select it, then click << to move it to the Available VLANs list.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.

Setting PSPF per VLAN Policy

Use this setting when a VLAN is defined on the access point to verify that PSPF is enforced.

This policy is disabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

Field	Description
Available Vlans	Lists all the VLAN ID numbers that are available. To apply the policy to one of the available VLANs, select it, then click >> to move it to the Selected VLANs list.
Selected Vlans	Lists the VLAN identification numbers to which this policy is applied. To remove a VLAN ID from the list, select it, then click << to move it to the Available VLANs list.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.

Setting Radio-802.11x Policies

When you set radio interface type policies, the policies are applicable only to the radio interface type (11a, 11b, or 11g) on which they are set. They are not set on the access point and are not reported by access point on the faults page.

Following are the radio-802.11x policies

- Broadcast SSID—See [Setting the Broadcast SSID Policy, page 3-24](#)
- Infrastructure SSID—See [Setting the Infrastructure SSID Policy, page 3-25](#)
- Broadcast Disabled—[Setting the Broadcast Disabled Policy, page 3-26](#)
- PSPF Enabled—See [Setting the PSPF Enabled Policy, page 3-26](#)
- WEP Key Length—See [Setting WEP Key Length Policy, page 3-27](#).
- EAP Enforced-Cisco Supplicant—See [Setting the EAP Enforced—Cisco Supplicant Policy, page 3-27](#).
- EAP Enforced-Other Supplicant—See [Setting the EAP Enforced—Other Supplicant Policy, page 3-28](#).
- EAP Enforced-Mixed Supplicant—See [Setting the EAP Enforced—Mixed Supplicant Policy, page 3-28](#).
- Dynamic Frequency Selection (DFS)—See [Setting the Dynamic Frequency Selection \(DFS\), page 3-29](#). Used for Radio-802.11a only.

Setting the Broadcast SSID Policy

Use this setting to check when an SSID that you do not want broadcast is being broadcast. If it is, a fault is generated. This policy is disabled by default.

Procedure

Step 1 To activate the policy, complete the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
All Available SSIDs	Lists all the available SSIDs per interface for this profile. From the list, select the SSIDs that you do not want broadcast, then click >>.
Do Not Broadcast SSIDs	Lists all the SSIDs that you do not want broadcast. To remove an SSID from the list, click <<.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.

Setting the Infrastructure SSID Policy

Use this setting to make sure the infrastructure SSID matches the infrastructure SSID set on the access point. A fault is generated if they do not match.



Note

This policy is only applicable to access points with firmware release 12.2(15)JA or later.

This policy is disabled by default.

Procedure

Step 1 To activate the policy, do the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
SSID	Enter the infrastructure SSID that is set on the access point, then click >>. The SSID appears in a list with all the infrastructure SSIDs per interface for this profile.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.
-

Setting the Broadcast Disabled Policy

Use this setting to check whether the broadcast mode for the SSID on the interface type is enabled. Entering an SSID in the Guest Mode field on the access point enables the broadcast SSID.

This policy is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.
-

Setting the PSPF Enabled Policy

Use this setting to check whether client devices associated to a bridge or access point have inadvertently shared files with other client devices on the wireless network.

This policy is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.
-

Setting WEP Key Length Policy

Use this setting if you want to verify that the WEP key length that has been entered into the WLSE matches the WEP key length specified on the radio interface type.

This policy is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
WEP Key Length	Select to indicate the bit length.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.
-

Setting the EAP Enforced—Cisco Supplicant Policy

Use this setting to make sure that client devices associating to the radio interface are using a Cisco authentication server.

If you set this policy on the interface, you cannot set the EAP Enforced- Other Supplicant or EAP Enforced-Mixed Supplicant policies on the interface. They are mutually exclusive.

This policy is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Verify	Select to enable the policy.

Field	Description
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.

Setting the EAP Enforced—Other Supplicant Policy

Use this setting to make sure that client devices associating to the radio interface are using a non-Cisco authentication server.

If you set this policy on the interface, you cannot set the EAP Enforced-Cisco Supplicant or EAP Enforced-Mixed Supplicant policies on the interface. They are mutually exclusive.

This policy is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.

Setting the EAP Enforced—Mixed Supplicant Policy

Use this setting to make sure that client devices associating to the radio interface are using a Cisco authentication server.

If you set this policy on the interface, you cannot set the EAP Enforced-Cisco Supplicant or EAP Enforced-Other Supplicant policies on the interface. They are mutually exclusive.

This policy is disabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to enable the policy.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.

Setting the Dynamic Frequency Selection (DFS)

Use this setting to make sure radar detection is enabled on the interface.

**Note**

This policy applies only to 802.11a radios.

This policy is enabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to enable the policy.
Severity	From the list, select a severity level to associate with this policy.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.

Setting Access Point/Bridge Thresholds

Using this option, you can set up thresholds for access point faults. When the thresholds are exceeded, faults are generated and can be viewed under **Faults > Display Faults**.

Following are the access point thresholds:

- SNMP Reachable—See [Setting the SNMP Reachable Threshold, page 3-30](#).
- CPU Utilization—See [Setting the CPU Utilization Threshold, page 3-31](#)
- Memory Utilization—See [Setting the Memory Utilization Threshold, page 3-31](#)
- Ethernet Port Status—See [Setting the Ethernet Port Status Threshold, page 3-32](#)
- Ethernet Port Utilization—See [Setting the Ethernet Port Utilization Threshold, page 3-33](#)
- Ethernet Port Packet Errors—See [Setting the Ethernet Port Packet Errors Threshold, page 3-33](#)

Setting the SNMP Reachable Threshold

Use this setting to make sure that the access point is reachable using SNMP.

This threshold is enabled by default.

**Note**

It is highly recommended that this threshold not be disabled. If it is disabled, and a device becomes unreachable, the SNMP-based faults cannot be detected, and there will be no SNMP unreachable faults displayed to alert you.

Procedure

Step 1 Complete the following:

Field	Description
Enable	Enabled by default. Select to disable.
Poll Interval	From the list, select the polling interval.
Settings	
Down	From the list, select the severity level and the number of polling cycles before the status is Down.
Up	From the list, select the number of polling cycles before the fault is cleared and the status is Up.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting the CPU Utilization Threshold

Use this setting to monitor CPU utilization on your access point.

This threshold is disabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable the threshold.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting the Memory Utilization Threshold

Use this setting to monitor memory utilization on your access point.

This threshold is disabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.

Field	Description
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting the Ethernet Port Status Threshold

Use this setting to monitor the Ethernet port to make sure it is up.

This setting is enabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Down	From the list, select the severity level and the number of polling cycles before the status is Down.
Up	From the list, select the number of polling cycles before the fault is cleared and the status is Up.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting the Ethernet Port Utilization Threshold

Use this setting to monitor the Ethernet port utilization in your access point.

This setting is disabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable the threshold.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting the Ethernet Port Packet Errors Threshold

Use this setting to monitor the Ethernet port packet errors in your access point.

This setting is disabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable the threshold.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.

Field	Description
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting Radio-802.11x Thresholds

Using this option, you can set up thresholds for Radio-802.11a, Radio-802.11b, and Radio-802.11g. When the thresholds are exceeded, faults are generated and can be viewed under **Faults > Display Faults**.

Following are the radio interface thresholds:

- RF Port Status—See [Setting RF Port Status Threshold, page 3-34](#)
- RF Port Admin Status—See [Setting RF Port AdminStatus Threshold, page 3-35](#)
- RF Port Utilization—See [Setting RF Port Utilization Threshold, page 3-36](#)
- RF Port Packet Errors—See [Setting Port Packet Errors Threshold, page 3-37](#)
- RF Port WEP Errors—See [Setting RF Port WEP Errors Threshold, page 3-38](#)
- Max Retry Count—See [Setting Max Retry Count Threshold, page 3-39](#)
- Associated Clients—See [Setting Associated Clients Threshold, page 3-38](#)
- Association Rate—See [Setting Association Rate Threshold, page 3-40](#)
- Voice Bandwidth—See [Setting Voice Bandwidth Threshold, page 3-41](#)
- Voice QoS Status—See [Setting Voice QoS Status Threshold, page 3-42](#)

Setting RF Port Status Threshold

Use this setting to determine the threshold for the radio interface's port to make sure that it is up and operating properly.

This threshold is enabled by default.



Tip

The WLSE is able to receive SNMP traps about this policy from access points rather than having to poll the access point for the information. If the WLSE is enabled to receive the traps, the poll interval can be increased, which reduces the load on the WLSE, and allows faster processing of the faults when they do occur. To enable traps sent to the WLSE, apply a configuration template to the access point with **Send all traps to this WLSE** enabled under **Configure > Templates > IOS > Services > SNMP**.

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval. If you have enabled traps to be sent to the WLSE from the access point (Configure > Templates > IOS > Services > SNMP), then set this value to no less than 60 minutes.
Settings	
Down	From the list, select the severity level and the number of polling cycles before the status is Down.
Up	From the list, select the number of polling cycles before the fault is cleared and the status is Up.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting RF Port AdminStatus Threshold

Use this setting to determine the threshold for the radio interface port's administrative status. This status indicates if the port has been set up or down by an administrator.

This threshold is disabled by default.

**Tip**

The WLSE is able to receive SNMP traps about this policy from access points rather than having to poll the access point for the information. If the WLSE is enabled to receive the traps, the poll interval can be increased, which reduces the load on the WLSE, and allows faster processing of the faults when they do occur. To enable traps sent to the WLSE, apply a configuration template to the access point with **Send all traps to this WLSE** enabled under **Configure > Templates > IOS > Services > SNMP**.

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval. If you have enabled traps to be sent to the WLSE from the access point (Configure > Templates > IOS > Services > SNMP), then should be no less than 60 minutes.
Settings	
Down	From the list, select the severity level and the number of polling cycles before the status is Down.
Up	From the list, select the number of polling cycles before the fault is cleared and the status is Up.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting RF Port Utilization Threshold

Use this setting to determine the threshold for the radio interface's port utilization.

This threshold is disabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.
-

Setting Port Packet Errors Threshold

Use this setting to determine the threshold for the radio interface's port packet errors.

This threshold is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.
-

Setting RF Port WEP Errors Threshold

Use this setting to determine the threshold for radio interface's port WEP errors.

This threshold is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting Associated Clients Threshold

Use this setting to determine the threshold for the associated clients.

This threshold is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.

Field	Description
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting Max Retry Count Threshold

Use this setting to determine the threshold for the maximum number of retries for the radio interface's request to send (RTS).

This threshold is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting Associated Clients Threshold

Use this setting to determine the threshold for the radio interface's associated clients.

This threshold is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting Association Rate Threshold

Use this setting to check for the total number of successful 802.11 association request operations to this radio interface.

This threshold is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.

Field	Description
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting Voice Bandwidth Threshold

Use this setting to enable voice bandwidth faults on a device or group of devices. When the specified bandwidth is exceeded, a fault is generated and can be viewed under **Faults > Display Faults** or **Faults > Voice Summary**.

This threshold is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Enable	Select to enable a voice bandwidth threshold for this component.
Settings	
Priority Fault	From the list, select a severity level to associate with this policy.
Voice Bandwidth in Use	From the list, select the maximum percentage of bandwidth allowed before a fault is generated.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Devices to <fault setting>** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Related Topics

- [Understanding Radio Management for VoWLAN, page 15-1](#)

Setting Voice QoS Status Threshold

Use this setting to enable voice quality of service (QoS) status faults on a device or group of devices. When the QoS status is Red or Yellow, a fault is generated and can be viewed under **Faults > Display Faults** or **Faults > Voice Summary**. The fault will be cleared automatically when the QoS status returns to Green.

This threshold is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Enable	Select to enable QoS status thresholds for this component.
Settings	
Degraded	From the list, select the severity level to be displayed when the QoS status is Red.
Fair	From the list, select the severity level to be displayed when the QoS status is Yellow.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Devices to <fault setting>** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Related Topics

- [Understanding Radio Management for VoWLAN, page 15-1](#)

Setting Switch Fault Thresholds

Using this option, you can set up thresholds for switch faults. When the thresholds are exceeded, faults are generated and can be viewed under **Faults > Display Faults**.

Procedure

- Step 1** In the left pane, select one of the following thresholds to apply to the setting:
- SNMP Reachable—See [Setting the SNMP Reachable Threshold, page 3-43](#)
 - CPU Utilization—See [Setting the CPU Utilization Threshold, page 3-43](#)
 - Memory Utilization—See [Setting the Memory Utilization Threshold, page 3-44](#)
 - Port Status—See [Setting the Port Status Threshold, page 3-45](#)
 - Port Utilization—See [Setting the Port Utilization Threshold, page 3-45](#)
 - Module Status—See [Setting the Module Status Threshold, page 3-46](#)

Setting the SNMP Reachable Threshold

Use this setting to make sure that the switch is reachable using SNMP.

This threshold is enabled by default.



Note

It is highly recommended that this threshold not be disabled. If it is disabled, and a device becomes unreachable, the SNMP-based faults cannot be detected, and there will be no SNMP unreachable faults displayed to alert you.

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Down	From the list, select the severity level and the number of polling cycles before the status is Down.
Up	From the list, select the number of polling cycles before the fault is cleared and the status is Up.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting the CPU Utilization Threshold

Use this setting to monitor CPU utilization in the switch.

This threshold is disabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.

Field	Description
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting the Memory Utilization Threshold

Use this setting to monitor memory utilization in the switch.

This threshold is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting the Port Status Threshold

Use this setting to monitor the port to make sure it is up.

This setting is enabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Down	From the list, select the severity level and the number of polling cycles before the status is Down.
Up	From the list, select the number of polling cycles before the fault is cleared and the status is Up.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting the Port Utilization Threshold

Use this setting to monitor the port utilization in the switch.

This setting is disabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.
-

Setting the Module Status Threshold

Use this setting to make sure the switch module is up.

This setting is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Down	From the list, select the severity level and the number of polling cycles before the status is Down.
Up	From the list, select the number of polling cycles before the fault is cleared and the status is Up.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.
-

Setting WLSM Fault Thresholds

Using this option, you can set up thresholds for WLSM faults. When the thresholds are exceeded, faults are generated and can be viewed under **Faults > Display Faults**.

Procedure

- Step 1** In the left pane, select one of the following thresholds to apply to the setting:
- SNMP Reachable—See [Setting the SNMP Reachable Threshold, page 3-47](#)
 - HSRP Standby to Active—See [Setting the HSRP Standby to Active Policy, page 3-47](#)

Setting the SNMP Reachable Threshold

Use this setting to make sure that the WLSM is reachable using SNMP.

This threshold is enabled by default.



Note

It is highly recommended that this threshold not be disabled. If it is disabled, and a device becomes unreachable, the SNMP-based faults cannot be detected, and there will be no SNMP unreachable faults displayed to alert you.

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Down	From the list, select the severity level and the number of polling cycles before the status is Down.
Up	From the list, select the number of polling cycles before the fault is cleared and the status is Up.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting the HSRP Standby to Active Policy

Use this setting to indicate when the WLSM that is configured for hot standby has become active.

This policy is enabled by default. When this policy is enabled, the WLSE monitors the WLSMs configured in hot standby mode. Whenever the WLSE detects a change in the HSRP state, it generates a "Standby WLSM has changed to Active" fault. This fault can be cleared manually and it will not reappear.

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to enable the policy.

Field	Description
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 3-51](#) for details.

Setting Router Fault Thresholds

Using this option, you can set up the router's SNMP reachable threshold. When the threshold is exceeded, a fault is generated and can be viewed under **Faults > Display Faults**.

This setting is enabled by default.



Note

It is highly recommended that this threshold not be disabled. If it is disabled, and a device becomes unreachable, the SNMP-based faults cannot be detected, and there will be no SNMP unreachable faults displayed to alert you.

Procedure

- Step 1** Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Down	From the list, select the severity level and the number of polling cycles before the status is Down.
Up	From the list, select the number of polling cycles before the fault is cleared and the status is Up.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting AAA Server Response Time

Using this option, you can set up a threshold for LEAP, PEAP, RADIUS, EAP-MD5, and EAP-FAST server response time. When the threshold is exceeded, a fault is generated and can be viewed under **Faults > Display Faults**.

This threshold is disabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Unavailable	From the list, select the severity level and the number of polling cycles before the status is Unavailable.
Authentication Failure	From the list, select the severity level and the number of polling cycles before the status indicates an Authentication Failure.
Overloaded	From the list, select the severity level, the response time, and the number of polling cycles before the status is Overloaded.
Degraded	From the list, select the severity level, the response time, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the response time, and the number of polling cycles before the status is OK.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting WLSE Policies

Setting WLSE Duplicate IP Detection

Using this option, you can make sure that there are no duplicate or conflicting IP addresses in the network. Duplicate IPs are found during discovery only, and the AP with the duplicate IP address is placed in the Duplicate IP folder under **Devices > Managed > Manage/Unmanage**. For more information, see [Handling Duplicate IP Addresses on Access Points, page 4-61](#).

When the policy is enabled and a duplicate IP is detected, a fault is generated and can be viewed under **Faults > Display Faults**.

**Note**

This policy is enabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to enable a threshold for this component.
Severity	From the list, select a severity level to associate with this setting.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.

Setting WDS Thresholds

Using this option, you can set the following thresholds for the access point providing wireless domain services (WDS) on the wireless LAN:

- Authentication Failures—See [Setting the Authentication Failures Threshold, page 3-50](#)
- WLSE-WDS Link Status—See [Setting the WLSE-WDS Link Status Threshold, page 3-51](#)

When a threshold is exceeded, a fault is generated and can be viewed under **Faults > Display Faults**.

Setting the Authentication Failures Threshold

Use this setting to make sure that authentication is used to open a WLCCP channel between the WLSE and the WDS.

This threshold is disabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Settings	
Down	From the list, select the severity level before the status is Down.
Up	The fault is cleared and the status is Up.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.
-

Setting the WLSE-WDS Link Status Threshold

Use this setting to make sure that the WDS is up and communicating with the WLSE.

This threshold is disabled by default.

Procedure

- Step 1** Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Settings	
Down	From the list, select the severity level before the status is Down.
Up	The fault is cleared and the status is Up.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Default to Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Default Setting to a Device, page 3-14](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 3-51](#) for details.
-

Viewing Current Faults

When you click the link at the bottom of any policy or threshold, a window appears that allows you to view all the faults associated with it.

Using this window, you can view the faults and clear them.

Procedure

- Step 1** To view the faults associated with each threshold or policy, click the **View current faults for this setting** link at the bottom of the screen.

The following table appears:

Field	Description
IP Address	The device IP address. Click to see various reports about the device. For information on the reports, see Using the Device Center, page 10-7 .
Hostname	The device for which the fault is reported. Click to see various reports about the device. For information on the reports, see Using the Device Center, page 10-7 .
Family	The product family.
Product	The product name.
Type	The device or the sub-device component.
Description	A description of the fault. Click to see fault details. See Viewing Fault Details, page 3-7 . Note For an explanation of the faults, in the online help click Troubleshooting , or on Cisco.com see the Fault Description Table in the <i>FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.13</i> .
Severity	The fault severity level.
State	The operational state of the device.
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed. See Understanding WLSE Time Displays, page 1-10 . Click to see fault details. See Viewing Fault Details, page 3-7 .

- To clear an individual fault, select it, then click **Clear**.
- To clear more than one fault, select them, then click **Clear**.
- To clear all the faults, click **Select All**, then click **Clear**.



Note It may be a few seconds before the faults clear.

Viewing the Status of the VoWLAN

The **Faults > Voice Summary** feature allows you to view a summary of the current voice status of the WLAN.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Faults > Voice Summary**. The Voice Summary window appears.
- Step 2** This window displays the following information:
- The number of occurrences of the following voice fault types:
 - Excessive Voice Bandwidth (CAC)
 - Degraded Voice QoS (TSM)
- Click on either fault type to display a table that contains the faults for that type (see [Viewing the Voice Fault Tables, page 3-53](#)).
- The quality of service status levels—see [Viewing the QoS Status Summaries, page 3-54](#)
- Step 3** To change how often you want the screen to refresh, enter the number of seconds (30 seconds or higher) in the Refresh (Sec) field. The default is 90 seconds.
-

Viewing the Voice Fault Tables

The Voice Fault Type links in the **Faults > Voice Summary** window display fault tables for the following voice fault types:

- Excessive Voice Bandwidth (CAC)
- Degraded Voice QoS (TSM)

You can use these fault tables to acknowledge, unacknowledge, or clear selected faults or to view the details of a selected fault. For information about the data reported by fault tables, see [Display Faults Table, Table 3-2 on page 3-5](#).

**Note**

For an explanation of the faults, in the online help click **Troubleshooting**, or on Cisco.com see the Fault Description Table in the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.13*.

Related Topics

[Viewing the Status of the VoWLAN, page 3-53](#)

Viewing the QoS Status Summaries

The QoS Status links in the **Faults > Voice Summary** window display the metrics for the group of APs assigned to one of the following quality of service (QoS) status levels:

- Calls (APs) with Degraded QoS
- Calls (APs) with Fair QoS
- Calls (APs) with Normal QoS

For more information about this report, see [AP Group Metrics Summary: Current, page 10-25](#).

Related Topics

- [Assigning Voice QoS Fault Settings, page 3-54](#)
- [Viewing the Status of the VoWLAN, page 3-53](#)

Assigning Voice QoS Fault Settings

Use **Faults > Voice QoS Settings** to enable Voice QoS fault detection and to assign a severity levels to the faults that are generated. Voice faults can be viewed under **Faults > Voice Summary** or **Faults > Display Faults**.

You can assign the following Voice QoS settings:

- Downstream Delay with U-ASPD not used
- Downstream Delay with U-ASPD used
- Upstream Delay
- Downstream Packet Loss Rate
- Upstream Packet Loss Rate
- Roaming Time



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Faults > Voice QoS Settings**. The Voice QoS Settings window appears.

Step 2 Define the following QoS settings:

	Description
Downstream Delay with U-ASPD not used	Assign the QoS status to Green when this percentage or more of the packets have a delay of less than 20 milliseconds.
	Assign the QoS status to Yellow when this percentage (or more) of the packets have a delay of greater than or equal to 20 milliseconds and less than 40 milliseconds delay per cell.
	Note The Red QoS status is automatically set to 100% minus the Yellow value.
Downstream Delay with U-ASPD used	Assign the QoS status to Green when this percentage or more of the packets have a delay of less than 20 milliseconds.
	Assign the QoS status to Yellow when this percentage (or more) of the packets have a delay of greater than or equal to 20 milliseconds and less than 40 milliseconds delay per cell.
	Note The Red QoS status is automatically set to 100% minus the Yellow value.
Upstream Delay	Assign the QoS status to Green when this percentage or more of the packets have a delay of less than 20 milliseconds.
	Assign the QoS status to Yellow when this percentage (or more) of the packets have a delay of greater than or equal to 20 milliseconds and less than 40 milliseconds delay per cell.
	Note The Red QoS status is automatically set to 100% minus the Yellow value.
Downstream Packet Loss Rate	Assign the QoS status to Green when the packet loss rate is less than this value (must be less than or equal to the Yellow value).
	Assign the QoS status to Yellow when the packet loss rate is less than this value (must be greater than or equal to the Green value).
	Note The Red QoS status is automatically assigned the Yellow value.
Upstream Packet Loss Rate	Assign the QoS status to Green when the packet loss rate is less than this value (must be less than or equal to the Yellow value).
	Assign the QoS status to Yellow when the packet loss rate is less than this value (must be greater than or equal to the Green value).
	Note The Red QoS status is automatically assigned the Yellow value.
Roaming Time	Assign the QoS status to Green when the roaming time is less than this number of milliseconds (must be less than or equal to the Yellow value).
	Assign the QoS status to Yellow when the roaming time is less than this number of milliseconds (must be greater than or equal to the Green value).
	Note The Red QoS status is automatically assigned the Yellow value.

Step 3 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Related Topics

- [Assigning Voice QoS Fault Settings, page 3-54](#)
- [Displaying Voice Reports, page 10-24](#)

Notification Settings

When a fault is detected, the WLSE can send automated notifications in the form of SNMP traps, syslog messages, and email alerts. You can specify multiple recipients for each notification type, and choose to deliver the message using either a plain text or XML format.

This section has the following options:

- [Setting Trap Notification](#)
- [Setting Syslog Notification](#)
- [Emailing Faults](#)



Note

Your login determines whether you can use this option.

Related Topics

- [Displaying Fault Information, page 3-1](#)
- [Setting Policies and Thresholds, page 3-14](#)

Setting Trap Notification

This option allows you to enable the WLSE to send north-bound exception notification to one or more SNMP trap receivers. The exception notification contains information such as device name and IP, fault number, timestamp, exception severity, and a message describing the problem.

The following MIB defines the trap and the varbinds:

CISCO-DEVICE-EXCEPTION-REPORTING-MIB.my. It can be downloaded from the Cisco.com download site and loaded into the trap receiver.

The WLSE supports only SNMP v2c traps. Solaris 2.8-based NetView 7.1 receives and displays the SNMP v2c fault notification traps from WLSE. Windows-based NetView 7.1 supports only v1 traps and cannot receive and display any v2c traps from the WLSE.

Before You Begin

Make sure your SNMP trap receiver's trap receiving daemon is set to the correct port. The default port is set to 162.

Procedure

Step 1 Select **Faults > Notification Settings**. The Fault Notification Settings dialog box appears.

- Step 2** Select the message format for the notification: Plain Text or XML. See [Trap Notification Message Format, page 3-57](#) for an example.



Note The plain text SNMP trap messages sent by the WLSE for fault notifications contain newlines (line feeds) as delimiters between the fields in the cderExcepData varbind.

- Step 3** Complete the following:

Field	Description
Trap	Select to enable trap notification.
Host	Enter the hostname/IP of the SNMP trap receiver to which you want to send SNMP trap notification.
Port	Enter the port number if different from the default of 162.
Community	Enter the community string.

- Step 4** If you want a different host to receive trap notification, click **Add Trap Receiver Host**. There is no limit to the number you can enter.

To a row, click **Delete**, next to the row you want to remove.

- Step 5** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to save your settings.

Trap Notification Message Format

The WLSE can report device alerts in the form of SNMP traps. The information can be formatted in either plain text or XML format. (See [Plain Text Trap Notification Message, page 3-59](#) and [XML Trap Notification message, page 3-60](#) for examples.



Note The plain text SNMP trap messages sent by the WLSE for fault notifications contain newlines (line feeds) as delimiters between the fields in the cderExcepData varbind.

The following information is reported:

Field	Description
cderExcepId	The unique fault ID associated with the alert being reported.
cderExcepHostAddressType	The type of device address stored in cderExcepHostAddress. Possible values include: unknown (0); ipv4 (1); ipv6 (2); and dns(16).
cderExcepHostAddress	The address of the device for which this alert is being reported.
cderExcepPriorityDescription	The severity of the alert. Possible values include: P1 through P5 and OK.
cderExcepIpTime	The time the alert was generated.

Field	Description
cderExcepData	The alarm information in name value pairs. Alarm information is formatted into either plain text or XML. For plain text messages, each name value pair is terminated by a newline; for XML, the value is enclosed by XML tags (for example, <name>value</name>). The information includes: • FaultId—The unique fault ID associated with the alert. • DeviceId—The unique device ID associated with the device. • DeviceIP—The IP address of the device for which the alert is being reported. • DeviceName—The name of the device for which the alert is being reported. The device name corresponds to the Name Format you defined under Devices > Discover > Discover > Advanced Options. By default, the format is %hostname%. In addition, the AP hostname is sent in the outgoing notification. If you change the Name Format to be, for example, %dns%, the fully qualified DNS name of the AP is sent. • MO—The managed object. • Change—the description of the alert prior to the state change. • ChangeSeverity—The severity of the alert prior to the state change. • StateChange—The description of the alert after the state change. • AlarmState—The state of the alarm: active or cleared. • OverallSeverity—The severity of the alert. • DeviceType—The device type. For example, AccessPoint.
cderExcepReprtdBy	The name of the WLSE that is reporting the alert.

Plain Text Trap Notification Message

An example of a trap notification message using plain text will appear as follows. Note the newline (linfeed, '\n', or 0x0a) characters at the end of each name-value pair in the cderExcepData field.)

```
community: public
bindings: sysUpTime => 3 days, 19:13:58
snmpTrapOID => 1.3.6.1.4.1.9.9.224.2.0.1
cderExcepId.2 => 1
cderExcepHostAddressType.2 => 1
cderExcepHostAddress.2 => 192.148.58.24
cderExcepPriorityDescription.2 => P1
cderExcepIpTime.2 => 3 days, 19:13:57
cderExcepData.2 =>
    FaultId: 1\n
    DeviceId: 100\n
    DeviceIP: 192.148.58.24\n
    DeviceName: 192.148.58.24\n
    MO: Device\n
    Change: HTTP access is enabled\n
    ChangeSeverity: P1\n
    StateChange: HTTPAccess is ViolatingPolicy\n
    AlarmState: Active\n
    OverallSeverity: P1\n
    DeviceType: AccessPoint\n
cderExcepReportedBy.2 => FaultNotifier@wlse-appliance2.cisco.com
```

XML Trap Notification message

An example of a trap notification message using XML will appear as follows:

```
community: public
bindings: sysUpTime          => 3 days, 19:20:46
          snmpTrapOID         => 1.3.6.1.4.1.9.9.224.2.0.1
          cderExcepId.11      => 1
          cderExcepHostAddressType.11 => 1
          cderExcepHostAddress.11 => 192.148.48.24
          cderExcepPriorityDescription.11 => P1
          cderExcepIpTime.11 => 3 days, 19:20:46
          cderExcepData.11 =>
<Msg> <FaultId>1</FaultId> <DeviceId>100</DeviceId> <DeviceIP>192.168.98.24</DeviceIP>
<DeviceName>192.148.48.24</DeviceName> <MO>Device</MO>
<Change>HTTP access is enabled</Change> <ChangeSeverity>P1</ChangeSeverity>
<StateChange>HTTPAccess is ViolatingPolicy</StateChange> <AlarmState>Active</AlarmState>
<OverallSeverity>P1</OverallSeverity> <DeviceType>AccessPoint</DeviceType> </Msg>
cderExcepReportedBy.11 => FaultNotifier@wlse-appliance2.cisco.com
```

Setting Syslog Notification

This option allows you to send syslog messages to selected syslog servers. The messages contain information such as device name and IP, fault number, date and time, exception severity, and a message about what is wrong.



Note

The device name used in the notifications is the name entered in the NameFormat field under **Devices > Discover > Discover > Advanced Options**. By default, it is set to %hostname%.

Before You Begin

Make sure your syslog server is turned on to be able to receive messages from the Wireless LAN Solution Engine. Also make sure that the receiving process is configured to receive messages from remote hosts (for example, start syslogd with -r option on some UNIX versions).

Procedure

- Step 1** Select **Faults > Notification Settings**. The Fault Notification Settings dialog box appears.
- Step 2** Select the message format for the notification: Plain Text or XML. See [Syslog Notification Message Format, page 3-61](#) for an example.



Note

The plain text Syslog messages sent by the WLSE for fault notifications contain newlines (line feeds) as delimiters between the message fields

Step 3 Complete the following:

Field	Description
Syslog	Select to send syslog messages to designated syslog servers.
Enter Syslog host names	Enter the hostname/IP for the syslog servers. Names must be separated by a space, a comma, a semicolon, or a new line.

Step 4 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to save your settings.

Syslog Notification Message Format

You have the option of sending the fault notification as plain text or in an XML format.



Note

The plain text Syslog messages sent by the WLSE for fault notifications contain newlines (line feeds) as delimiters between the message fields.

In these notifications, a P1 severity notification corresponds to %FLT-1-MSG, a P2 severity notification corresponds to %FLT-2-MSG, and so on. A cleared fault (OK) notification corresponds to %FLT-6-MSG.

- An example of a syslog fault notification message using plain text will appear as follows:

```
<189> Jun 03 01:26:59 samuraiwhat FaultNotifier:%FLT-6-MSG:FaultId 48\nDeviceId
1784\nDeviceIP 10.10.10.31\nDeviceName 10.10.10.31\nMO RF Port awc0\nChange Cleared by
user admin\nChangeSeverity OK\nStateChange SSID is OK\nAlarmState
Cleared\nOverallSeverity OK
```

- An example of a syslog fault notification message using XML will appear as follows:

```
<189> Jun 03 00:57:15 samuraiwhat FaultNotifier:%FLT-6-MSG:<Msg><FaultId>48</FaultId>
<DeviceId>1784</DeviceId> <DeviceIP>10.10.10.31</DeviceIP>
<DeviceName>10.10.10.31</DeviceName> <MO>RF Port awc0</MO> <Change>Cleared by user
admin</Change> <ChangeSeverity>OK</ChangeSeverity>
<StateChange>SSID is OK</StateChange> <AlarmState>Cleared</AlarmState>
<OverallSeverity>OK</OverallSeverity></Msg>
```

Emailing Faults

E-mail recipients can be configured to receive fault notifications based on fault priority.

Before You Begin

Configure the mailroute so that the WLSE knows where to send the e-mails. Enter the mail server hostname or IP address by selecting **Administration > Appliance > Configure Mailroute**.

Procedure

Step 1 Select **Faults > Notification Settings**. The Fault Notification Settings dialog box appears.

Step 2 Select the message format for the notification: Plain Text or XML. See [Email Notification Message Format, page 3-62](#).

Step 3 Complete the following:

Field	Description
Email	Select to enable email notification of exception information.
Enter email addresses	Enter the email addresses of users you want to receive exception notification. Addresses must be separated by a space, a comma, a semicolon, or a new line. Note The following characters are not allowed in email addresses: &, ?, ^, *, <, /, \, and > .
IDS Faults	Click to select the priority of the IDS exceptions you want emailed. After an exception is cleared, a corresponding OK email is sent. Note When you select or deselect any of these IDS priority settings, the changes are reflected under both the IDS > Notification Settings <i>and</i> Fault > Notification Settings tabs.
Non-IDS Faults	Click to select the priority of the non-IDS exceptions you want emailed. After an exception is cleared, a corresponding OK email is sent. Note When you select or deselect any of these non-IDS priority settings, the changes are reflected under both the IDS > Notification Settings <i>and</i> Fault > Notification Settings tabs.



Tip If email notification is not working, you might need to configure the mailroute by selecting **Administration > Appliance > Configure Mailroute**.

Step 4 If you want a different group of users to receive different priority level exceptions, click **Add Group** to add another set of email addresses. There is no limit to the number of email addresses you can enter.

To delete a row, click **Delete**, next to the row you want to remove.

Step 5 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to save your settings.

Email Notification Message Format

The emailed exception notification contains the following information:

Attribute	Description
FaultId	A unique identifier for the fault.
DeviceId	A unique identifier used by the WLSE for the device with the fault.
DeviceIp	The IP address of the device with the fault.

Attribute	Description
DeviceName	The name of the device with the fault. The device name used in the notification is the name entered in the NameFormat field under Devices > Discover > Discover > Advanced Options . By default, it is set to %hostname%.
MOId	The identifier used by the WLSE for the subcomponent of the device with the fault.
AlarmState	The state of the Alarm (Active or Cleared).
Description	A description of the last updated to the fault.
Severity	The severity of the fault. Note OK indicates a cleared (fixed) fault.

You have the option of sending the fault notification as plain text or in an XML format.

- An example of an email notification message using plain text will appear as follows:

```
Subject:10.10.10.31[10.10.10.31] OK notification. FaultId 48. RF Port awc0 SSID is OK.
Cleared by user admin
From:FaultNotifier@samuraiwhat.cisco.com
Date:Tue, 3 Jun 2006 01:26:59 GMT
To:user@cisco.com
FaultId 48
DeviceId 1784
DeviceIP 10.10.10.31
DeviceName 10.10.10.31
MO RF Port awc0
Change Cleared by user admin
ChangeSeverity OK
StateChange SSID is OK
AlarmState Cleared
OverallSeverity OK
```

- An example of an email notification message using XML will appear as follows:

```
Subject:10.10.10.31[10.10.10.31] P1 notification. FaultId 48. RF Port awc0 SSID is
ViolatingPolicy. SSID policy violation tracyv
From:FaultNotifier@samuraiwhat.cisco.com
Date:Tue, 3 Jun 2006 00:57:55 GMT
To:user@cisco.com
<Msg><FaultId>48</FaultId><DeviceId>1784</DeviceId><DeviceIP>10.10.10.31</DeviceIP><De
viceName>10.10.10.31</DeviceName><MO>RF Port awc0</MO><Change>Cleared by user
admin</Change><ChangeSeverity>OK</ChangeSeverity><StateChange>SSID is
OK</StateChange><AlarmState>Cleared</AlarmState><OverallSeverity>OK</OverallSeverity><
/Msg>
```




Device Discovery and Management

The Devices tab provides options for basic device management on the WLSE. The options in this tab allow you to discover and manage devices and organize devices into easily manageable groups.

The topics covered in this chapter are:

- [Getting Started with Device Management, page 4-1](#)
- [How the WLSE Communicates with Devices, page 4-3](#)
- [Overview: Devices Tab Functions, page 4-3](#)
- [Entering Device Credentials, page 4-5](#)
- [Monitoring AAA Servers, page 4-14](#)
- [Managing Device Discovery, page 4-23](#)
- [Managing Devices, page 4-54](#)
- [Managing Device Inventory, page 4-63](#)
- [Using Enhanced \(WDS\) Client Tracking, page 4-18](#)
- [Exporting Devices, page 4-71](#)
- [Managing Groups, page 4-74](#)

Getting Started with Device Management

This section describes two methods for deploying devices in a wireless network:

- The Deployment Wizard for devices used in a [SWAN](#) framework—See [Using the Deployment Wizard, page 4-1](#).
- Manual configuration—See [Using Manual Methods, page 4-2](#).

Using the Deployment Wizard

For IOS access points used within a Cisco [SWAN](#) framework, you can use Wireless Domain Services ([WDS](#)) and the WLSE's Deployment Wizard for device configuration and deployment, instead of using manual deployment procedures. The Deployment Wizard is the preferred method for SWAN deployments. If you are using the Deployment Wizard, see [Chapter 2, “Using the Deployment Wizard.”](#)

The Deployment Wizard handles device configuration and discover. You can also set up device groupings to make management easier, if desired. See [Managing Groups, page 4-74](#).

Using Manual Methods

If you do not use the Deployment Wizard, you can use the configuration methods described in the following paragraphs.

Before you can use the WLSE to manage newly added devices, the following tasks must be performed:

- Configure the devices
- Configure the WLSE
- Discover the devices
- Move the devices to the managed state
- (Optional) set up your own device groupings to make management easier.

To get started, follow the steps explained in the following paragraphs.

Step 1: Set up devices

Before devices can be discovered and managed by the WLSE, they must be properly configured. In addition, if you are using WLSE radio management, access points must be configured for Wireless Domain Service (WDS) and for LEAP authentication. You can:

- Configure devices manually. For information on setting up devices manually, see *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.13* on Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html.
- Use auto-config. See [Automating Configurations](#), page 8-39.

Step 2: Enter device credentials

Enter device credentials on the WLSE as follows:

- Community strings for all managed devices—see [Enter or Modify SNMP Community Strings for All Devices](#), page 4-6.
- Telnet/SSH credentials for access points—see [Enter Telnet/SSH Usernames and Passwords—Access Points](#), page 4-10.
- HTTP ports for access points—see [Enter HTTP/HTTPS Port Settings—Access Points](#), page 4-13.
- WLCCP credentials—see [Enter WLCCP Credentials for Wireless Domain Services](#), page 4-13.
- Information about AAA servers that you want to monitor—see [Monitoring AAA Servers](#), page 4-14.

Step 3: Discover devices

Initiate discovery from the WLSE or import devices:

- Add seed devices and run discovery—see [Managing Device Discovery](#), page 4-23.
- Import devices—see [Importing Devices from a File](#), page 4-38 and [Importing Devices from a CiscoWorks Server](#), page 4-39.

Step 4: Verify discovery

Verify that devices were discovered—see [Viewing Discovery Logs](#), page 4-48.

Step 5: Move devices to managed state

Before you can use configuration, reporting, and monitoring features, devices must be managed by the WLSE. You must either manually move devices to the managed state on the WLSE after discovery, or specify that all discovered devices be automatically managed—see [Managing Devices, page 4-54](#).

Step 6: Run inventory

After the devices are in the managed state, an immediate inventory runs automatically to obtain device information needed to use such WLSE features as reports and automatic grouping—see [Managing Device Inventory, page 4-63](#).

You can also run inventory polling on demand for one or more devices. When new devices are discovered and managed, basic inventory and client reports are not populated until the next inventory polling occurs. However, you can use on-demand inventory to populate these reports before the next inventory cycle starts. You can also use on-demand inventory when configuration changes are made on network devices and you want the changes quickly reflected in the basic and client inventory reports.

Step 7: Create device groups

The WLSE grouping feature lets you organize managed devices into logical subsets and hierarchies. Using device grouping, you can quickly configure and upgrade a set of access points, and view reports for a set of access points as a single operation—see [Managing Groups, page 4-74](#).

Step 8: Use All WLSE Management Features

Now you can use fault monitoring, reports, firmware upgrade, configuration, and radio management. You can also export devices, monitor AAA servers, and use Wireless Domain Services.

How the WLSE Communicates with Devices

The WLSE communicates directly with devices through SNMP and through the device CLI. For status analysis, communication takes place through most of the MIBs supported on access points. To configure IOS-based access points, the access point CLI is used. To check device configuration, the WLSE can be configured to inventory all managed access points at user-defined intervals. For status analysis, polling intervals can be configured.

For radio management, the WLSE communicates directly with access points through Wireless Domain Service (WDS) and, for some operations, directly through SNMP. This communication takes place via Cisco's Wireless LAN Context Control Protocol (WLCCP). For this communication to occur, the access points and the WLSE authenticate with the WDS through LEAP-over-WLCCP. The frequency of radio management operations can be specified through the job scheduling interface for radio management.

From the WLSE's viewpoint, all communication is through its Ethernet interfaces. For some radio management operations, the access points communicate with each by using their radios.

Overview: Devices Tab Functions

The Devices tab covers basic device management on the WLSE. The options under this tab allow you to discover and manage devices, inventory devices, and organize devices into easily manageable groups. After devices are discovered and managed, you can use all of the other WLSE management features. For more explanation of these options, see [Getting Started with Device Management, page 4-1](#).

Managed devices can be exported to a file and to CiscoWorks Resource Manager Essentials.

**Note**

These subtabs may not be visible to some users; what you see under the Devices tab depends on the roles assigned to your login.

The Devices tab leads to two subtabs:

- Discover—Discovery, inventory, and device management options. The subtabs and options are briefly described in [Table 4-1 on page 4-4](#).
- Group Management—Allows you to view system groups and to create your own custom static and dynamic groups—See [Managing Groups, page 4-74](#) for information on system groups and procedures for using custom groups.

Table 4-1 **Functions of the Discover Subtab**

Subtab	Option	Reference
Managed Devices	Managed Devices—View details about a device, manage and unmanage devices, delete devices, add descriptions.	Managing Devices, page 4-54
Discover	Discovery Wizard—Run CDP discoveries or import devices.	Using the Discovery Wizard, page 4-33
	Advanced Options—Specify how devices are named, use reverse DNS lookup, auto-manage devices (with or without filtering), set discovery filtering.	Setting Advanced Discovery Options, page 4-41
	IP Filter Rules—Specify the rules for discovery filtering.	Using Discovery IP Address Filtering, page 4-47
	Logs—View discovery run logs.	Viewing Discovery Logs, page 4-48
Device Credentials	SNMP Communities	Enter or Modify SNMP Community Strings for All Devices, page 4-6
	Telnet/SSH User/Password	Enter Telnet/SSH Usernames and Passwords—Access Points, page 4-10
	IOS HTTP/HTTPS Port Settings	Enter HTTP/HTTPS Port Settings—Access Points, page 4-13
	WLCCP Credentials	Enter WLCCP Credentials for Wireless Domain Services, page 4-13
Inventory	Run Inventory	Running Immediate Inventories, page 4-65
	Polling—Specify polling intervals, how long to retain fault and job history data, and how long to retain aggregated data. Delete discovery and inventory logs.	Managing Polling Parameters, page 4-66
	Logs—View inventory logs.	Viewing Inventory Logs, page 4-69

Table 4-1 Functions of the Discover Subtab (continued)

Subtab	Option	Reference
Export Devices	To CiscoWorks—Export devices to CiscoWorks RME.	Exporting Devices, page 4-71
	To CSV File—Export devices to a file.	
AAA Server	Enter AAA servers to be monitored by the WLSE.	Monitoring AAA Servers, page 4-14
Client Tracking	Enable enhanced client tracking on WDS devices.	Using Enhanced (WDS) Client Tracking, page 4-18

Entering Device Credentials

The Device Credentials options allow you to enter the various credentials required for WLSE management and other features to work. These options are listed in [Table 4-2 on page 4-5](#).



Note

If you are using the WLSE Deployment Wizard to deploy IOS access points used within a Cisco [SWAN](#) framework, you can enter credentials in the Wizard instead of using the screens described in this section. For information on the Deployment Wizard, see [Chapter 2, “Using the Deployment Wizard.”](#)

The Device Credentials option lets you enter the following required device credentials:

- All managed devices must have SNMP credentials entered on the WLSE. Before the WLSE device discovery or device polling can successfully communicate with devices, the WLSE must be aware of the appropriate device SNMP credentials to use.
- For IOS-based access points, you must enter Telnet or SSH credentials and IOS HTTP port settings.
- If you are using Wireless Domain Services (WDS), you must enter RADIUS credentials and configure the WDS access point.

The Device Credentials options are:

Table 4-2 Device Credential Options

Option	Function	Reference
SNMP Communities	All devices—Enter community strings. Required for discovery. Note Community strings can also be entered in the Discovery Wizard and the Deployment Wizard.	Enter or Modify SNMP Community Strings for All Devices, page 4-6
Telnet/SSH User/Password	IOS APs—Enter the Telnet or SSH usernames and passwords. Note Telnet/SSH credentials can also be entered in the Deployment Wizard.	Enter Telnet/SSH Usernames and Passwords—Access Points, page 4-10
IOS HTTP Port Settings	IOS APs—Enter HTTP port numbers.	Enter HTTP/HTTPS Port Settings—Access Points, page 4-13

Table 4-2 **Device Credential Options (continued)**

Option	Function	Reference
WLCCP Credentials	WDS—Enter RADIUS credentials for WDS.	Enter WLCCP Credentials for Wireless Domain Services, page 4-13

Enter or Modify SNMP Community Strings for All Devices

The WLSE uses [SNMP](#) community strings to discover devices and enable other WLSE options, such as firmware updates, configuration, and radio management. If community strings are not entered correctly, the WLSE cannot communicate with the device. Both read-only and read/write community strings are required.

The default community string covers all devices and uses *public* for both the read-only string and the read-write string. If the community strings on your devices differ from the default, you must specify the community strings on the WLSE before devices can be discovered and managed. For guidelines on configuring community strings on your devices, see the document *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine* at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html.

If you are importing devices from a file or CiscoWorks (instead of using the discovery mechanism), the community strings will also be imported. You do not need to enter the community strings here; however, if you import the strings and want to edit them, you can use this screen to do so. Also, if you imported devices and you want to customize the timeouts and retries, you can use this screen. For information about importing devices, see [Importing Devices from a File, page 4-38](#) and [Importing Devices from a CiscoWorks Server, page 4-39](#).

If you are using the Discovery Wizard to run CDP discovery, you can enter community strings in the wizard. For more information, see [Using the Discovery Wizard, page 4-33](#).

If you are using the Deployment Wizard to deploy access points in a WDS environment, you can enter community strings in the Wizard. For more information, see [Chapter 2, “Using the Deployment Wizard.”](#)



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Devices > Discover > Device Credentials > SNMP Communities**.



Note

The SNMP Communities dialog box contains a default entry that covers all devices, provided that device community strings are set to the default (*public*). This entry is also used when none of the specified rules match a given IP address.



Note

For information on guidelines for entering community strings, click **Learn more about community strings guidelines**.

Step 2 To add an entry:

- a. Enter data in the individual text boxes: IP address, Read Community, SNMP Timeout, SNMP Retries, and Write Community. [Table 4-3](#) describes the community string variables. For more guidelines, see [Recommendations For Configuring SNMP Credentials, page 4-8](#).
- b. Click **Add**.

Result: The community string appears in the list of entries.

Table 4-3 Community String Variables

Variable	Description	Notes
IP Address	IP address of a device or range of devices that use these community strings.	If you do not specify an IP address, the default community strings apply to all devices in the network.
Read Community	Password allowing read-only access to the devices.	You must specify the read community string. Otherwise, the default value of <i>public</i> is used.
SNMP Timeout	Length of time (seconds) the server waits for a response from the device before performing the first retry.	The default is 10 seconds. If you increase the timeout period, discovery could take significantly longer to complete. The minimum is one and the maximum is 60.
SNMP Retries	Number of attempts the server makes to communicate with the device before declaring that the device has timed out.	The default is one retry. If you increase the number of retries, discovery takes significantly longer to complete. The default retry policy doubles the previous timeout value for retry.
Write Community	Password that allows write access to the devices.	You must specify the write community string. Otherwise, the default value of <i>public</i> is used.

Step 3 To modify an entry:

- a. Select the entry in the list of entries.
- b. Change the desired fields in the individual text boxes.
- c. Click **Modify**.



Note The IP Address field of an existing entry cannot be changed.

Step 4 To delete an entry:

- a. Select the entry in the list of entries. To select a number of community strings, hold down the Ctrl key while dragging the mouse down the list.
- b. Click **Delete**.



Note The default entry cannot be deleted.

Step 5 Click **Save** to apply your changes.

Related Topics

- [Community String Format, page 4-8](#)
- [Recommendations For Configuring SNMP Credentials, page 4-8](#)

Recommendations For Configuring SNMP Credentials

This section contains the following information:

- [Unsupported Characters, page 4-8](#)
- [Community String Format, page 4-8](#)
- [Multiple Entries and Order of Use, page 4-8](#)
- [Example of Matching, page 4-9](#)
- [SNMP Timeouts and Retries, page 4-9](#)

Unsupported Characters

You cannot enter the <> sequence of characters in the Read Community and Write Community textboxes; for example <abc> is not allowed. The sequence >< is allowed, and the single characters < and > are allowed.

Spaces not allowed.

The following characters are not recommended for community strings: question mark (?), double-quotes ("), dollar sign (\$), plus (+), left square bracket ([), pound sign at the beginning of the string (#), exclamation mark (!), and semi-colon (;).

Community String Format

Use these guidelines when constructing entries:

- You can assign community strings to any of the following:
 - Complete IP address; for example, 172.20.4.9
 - Wild cards based on IP addresses; for example:
 ..*.*.
 172.*.*.*
 - Address ranges, which can be combined with wild cards; for example:
 27.20.[4-55].*
 172.[21-30].[44-88].*
 172.*.*.[121-255]
- All printable characters, except for colons (:), are allowed in community strings.
- Spaces are not allowed in community strings.
- Comments are not allowed.

Multiple Entries and Order of Use

The default entry (*.*.*.*) is used when none of the specified rules match a given IP address. The default entry cannot be removed.

When there are multiple entries that are potential matches for an IP address:

- The WLSE will use the best (longest) matching community string. So, a fully formed IP address always takes the highest precedence.
- Matching is done from left to right on the IP address field.
- In case of conflicts caused by overlapping address specifications, the entry listed first will be used.

It is strongly recommended that you remove any ambiguity by breaking address specifications into non-overlapping sets.

The order in which you add entries does not matter.

Example of Matching

For example, assume that the user specifies community strings in the following order:

Row	Community String
1	172.20.[20-40].*
2	*.*.*.*
3	172.*.[20-40].*
4	172.20.30.44
5	172.[20-30].[20-50].*
6	172.[20-30].[30-40].*

The following device IP addresses match the user's community string specifications as follows:

- 172.20.30.40 matches row 1
- 172.20.50.40 matches row 5
- 172.50.30.40 matches row 3
- 192.168.98.98 matches row 2
- 172.20.30.44 matches row 4 (fully formed IP address)
- 172.30.40.44 matches row 6 (higher precedence than row 5)

Internally, the WLSE reorders the user specifications as follows:

```
172.20.30.44
172.20.[20-40].*
172.[20-30].[30-40].*
172.[20-30].[20-50].*
172.*.[20-40].*
*.*.*.*
```

SNMP Timeouts and Retries

Use caution in configuring the SNMP timeouts and retries because the timeout/retry mechanism uses an exponential back-off algorithm. Follow these guidelines:

- In almost all circumstances, the default timeout of 10 seconds should not be changed.
- Because SNMP is UDP-based and UDP packets can easily be lost in normal network conditions, it is usually advisable to increase the number of retries to two.

However, if you are managing devices across high latency links (for example, thin or congested WAN links) or you encounter problems with SNMP timeouts, you might need to increase the timeouts or retries. If you need to change the default timeout and retries settings, the only way to arrive at optimal settings is through experimentation. One recommended procedure is to incrementally increase the timeout settings without increasing the retries until SNMP timeouts cease:

1. Validate that the devices have the proper SNMP configuration and that the correct SNMP credentials are entered into the WLSE.
2. Increase the timeout by a small amount of time, perhaps 5 seconds.
3. Use the SNMP connectivity tool (see [Using Network Tools, page 16-47](#)) to check if SNMP requests time out. If they do, increase the timeout and test reachability again.

Continue the process until SNMP requests no longer time out. Then leave the timeout setting in place, allowing the WLSE to operate normally with these settings. If you continue to see SNMP timeouts, you might need to increase the timeout setting or increase the retries settings again.

Related Topics

[Community String Format, page 4-8](#)

Enter Telnet/SSH Usernames and Passwords—Access Points

Telnet or SSH (SSH1 only) usernames and passwords are required for applying configuration templates to access points and for upgrading firmware on access points. You can enter as many usernames and passwords as necessary on the WLSE. For more information about setting passwords on IOS access points, see *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.13* at

http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html.

The Telnet/SSH credentials you enter in this dialog must match the login sequence on the IOS access points. If the credentials and login sequence do not match the device, the WLSE will not be able to access the device. For more information on supported login sequences, see [Supported Telnet/SSH Login Sequences for APs, page 4-11](#).

If you are using the Deployment Wizard for setting up a wireless network using WDS, you can enter these usernames and passwords in the Wizard. For more information, see [Chapter 2, “Using the Deployment Wizard.”](#)



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Devices > Discover > Device Credentials > Telnet/SSH User/Password**.
- Step 2** Enter the credentials that match the login sequence on devices, as shown in the following table.
When adding credentials:
 - Always enter the IP address information.
 - Enter only the username and password information that matches the credentials requested by the access points that use the IP address or range of IP addresses.

Field	Description
IP address	IP address or range of IP addresses for access points using this username and password. For details on entering address ranges and using wildcards, see Entering IP Addresses, page 4-12 .
Username	Telnet/SSH username. Note The following characters are not supported and cannot be entered in this field: double quote, single quote, and angle brackets (< >).
User Password	Telnet/SSH password.
Confirm Password	
Enable User	Telnet/SSH enable username. Note The following characters are not supported and cannot be entered in this field: double quote, single quote, and angle brackets (< >).
Enable Password	Telnet/SSH enable password.
Confirm Enable Password	

Step 3 To add more entries, repeat Step 2.

Step 4 To modify an entry:

- a. Select the entry from the Current Entries text box.
- b. Modify fields as needed and click **Save**.

Step 5 To clear the current entry, click **Clear Fields**.

Step 6 To delete an entry, select it from the Current Entries text box and click **Delete**.

Supported Telnet/SSH Login Sequences for APs

The Telnet/SSH credentials you enter on the WLSE must match the login sequence on the access points.

For example:

- If the device prompts for a password but not a username, do not provide a username.
- If the device prompts for a username and password and logs you directly into enable mode without asking for an enable password, do not provide an enable password.
- If the device prompts for an enable password only, enter the enable password only. Do not enter a username or user password.

If the credentials and login sequence do not match the device, the WLSE will not be able to open a session on the device. Match the credentials and login sequence as shown in the following table.

Device Login Sequence	Telnet Credential Fields Required
Username: Password: prompt> enable Password: enable prompt #	User Name User Password Enable Password
Password: prompt> enable Password: enable prompt#	User Password Enable Password
Username: Password: enable prompt#	User Name User Password
enable prompt#	(no credentials required)
Username: prompt> enable Password: enable prompt#	User Name Enable Password
prompt> enable Password: enable prompt#	Enable Password
Username: prompt#	User Name
Username: Password: prompt> enable Username: Password: enable prompt#	User Name User Password Enable User Name Enable Password

Entering IP Addresses

IP addresses can consist of the following:

- A complete IP address; for example, 172.20.4.9.
- An IP address with * wildcards; for example:
 - *.*.*.*
 - 172.*.*.*
- An IP address with ranges [x - y], where x is less than y, and wildcards; for example:
 - 27.20.[4-55].*
 - 172.[21-30].[44-88].*
 - 172.*.*.[121-255]



Note

When two or more entries match the IP address of a device, the most specific entry will be used.

Enter HTTP/HTTPS Port Settings—Access Points

HTTP or HTTPS port settings are required for reports on access points; the port settings are used for the links from reports to the Web interfaces of access points. The port you should supply for each device is the port for accessing the access point's Web interface.

Access points with version 12.3 and later firmware use HTTPS.

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **Devices > Discover > Device Credentials > IOS HTTP/HTTPS Port Configuration**.

Step 2 To add a port:

- a. Enter the IP address or range of IP addresses that use this port number.

For information on using ranges and wildcards in IP addresses, click **Learn More**, or see [Entering IP Addresses, page 4-12](#).

- b. Select HTTP or HTTPS.
- c. Enter the port number.

**Note**

The port numbers allowed for HTTPS are 443 (the default) and port numbers above 1024.

- d. Click **Save**.

Step 3 Repeat Step 2 to add more IP addresses and ports.

Enter WLCCP Credentials for Wireless Domain Services

If you are using the WLSE to monitor Wireless Domain Services ([WDS](#)) on your network, you must enter [WLCCP](#) credentials on the WLSE for the WDS devices or an AAA server providing LEAP authentication services.

The purpose of entering the RADIUS username and password in this screen is to allow the WLSE to authenticate with the WDS device.

The WLSE authenticates to each WDS device using the same credentials.

For more information about WDS devices, see [What is WDS and Why Do I Need It?, page 11-8](#).

**Note**

WLCCP credentials are required for WDS discovery. For more information about this method of discovery, see [About WLCCP/WDS Discovery, page 4-27](#).

**Note**

The WLSE uses UDP port 2887 for WLCCP.

To enter WLCCP credentials on the WLSE:

-
- Step 1** Select **Devices > Discover > Device Credentials > WLCCP Credentials**.
- Step 2** In the Radius Username and Radius Password fields, enter the username and password for LEAP authentication that you set for the WLSE on the WDS device or the AAA server.



Note The following characters are not supported for the Radius Username and cannot be entered in this field: double quote ("), single quote ('), and angle brackets (< >).

- Step 3** In the Confirm Password field, re-enter the password that you entered in the Radius Password field.
- Step 4** To modify the WLCCP credentials, change the fields as needed.
- Step 5** To save the credentials, click **Save**.
- To clear all fields and remove the WLCCP credentials, click **Clear Fields**.
-

Monitoring AAA Servers

The options in this screen allow you to:

- Add AAA servers—See [Adding an AAA Server, page 4-16](#).
- Remove AAA servers—See [Removing an AAA Server, page 4-17](#).
- Edit AAA server entries—See [Modifying an AAA Server, page 4-17](#).

Related Topics

- [About AAA Servers, page 4-14](#)

About AAA Servers

The WLSE can monitor AAA services provided by supported AAA (authentication, authorization, accounting) servers, Cisco Aironet 1100 or 1210 access points configured as AAA servers, and the WLSE's internal AAA server. The internal server is available on the [WLSE Express](#) only. The WLSE monitoring functionality is intended primarily to monitor AAA servers for availability and response time. Therefore, monitoring multiple protocols on the same AAA server is not supported.

For information on the external AAA servers supported by the WLSE, see the *Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine, 2.13* on Cisco.com at

http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_device_support_tables_list.html.

Once an AAA server's credentials are added, the WLSE can monitor the availability, authentication, and response time for the server.

The AAA services supported by the WLSE are:

- EAP-MD5
- LEAP
- PEAP (EAP-GTC only)

- RADIUS
- EAP-FAST



Note The WLSE does not monitor EAP-FAST on the internal AAA server.

Before adding AAA servers to the WLSE, configure the servers to add the WLSE as a client. For information on adding the WLSE as a client on an ACS server, see *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.13* at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html.

There are additional prerequisites for using an EAP-FAST server; see [Prerequisites for Adding an EAP-FAST Server, page 4-15](#).

After you add AAA servers to the WLSE, the WLSE automatically performs periodic logins on each server to monitor the server's response time and availability and displays this information under **Reports > Trends**.

If authentication fails, a fault will be generated and displayed by the WLSE fault monitoring system.

If an AP 1100 or AP 1210 is registered with the WLSE as an AAA server, it cannot be managed by the WLSE as an access point that also provides wireless services. An access point can either be monitored as an AAA server *or* managed as an access point that provides wireless services.

For information about changing the polling interval and response time fault thresholds for AAA server monitoring, see [Setting AAA Server Response Time, page 3-49](#).

Prerequisites for Adding an EAP-FAST Server

Before the WLSE can monitor an EAP-FAST server, the PAC (protected access credentials) must be provisioned. Use the following procedure to issue the PAC and import it to the desktop.

Procedure

-
Step 1	On the Cisco Secure ACS server, use the csutil command to provision a PAC for each user. If more than one PAC is generated, ACS will generate a CAB file containing the PAC files. The PACs are exported one per file and have the naming format <i>username.pac</i> . For information on this command, see the documentation for Cisco Secure ACS server on Cisco.com.
Step 2	FTP the .pac files to your desktop (WLSE browser client machine).
Step 3	Configure EAP-FAST server monitoring on the WLSE by following the procedures in Adding an AAA Server, page 4-16 .
-

Adding an AAA Server

**Note**

For information about other requirements for AAA servers, see [About AAA Servers, page 4-14](#). In addition, for EAP-FAST servers, see [Prerequisites for Adding an EAP-FAST Server, page 4-15](#).

If you add an AP as an AAA server, it can no longer be managed by the WLSE as an access point providing wireless services.

You can monitor only one protocol on a given AAA server. For example, if you have added an AAA server and specified the PEAP protocol, you cannot add the same server a second time and specify the RADIUS protocol. When you try to add the server the second time, an error message is displayed.

There is no limitation on the number of AAA servers you can add.

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **Devices > Discover > AAA Server**.

Step 2 Enter the following data.

Table 4-4 AAA Server Parameters

Field	Description
Show List	Select the protocol type from the pulldown list: ¹ - EAP-MD5 - LEAP - PEAP (EAP-GTC only) - RADIUS EAP-FAST
Server Name	Hostname or IP address of the AAA server. In WLSE displays, the server is identified by this name.
Server Port	Port on the server that is used for authentication; this should always be 1645.
Username	Client username that you entered on the AAA server.
Password	Client password that you entered on the AAA server.
Secret	Shared secret key that you entered on the AAA server.
PAC File Password (EAP-FAST only)	Password for decrypting the .pac file and the filename of the .pac file to be uploaded from the desktop.
PAC Filename (EAP-FAST only)	Note If you have not created a .pac file for this EAP-FAST server, see Prerequisites for Adding an EAP-FAST Server, page 4-15 .

1. The WLSE monitors only one protocol for a given AAA server.

Step 3 Click **Save**. To discard your entries, click **Cancel**.

- Step 4** Edit the default faults profile to enable polling for the AAA protocol you selected. See [Managing Fault Settings, page 3-10](#) for procedures.
- Step 5** If authentication fails, a fault will be generated.
- For EAP-FAST, check the user credentials and make sure that the valid PAC file has been imported. If the PAC has expired or is invalid, re-import the PAC file from the desktop.
- Step 6** After a few polling cycles, you can view the trend data for the server response time in the Server Response Time Graph.
- Select **Reports > Trends**.
 - Choose the protocol type from the **Device Type > AAA Servers > protocol** folder.

**Note**

For EAP-FAST, choose EAP.

- Select the server's IP address.

Removing an AAA Server

**Note**

Your login determines whether you can use this option.

Procedure

- Select **Devices > Discover > AAA Server**.
- Select the server type from Show List
Result: All servers of that type are displayed.
- Select the server to be removed.
- Click **Remove**.

Modifying an AAA Server

The WLSE monitors only one protocol for a given AAA server.

**Note**

Your login determines whether you can use this option.

Procedure

- Select **Devices > Discover > AAA Server**.
- Select the server type from Show List.
Result: All servers of that type are displayed.

Step 3 Select the server to be modified.

Step 4 You can modify only the following characteristics of an existing AAA server entry.

Modifying the hostname or IP address of an existing AAA server entry requires removing the existing server and adding it back with the new IP address or hostname.

Characteristic to Modify	Description
Server Port	Port on the server that is used for authentication; this should always be 1645.
Username	Client username that you entered on the server.
Password	Client password that you entered on the server.
Secret	Shared secret key that you entered on the server.
PAC File Password (EAP-FAST only)	Password for decrypting the .pac file and the filename of the .pac file to be uploaded from the desktop.
PAC Filename (EAP-FAST only)	

Step 5 Click **Save**.

Step 6 To discard your entries, click **Cancel**.

Related Topics

- [Removing an AAA Server, page 4-17](#)
- [Adding an AAA Server, page 4-16](#)

Using Enhanced (WDS) Client Tracking

The WLSE can track clients of access points by querying Wireless Domain Service (WDS) for all client associations. You can use the following procedure to enable or disable this type of client tracking globally or enable it on selected WDS devices (access points or WLSM). By default, client tracking is globally disabled.

In addition to enabling client tracking, you must configure access points and the WLSE. See [Prerequisites for Enhanced Client Tracking, page 4-20](#) for more information.

For more information on client tracking and client polling, see [About WDS Client Tracking, page 4-20](#).

For information on the IOS firmware versions that support enhanced client tracking, see the *Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine, 2.13* at

http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_device_support_tables_list.html.

Configuring Enhanced Client Tracking


Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Devices > Discover > Client Tracking**. The client tracking options are displayed.

Step 2 Select an option:

- **Enable client tracking on all WDS devices**—client tracking will be enabled on all WDS access points.
- **Disable client tracking on all WDS devices**—this is the default state.
- **Enable client tracking only on selected WDS devices:**
 - A list of the configured and managed WDS devices appears. The information in the list is described in [Table 4-5](#).
 - Select the WDS devices on which you want to enable client tracking.

Table 4-5 *Client Tracking Devices*

Field	Description
Name	Name and IP address of an active WDS device that is being managed by the WLSE.
IP Address	Note Although only active WDS devices are listed, the configuration settings of an active WDS will be applied automatically to the backup WDS when the backup becomes active.
Subnet	Subnet to which the WDS is assigned.
Version	Firmware image on the WDS device.
Backup Count	Number of WDS devices (in the same subnet) that are acting as backup for this active WDS device.
Registered Node Count	Number of access points registered with this WDS device.
WNM Authentication State	Status of the authentication of the WLSE with the WDS device.
WDS Tracking Status	Current state of client tracking for the WDS device: • Enabled—the WLSE is receiving client tracking events from this WDS device. • Disabled—the WLSE is not receiving client tracking events from this WDS device.

Step 3 To reset to the previous setting, click **Reset**. To save your changes, click **Apply**.

Related Topics

- [About WDS Client Tracking, page 4-20](#)
- [About Inventories, page 4-63](#)
- [Displaying Wireless Client Reports, page 10-37](#)

About WDS Client Tracking

This section contains information about the following:

- [Prerequisites for Enhanced Client Tracking, page 4-20](#)
- [Client Tracking vs. Client Polling, page 4-21](#)
- [Wireless Client Reports, page 4-22](#)
- [Display of RADIUS Username in Wireless Client Reports, page 4-22](#)

Prerequisites for Enhanced Client Tracking

In addition to enabling client tracking on the WLSE, you must configure the following for WDS-based client tracking to work.

**Note**

You can also use the WLSE's Deployment Wizard for configuring access points and the WLSE for WDS.

- Configure the WLSE for WLCCP—See [Enter WLCCP Credentials for Wireless Domain Services, page 4-13](#).

WLCCP messages are required for the WDS to perform client tracking.

- Configure primary and (optional) backup [WDS devices](#)—See *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.13* at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html.

This feature is not available on all IOS firmware versions. All WDS access points must be upgraded to IOS firmware version 12.2(15)JA or later. For the latest information, see the WLSE 2.13 Supported Device Table at

http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_device_support_tables_list.html.

If the WDS devices have firmware earlier than 12.2(15)JA, enhanced client tracking is not available. However, client tracking via client polling is available. For more information, see [Client Polling, page 4-21](#).

- Configure [infrastructure access points](#) for WDS—See *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.13* at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html.

These access points need not necessarily be upgraded.

- (Strongly recommended) Configure Network Time Protocol (NTP) on the network.

Client tracking event reports include a WDS timestamp, which is used to display the order of events at the WDS. If all clocks are not NTP synchronized, events from different WDS devices may not be ordered correctly. You should ensure clock synchronization by configuring NTP service on the WDS

and the WLSE. The NTP server should be a network NTP server that is used by all WDS devices. For information on enabling NTP on the WLSE, see [Setting Time, Time Servers, Name Servers, and Web Session Timeout, page 16-43](#). For information on enabling NTP on WDS devices, see the device documentation.

Client Tracking vs. Client Polling

The WLSE obtains client data in two ways:

- Automatic client inventory polling—see [Client Polling, page 4-21](#).
- WDS client tracking—see [Client Tracking, page 4-21](#).

Client Polling

The WLSE automatically collects client data by polling all access points, using a configurable polling interval. Data obtained from client polling is detailed and includes traffic statistics. Polling data is only as timely as the last client polling cycle, which means that the client polling interval greatly affects the accuracy of client reports:

- In environments where clients are highly mobile, such as health care and retail deployments, you should set the client polling interval to the minimum if the network can tolerate the polling traffic.
- In enterprise deployments, most WLAN users have laptops and tend to be stationary for long periods of time, so client polling should be less frequent.

Wireless client polling is a fairly heavyweight process. If you have many access points to poll for client associations, polling should be less frequent. As a result, the client data will not be as accurate. Wireless client reports are updated every 51 minutes by default. To reset the client polling interval, see [Changing the Polling Intervals for Automatic Inventories, page 4-64](#).



Note

You can also obtain detailed client information by running on-demand or scheduled inventories on one or more specific access points. See [Running Immediate Inventories, page 4-65](#).

Client Tracking

With client tracking, the WLSE obtains client data from WDS devices, instead of from all of the individual infrastructure access points. Client tracking provides only historical information.

Any clients that have associated with a managed access point are reported and tracked either by a corresponding managed, active WDS device which is serving the same subnet as the managed access point or a WLSM (Wireless LAN Services Module). WLSM-WDS devices can manage multiple access point subnets.

WDS devices send notifications to the WLSE when certain events occur about any client associated with access points that are registered with that WDS. Each WDS maintains an updated active cache of all clients that are associated with each registered access point within the WDS domain. These events are recorded by the WLSE and can be viewed from the Client Historical Association Report and Client Access Failure Report. These events also keep the current client association information up to date. For performance reasons, there is approximately a 2-minute delay between when the event occurs and when the event is available in reports. The reported events are:

- Refresh—Occurs when the WLSE synchronizes with the WDS. This happens when the WLSE reboots and when the WDS-to-WLSE management link is established or restored. During this phase, the WLSE learns about all of the registered clients within a specific WDS domain.

- Registration with WDS—When a client successfully registers with the WDS for the very first time.
- Detachment from WDS—When the WDS cleans up the internal cache of a stale client or the associated access point indicates to the WDS that a client has become inactive.
- Roam—When a client roams to another access point within the same WDS domain.
- Access failure—When a client fails to access an access point during EAP authentication.

Even when client tracking is enabled, the wireless client polling described in [Client Polling, page 4-21](#) is still required to obtain other information about client activity, such as client as client traffic statistics.

If you have a high volume of client roaming or client activity, enabling client tracking will add extra overhead and WLSE performance may be affected. However, client tracking events are optimized to consume very little network traffic and WLSE processing resources.

Although client polling occurs automatically, client tracking must be enabled on [WDS devices](#) by selecting **Devices > Discover > Client Tracking**. To enable client tracking and view the current state of client tracking, see [Using Enhanced \(WDS\) Client Tracking, page 4-18](#).

Wireless Client Reports

Wireless client reports provide information about the type of client that is associating with an access point, how much bandwidth the client is using, which access points the client has associated with, and the kind of client activity.

For information on displaying wireless client reports, see [Displaying Wireless Client Reports, page 10-37](#).

Display of RADIUS Username in Wireless Client Reports

The client RADIUS username is not available for:

- Non-EAP authentication.
- PEAP and EAP-TLS authentication if certain RADIUS servers are used. [Table 4-6 on page 4-22](#) lists username support for various authentication types and AAA servers.

Table 4-6 *RADIUS Username in Client Tracking Reports*

Authentication Type	RADIUS Server	RADIUS Username Supported?	Configuration Required on RADIUS Server?
non-EAP	Not applicable	No	Not applicable
EAP EAP-MD5 EAP-TLS EAP-SIM	Any server that supports the authentication type	Yes	No
Cisco PEAP Microsoft PEAP EAP-FAST	Cisco ACS server	Yes	No

Table 4-6 *RADIUS Username in Client Tracking Reports*

Authentication Type	RADIUS Server	RADIUS Username Supported?	Configuration Required on RADIUS Server?
Cisco PEAP Microsoft PEAP EAP-FAST	Other RADIUS servers that support Cisco PEAP	Unknown	Unknown
EAP-TTLS	Any RADIUS server that supports EAP-TTLS	Unknown	Unknown

Managing Device Discovery



Note

If you are using the WLSE Deployment Wizard to deploy access points used within a Cisco [SWAN](#) framework, you can use the Wizard to discover these devices instead of using the discovery methods described in this section. For information on the Deployment Wizard, see [Chapter 2, “Using the Deployment Wizard.”](#)

By default, the WLSE runs Cisco Discovery Protocol (CDP) discovery every 24 hours. After devices are discovered, they must be put under management—see [Managing Devices, page 4-54](#). Unmanaged devices do not appear in WLSE displays.

The functions under the Discover subtab are described in [Table 4-7 on page 4-23](#).

To learn more about discovery, see [About Discovery, page 4-24](#).

Table 4-7 *Discovery Options*

Option	Description	Reference
Discovery Wizard	Run additional CDP discoveries and modify the default schedule.	Running CDP Discovery, page 4-34
	Discover devices by importing them from a file or from a CiscoWorks server.	Importing Devices from a File, page 4-38 Importing Devices from a CiscoWorks Server, page 4-39
Advanced Options	Set advanced options that modify the behavior of discovery and device management and allow you to specify how devices are identified in displays.	Setting Advanced Discovery Options, page 4-41
IP Filter Rules	Set up IP address filtering for discovery	Using Discovery IP Address Filtering, page 4-47
Logs	View discovery job details	Viewing Discovery Logs, page 4-48

About Discovery

The topics covered in this section are:

- [Understanding Discovery and Management, page 4-24](#)
- [Understanding WLSE Discovery Methods, page 4-25](#)
- [About CDP-Based Discovery, page 4-26](#)
- [About WLCCP/WDS Discovery, page 4-27](#)
- [About Individual Device Seeding, page 4-28](#)
- [About Device Import From a File, page 4-29](#)
- [About Device Import From CiscoWorks, page 4-31](#)
- [About CSV Files, page 4-30](#)

Understanding Discovery and Management

Network devices are interrogated by the WLSE by using discovery and inventory polling.

Device discovery is a periodic process that finds new devices and, possibly, topology and network changes. The discovery process can be run at scheduled intervals or on demand.

The WLSE can discover Cisco wireless access points and bridges, and Cisco switches or routers that have Cisco wireless devices directly connected to them.

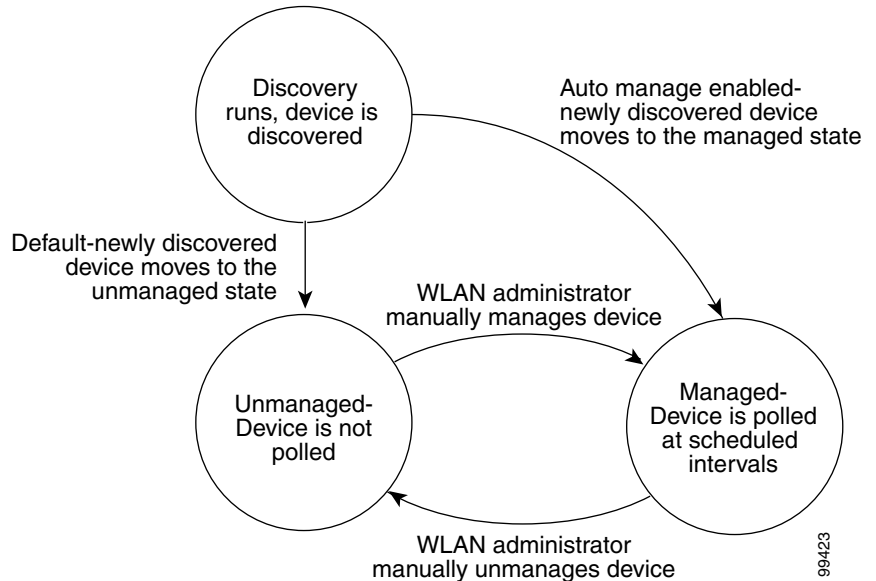
Discovered devices are either managed and unmanaged. By default, newly-discovered devices are in the unmanaged state and will not be polled until you manually move them to the managed state.

You can enable an auto-manage feature that automatically moves newly discovered devices to the managed state when they are discovered. You can also apply a default device configuration to auto-managed wireless devices. [Figure 4-1](#) illustrates the managed/unmanaged state machine.

Assuming the discovery process is successful, the WLSE discovery footprint is approximately 2500 bytes per device per discovery cycle. *This is just the discovery footprint.* The 2500 bytes represent a single SNMP get-request and a single SNMP get-response. This footprint may be larger if the SNMP get-response needs to be broken up across multiple protocol data units (PDU), which often happens if the device receiving the SNMP get-request has a large CDP neighbor table.

After a device is discovered for the first time and the device is auto-managed, an immediate inventory will run. However, inventory is not run automatically when discovery is run on a device that was already discovered (even if the device is automanaged). You can run an immediate inventory to update device information on the WLSE or wait for the next regular scheduled inventory.

You can view information about discovery jobs in the discovery logs (see [Viewing Discovery Logs, page 4-48](#)) and in the jobvm log. To view or download the jobvm log, select **Admin > Appliance > Status > View Log File** and select the jobvm.log file.

Figure 4-1 Device Management State Machine

Understanding WLSE Discovery Methods

Before the WLSE can manage devices, it must discover them. There are several discovery techniques:

- CDP-based discovery—See [About CDP-Based Discovery, page 4-26](#).
- WLCCP/WDS discovery—See [About WLCCP/WDS Discovery, page 4-27](#).
- Individual device seeding—See [About Individual Device Seeding, page 4-28](#).
- Device import from a file—See [About Device Import From a File, page 4-29](#).
- Device import from CiscoWorks Resource Manager Essentials (RME)—See [About Device Import From CiscoWorks, page 4-31](#).

Use the following table to help you decide which technique to use:



Note AAA servers must be entered individually regardless of discovery method. See [About AAA Servers, page 4-14](#).

Table 4-8 Discovery Options

Discovery Method	Use This Method When...
CDP-based discovery	Use this method when wireless devices are attached to Cisco switches or routers running Cisco discovery protocol. For more information, see About CDP-Based Discovery, page 4-26 .

Table 4-8 *Discovery Options (continued)*

Discovery Method	Use This Method When...
Individual device seeding	If the wireless devices are connected to switches or routers that don't run CDP (for example, non-Cisco switches), this is one option. Note You must enter an IP address for each managed device. For more information, see About Individual Device Seeding, page 4-28.
Device import from a file	If the wireless devices are connected to switches or routers that don't run CDP (for example, non-Cisco switches), this is an option. This technique adds an entry for each device for SNMP credentials. Note Using this method, you might need to create a large CSV file listing each device. For more information, see About Device Import From a File, page 4-29.
Device import from CiscoWorks Resource Manager Essentials (RME)	Use this technique if you have already inventoried the wireless devices using RME. This technique adds an entry for each device for SNMP credentials. For more information, see About Device Import From CiscoWorks, page 4-31.

About CDP-Based Discovery

When the WLSE runs a CDP-based discovery, it begins by using SNMP to retrieve the list of devices in the [CDP](#) neighbor table of each [seed](#) device. It then retrieves the devices in the CDP neighbor tables from each of the CDP neighbors of the seeds. This process continues until all devices in the network are discovered for the [CDP distance](#) is reached.



Note Only Cisco wireless devices and Cisco switches or routers attached to properly configured access points are recognized by the discovery process.

The CDP distance determines the depth of the discovery. With a CDP distance of 1, only the immediate neighbors of the seed device are discovered. With a CDP distance of 2, devices A and B that are directly connected to the seed device are discovered, and the immediate neighbors of A and B are also discovered.

You can specify multiple seed devices to:

- Shorten the discovery time.
- Discover “disconnected” networks; that is, discover devices across links on which CDP is disabled or discover devices outside the firewall.

**Note**

Supported access points, bridges, routers, and switches are all valid seed devices. PCs and workstations are not valid seed devices.

Interesting devices from the perspective of the WLSE are:

- Cisco wireless bridges and access points
- Cisco routers or switches that are CDP neighbors of a Cisco wireless device and, for Cisco switches, that also contain a WLSM module
- WLSM devices

**Note**

If CDP can discover the Cat6K switch, then the WLSM devices attached to that switch are automatically discovered.

Because the WLSE keeps only interesting devices, try to select seed devices in a way that minimizes unnecessary WLSE discovery traffic on the network by selecting devices so that the discovery process will only touch interesting devices. This is usually not possible, but by selecting seeds wisely, a minimum number of uninteresting devices will be touched by the discovery process.

CDP-based discovery can be run on-demand, at a scheduled time, or at recurring intervals. Typically, you only need to run discovery when you initially deploy the WLSE and when you deploy new wireless devices.

By default, CDP discovery is enabled and runs every 24 hours. The discovery wizard allows you to run additional immediate CDP discoveries and change the default CDP schedule. See [Using the Discovery Wizard, page 4-33](#).

Devices must be properly configured for access by the WLSE before they can be discovered and managed. See *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.13* at

http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html.

If CDP is disabled, you can still discover devices by entering their IP addresses as seed values in the discovery dialogs or by importing them. However, the connectivity between access points and switches will not be discovered and switch-related reports will be empty. For more information, see [About Individual Device Seeding, page 4-28](#).

About WLCCP/WDS Discovery

**Note**

You can also use the Deployment Wizard to deploy access points in a WDS environment. See [Chapter 2, “Using the Deployment Wizard.”](#)

If you use WDS, all of the IOS access points in a subnet register with the WDS, and WDS sends this data to the WLSE via **WLCCP**. The WLSE checks whether these devices are in the WLSE database. If not, a regular CDP discovery is run, using each device as a seed. So, new devices that register with the WDS will be automatically discovered.

These WDS discoveries do not appear in the discovery log. WDS discoveries are affected by any discovery filters that you have set. See [Setting Advanced Discovery Options, page 4-41](#) and [Using Discovery IP Address Filtering, page 4-47](#).

For WLCCP discovery to work:

- WDS devices and infrastructure APs must be configured for network management and radio management—See *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine*, 2.13 at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html.

**Note**

If the WDS device is configured with the WLSE's address, the WLSE will auto discover the device without waiting for the next scheduled discovery job to run.

- The WDS devices must be in the managed state.

About Alternatives to CDP

Instead of enabling CDP and using it for discovery, you can use the following methods of discovering devices:

- [About Individual Device Seeding, page 4-28](#)
- [About Device Import From a File, page 4-29](#)
- [About Device Import From CiscoWorks, page 4-31](#)

About Individual Device Seeding

Although CDP-based discovery is usually the preferred option, in some network environments a CDP-based discovery is undesirable or impossible. For example, the wired network infrastructure may have non-Cisco switches or hubs that do not support CDP, or IT security policies may prohibit the use of CDP in the network.

As an alternative to using Cisco Discovery Protocol (CDP) to run discovery, you can seed each device IP into the WLSE. The WLSE setup process is similar to the regular CDP-based discovery, and is treated as such by the WLSE discovery process. Rather than using a few, well-chosen seed devices:

1. Enter each device to be managed as a seed device prior to running discovery.
2. Set the [CDP distance](#) to 1.
3. Use either the on-demand discovery option or the scheduled discovery option from **Devices > Discover > DISCOVER**.

**Note**

This technique will not discover switches or routers attached to wireless devices unless the wireless devices and switches and/or routers are CDP-enabled. Because the WLSE cannot establish a neighbor relationship between switches or routers and the wireless devices if the switches or routers are not CDP-enabled, they will not be included as manageable by the WLSE.

**Note**

Because this technique requires that you enter each device as a seed, it may add significant overhead to the WLSE discovery setup time.

About Device Import From a File

When a CDP-based discovery is undesirable or impossible, importing a list of devices from a file is another option in many environments. For example, the wired network infrastructure may have non-Cisco switches or hubs that do not support CDP or IT security policies may prohibit the use of CDP in the network.

Using an import file in comma separated variable (CSV) format is an alternative to individual device seeding. Because the import file may be obtained from another network inventory management application, this technique may be more practical than individual device seeding.

Use the option **Devices > Discover > DISCOVER > Import From File** to import devices from a CSV file. You can choose to discover some devices and import others, however devices not supported by the WLSE are ignored during device import.

A one-time discovery job starts immediately after you import devices from a CSV file. This means the following discovery options affect device import:

- Advanced Options—See [Setting Advanced Discovery Options, page 4-41](#).
- IP Filter Rules—See [Using Discovery IP Address Filtering, page 4-47](#).

When you import the devices from a CSV file, the WLSE:

1. Treats each entry as a seed device and uses a [CDP distance](#) of 1.
2. Attempts to retrieve the CDP neighbor table of each entry, discarding any devices in the CSV file that are not interesting. Interesting devices from the perspective of the WLSE are:
 - Cisco wireless bridges and access points
 - Cisco routers or switches that are CDP neighbors of a Cisco wireless device and, for Cisco switches, that also contain a WLSM module
 - WLSM devices

If CDP is not enabled on the wireless devices or if there are no CDP neighbors, then the WLSE will only discover the wireless devices and the WLSE cannot be used to manage the neighboring switch or router.



Note Because the WLSE will attempt to determine the device type and CDP neighbors of each device imported from the CSV file, a large number of uninteresting (to the WLSE) devices may add significant time to the discovery process and add unnecessary traffic to the network. To minimize discovery time, you should edit the CSV file to contain only devices of interest.

3. Adds a row in the SNMP device credentials fields (see [Enter SNMP Communities, page 4-36](#)) for each device during the import process. The WLSE will do this even if there are already entries that qualify for the devices configured.

You can choose to delete the specific entries and leave only the general entries. This is not a required step because the WLSE will choose the most specific entry when looking up SNMP credentials for a device, but it is recommended because it will make managing device credentials easier.

4. Imports the following information:
 - IP addresses are accepted as is, and hostnames are resolved to obtain the IP address. Hostnames that cannot be resolved are ignored.
 - Read-only and read/write community strings are inserted into the SNMP Communities table (**Devices > Discover > Device Credentials**).

The community strings that you import will overwrite the information already entered on the WLSE. You can view the information already entered in **Devices > Discover > Device Credentials > SNMP Communities**. Community strings that contain wildcards will not be overwritten unless these entries are exactly matched by entries in the CSV file.

- SNMP timeout and retry settings are not imported but you can specify values, while setting up the discovery job.

The timeouts and retries that you enter will overwrite information already entered on the WLSE.

During the subsequent discovery:

- All WLSE-supported devices in the file are used as seed devices with a [CDP distance](#) of 1. These devices are listed in the Discovery Run Log.
- In the discovery logs (see [Viewing Discovery Logs, page 4-48](#)), the name of the import from file is shown as CDPDiscovery_Import_Devices.

About CSV Files

The file used for imports is an ASCII [CSV](#) (comma-separated values) file with a .txt filename suffix. You can create a CSV file by exporting devices from CiscoWorks or by creating the file with a text editor. You can view a sample CSV file from the Discovery Wizard screens for file import, or see the following example.

A CSV file can contain the following device information:



Note

Only the device name or IP address and the community strings are used by the WLSE.

- Full device name or IP address (required). Include the domain in the device name unless your site has unqualified device names registered in the name service.
- Read-only community string (required).
- Read-write community string (optional).
- Serial number (optional).
- User Fields 1, 2, 3, and 4 (optional).
- Telnet password, enable password, enable secret, TACACS user, TACACS password, TACACS enable user, TACACS enable password, local user, local password, and RCP (remote copy protocol) user.
- RCP password (not used).

An example file follows.

```
;
; The possible columns in the CSV file are listed below.
;
; For importing to WLSE, columns 1,2,3 are required and the
; rest are optional.
;
; Col# = 1: Name = Device name (include domain unless your site
;                has unqualified device names registered in
;                the name services)
;                - or -
;                IP Address in dotted decimal notation
;
; Col# = 2: Name = RO community string
; Col# = 3: Name = RW community string
; Col# = 4: Name = Serial Number
```

```

; Col# = 5: Name = User Field 1
; Col# = 6: Name = User Field 2
; Col# = 7: Name = User Field 3
; Col# = 8: Name = User Field 4
; Col# = 9: Name = Telnet password
; Col# = 10: Name = Enable password
; Col# = 11: Name = Enable secret
; Col# = 12: Name = Tacacs user
; Col# = 13: Name = Tacacs password
; Col# = 14: Name = Tacacs enable user
; Col# = 15: Name = Tacacs enable password
; Col# = 16: Name = Local user
; Col# = 17: Name = Local password
; Col# = 18: Name = Rcp user
; Col# = 19: Name = Rcp password; Comment = Not used, leave blank
;
; Here are examples of rows of data:
;
1.2.3.4,public,public,,
1.2.2.5,public,public,,,,,telnetpwd
bigrouter.yourcompany.com,public,private,,,,,telnetpwd
dev-2501.yourcompany.com,"Not so, " " public as, thought",private,sn2501,
dev-2502.yourcompany.com,public,"private",sn2502,
dev-2503.yourcompany.com,public,private,sn2503,""
dev-2510.yourcompany.com,public,private,sn2510,
dev-4000.yourcompany.com,public,private,,Big Boys
dev-2517.yourcompany.com,public,private,,nm 25xx
dev-2520.yourcompany.com,public,private,,mylabel2
dev-4700.yourcompany.com,public,private,,yourlabel1,,yourlabel3,yourlabel4
dev-7206.yourcompany.com,public,private,,
dev-7505.yourcompany.com,public,private,,,,yourlabel4

```

About Device Import From CiscoWorks

If you are using CiscoWorks Resource Manager Essentials (RME) to manage your wireless devices, you can import the devices from RME to the WLSE without configuring, scheduling, or running WLSE discovery. This process is analogous to using a CSV file to import a list of devices. Use the option **Devices > Discover > DISCOVER > Discovery Wizard > Import From CiscoWorks** to import devices from RME.

Immediately after a successful import, the WLSE runs discovery on all of the imported devices. Therefore, the following discovery options affect device import:

- Advanced Options—See [Setting Advanced Discovery Options, page 4-41](#).
- IP Filter Rules—See [Using Discovery IP Address Filtering, page 4-47](#).

You can specify an immediate import, schedule an import for a future time, or schedule recurring imports. The time required to import devices depends on the response from the CiscoWorks server and the number of devices imported. You can check the status of the operation while it is running.

When you import the devices from CiscoWorks, the WLSE:

1. Interrogates the RME server for its device list and credentials, and then treats each device retrieved from RME as a seed device.
2. Attempts to determine the CDP neighbors of each device, discarding devices from RME that are not interesting. Interesting devices from the perspective of the WLSE are:
 - Cisco wireless bridges and access points
 - Cisco routers or switches that are CDP neighbors of a Cisco wireless device.

**Note**

Because the WLSE will attempt to determine the device type and CDP neighbors of each device imported from RME, a large number of uninteresting (to the WLSE) devices may add significant time to the discovery process and add unnecessary traffic to the network.

If CDP is not enabled on the wireless devices or if there are no CDP neighbors, the WLSE will only discover the wireless devices.

3. Adds a row in the SNMP device credentials fields for each device during the import from RME process. This process may result in duplicate entries for SNMP credentials.

You can choose to delete the specific entries and leave the general entries. This is not a required step because the WLSE will choose the most specific entry when looking up SNMP credentials for a device, but it is recommended because it will make managing device credentials easier.

**Note**

Only the device's hostname or IP address and the read and write community strings are imported from a CiscoWorks server. The SNMP timeout and retry settings are not imported (the WLSE default settings are used).

4. During the subsequent discovery, two items are listed in the discovery log for each import from CiscoWorks:
 - Cisco Works Device Import—Click this item to display a run log that shows the information imported for each device found on the CiscoWorks server. The WLSE uses only the hostname or IP address and the community strings.
 - CDPDiscovery_Import_Devices—Click this item to display a run log that shows the results of the discovery that was run by using the information imported from the CiscoWorks server.

The WLSE provides scheduled, automated inventory imports from RME. Many customers prefer keeping a master Cisco device inventory on the RME server. Using the scheduled, automated inventory import allows customers to keep their WLSE device list in sync with the master list.

Most networks have a fairly static inventory. That is, new devices are typically added in planned roll-outs. So there really is no need to have the recurring RME import interval set very frequently. In most cases, once a week is more than frequent enough.

Using the WLSE Discovery Methods

Discovery of devices is a prerequisite to managing and monitoring them. You can discover devices by:

- Enabling CDP on the devices and running a discovery—See [Running CDP Discovery](#), page 4-34.
- Entering all the devices as seeds in the discovery wizard—See [Running CDP Discovery](#), page 4-34.
- Importing devices from a file—See [Importing Devices from a File](#), page 4-38.
- Importing devices from CiscoWorks RME—See [Importing Devices from a CiscoWorks Server](#), page 4-39.

Pre-Discovery Checklist

The following checklist will help you confirm that the prerequisites for successful discovery have been met.

This list is only the requirements for successful device discovery. To use other WLSE features, other configuration requirements exist.

For details on setting up devices for discovery and for other configuration requirements, see *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.13* at

http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html.

For information on using the Wizard for setting up devices, see [Chapter 2, “Using the Deployment Wizard.”](#)

Prerequisites for discovery:

- CDP enabled on network devices (for CDP-based discovery).
- SNMP communities configured on network devices.
 - Read-only SNMP community strings configured on switches and routers.
 - Read-only SNMP community strings configured for IOS-based wireless access points.
- SNMP community strings entered into WLSE device credentials fields.
- WLSE configured as network access server (NAS) for CiscoSecure Access Control Server (ACS) (for AAA server monitoring) or equivalent in other AAA servers.

Related Topics

[Managing Device Discovery, page 4-23](#)

About the Discovery Wizard

From **Devices > Discover > DISCOVER > Discovery Wizard**, you can use all of the discovery methods. To start using the wizard, see [Using the Discovery Wizard, page 4-33](#). The discovery methods are:

- [Running CDP Discovery, page 4-34](#)
- [Importing Devices from a File, page 4-38](#)
- [Importing Devices from a CiscoWorks Server, page 4-39](#).

Using the Discovery Wizard

The discovery wizard provides the following choices for discovering devices.



Note

Your login determines whether you can use this option.

Procedure

**Note**

Before devices can be discovered, they must be properly configured. For more information, see [Pre-Discovery Checklist, page 4-33](#).

Step 1 Select **Devices > Discover > Discover > Discovery Wizard**.

Step 2 Select the type of discovery you want to run:

Option	Description	Reference
Automatic Device Discovery based on Cisco Discovery Protocol	Run immediate or scheduled discovery by using Cisco Discovery Protocol (CDP).	About Discovery, page 4-24
Import from File	Import devices from a file.	
Import from CiscoWorks	Import devices from a CiscoWorks server (using Resource Manager Essentials), on an immediate or scheduled basis.	

Step 3 (Optional) To use discovery advanced options, click **Advanced Options**.

You can use advanced options to:

- Customize the device name format.
- Use reverse DNS lookup.
- Auto manage the discovered devices and use automanagement filtering for access points. For more information on these options, see [Setting Advanced Discovery Options, page 4-41](#).

Step 4 (Optional) To set up discovery filtering by IP address, click **IP Filter Rules**.

Filtering by IP address limits the range of discovery. For more information, see [Using Discovery IP Address Filtering, page 4-47](#).

Step 5 Click **Next**.

**Note**

In the following screens, you can click **Back** to modify a previous screen or **Cancel** to cancel the discovery or import.

Running CDP Discovery

This section provides procedures for using the Discovery Wizard screens for CDP discovery. To get started, select **Devices > Discover > DISCOVER > Discovery Wizard > Automatic Device Discovery based on Cisco Discovery Protocol**.

**Note**

Your login determines whether you can use this option.

The tasks for running CDP discovery are described in [Table 4-9 on page 4-35](#).

Table 4-9 *Tasks for CDP Discovery*

Type Discovery	Task	Reference
Run Now	Select Run Now.	Select the Type of CDP Discovery, page 4-35
	Specify SNMP communities.	Enter SNMP Communities, page 4-36
	Specify initiating IP addresses (seeds).	Enter Initiating IP Addresses (Seeds), page 4-36
	Verify your settings and finish.	Verify Your Settings and Finish—Run Now, page 4-37
	View discovery run details.	
Modify Schedule	Select Modify Schedule	Select the Type of CDP Discovery, page 4-35
	Modify the schedule	Specify the Schedule, page 4-35
	Specify SNMP communities	Enter SNMP Communities, page 4-36
	Specify initiating IP addresses (seeds)	Enter Initiating IP Addresses (Seeds), page 4-36
	Verify your settings and finish	Verify Your Settings and Finish—Modify Schedule, page 4-37
	View discovery run details	

Select the Type of CDP Discovery

The Select Type of CDP Discovery screen provides choices for running CDP Discovery.



Note

By default, discovery runs once every 24 hours.

Procedure

- Step 1** Choose an option:
- To run a one-time discovery now, select **Run Now**.
 - To modify the default discovery schedule, select **Modify Periodic**.
- Step 2** Click **Next** to continue.

Related Topics

[About CDP-Based Discovery, page 4-26](#)

Specify the Schedule

In this screen, you can modify the discovery schedule.

Procedure

- Step 1** Select the Start Date and Start Time from the pulldown lists.

*Do not schedule a discovery to begin within 5 minutes of the current time. Otherwise, the first discovery might not run. Use the **Run Now** option instead.*

- Step 2** To repeat discovery at specified intervals, click **Enable**. Then enter a number in the Every text box and select the interval from the list.
- Step 3** Click **Next**.
-

Enter SNMP Communities

The community strings for all devices to be discovered by using CDP must be entered on the WLSE.

Procedure

- Step 1** If you have not yet entered community strings for the devices in this discovery job or you need to change the community strings, you can do it now.
- Step 2** There are two methods for entering community strings:
- Enter community strings directly in the large text box.
 - Use the individual text boxes and click **Add** after entering the data for each string.



Note The large text box lists all SNMP credentials that have been entered on the WLSE.

- Step 3** For guidelines on community string syntax, click **Learn more about community string guidelines**.
- Step 4** Click **Next**.
-

Related Topics

[Recommendations For Configuring SNMP Credentials, page 4-8](#)

Enter Initiating IP Addresses (Seeds)

You must enter at least one initiating IP address (seed device).

Procedure

- Step 1** Add seed devices by entering their comma-separated IP addresses in the Add Values text box and click >>.



Note Seed devices entered during **Run Now** are not retained after the discovery. Seed devices added during **Modify Schedule** are retained and you can use them for subsequent discoveries.

- Step 2** Set the [CDP distance](#) by selecting a number from the list.
- Set this value appropriately to discover the entire wireless network or the set of devices you are discovering. A CDP distance of 1 only discovers the immediate neighbors of the seed devices.

Routers and switches that do not have access points attached to them are used when computing CDP distance. However, these routers and switches will not be discovered.

Step 3 Click **Next**.



Note

To verify SNMP connectivity using the credentials you enter, use the SNMP Reachable Tool under **Admin > Appliance > Connectivity Tools > Network Tools**.

Related Topics

[About CDP-Based Discovery, page 4-26](#)

Verify Your Settings and Finish—Run Now

Procedure

Step 1 Enter a job name, if desired. For guidelines on naming jobs, see [Appendix B, “Naming Guidelines.”](#)



Note

Job names must be unique. Do not use the same job name for discovery jobs and other jobs (such as firmware or configuration jobs).

Step 2 Verify that your settings are correct.

Step 3 If settings are not correct, click **Back** to make changes.

Step 4 When settings are correct, click **Finish**.

Discovery will begin immediately and the Discovery Run Details screen will appear, showing the details of the discovery job.

For more information about Discovery Run Details, see [Viewing Discovery Logs, page 4-48](#).

Related Topics

[Viewing Discovery Logs, page 4-48](#)

Verify Your Settings and Finish—Modify Schedule

Procedure

Step 1 Verify that your settings are correct.

Step 2 If not, click **Back** to make changes.

Step 3 When settings are correct, click **Finish**.

Discovery will begin at the Start Time you selected.

**Note**

If a warning message appears saying that WLSE server is ahead of or behind your local time, see [Understanding Time Discrepancy Problems in Job Scheduling, page 1-11](#).

Related Topics

[Viewing Discovery Logs, page 4-48](#)

Importing Devices from a File

This section gives procedures for using the Discovery Wizard screens for importing devices from a file. To get started, select **Devices > Discover > DISCOVER > Discovery Wizard > Import From File**.

**Note**

Your login determines whether you can use this option.

The tasks for importing devices from a file are:

Table 4-10 *Tasks for Import from File*

Task	Reference
Specify the file and set the SNMP retry and timeout (optional).	Select the File and Set SNMP Parameters, page 4-38
Verify your settings and finish.	Finish the Import, page 4-39
View import details.	

Select the File and Set SNMP Parameters

To import devices from a file, you can create the file by using a text editor or by exporting devices from a CiscoWorks server that is running Resource Manager Essentials.

For information about CSV files, see [About CSV Files, page 4-30](#).

Procedure

-
- Step 1** To see a sample CSV device file, click **See Sample CSV File**.
- Step 2** Enter a pathname for the file in the Select File dialog box or click **Browse** to find the file on the desktop or another network system.
- Step 3** The read and write community strings for the imported devices will be imported and will overwrite existing community strings. Existing entries that use wildcards will not be overwritten unless they are exactly matched by entries in the CSV file.
- To see or edit the existing community strings on the WLSE, select **Devices > Discover > Credentials > SNMP Communities**.

- Step 4** The timeout and retry settings in a CSV file are not imported. If you do not specify timeout and retries, the default settings (10 seconds and 1 retry) will be assigned to the imported devices. The timeouts and retries you enter here will overwrite any timeouts and retries already entered for existing community strings. To specify the timeout and retries for the imported devices:
- Enter the number of seconds in the SNMP Timeouts text box.
 - Enter the number of retries in the SNMP Retries text box.
- Step 5** To view the status of the last import, if any, click **Check Last Status**. Details on the latest import are shown.
- Step 6** To import devices from the file you selected, click **Next**. The file will be imported and a one-time discovery will begin immediately.
-

Finish the Import

Procedure

- Step 1** This screen shows the devices that will be imported.
- Step 2** To view the status of this import, click **Check Last Status**.
- Step 3** Click **Finish**. The Import from File Status screen will appear, showing the job details.
-

Related Topics

[Viewing Discovery Logs, page 4-48](#)

Importing Devices from a CiscoWorks Server

This section provides procedures for using the Discovery Wizard screens for importing devices from CiscoWorks server that is running Resource Manager Essentials.

To get started, select **Devices > Discover > DISCOVER > Discovery Wizard > Import from CiscoWorks**.



Note

Your login determines whether you can use this option.

The tasks for importing devices from CiscoWorks are:

Table 4-11 *Tasks for Import from CiscoWorks*

Task	Description
Specify the CiscoWorks server.	Schedule the Import and Finish, page 4-40
Schedule the import.	
View import details.	

Schedule the Import and Finish

This screen allows you specify a CiscoWorks server as the source of the devices to be imported. You can run a one-time import or schedule imports.

Procedure

- Step 1** Enter the following information. All fields are required; if any fields are left blank, the display will clear when you try to save your settings.

Field	Description
Host	CiscoWorks server IP address. Note The following characters are unsupported and cannot be entered in this field: double quote, single quote, and angle brackets (< >).
Port	Port number on which the CiscoWorks server listens for HTTP requests. You may need to contact the administrator of the CiscoWorks server to obtain this information.
User	Username and password of any user who has the authority to export and import device credentials on the CiscoWorks server. Note The following characters are unsupported and cannot be entered in the User field: double quote, single quote, and angle brackets (< >).
Password	
Confirm Password	

- Step 2** To run a one-time import:

- Select **Run Now**.
- Click **Finish**. The import will begin immediately.

- Step 3** To schedule a one-time import or repeated imports:

- Select the start date from the Start Date pulldown lists.
- Enter the start time from the Start Time pulldown lists.
- To schedule repeated imports, click **Enable Repeat** and set the interval by entering a number after Every and selecting Minutes, Hours, Days, Weeks, or Months from the pulldown list.
- Click **Finish**. A one-time import will begin immediately.



Note If a warning message appears saying that WLSE server is ahead of or behind your local time, see [Understanding Time Discrepancy Problems in Job Scheduling, page 1-11](#).

- Step 4** To view the status of the last import from CiscoWorks, click **Check Last Status**. Details on the latest import are shown. Click **Refresh** to update the display. You might see the error messages listed in [Table 4-12 on page 4-41](#).

Table 4-12 **Device Import Status Messages**

Message	Meaning
Error: Could not connect to CiscoWorks server: <i>ip_address</i> on port: <i>port_number</i> .	Either the host or the port specified in the WLSE import dialog was wrong.
Error: Connected to CiscoWorks server: <i>ip_address</i> on port: <i>port_number</i> successfully, but server returned error after connection.	Either the user or password specified in the WLSE import dialog was wrong.

Related Topics

- [Viewing Discovery Logs, page 4-48](#)
- [About Device Import From CiscoWorks, page 4-31](#)

Setting Advanced Discovery Options

This option provides the following customizations for discovery and device management:

- Select the name format for the device identifier in WLSE displays—See [Selecting the Device Name Format, page 4-41](#).
- Enable or disable reverse DNS lookup—See [Enabling Reverse DNS Lookup, page 4-44](#).
- Specify automatic management of newly discovered devices—See [Enable Auto-Management, page 4-45](#).
- Specify filtering for time-limited access point management—See [Enable MAC Address Auto-Manage Filtering for Access Points, page 4-45](#).

**Note**

Your login determines whether you can use these options.

Selecting the Device Name Format

The Name Format option lets you define the format of the device name shown in WLSE displays. You can choose from the following formats and you can specify a combination of more than one format:

- DNS name
- Hostname
- IP address
- Description of your choice

If you chose this option, you must enter a description for each device in the Device Details screen under **Devices > Discover > Managed Devices**.

- Ethernet MAC address (APs only)
- Radio interface MAC address (APs only)

Your choice of name format affects the display of all devices, except for AAA servers. For AAA servers, the device name displayed is always the name you specify when adding the AAA server as a device to be monitored by the WLSE.

The name format(s) that you choose are used to make up a device identifier string. This string is computed for each device and shown in all WLSE displays.

The fact that long names will be truncated in some WLSE displays may influence your choice of device identifier string. For example, in device trees, only 30 characters are shown. If you choose the hostname plus IP address as the string and you are using the fully qualified domain name as the hostname, it may be difficult to distinguish between different devices in the tree if the hostname is the first part of the string. As a workaround, you could construct the string so that the IP address is first.

You can search for devices by specifying the device description.

Procedure

To change the device identifier used for managed devices:

-
- Step 1** Select **Devices > Discover > DISCOVER > Advanced Options**.
 - Step 2** To view information about the name formats, click **Learn About Name Format**.
 - Step 3** To specify the device identifier format, compose a string from the list of variables in [Table 4-13 on page 4-42](#), and enter the string in the Name Format field. For examples and rules, see [Examples and Rules for the Name Format Option, page 4-43](#).
 - Step 4** Click **Save** to save all of your settings in the Advanced Options screen.
- Result: All device names (except for AAA servers) in WLSE displays will be changed to the new format.



Note If a device is in the unmanaged state and you move it to the managed state, the device name does not immediately change to the currently specified name format. The change occurs after the next inventory is run. To change to the correct name format immediately, you can run an immediate inventory on that device. For more information, see [Running Immediate Inventories, page 4-65](#).

Table 4-13 **Name Formats**

Name Format String ¹	Result
%dns%	The device DNS name is displayed, Whether the DNS name is displayed, or a different identifier is displayed, depends on several factors. For details, see Enabling Reverse DNS Lookup, page 4-44 . If there is no DNS name, the device name is displayed as %dns%.
(%ip%)	The device IP address is displayed. Using this string guarantees that the device name display will always be correct.
%hostname%	The device hostname is displayed. This is the default. If the device has no hostname assigned to it, the device name is displayed as %hostname%.

Table 4-13 **Name Formats (continued)**

Name Format String ¹	Result
%description%	A description of your choice is displayed. You must enter a description for each device in the device detail screen accessible from Devices > Managed Devices. Note If you select %description% as the name format and do not enter a description for a device, the device name is displayed as %description%. Note The following characters are unsupported and cannot be used in a device description: double quote, single quote, and angle brackets (< >).
%r0MAC%	The MAC address of the radio interface is displayed. The MAC address formats apply only to access points and bridges, and are not applicable to switches and routers.
%r1MAC%	
%e0MAC%	
	The MAC address of the Ethernet 0 interface is displayed. Only the last 6 characters of the MAC address are used in the device identifier. If you use one of these name formats for devices other than access points, the DNS name, sysName, or IP address will be used instead. Which identifier is used depends upon whether reverse DNS lookup is enabled and the sysName is set on the device; for more information, see Enabling Reverse DNS Lookup, page 4-44.

1. Does not affect the display the identifiers of AAA servers.

Related Topics

- [Examples and Rules for the Name Format Option, page 4-43](#)
- [Enabling Reverse DNS Lookup, page 4-44](#)
- [Entering Device Descriptions, page 4-59](#)

Examples and Rules for the Name Format Option

The name format can be any of the types listed when you select **Learn About Name Format** or any combination of these types, for example:

- (%ip)%dns%
- %hostname%
- %dns%%r0MAC%
- %e0MAC%(%ip%)
- %e0MAC%%description%
- (%ip)%e0MAC%%description%
- (%ip%)%dns%%description%%r0MAC%%e0MAC%%r1MAC%

If the computed device identifier is longer than 30 characters, the WLSE will display only the first 30 characters in the device tree.

For name formats that include %e0MAC%, %r0MAC%, or %r1MAC%, only the last 6 characters of the MAC address will be used.

Name formats that include %e0MAC%, %r0MAC%, or %r1MAC% are not applicable to switches and routers.

Name formats do not apply to AAA servers; AAA servers are displayed according to the name entered when the server was added to the WLSE.

Enabling Reverse DNS Lookup

Enabling reverse DNS lookup affects hostname display on the WLSE as shown in [Table 4-14 on page 4-44](#). The actual identifier displayed for a device is also affected by the choices you make when specifying a device name format in **Devices > Discover > DISCOVER > Advanced Options** (for more information, see [Selecting the Device Name Format, page 4-41](#)).

Table 4-14 *Effects of Reverse DNS Lookup on Device Name Display*

Reverse DNS lookup enabled?	Effect on Display
Yes	If the lookup succeeds, the device name is displayed.
	If the lookup fails, the device IP address is displayed.
No	If the device's SNMP sysName is set, the sysName is displayed. ¹
	If the sysName is not set, the device IP address is displayed.

1. If a device's sysName contains a single quote (') and DNS is not enabled, the IP address will be displayed instead of the sysName.



Note

The hostname (device name) is not updated during every inventory cycle. This information is updated only after the device is rediscovered.

Procedure

- Step 1** Select **Devices > Discover > DISCOVER > Advanced Options**.
- Step 2** If DNS is configured on devices, you can enable reverse DNS lookup by selecting **Use reverse DNS lookup**.
- Step 3** Click **Save** to save all of your settings in the Advanced Options screen.

Related Topics

[Selecting the Device Name Format, page 4-41](#)

Enable Auto-Management

Enabling this option causes all discovered devices to be automatically managed.

**Note**

The Deployment Wizard enables auto-management. For more information on the Deployment Wizard, see [Chapter 2, “Using the Deployment Wizard.”](#)

Procedure

To enable automatic management for all discovered devices:

Step 1 Select **Devices > Discover > DISCOVER > Advanced Options**.

Step 2 Select **Auto-Manage Devices without Filtering**.

All discovered devices will be automatically placed in the Managed folder.

**Note**

If you are using the automatic device configuration feature, make sure you enable auto-management. Access points and bridges that you add to the network will be automatically configured only if Auto-Manage is enabled. For more information, see [Automating Configurations, page 8-39](#).

Step 3 To use the option for auto-managing selected access points within specified time limits, see [Enable MAC Address Auto-Manage Filtering for Access Points, page 4-45](#).

Step 4 Click **Save** to save all of your settings in the Advanced Options screen.

Related Topics

- [Managing Devices, page 4-54](#)

Enable MAC Address Auto-Manage Filtering for Access Points

This option allows you to specify access points that you want to auto-manage during a specified time interval.

Filtering also affects devices discovered through Wireless Domain Service (WDS). For more information, see [About WLCCP/WDS Discovery, page 4-27](#).

Auto-management affects all discovered devices. Access point filtering affects only access points. See the following table for details on the effects of these two options.

**Note**

The auto-manage filtering settings that you make here affect the Timer option in the Deployment Wizard and will be reflected in the Deploy Config screen of the Wizard. For more information on the Deployment Wizard, see [Chapter 2, “Using the Deployment Wizard.”](#)

Table 4-15 **Access Point Filtering Outcomes**

Auto-Manage selected?	MAC Filtering selected?	Result
No	No	All discovered devices must be manually moved to the managed state.
Yes	No	All discovered devices are automatically moved to the managed state.
Yes	Yes	Only access points listed in Access Points to Auto-Manage will be auto-managed and they will be auto-managed only during the specified interval. Note If the interval expires, newly discovered APs will not be auto-managed. However, any APs that you have manually placed in the Managed folder will still be managed.

You can specify the access points to be auto-managed by entering Ethernet MAC addresses in the screen or importing a file containing Ethernet MAC addresses. For example files, see [Example MAC Address Files, page 4-47](#).

To enable MAC address filtering:

-
- Step 1** Select **Devices > Discover > DISCOVER > Advanced Options**.
- Step 2** Select **Auto-Manage Devices without Filtering**.
- Step 3** Select **Enable Filtering for Auto-Manage devices**.
- Step 4** In the **Filters Valid From** and **To** fields, specify the time period for auto-management.



Note When the time period expires, you must deselect **Enable Filtering**. Otherwise, no newly discovered access points will be auto-managed.

- Step 5** To enter Ethernet MAC addresses in the screen:
- Remove the default * entry before beginning. Otherwise, all access points will be auto-managed regardless of the MAC addresses you enter.
 - Enter an Ethernet MAC address in the **Enter MAC Address of access point** text box (in hexadecimal format) and click >>. For example, 000b46fd0286. You can use the asterisk (*) as a wildcard; for example, *b46fd0286.
 - Repeat Step b to add more addresses.
- Step 6** To import a list of Ethernet MAC addresses from a file:
- Create an ASCII file (.txt file) consisting of one address per line or a comma-separated list. For sample files, see [Example MAC Address Files, page 4-47](#).
 - Enter the path to the file in the **Import From File** text box or click **Browse** to find the file.
 - Click **Import**.
- Step 7** To remove an address, select it in the **Valid MAC Addresses** text box and click <<.
- Step 8** Click **Save** to save all of your changes in the Advanced Options screen.
-

Example MAC Address Files

You can use either of the following file formats to import MAC addresses for limited discovery of access points:

- One address per line. For example:

```
0040965b611f
000a41047e3b
0040965b5f75
004096588420
004096543a84
000bbe6d8bd4
000af4fb658a
```

- Comma-separated list. For example:

```
000b466e482,0000bbe8190c2,0040965b611f,000a41047e3b,0040965b5f75,
004096588420,004096543a84,000bbe6d8bd4
```

Using Discovery IP Address Filtering

You can limit discovery to selected devices by setting up filter rules to include or exclude devices. Filter rules consist of device IP addresses with optional wildcards and ranges.

IP address filtering also affects devices discovered through Wireless Domain Service (WDS). For more information, see [About WLCCP/WDS Discovery, page 4-27](#).



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Devices > Discover > DISCOVER > IP Filter Rules**. For details on creating rules, click **Learn more about IP filter rules**.
- Step 2** Add IP addresses to the Include Rules or Exclude Rules text boxes, one entry per line. Use standard IP address format (four octets separated by periods) in which any octet can be:
 - A value between 0 and 255.
 - An asterisk (*) wildcard, denoting any number from 0 to 255; for example, 10.20.*.*.
 - A range in which the first number is less than the second; for example, 10.20.30[50-60].

Rules cause discovery to be limited as described in [Table 4-16](#).



Note

Exclude rules take precedence over include rules.

Table 4-16 *Effects of Include and Exclude Rules in Discovery Filters*

Include Rules Defined?	Exclude Rules Defined?	Result
No	No	All devices are discovered.
No	Yes	All devices are discovered, but devices that match the Exclude Rules are discarded.
Yes	No	Only devices that match the Include Rules are discovered.
Yes	Yes	Only devices that match the Include Rules are discovered. Devices that match the Exclude Rules are discarded.

For example, assume the IP addresses of the devices in a network are from 10.10.10.1 through 10.10.10.200:

- The include rule is 10.10.10.[40-80]
- The exclude rule is 10.10.10.[60-70]

All of the devices with the IP addresses 10.10.10.[40-80] are discovered, but those with IP addresses 10.10.10.[60-70] are discarded. Therefore, the devices discovered and retained have IP addresses 10.10.10.[40-59] and 10.10.10.[71-80].

Step 3 Click **Save**. Your rules will take effect for all subsequent discoveries.

Related Topics

[Understanding WLSE Discovery Methods, page 4-25](#)

Viewing Discovery Logs

This option displays detailed logs on the results of discoveries and imports.

To delete all discovery logs, see [Deleting Inventory and Discovery Logs, page 4-65](#).



Note

WDS discoveries are not logged.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Devices > Discover > DISCOVER > Logs**.

A table of discovery jobs is displayed.

Step 2 The names of the jobs indicate the type of discovery that was run, as explained in the following table:

Table 4-17 **Discovery Job Log**

Field	Description
Name	Type of discovery that was run: - Periodic CDP Discovery—scheduled discovery - Run Now CDP Discovery—on-demand discovery - CDPDiscovery_Import_Devices—device import from a file or CiscoWorks server - CiscoWorks Device Import—device import from a CiscoWorks server¹
Start Time	When the discovery started.
Recurring	- Yes—scheduled job that repeats at regular intervals. - No—on-demand or scheduled for one time only.
State	Scheduled—Discovery will occur in the future. Not scheduled—Run Now discoveries
User	User name—Name of the user who ran the job or who was the last user to modify the job. WLSE—Automatic, scheduled discovery that has not been modified by a user.
End Time	When the discovery ended.

1. Two items are listed in the discovery log for each import from a CiscoWorks server: CDPDiscovery_Import_Devices and CiscoWorks Device Import.

Step 3 To view details about a job, select the job and click **Discovery Run Detail**. The Discovery Run Detail window shows the start and end times of the job run, whether it succeeded, and other details. For scheduled discoveries, there will be several runs listed.

- To view the next page, click the arrow.
- To view the next 8 rows or all rows, click **8** or **All**.
- To close the window click **Close**.
- To refresh the display click **Refresh**.

For more information on data shown in the Discovery Run Detail window, see [Discovery Run Details Display, page 4-50](#).

If the log files show that problems occurred while running discovery, see [Diagnosing Common Discovery Problems, page 4-52](#).

Step 4 To filter the list of jobs, select All, Running, or Scheduled from the Discovery Job State list.

Step 5 To refresh the display, click **Refresh**.

Related Topics

[Deleting Inventory and Discovery Logs, page 4-65](#)

Discovery Run Details Display

A typical, healthy discovery run produces a log file similar to the following:

```
Seed value entered: 10.2.8.3
Hop count defined: 1
CDP Discovery started at 2003-03-27 22:40:11.437 (UTC)
New device discovered:10.2.8.3 ( AP1200-CHAR-NET )
Number of devices (re)discovered: 1
CDP Discovery completed at 2003-03-27 22:40:11.737 (UTC)
```

The log in the Discovery Run Details window shows the following information:

- Start and end times.
- The hop count (CDP distance) that was specified.
When you import devices, each imported device is listed as a “Seed value entered” in the log, and the “Hop count defined” value is 1.
- The seed devices that were entered or imported.
- Devices that were previously discovered and are being updated.
- Devices that were discovered for the first time.
- Devices that are being auto-managed. An immediate inventory collection will run automatically on auto-managed devices.
- Number of devices discovered or rediscovered.



Note

An immediate inventory does not run automatically after a device is rediscovered. You can run an immediate, on-demand inventory or wait for the next regularly scheduled inventory. For more information, see [Managing Device Inventory, page 4-63](#).

The messages listed in [Table 4-18 on page 4-50](#) may appear in the Discovery Run Details display.

Table 4-18 **Messages—Discovery Run Log**

Message	Meaning
172.19.12.39,public,private,14,1.3.6 .1.4.1.9.1.507, ![NOVALUE]!,...	Messages similar to this are informational and show data obtained during device import from CiscoWorks.
CDP Discovery completed	Periodic CDP discovery end time.
Number of devices (re)discovered <i>number</i>	Number of devices discovered or rediscovered.
No seeds defined.	Although discovery is initially enabled and runs every 24 hours, it will not run unless you add seed devices. See Using the Discovery Wizard, page 4-33 .
<i>ip_address</i> Device updated (<i>sysname</i>)	Device was previously discovered and information is being updated.
Inventory collection was not run for updated devices, run on-demand inventory or wait for the next scheduled inventory	An automatic inventory does not run for rediscovered devices. Run an on-demand inventory or wait for the next scheduled inventory. This is an informational message.

Table 4-18 **Messages—Discovery Run Log (continued)**

Message	Meaning
<code>ip_address</code> New device discovered (<code>sysname</code>)	Device was discovered for the first time.
<code>ip_address</code> Device being auto-managed (<code>sysname</code>)	Auto-management is enabled.
Inventory collection will run immediately for auto-managed devices.	Auto-management is enabled; therefore, inventory collection will run immediately for the auto-managed devices.
<code>ip_address</code> is SNMP unreachable, unable to read CDP cache.	The community strings may be set up incorrectly. See <i>Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.13</i> at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_13/index.htm. This message might indicate a network problem, or the device might be an invalid seed device (not running CDP and SNMP), such as a PC or workstation. For more information on troubleshooting SNMP problems, see Diagnosing Common Discovery Problems, page 4-52.
No logs available. Waiting for resources to start job.	Other running jobs are using all available resources. Information on this job will be displayed when resources are available.
<code>x.x.x.x</code> is reachable but unable to provide the information you requested. For IOS access points, make sure the SNMP community does not have an object identifier associated with it.	The community string associated with the device might not have an SNMP ISO view associated with it, and the WLSE cannot poll some attributes. Configure the community string in the AP as follows: <pre># snmp-server view iso iso included # snmp-server community community_string view iso RO</pre> where <i>community_string</i> is the AP's read-only community string.

Table 4-18 Messages—Discovery Run Log (continued)

Message	Meaning
IP conflict for <i>ip_address</i> (<i>hostname</i>). Identifier or ethernet MAC is <i>identifier</i> or <i>MAC address</i> . A device already exists under this IP address. If the original device was replaced, please delete it first and run discovery again.	A newly discovered device has the same IP address as a previously discovered device. The new device will not be discovered until the conflict is resolved. The identifier shown is for the previously discovered device. For access points, the identifier shown is the Ethernet MAC address. If you want both devices to be managed, assign a different IP address to the newly discovered device. If you substituted a new device for a previous device and want to retain the IP address, delete the old device. In either case, run discovery again or wait for the next scheduled discovery. See Managing Device Discovery, page 4-23 .
Unable to auto-manage device: x.x.x.x due to MAC filter values or time period for auto-management has expired.	A new device is being discovered but could not be auto-managed because the MAC filter values exclude the device or the time period selected for auto-management has expired. See Enable MAC Address Auto-Management for Access Points, page 4-45 .

Related Topics

- [Running CDP Discovery, page 4-34](#)
- [Diagnosing Common Discovery Problems, page 4-52](#)

Diagnosing Common Discovery Problems

This section contains information on:

- [Troubleshooting SNMP Connectivity Problems, page 4-52](#)
- [Obtaining Detailed Discovery Logs, page 4-53](#)

**Note**

For more troubleshooting information and FAQs, see the *Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine, 2.13*. For help locating this document, see [Finding WLSE Documentation on Cisco.com, page 1-15](#).

Troubleshooting SNMP Connectivity Problems

The most common discovery problems are related to SNMP connectivity. This type of message indicates that the WLSE attempted to retrieve the CDP neighbor table of the device, but was unable to do so because of an SNMP connectivity issue:

172.20.98.230 is SNMP unreachable, unable to read CDP cache.

Typical causes of SNMP connectivity issues are:

- No IP connectivity to the device
- SNMP community misconfigurations and/or mismatch
- SNMP agent is not running on devices
- SNMP timeouts, retries need to be adjusted

To determine the cause of the problem:

1. Confirm IP connectivity from the WLSE to the unreachable devices with the Ping Connectivity Tool (see [Using Network Tools, page 16-47](#)). Note that the WLSE Ping Connectivity Tool will attempt reverse name resolution on the IP address. If your network does not support reverse name resolution for the devices, you typically see 80% ICMP packet loss using the Ping Connectivity Tool unless you enter the `-n` flag in the Device field. If your network does not support reverse name resolution for your devices, enter `-n dvc_ip_address` in the Device field before clicking on the Ping button.



Note Cisco's Technical Assistance Center (TAC) has published a number of useful hints and documents on network troubleshooting. Visit the Cisco.com TAC web-site for more information.

2. After IP connectivity has been confirmed, use the SNMP Connectivity Tool (see [Using Network Tools, page 16-47](#)) to verify SNMP connectivity to the devices in question. This tool retrieves a single object—the SNMP sysObjectID of the device.

One common problem with both IP and SNMP connectivity is the presence of access control lists (ACLs) or firewalls in the network between the WLSE and the managed devices that might reject management traffic. Verify that management traffic is permitted from the WLSE to each of the managed devices.

3. If SNMP connectivity *can* be confirmed using the SNMP Connectivity Tool and devices cannot be discovered (the log lists the devices as SNMP unreachable), you might need to adjust the SNMP timeout and retries. See [Recommendations For Configuring SNMP Credentials, page 4-8](#).

The SNMP Connectivity Tool retrieves a single object, whereas the discovery retrieves multiple objects. You can use the SNMP Query Tool (see [Using the SNMP Query Tool, page 16-48](#)) to retrieve a larger SNMP table. Then, if you have SNMP connectivity for one variable but not for the larger table, it is likely that the issue is related to the timeout and retry settings. See Step 5.

4. If SNMP connectivity *cannot* be confirmed using the SNMP Connectivity Tool, verify that:

- The SNMP agent is running on the devices.
- The SNMP communities are correctly configured on the devices.
- The SNMP credentials are correctly configured on the WLSE.

If the SNMP configuration is not correct, reconfigure the devices and WLSE as necessary and re-run the discovery.

5. If the SNMP configuration is correct and IP connectivity has been confirmed, you may need to adjust the SNMP timeout and retries (see **Devices > Discover > Device Credentials**). Increase the timeouts and retries in small increments, re-running discovery after each adjustment, until the devices are no longer SNMP unreachable.

Obtaining Detailed Discovery Logs

If the procedures in the preceding section do not solve your discovery problems, open a case with the Cisco TAC. You might be able to assist the Cisco TAC by getting more detailed discovery logs. To increase the level of logging:



Note You must be logged in with admin privileges to use this interface.

1. Navigate to the WLSE interface at `http://wlse_ip:1741/debug/logging.jsp`.
2. Select **Debug**.

3. Click **Save**.
4. Run the discovery again to get more logging details.

After the discovery runs:

1. Navigate back to WLSE interface at http://wlse_ip:1741/debug/logging.jsp.
2. Select **Default**.
3. Click **Save**.

**Note**

Except for troubleshooting purposes, do not run any logging level other than Default for any task. Running at a level higher than Default might impact the performance of the WLSE.

Managing Devices

**Note**

If you are using the WLSE Deployment Wizard to deploy access points used within a Cisco [SWAN](#) framework, all discovered devices will be automatically managed. For information on the Deployment Wizard, see [Chapter 2, “Using the Deployment Wizard.”](#)

The Managed Devices option under **Devices > Discover > Managed Devices** shows the management state of all discovered devices. Devices must be in the managed state before they can be polled, and before you can use the WLSE to monitor or configure them or use any of the other WLSE network management or radio management features.

By default, newly discovered devices are in the unmanaged state. You can arrange for devices to be automatically managed after they are discovered, or you can manually move devices to the managed state.

From the device tree you can also view details on any device in a folder.

**Note**

The device tree shows the state of the system at the time you select the Managed Devices option. Therefore, if device details change or the device changes to another state after you display the page, these changes not automatically displayed. If you refresh the page from the browser or navigate to another page and then return to Managed Devices, the page will be updated to show changes.

This section contains information on the following device management options:

- The folders under **Devices > Discover > Managed Devices** and how to use the available functions—See [Device Management Folders and Functions, page 4-55](#).
- The number of devices that a WLSE can manage—See [Limitation on the Number of Managed Devices, page 4-60](#).
- What to do when the same IP address is assigned to more than one access point or you replace a managed access point—See [Handling Duplicate IP Addresses on Access Points, page 4-61](#).

Device Management Folders and Functions

The Managed Devices option provides the following functions:

Table 4-19

Function	Reference
View all devices that have been discovered: newly discovered devices that are not yet managed, managed devices, unmanaged devices (devices that were once managed but are no longer managed), and devices with changed IP addresses. Note Only managed devices appear in other WLSE displays, such as groups and reports.	About Managed Devices Folders, page 4-55
Manually change a device's management state. ¹	Manually Changing the State of Devices, page 4-56
View details about a device.	Viewing Device Details, page 4-57
Enter a different description for each device.	Entering Device Descriptions, page 4-59
Delete devices.	Deleting Devices, page 4-60

1. You can also configure the WLSE to automatically manage devices as they are discovered. See [Setting Advanced Discovery Options, page 4-41](#).



Note

The roles assigned to your login determine whether you can use the Managed Devices option.

About Managed Devices Folders

The Managed Devices display contains the following top-level folders. There is a subfolder for each type of device contained in a top-level folder; the subfolders appear only if there is at least one device of that type in the top-level folder.

Table 4-20 *Managed Devices Folders*

Top-Level Folder	Contents	Permitted Actions
Search Results	This folder is populated after you run a successful search for devices. This folder does not contain subfolders. For information on searching for devices, see Using the Device Selector, page 1-12 .	If a device is in any of these folders, you can view details about it, delete it from the database, or change its managed/unmanaged state.
New	Contains all devices that have been discovered but are not in the managed state.	
Managed	Contains all devices that are in the managed state	
Unmanaged	Contains all devices that were once managed but are not longer in the managed state.	

Table 4-20 **Managed Devices Folders (continued)**

Top-Level Folder	Contents	Permitted Actions
Duplicate IP	Contains access points that are in the <i>pending</i> state. A device becomes pending and is placed in this folder: • When the same IP address is assigned to more than one access point. • When an access point's IP address changes. • When you replace a managed access point. The IP address shown for a device in this folder is the last known address for the device, before the address change occurred. For information on how to move devices from the pending state, see Handling Duplicate IP Addresses on Access Points, page 4-61.	If a device is in this folder you can view details about it or delete it from the database.

Manually Changing the State of Devices

Procedure

Step 1 Select **Devices > Discover > Managed Devices > Manage/Unmanage**. The Discovered Devices tree is displayed.

For information on the folders and subfolders in the tree, see [About Managed Devices Folders](#), page 4-55.

Step 2 Select a folder. The Group Change Status window appears and all devices in the folder are displayed. Select the devices you want to change, then click **Manage** or **Unmanage**. Devices will be moved into the Managed or Unmanaged folder.



Note After you move devices to the managed state, an immediate inventory is run for those devices. This ensures that device attributes appear in displays immediately, without waiting for the next scheduled inventory.

Step 3 You can also change the status of a single device from its Device Detail display:

- a. Expand the folder and select the device.

Result: The Device Detail pane is displayed. For more information on device details, see [Viewing Device Details](#), page 4-57.

- b. Click **Manage** or **Unmanage** at the bottom of the pane.
- c. The device will be moved into the Managed or Unmanaged folder.

**Note**

After you move a device to the managed state, an immediate inventory is run for that device. This ensures that device attributes appear in displays immediately, without waiting for the next scheduled inventory.

Related Topics

- [Viewing Device Details, page 4-57](#)
- [Entering Device Descriptions, page 4-59](#)
- [Deleting Devices, page 4-60](#)
- [Limitation on the Number of Managed Devices, page 4-60](#)
- [Managing Device Inventory, page 4-63](#)

Viewing Device Details

Procedure

Step 1 Select **Devices > Discover > Managed Devices > Manage/Unmanage**. The Discovered Devices tree is displayed.

For information on the folders and subfolders in the tree, see [About Managed Devices Folders, page 4-55](#).

Step 2 To view details about an individual device:

- a. Expand the folder and subfolder containing the device.
- b. Select the device.

Result: The Device Details pane appears.

For information on the device details displayed, see [Understanding Device Details, page 4-57](#).

For information on entering a description in the Description field, see [Entering Device Descriptions, page 4-59](#).

Related Topics

- [Manually Changing the State of Devices, page 4-56](#)
- [Entering Device Descriptions, page 4-59](#)
- [Deleting Devices, page 4-60](#)

Understanding Device Details

Some device details are not displayed unless the corresponding parameters are set on the device; for example, location and contact information.

The details shown in the Device Details pane are described in [Table 4-21 on page 4-58](#).

Table 4-21 **Device Details Pane**

Field	Description
Description	A description to be used as the device identifier in WLSE displays. Only the first 30 characters of the device identifier string will be displayed. For information on entering a description in this field, see Entering Device Descriptions, page 4-59. For details on formatting the device identifier string, see Selecting the Device Name Format, page 4-41. Note If you select description as the name format and do not enter a description in Device Details, the name of the device in WLSE displays will be “%description%.”
Device Name	By default, DNS name, IP address, or sysName. For information on which identifier will be displayed, see Enabling Reverse DNS Lookup, page 4-44 .
State	Current state of the device: • New—Device was discovered but is neither managed nor unmanaged. • Unmanaged—Device was discovered but was moved to the unmanaged state. • Managed—Device was discovered and is being managed by the WLSE. • Pending—During discovery, a device was found that has the same IP address as this device. For more information on handling duplicate IP addresses, see Handling Duplicate IP Addresses on Access Points, page 4-61. • Deleted—Someone has deleted the device.
SysDescription	Detailed device description.
Version	Software version installed on the device.
Device Family	Device type; for example, Aironet.
SysName	The system name. Not displayed unless set on the device. Note If a device’s sysName contains a single quote (‘) and DNS is not enabled, the IP address will be displayed instead of the sysName.
SysObjectId	Unique identifier that identifies the device type.
Location	Where the device is located. Not displayed unless set on the device.
Device Identity	MAC address. For access points, this is the FastEthernet MAC address.
Serial Number	Device serial number.
IP Address	Device IP address.
Subnet	Subnet in which the device is located.
Network Segment	The network segment in which the device is located.
Contact	The person to contact for this device. Not displayed unless set on the device.
Profile	Name of the fault profile that contains threshold values and policy settings for this device; for example, the Default profile.

Related Topics

- [Manually Changing the State of Devices, page 4-56](#)
- [Viewing Device Details, page 4-57](#)
- [Entering Device Descriptions, page 4-59](#)
- [Limitation on the Number of Managed Devices, page 4-60](#)

Entering Device Descriptions

You can enter a description for each device in the Device Details pane. The description you enter is used in displays in one of the following ways:

- This description can be shown as additional information on the device in device detail displays.
- You can specify that this description be used in place of the normal device name in all WLSE displays. To use the description as the device name, you must select the description type as the name format for all devices. You specify the name format in **Devices > Discover > DISCOVER > Advanced Options**.

**Note**

You can search for devices by specifying the description.

Procedure

- Step 1** Select **Devices > Discover > Managed Devices > Manage/Unmanage**. The Discovered Devices tree is displayed.
- Step 2** Expand the folder and subfolder containing the device.
- Step 3** Select the device.
- Result: The Device Details pane appears.
- Step 4** Enter a description in the Description field, then click **Save**.

**Note**

For the rules about types and numbers of characters you can enter in this field, see [Appendix B, “Naming Guidelines.”](#)

- Step 5** If you want to use this description as the device name in all displays, make sure to chose %description% as the name format type in **Devices > Discover > DISCOVER > Advanced Options**.

For more information about selecting the name format, see [Selecting the Device Name Format, page 4-41](#).

Result: The Device Name field changes to the new name. The new name appears in device trees and other displays.

**Note**

Only the first 30 characters of the device identifier string will be displayed in the device tree.

Related Topics

- [Manually Changing the State of Devices, page 4-56](#)
- [Viewing Device Details, page 4-57](#)
- [Deleting Devices, page 4-60](#)

Deleting Devices

Procedure

-
- Step 1** Select **Devices > Discover > Managed Devices > Manage/Unmanage**. The Discovered Devices tree is displayed.
- Step 2** Select a folder.
- Result: The Group Change Status window appears and all devices in the folder are displayed.
- Step 3** Select the devices you want to delete, then click **Delete**.
- Step 4** You can also delete a single device from its Device Detail screen:
- a. Select the device from its folder.
- Result: The Device Detail pane is displayed.
- b. Click **Delete** at the bottom of the pane.
- Result: Deleted devices are removed from the database and from WLSE displays. Database updates could take some time if many devices are being deleted at the same time.
-

Related Topics

- [Manually Changing the State of Devices, page 4-56](#)
- [Limitation on the Number of Managed Devices, page 4-60](#)

Limitation on the Number of Managed Devices

The number of devices that can be managed by a single WLSE is limited, depending on the hardware platform and (for the [WLSE Express](#)) the installed software.

- [Managed Device Limit on the WLSE 1130 Series, page 4-60](#)
- [Managed Device Limit on the WLSE 1030 Express, page 4-61](#)
- [Finding the Managed Device Limit on Your WLSE, page 4-61](#)

Managed Device Limit on the WLSE 1130 Series

The WLSE 1130 series can manage 2,500 access points and wireless bridges and up to 5,000 radios if you are using only network management features. If you are also using radio management features, the WLSE 1130 series can manage 1,800 access points and 3,600 radios.

When you are using only network management features, after you have placed 2,500 access points under management, warning messages are displayed each time you add more devices to the Managed folder. After 2,550 devices are under management, no additional devices can be placed in the Managed folder.

Device discovery continues after the absolute limit (2,550 access points) is reached, but no additional devices can be placed under management.

**Caution**

If you are also using radio management features, you will not get a warning message when you have exceeded 1,800 access points under management.

Routers, switches, and AAA servers are not included in the 2,500-device limit.

Managed Device Limit on the WLSE 1030 Express

As shipped, the [WLSE Express](#) can manage 50 access points and wireless bridges and up to 100 radios.

After you have placed 45 access points under management, warning messages are displayed each time you add more devices to the Managed folder. After the first warning message appears, you can still add a few more devices. After 50 devices are under management, no additional devices can be placed in the Managed folder.

Device discovery continues after the absolute limit has been reached, but no additional devices can be placed under management.

Routers, switches, and external AAA servers are not included in the device limit.

**Note**

You can upgrade a WLSE Express to manage 100 devices and up to 200 radios.

Finding the Managed Device Limit on Your WLSE

You can display the device management limit on your WLSE by running the **show version** CLI command. For example:

show version

```
(C) Copyright 2005 by Cisco Systems Inc.
WLSE 1030 Release 2.13FCS Mon Mar 7 12:59:06 UTC 2005
Device Limit = 100
Build Version (66) Tue Mar 8 06:47:27 UTC 2005
Uptime: 0 days 1 hour 34 mins
Linux version 2.4.28-5_WLSE (root@app20.cisco.com) (gcc version 2.96 20000731 (Red Hat
Linux 7.3 2.96-113)) #1 Mon Jan 31 16:16:56 PST 2005

1030
VIA CPU at 1000.058 Mhz with 1025592K bytes of memory.
1 Ethernet interfaces

18.464Gb on disk
```

For information on accessing and using the CLI, see [Appendix A, “Command Line Interface \(CLI\) Commands.”](#)

Related Topics

[Managing Devices, page 4-54](#)

Handling Duplicate IP Addresses on Access Points

The WLSE uniquely identifies a device in network by its identity, which is the MAC address for an access point and the sysname for routers and switches.

The IP address assigned to a device might change for any of the following reasons:

- An existing AP is replaced by a new AP that has the same IP address.
- Addresses are assigned by DHCP. Either the lease time expires or multiple APs are rebooted, causing the APs to renew their IP addresses. Thus, DHCP might assign different IP addresses.
- A user reorganizes the network.

If the WLSE discovers a device (device A) that has an IP address that was previously assigned to device B, the WLSE will assign the correct IP address to device A. The WLSE will then declare that device B has an IP address conflict, and places device B in the Duplicate IP folder.

When the WLSE finds the correct IP address for device B during discovery, it will automatically assign the IP address to device B and also remove device B from the Duplicate IP folder.

The WLSE raises a single “Duplicate IP Address Detected” fault on IP address 127.0.0.1 regardless of the number of devices in the Duplicate IP folder. The fault will remain until the Duplicate IP folder becomes empty.

Such conflicts within the WLSE might be temporary while discovery is in progress and will likely be resolved at the completion of device discovery. This depends on the discovery seeds and the CDP distance. These parameters should be set so that the WLSE discovers or rediscovers all the affected devices.

The WLSE temporarily treats the devices in the Duplicate IP folder in the same way as unmanaged devices. No active management activity will occur on these devices. The WLSE begins to actively manage such a device as soon as it discovers its correct IP address.

The WLSE can usually automatically detect and handle such IP address changes during device discovery if:

- All devices, including the affected devices, are SNMP reachable.
- Device discovery is configured with the correct seeds and CDP distance so that all affected devices will be accessed.

If any devices still remain in the Duplicate IP folder, you may need to do one of the following to resolve this:

- If the device has been removed from the network, you can delete it from the WLSE.
- Check the network to ensure that the device is SNMP reachable. Then explicitly discover the affected devices using the new IP addresses assigned to them with appropriate CDP distance.

When the WLSE resolves all conflicting devices, the “Duplicate IP Address Detected” fault will be automatically cleared.

Managing Device Inventory

During inventory, the WLSE retrieves device attributes to populate its displays (such as reports) and place devices in groups.

The WLSE automatically runs basic inventories on all managed devices and inventories on client associations and trends for specific types of devices. For information about automatic inventories, see [About Inventories, page 4-63](#).

The inventory options are described in [Table 4-22 on page 4-63](#).

Table 4-22 *Inventory Options*

Option	Description	Reference
Run Inventory	Run immediate inventories of selected devices.	Running Immediate Inventories, page 4-65
Polling	Reset the polling intervals for automatic inventories, job retention, and retention of aggregated data for reports.	Changing the Polling Intervals for Automatic Inventories, page 4-64
	Delete all discovery and inventory logs.	Deleting Inventory and Discovery Logs, page 4-65
Logs	View inventory run details.	Viewing Inventory Logs, page 4-69

Related Topics

[About Inventories, page 4-63](#)

About Inventories

Periodic device inventory polling processes retrieve key data from managed devices. Polling processes support these features:

- Inventory-related polled data populate WLSE current and inventory reports.
- Aggregated inventory polled data populates WLSE trending reports.
- Inventory polling is typically run at regular intervals, but can also be run on-demand.
- Other polled data is processed and compared against fault, performance, and configuration policy thresholds.
- Device polling and data aggregation intervals are configurable.

You can view information about inventory jobs in the logs (see [Viewing Inventory Logs, page 4-69](#)) and in the jobvm log. To view or download the jobvm log, select **Admin > Appliance > Status > View Log File** and select the jobvm.log file.

The WLSE features the following kinds of inventories and polling:

- [Automatic Scheduled Inventories, page 4-64](#)
- [Immediate \(Run Now\) Inventories, page 4-64](#)

Automatic Scheduled Inventories

The WLSE runs 3 types of automatic inventories on a regularly scheduled basis:

- **Basic** inventories of all devices. These inventories collect all the information required by the WLSE to populate displays, such as reports, and to place devices in system-defined groups.

In the inventory log, these inventories are named Periodic Inventory.

**Note**

An automatic basic inventory runs immediately after a device is discovered for the first time if auto-management is turned on. Inventory does not run immediately after a device is rediscovered.

- **Client** inventories that collect only information about associations of clients to access points.

In the inventory log, these inventories are named Client Inventory.

- **Performance** inventories that collect only the performance attributes used in trend reports for access points, bridges, and AAA servers.

In the inventory log, these inventories are named Performance Inventory.

You can reset the polling intervals for automatic inventories. See [Changing the Polling Intervals for Automatic Inventories, page 4-64](#). You can run immediate or scheduled inventories. See [Running Immediate Inventories, page 4-65](#).

Immediate (Run Now) Inventories

You can run immediate inventories. You select the devices for these inventories.

These are basic inventories of all devices. These inventories collect all the information required by the WLSE to populate displays, such as reports, and to place devices in system-defined groups.

In the inventory log, these inventories are named Run Now Inventory.

**Note**

The radio management module of the WLSE runs periodic immediate inventories. These inventories appear in the log as normal immediate inventories.

Changing the Polling Intervals for Automatic Inventories

Use the following procedure to change intervals for automatic inventories. For guidelines on choosing intervals, see [Guidelines For Choosing Inventory Intervals, page 4-65](#).

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **Devices > Discover > Inventory > Polling**.

Step 2 Reset polling intervals as follows:

- To reset the interval for the scheduled complete inventory, use the Inventory Poll Interval parameter.
- To reset the interval for the scheduled client inventory, use the Wireless Client Poll Interval parameter.

- To reset the interval for the scheduled performance inventory, use the Performance Attributes Poll Interval parameter.

Step 3 To save your changes, click **Apply**.

Related Topics

- [Managing Polling Parameters, page 4-66](#)
- [Guidelines For Choosing Inventory Intervals, page 4-65](#)

Guidelines For Choosing Inventory Intervals

Following are some suggestions for deciding how to set the polling intervals.

At each interval, the WLSE runs basic, performance, and client inventory. If the actual inventory data collection time exceeds the interval, the WLSE will skip an inventory polling cycle. The next inventory polling will start at the next expected time.

For example, if the recurring scheduled inventory interval is configured to run every 30 minutes and the inventory polling begins at 10:00AM and runs for 32 minutes, the next polling will not begin until 11:00AM. This means that the data may not be as granular as expected.

A second potential problem occurs when the inventory polling takes just slightly less than the interval. In this case, the WLSE will almost always be running inventory polling processes. For example, suppose the recurring scheduled inventory interval is configured to run every 30 minutes, but inventory polling takes just under 30 minutes. In this case, if an inventory polling cycle begins at, for example, 10:00AM and runs until 10:29AM, the next inventory polling begins almost immediately at 10:30AM. This situation may be completely acceptable if the network can tolerate almost constant management polling from the WLSE and if the WLSE CPU and memory utilization do not become overtaxed.

Deleting Inventory and Discovery Logs



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Devices > Discover > Inventory > Polling**.

Step 2 Click **Delete all Discovery and Inventory Logs**.

Result: All discovery and inventory logs will be deleted. There is no way to delete selected logs.

Running Immediate Inventories

You can run immediate inventories of devices that you specify. The inventories you run are basic inventories that collect all the information required by the WLSE to populate displays, such as reports, and to place devices in defined groups.

**Note**

Your login determines whether you can use this option.

When new devices are discovered and managed, basic inventory and client reports are not populated until the next inventory polling occurs. However, you can use this option to populate these reports before the next inventory cycle starts.

This feature can also be useful when configuration changes are made on network devices and you want the changes quickly reflected in the basic and client inventory reports.

Procedure

-
- Step 1** Select **Devices > Discover > Inventory**.
- Step 2** Select a group from the Device Selector in the left pane.
- For information on how to use the device selector and search for devices, see [Using the Device Selector, page 1-12](#).
- For information on the folders and groups listed in the Device Selector, see [System-Defined Groups, page 4-75](#).
- Step 3** All of the devices in the group are added to the list in the Run Inventory Now window. From the list of devices in the group, select the devices you want to inventory.
- Step 4** Click **Run Inventory**. The inventory job starts immediately. Managed devices are polled and information is collected. WLSE displays are updated accordingly.
- Step 5** To view details of an inventory, see [Viewing Inventory Logs, page 4-69](#).
-

Managing Polling Parameters

The Polling option allows you to:

- Reset global parameters that affect inventory polling intervals, job history retention, and retention of data used in reports.
- Delete all inventory and discovery logs.
- Disable specific WLSE jobs such as inventory polling, hourly performance aggregations, and monthly performance aggregation.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Devices > Discover > Inventory > Polling**. The parameters described in [Polling Parameter Details, page 4-67](#) are displayed.
- Step 2** To work with parameters:
- a. To change parameter values, select new values from the pulldown lists.
 - b. To reset parameters to their previous values, click **Reset** before clicking **Apply**.

c. To save your changes, click **Apply**. To return to the System Parameters window, click **Back**.

Step 3 To disable any polling parameters, uncheck the box that corresponds to the parameter. If you disable a polling parameter, the corresponding data is not collected or computed. By default, all parameters are enabled.



Note To stop all client data collection, you must disable both client polling *and* client tracking. Client tracking is disabled by default.

Step 4 To delete data for the polling parameters you disabled, click **Delete Disabled Data**.



Caution

If you click **Delete Disabled Data**, all data for the polling parameters you disabled will be deleted and none of the relevant data will be available on some or all trend reports. After the data is deleted, the WLSE is automatically reloaded.

Step 5 To delete all inventory and discovery logs, click **Delete All Discovery and Inventory Logs**.

Related Topics

[About Trending and Aggregation Data, page 4-69](#)

Polling Parameter Details

The following tables describe the WLSE's polling parameters.

- [Polling Interval Parameters](#)—Control the intervals during which inventory, wireless client, and performance data will be collected (see [Table 4-23 on page 4-67](#)).
- [Fault and Job Truncation Parameters](#)—Control the amount of data displayed in fault history tables and job history tables (see [Table 4-24 on page 4-68](#)).
- [Data Retention Parameters](#)—Control how long to retain the aggregated data used in trend reports (see [Table 4-25 on page 4-68](#)).

For general information about polling intervals and data retention parameters and guidelines for choosing the appropriate settings, see [About Inventories, page 4-63](#).

Table 4-23 **Polling Interval Parameters**

Parameter	Description	Values
Inventory Poll Interval	Interval during which configuration data will be collected from the devices for inventory. This is the data shown in any Web interface device detail table. Tip For more accurate trending, set this parameter at a lower interval than the Performance Attributes Poll Interval .	Default values: Hourly—72 hours Daily—15 days Weekly—12 weeks Monthly—6 months Minimum: 10 minutes Maximum: 7 days

Table 4-23 Polling Interval Parameters (continued)

Parameter	Description	Values
Wireless Client Poll Interval	Interval during which data is collected for client inventory. Also, the interval at which Wireless Client reports are updated. Decreasing the interval provides more data points in reports. Tip When managing more than 1,000 access points, you should increase this parameter. The default polling interval generates too much traffic when large numbers of access points are being managed. To poll a set of clients at frequent intervals, use the Scheduled Inventory feature instead of decreasing this parameter; see Running Immediate Inventories, page 4-65 .	Default: 51 minutes Minimum: 17 minutes Maximum: 7 days
Performance Attributes Poll Interval	Interval during which performance and utilization data are collected from the devices for the performance inventory.	Default: 31 minutes Minimum: 13 minutes Maximum: 7 days

Table 4-24 Fault and Job Truncation Parameters

Parameter	Description	Values
Fault History Truncation Interval	How long displayed fault data is retained. This is the data shown in Fault displays.	Default: 30 days Minimum: 15 days Maximum: 60 days
Job History Truncation Interval	How long displayed job data is retained. Note Recurring jobs are truncated every day to retain the last 30 runs.	Default: 30 days Minimum: 1 day Maximum: 60 days

Table 4-25 Data Retention Parameters

Parameter	Description	Values
Hourly Aggregated Data	How long to retain the reports data that is aggregated hourly.	Default: 7 days Minimum: 1 day Maximum: 15 days
Daily Aggregated Data	How long to retain the reports data that is aggregated daily.	Default: 30 days Minimum: 8 days Maximum: 30 days

Table 4-25 **Data Retention Parameters (continued)**

Parameter	Description	Values
Weekly Aggregated Data	How long to retain the reports data that is aggregated weekly.	Default: 6 months Minimum: 1 month Maximum: 12 months
Monthly Aggregated Data	How long to retain the reports data that is aggregated monthly.	Default: 12 months Minimum: 1 month Maximum: 24 months

About Trending and Aggregation Data

Raw trending data retrieved from inventory polling is placed in database trending tables as follows:

- Every hour, this trending table data is processed into an **hourly** aggregation table.
- Every 24 hours, the first level aggregated data is processed into the **daily** aggregation table.
- The daily aggregation table data is aggregated every seven days into a **weekly** aggregation table.
- The weekly aggregation table is aggregated every 30 days into the **monthly** aggregation table.

The data in the trending and aggregation tables is periodically purged. For the minimum, default, and maximum data retention intervals, see [Polling Parameter Details, page 4-67](#).

Data retention intervals are configurable globally through the system parameters interface. Under almost all circumstances, there is no reason to change the defaults. In some large WLAN deployments, however, the WLSE database may begin to grow so large that it makes sense to purge data more often. Because it may affect the accuracy of the data in the trending reports, be careful when you change the data retention intervals.

Viewing Inventory Logs

This option allows you to view historical information about inventories.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Devices > Discover > Inventory > Logs**.
- Step 2** The names of inventory jobs indicate the type of inventory that was run, as explained in the following table.

Table 4-26 *Inventory Job Log*

Field	Description
Name	Type of inventory: • Periodic—basic automatic, scheduled inventory of all devices. • Client Inventory—automatic inventory of client associations with access points. • Performance Inventory—automatic inventory of performance attributes for trend reports. • Run Now Inventory—on-demand inventory of selected devices run by a user, or generated by the radio management module.
Start Time	When the inventory started.
Recurring	Yes—automatic scheduled inventory or inventory scheduled by a user. No—on-demand inventory run by a user or the radio management module.
State	Scheduled—scheduled to run at a later time. Blank field—a Run Now inventory.
User	Username—User who ran the inventory. WLSE—Automatic, scheduled inventory or inventory run by the radio management module.

Step 3 To view details about a job, select the job. The Run Log shows the start and end times of the job and type of data that was collected. The Run Log for immediate inventories shows which devices you selected for inventory. For more information, see [Run Log Details—Inventory, page 4-70](#).

Step 4 You can change the job history retention period. For information, see [Managing Polling Parameters, page 4-66](#).

Related Topics

[Diagnosing Common Inventory Problems, page 4-71](#)

Run Log Details—Inventory

Most inventory run log messages show the start and end time, the type of data collected, and the devices that were inventoried.

You may also see error messages, such as the following:

- No logs available. Waiting for resources to start job—Other jobs are running. Information on your job will be displayed when resources are available.

This message also appears if there are many SNMP timeouts on the network or devices are not reachable through SNMP. In that case, the inventory job will take much longer to finish, and the next scheduled inventory will not run until the current job finishes.

Related Topics

[Diagnosing Common Inventory Problems, page 4-71](#)

Diagnosing Common Inventory Problems

You can view the inventory process log files using the interface in **Devices > Discover > Inventory > Logs**. Open the appropriate folder within the Inventory sub-tree—the tree leaves correspond to the inventory runs. The logs are sorted in each folder by start time, with the most recent runs at the top.

If you have problems with your inventory processes and you open a case with the Cisco TAC, they may ask you for the jobvm log, which you can retrieve by selecting **Admin > Appliance > Status > View Log File**.

You might be able to assist the Cisco TAC by getting more detailed information than what normally appears in the logs. To increase the level of logging:



Note You must be logged in as an administrative user to use this interface.

1. Navigate to the WLSE interface at http://wlse_ip:1741/debug/logging.jsp.
2. Select **Debug**.
3. Click **Save**.
4. Run the inventory again to get more logging details.

After the inventory runs:

1. Navigate back to WLSE interface at http://wlse_ip:1741/debug/logging.jsp.
2. Select **Default**.
3. Click **Save**.



Note Except for troubleshooting purposes, do not run any logging level other than Default. Running at a level higher than Default might impact the performance of the WLSE.

Exporting Devices

You can export all managed devices (access points, routers, switches, and AAA servers) to:

- A CiscoWorks server running Resource Manager Essentials—see [Exporting Devices to a CiscoWorks Server, page 4-71](#).
- A comma-separated values (CSV) file—see [Exporting Devices to a CSV File, page 4-73](#).



Note Unmanaged devices are not exported.

Exporting Devices to a CiscoWorks Server

This option allows you to export all managed devices (access points, switches, and routers) and any AAA servers you have added to a CiscoWorks server. Unmanaged devices are not exported.

The information exported consists of the IP addresses and credentials.

The time required to export devices depends on the number of devices exported and the response from the CiscoWorks server. The following procedure explains how to check the status of the operation.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Devices > Discover > Export Devices**, then select **To CiscoWorks**.
- Step 2** Enter the following information:
- The CiscoWorks server IP address.
 - The CiscoWorks server port number. You may need to contact the administrator of the CiscoWorks server.
 - The username and password of any user who has the authority to export and import device credentials on the CiscoWorks server.
- Step 3** Click **Export**.
- Step 4** To see the export status log, click the **Status** or **Last Status**.
- If the Last Status button is displayed, you can review the results of a previous export.
- The following information is included in the export status log:

Table 4-27 Messages—Export Status Log

Type of Information or Message	Description
Device information	Name of the device, device status, and device status details. The string ![NO VALUE]! does not indicate an error; it means information was not available to the CiscoWorks server while it was sending a response to the WLSE.
Error: Could not connect to CiscoWorks server: <i>ip_address</i> on port: <i>port_number</i> .	Either the host or the port specified in the WLSE export dialog was wrong.
Error: Connected to CiscoWorks server: <i>ip_address</i> on port: <i>port_number</i> successfully, but server returned error after connection.	Either the username or the password specified in the WLSE export dialog was wrong.

- Step 5** To see other information about the export, go to **Admin > Appliance > Log File** and select the `cwexport.log` file. For more information about viewing logs, see [Using WLSE Log Files, page 16-4](#).
- Step 6** After you export devices, you can view them in CiscoWorks Resource Manager Essentials (RME) (see the RME online help for details).

Exporting Devices to a CSV File

This option allows you to export all managed devices (access points, switches, and routers) and any AAA servers you have added to a CSV file. Devices that are unmanaged are not exported.

The information exported for each device is:

- IP address or hostname
- Community strings
- Telnet password
- Enable password

For more information on CSV files, see [About CSV Files, page 4-30](#).



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Devices > Discover > Export Devices**, then select **To CSV File**.



Note

Device credentials are exported to a plain text file.

Step 2 For added security during the transmission of credentials, you can switch your browser to HTTPS and use HTTPS for downloading the file.

To launch an HTTPS session, enter the following URL:

`https://wlse_ip/`

where *wlse_ip* is the IP address of the WLSE. Note that you do not append a port number to the IP address when using HTTPS.

- If you did not create an unsigned certificate when you initially configured the WLSE, a Security Client dialog box appears, telling you that there is no valid certificate. For information about creating a certificate, see [Managing SSL \(HTTPS\), page 16-18](#).
- If you created a certificate but have not previously logged in via HTTPS, a Security Client dialog box appears. Enter the following information when prompted:
 - Click **Yes**.
 - Click **View Certificate**.
 - Click **Install Certificate**.
 - Click **Next** on remaining screens, then click **Finish**
 - Click **OK**.
 - Log out of the HTTP session on the browser and log back in to an HTTPS session.
 - Click **Yes** in the Security Client window that appears after you log in.
 - Select **Devices > Discover > Export Devices**, then select **To CSV File**.

Step 3 Click **Download CSV File**, then click **Save**. Specify the filename and location if different from the default.



Note The filename should have a .txt extension.

Result: The file is saved to your desktop.

Managing Groups

When you select **Devices > Group Management**, the Group Details window appears. Both system-defined and user-defined groups appear in the device selector. System-defined groups cannot be edited or deleted. For detailed information on system-defined and user-defined groups, see [About Groups, page 4-74](#).

The group management window allows you to:

Function	Reference
View system and user-defined groups	Using the Group Details Window, page 4-77
Create a new static group	Creating a Static Group, page 4-80
Create a new dynamic (rule-based) group	Creating a Rule-Based Group, page 4-81
Create a new static or rule-based group by copying an existing group	Creating a Static Group by Copying a Static or Rule-Based Group, page 4-82 Copying a Rule-Based Group, page 4-83
Edit a group	Editing a Static Group, page 4-84 Editing a Rule-Based Group, page 4-85
Delete a group	Deleting a Static or Rule-Based Group, page 4-86

Related Topics

- [Managing Device Discovery, page 4-23](#)
- [Managing Device Inventory, page 4-63](#)

About Groups

The WLSE grouping feature lets you organize managed devices into logical subsets and hierarchies. Using device grouping, you can quickly configure, upgrade, and view reports for a set of access points as a single operation.



Note Only managed devices can become members of groups.

The Group Details window allows you to view the existing device groups and categorize devices into named groups. A group is a named entity that can contain devices, other groups, or a combination of devices and groups. There are two types of groups:

- System-defined groups—See [System-Defined Groups, page 4-75](#).
- User-defined groups—See [User-Defined Groups, page 4-77](#).

The device selector lists all the current groups, both system-defined groups and user-defined groups. The number after a group name or folder shows how many objects it contains (devices and other groups) or how many groups are in the folder. Every managed device appears in one or more of the system-defined groups, and may also appear in one or more user-defined groups.

Groups can be dynamic or static:

- In dynamic groups, devices are added as they are discovered or as polling indicates key parameters have changed. Dynamic groups are either the pre-configured, system-defined groups or user-defined groups that have rules assigned to them (rule-based groups).
- Static groups are user-created groups that must have devices added or deleted from them manually.

System-Defined Groups

You cannot edit or delete a system-defined group. The system-defined groups are dynamic (rule-based), and are automatically populated by reading information from the devices during discovery and inventory collection. Any changes to devices are reflected in the system-defined groups only after the next discovery or inventory collection has completed.

System-defined groups are contained in folders; for example, the system-defined groups for device type are contained in the Device Type folder.

If devices are not configured correctly, they may not appear in the system-defined groups. For example, a WDS access point that is not correctly configured will not be included in the Active WDS or Backup WDS system groups.



Tip

A complete listing of supported devices can be found in the *Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine, 2.13* on Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_device_support_tables_list.html.

For details on the system defined groups, see [Table 4-28 on page 4-76](#).

Table 4-28 **System-Defined Groups**

Folder Name	Group Name/Description
Device Type	A group for each device type: • AAA Servers—EAP and RADIUS. AAA servers include APs configured as AAA servers and the built-in AAA server on the WLSE Express. Servers are added to groups after you add the servers to the WLSE (see Monitoring AAA Servers, page 4-14). • WLSM Modules—Active WLSM and Backup WLSM.¹ • AP 1100 • AP 1130 • AP 1210 (also contains AP 1230 devices) • AP 1240 • AP 350-IOS • Bridge 1300 • Bridge 1400 • Routers • Switches
More System Groups	• SSID—Group for each SSID configured on access points. • Software Version—Group for each software version installed on access points. • Subnet—Group for each subnet in the network. For example, 10.10.10.5.
Physical Location	Group for each building defined by users in the Location Manager. • To create, modify, and delete Physical Location groups, use the Location Manager. • To add devices to Physical Location groups or remove them from Physical Location groups, use the Location Manager. If you delete devices from the WLSE by using Devices > Discover > Managed Devices, those devices are automatically removed from the Physical Location groups.
Wireless Domain Services (WDS)	Groups for WDS devices: • Active WDS—Contains the access point or Wireless LAN Services Module (WLSM) that is actively providing WDS services.² • Backup WDS—Contains the backup WDS access points or WLSMs.
Scanning AP	Group for access points that are configured for scanning-only mode or that have an interface configured for scanning mode.

1. Both the Active WLSM and the Backup WLSM might also appear in the Active WDS folder if they are both in active service.

2. Both the Active WLSM and the Backup WLSM might also appear in the Active WDS folder if they are both in active service.

User-Defined Groups

You can define any number of groups. User-defined groups can either be static or rule-based:

- You add devices manually to static groups. Static groups can be subgroups of other static groups or can be placed at the top (root) level.

Although there is no limit on the number of levels in a group hierarchy, we recommend that you define no more than four levels. With too many levels, system performance degrades and navigation becomes difficult.

- For rule-based groups, you specify a set of rules that determine which devices are to be included in the group. The membership in rule-based groups is dynamic; when devices that match the defined rules become managed, they automatically become members of the group. All user-defined rule-based groups are placed at the top (root) level. You cannot create a subgroup of a rule-based group.

Useful user-created groups in a WLAN greatly depend on the structure of the network and the application demands. [Table 4-29](#) contains examples of groups that might be worthwhile in a typical wireless LAN environment.

Table 4-29 Examples of User-Defined Groups

Main Group	Sub-Groups
Campus	Main, Library, Dormitory, Athletic Field
RF Power	1mw, 2mw, 5.5mw, 30mw, 100mw
Radio Combinations	802.11a&b, 802.11a&g, 802.11b only
Department	Accounting, Marketing, Sales, Manufacturing
Special Features	Proxy Mobile IP
Antenna Type	Patch, Omni
Channels	1,2,3,4,5,6,7,8,9,10,11

Using the Group Details Window



Note

Your login determines whether you can use this option.

To view details about a group and use group management functions:

Procedure

- Step 1** Select **Devices > Group Management**.
- Step 2** Select a group from the device selector. The following details about the group are displayed.

Table 4-30 Group Details Window Fields

Field		Description
Description		Description entered when the group was created or edited (if any). Can be up to 256 characters long.
Created by		Username of the creator of the group.
Type		System Group, Static Group, or Rules-Based Group.
Group Members	Member Type	Device—A device, such as access point or switch. Subgroup—A subgroup of the group you selected.
	Name	Hostname of a member device or name of a subgroup. - Click a device name to display a window containing links to available reports and (for access points) a link to the AP's web interface. For a list of the items displayed, see Links to Reports from the Group Details Display, page 4-79. - Click a subgroup name to see details for the subgroup in a separate window.
	IP Address	IP address of a member device.
	Device Type	Device type of a member device
	Software Version	Software version installed on a member device.

Step 3 Depending on the type of group you selected, the following buttons appear at the bottom of the window.

Table 4-31 Group Details Window Buttons

Button	Function	Reference
Create Static Group	Create static group.	Creating a Static Group, page 4-80 .
Create Rule Based Group	Create rule-based group.	Creating a Rule-Based Group, page 4-81 .
Copy	Copy static or rule-based group.	Creating a Static Group by Copying a Static or Rule-Based Group, page 4-82 Copying a Rule-Based Group, page 4-83
Copy As Static	Make static copy of a rule-based group.	Copying a Rule-Based Group, page 4-83
Edit	Edit static or rule-based group.	Editing a Static Group, page 4-84 or Editing a Rule-Based Group, page 4-85
Delete	Delete group.	Click Delete to delete the group.

Links to Reports from the Group Details Display

The following reports can be displayed from the Group Details window by clicking the name of a device in the current group. A window opens displaying links to the following reports and a link to the Web interface of the access point.

Table 4-32 **Report Types**

Device Type	Reports Displayed	Reference
Access point	Summary Report	Displaying an AP Summary Report, page 10-65
	Detailed Report	Displaying a Detailed Report, page 10-67
	Fault Status	Viewing the Fault Status Report, page 10-13
	Device History	Viewing Device History, page 10-13
	Config History	Viewing Config History, page 10-14
	Firmware History	Viewing Firmware History, page 10-14
	AP Web Page	Opens a browser window to the AP, displaying Summary Status.
	AP Config	Current configuration of the access point.
	Auto Config Retry	Viewing the Auto Config Retry Report, page 10-15
Switch	Summary Report	Displaying a Switch Summary Report, page 10-77
	Fault Status	Viewing the Fault Status Report, page 10-13
	Device History	Viewing Device History, page 10-13
Router	Summary Report	Displaying a Router Summary Report, page 10-79
	Fault Status	Viewing the Fault Status Report, page 10-13
	Device History	Viewing Device History, page 10-13
AAA Server	Summary Report	Displaying a Server Summary Report, page 10-80
	Fault Status	Viewing the Fault Status Report, page 10-13
WDS	WDS Summary Report	Viewing the WDS Summary Report, page 10-10
	Detailed Report	Displaying a Detailed Report, page 10-67
	Fault Status	Viewing the Fault Status Report, page 10-13
	Device History	Viewing Device History, page 10-13
	Config History	Viewing Config History, page 10-14
	Firmware History	Viewing Firmware History, page 10-14
	AP Web Page	Opens a browser window to the AP, displaying Summary Status.
	AP Config	Current configuration of the access point.
	Auto Config Retry	Viewing the Auto Config Retry Report, page 10-15
	WDS Registered APs	Viewing the WDS Registered APs Report, page 10-12

Creating a Static Group

**Note**

Your login determines whether you can use this option.

To create a new static group:

Procedure

Step 1 Select **Devices > Group Management**.

Step 2 Click **Create Static Group** and enter the following information:

- Enter a name in the Name text box. Names can be up to 64 characters long.
- Enter a description in the Description text box (optional). Descriptions can be up to 256 characters long.

For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page B-1](#).

Step 3 The new group becomes the subgroup of whatever choice you make from the **Subgroup Of** list. To place the group at the top level of the tree, select **root**.

**Note**

Your new group will be added to the **Subgroup Of** list.

Step 4 Select a group or device from the device selector in the left pane. For information on how to use the device selector or search for devices, see [Using the Device Selector, page 1-12](#).

The group or device is added to the Available Devices list in the Create Group dialog.

Step 5 To add devices to the group, select the group or individual devices from the Available Devices list and click >>.

**Note**

After a device or group is added to the Devices in Group list, it is removed from Available Devices. Clicking on the device or group adds it back to the Available Devices list.

Step 6 To add more devices, repeat Step 5.

Step 7 To remove devices from the group, select them from the **Devices in Group** list and click <<.

Step 8 To save the group, click **Save**. The new group is displayed in alphabetical order in the group list.
To cancel the group creation and discard your changes, click **Cancel**.

Related Topics

[Creating a Static Group by Copying a Static or Rule-Based Group, page 4-82](#)

[Copying a Rule-Based Group, page 4-83](#)

Creating a Rule-Based Group

To create a new rule-based group:


Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Devices > Group Management**.

Step 2 Click **Create Rule Based Group** and enter the following:

- Enter a name in the Name text box. Names can be up to 64 characters long.
- (Optional) enter a description in the Description text box. Descriptions can be up to 256 characters long.


Note

New groups are always added at the top level ([root]).

For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page B-1](#).

Step 3 The new group becomes the subgroup of whatever choice you make from the **Subgroup Of** list. To place the group at the top level of the tree, select **root**.


Note

Your new group will be added to the **Subgroup Of** list.

Step 4 Define the rules for determining the devices that will be added to the group.

The available rules are described in the following table. You can use an asterisk (*) as a wildcard to match any number of characters.

- You must select at least one rule. A rule determines which devices are in the group or which devices are excluded from the group:
 - If you select Equals, devices that match the rule definition will be included in the group.
 - If you select Not Equals, devices that match the rule definition will be excluded from the group.

Rule Name	Data to Select or Enter
Software Version	The name of the software version; for example, 12.01T1, 12.2(4)JA1, or 12*
sysLocation	The sysLocation defined on devices, if any. An empty string matches all devices that do not have this variable set.
Device Type	Select an access point type from the list, if this group contains access points.
Subnet	A subnet, in decimal-dot format; for example 172.10.10.10 or 172.*
SSID	An SSID defined on devices.
VLAN ID	The existing VLANs configured on managed access points.

All of the rules you select are added together (logical *and*). For example, if you select the following Equals rules: Device Type AP1100, subnet 171.69.* and Software Version 12.2*, only the AP1100 access points in the specified subnet and running the specified firmware will be part of the group.

If you need to group devices that match more than one parameter in a given rule you can create a group that contains subgroups. For example, a group consisting of the AP1100 access points at two different sysLocations could be constructed by creating a group that contains a subgroup for each sysLocation.

Step 5 To preview the group, click **Preview**. The rule(s) you defined and any currently managed devices that match the rule(s) are displayed.

Step 6 To reset the window to its contents before this session, click **Reset**.

Step 7 To save the group, click **Save**. The new group is added, in alphabetic order, to the list of groups.

All currently managed devices that match the group rules will be added to the group. All devices that become managed later and match the rules will also be added to the group.

Related Topics

[Copying a Rule-Based Group, page 4-83](#)

Creating a Static Group by Copying a Static or Rule-Based Group



Note

Your login determines whether you can use this option.

Use this procedure to create a new static group by copying an existing static or rule-based group (including system-defined groups).

Procedure

Step 1 Select **Devices > Group Management**. The group selector pane and group dialog box are displayed.

Step 2 Select any group:

- For system-defined groups and other rule-based groups, click **Copy as Static**.
- For static groups, click **Copy**.

Step 3 Edit the name and description. The description is optional.

Names and descriptions can be up to 64 characters in length. For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page B-1](#).

Step 4 To change the place of the group in the hierarchy, select a group from the **Subgroup Of** list. The group you are editing becomes a subgroup of whatever group you choose. To place the group at the top level of the tree, select **root**.

Step 5 The devices in the group you copied appear in the Devices in Group list.

Step 6 To add more devices, you can search for devices or select a group or device from the device selector in the left pane. For information on how to use the device selector or search for devices, see [Using the Device Selector, page 1-12](#).

- a. The device or group is added to the Available Devices list in the Create Group dialog.
- b. Select the group or individual devices from the **Available Devices** list and click >>.

c. To add more devices, select another group.

Step 7 To remove devices from the group, select them from the Devices in Group list and click <<.

Step 8 To save the new group, click **Save**. The group is added, in alphabetic order, to the list of groups. By default, new static groups are placed under the same parent as the group you are copying; you can select another parent from the **Subgroup of** list. New static groups are added to the **Subgroup of** list. To cancel group creation and discard your changes, click **Cancel**.

Related Topics

- [Editing a Static Group, page 4-84](#)
- [Deleting a Static or Rule-Based Group, page 4-86](#)
- [About Groups, page 4-74](#)

Copying a Rule-Based Group

By copying an existing rule-based group (a user-defined group or a system group), you can create a new rule-based group or a new static group.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Devices > Group Management**.

Step 2 Select the group you want to copy and click **Copy** to create a rule-based group or **Copy As Static** to create a static group.

- If you selected **Copy As Static** to create a new static group, see [Creating a Static Group by Copying a Static or Rule-Based Group, page 4-82](#).
- If you are creating a new rule-based group, continue to Step 3. The new group will be placed at the top (root) level.

Step 3 Edit the group name and description, if desired. A description is optional.

Names and descriptions can be up to 64 characters in length. For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page B-1](#).

Step 4 To change the place of the group in the hierarchy, select a group from the **Subgroup Of** list. The group you are editing becomes a subgroup of whatever group you choose. To place the group at the top level of the tree, select **root**.

Step 5 Add rules as follows:

Rule Name	Data to Select or Enter
Software Version	The name of the software version; for example, 12.01T1, 12.2(4)JA1, or 12*.
sysLocation	The sysLocation defined on devices, if any. An empty string matches all devices that do not have this variable set.
Device Type	Select an access point type from the list, if this group contains access points.
Subnet	A subnet, in decimal-dot format; for example 172.10.10.10, or 172.*.
SSID	An SSID defined on devices.
VLAN ID	An existing VLAN configured on managed access points.

Step 6 To save the group, click **Save**. The new group is displayed and added to the top (root) level in alphabetic order.

To reset the window to its contents before this session, click **Reset**.

To cancel group creation and discard your changes, click **Cancel**.

Editing a Static Group



Note

Your login determines whether you can use this option.

To edit a static group:

Procedure

Step 1 Select **Devices > Group Management**.

Step 2 Select the group and click **Edit**.

Step 3 Change the Name or Description by editing the text in the relevant text boxes.

Names can be up to 64 characters long, and descriptions can be up to 256 characters long. For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page B-1](#).

Step 4 To change the place of the group in the hierarchy, select a group from the **Subgroup Of** list. The group you are editing becomes a subgroup of whatever group you choose. To place the group at the top level of the tree, select **root**.

- Step 5** To add devices to the group, select a group or device from the device selector in the left pane. For information on how to use the device selector or search for devices, see [Using the Device Selector, page 1-12](#).
- Select the group or individual devices from the list and click >>. Devices are placed in the Devices in Group list.
 - To add more devices, select another group.
- Step 6** To delete devices from the group, select one or more devices from the Devices in the Group list and click <<.
- Step 7** To save your changes, click **Save**. The edited group is displayed. To discard your changes, click **Cancel**.
-

Related Topics

- [Creating a Static Group, page 4-80](#)
- [Deleting a Static or Rule-Based Group, page 4-86](#)
- [About Groups, page 4-74](#)

Editing a Rule-Based Group



Note

Your login determines whether you can use this option.

To edit a user-defined rule-based group:

Procedure

- Step 1** Select **Devices > Group Management**.
- Step 2** Select the group and click **Edit**.
- Step 3** Change the Name or Description by editing the text in the relevant text boxes. A description is optional. Names can be up to 64 characters long, and descriptions can be up to 256 characters long. For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page B-1](#).
- Step 4** To change the place of the group in the hierarchy, select a group from the **Subgroup Of** list. The group you are editing becomes a subgroup of whatever group you choose. To place the group at the top level of the tree, select **root**.
- Step 5** Edit rules as follows:

Rule Name	Data to Select or Enter
Software Version	The name of the software version; for example, 12.01T1, 12.2(4)JA1, or 12*
sysLocation	The sysLocation defined on devices, if any. An empty string matches all devices that do not have this variable set.
Device Type	Select an access point type from the list, if this group contains access points.

Rule Name	Data to Select or Enter
Subnet	A subnet, in decimal-dot format; for example, 172.10.10.10, or 172.*.
SSID	An SSID defined on devices.
VLAN ID	The existing VLANs configured on managed access points.

- Step 6** To save your changes, click **Save**. The edited group is displayed.
 To reset the window to its contents before this session, click **Reset**.
 To discard your changes, click **Cancel**.

Deleting a Static or Rule-Based Group



Note

Your login determines whether you can use this option.

To delete a user-defined (static or rule-based) group:

Procedure

- Step 1** Select **Devices > Group Management**.
- Step 2** Select the group from the group selector list.
- Step 3** Click **Delete**.
- Step 4** Click **OK** in the popup window. The group will be deleted.

Related Topics

- [About Groups, page 4-74](#)
- [Editing a Static Group, page 4-84](#)
- [Creating a Static Group, page 4-80](#)



Using IOS Templates

The WLSE allows you to view, create, copy, edit, and delete IOS configuration templates and apply them to large numbers of devices at a time.



Tip

It is strongly recommended that you *not* use multiple templates to configure the same access point. While you can create multiple templates to configure different groups of access points, it is good practice to use the same template to configure the same access point every time.

The topics covered are:

- [What is a Configuration Template, page 5-1](#)
- [Creating a Template, page 5-2](#)
- [Copying a Template, page 5-3](#)
- [Editing a Template, page 5-3](#)
- [Deleting a Template, page 5-4](#)
- [Importing a Template, page 5-4](#)
- [Exporting a Template, page 5-5](#)
- [Template Choices, page 5-6](#)

Related Topics

- [Using WLSM Templates, page 6-1](#)
- [Using Wizard Templates, page 7-1](#)
- [Managing Configuration Jobs, page 8-7](#)

What is a Configuration Template

You can think of a configuration template as a configuration update file that you can apply to large numbers of devices at a time. This file might contain the update for only one parameter or a complete access point configuration.

IOS-based templates are stored as text files containing IOS commands.

You can use the **Configure > Templates** option to:

- Viewing existing templates—See [Viewing the Existing Templates, page 5-2](#)

- Create a configuration template—See [Creating a Template, page 5-2](#)
- Copy an existing template—See [Copying a Template, page 5-3](#)
- Edit an existing template—See [Editing a Template, page 5-3](#)
- Delete a template—See [Deleting a Template, page 5-4](#).
- Import a template—See [Importing a Template, page 5-4](#)
- Export a template—[Exporting a Template, page 5-5](#)

Viewing the Existing Templates

Use this option to create a configuration template.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** From the list, select the type of templates you want to display, then click Filter.
- Step 3** The selected template types are displayed in the Existing Templates table.
-

Creating a Template

Use this option to create a configuration template.

**Tip**

It is strongly recommended that you not use multiple templates to configure the same access point. While you can create multiple templates to configure different groups of access points, it is good practice to use the same template to configure the same access point every time.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** From the list, select **IOS**.
- Step 3** Enter a unique name. See [Naming Guidelines, page B-1](#) for details.

- Step 4** Click **New**. The window refreshes with the Template Creation menu in the left pane and the Template Name dialog box in the right pane.
- Step 5** Select the choices in the left pane to create a configuration template. For a description, see [Template Choices, page 5-6](#).
-

Copying a Template

Use this option to copy a configuration template that you can use as a base for another template.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Select the template you want to copy from the Existing Templates table, then click **Copy**. A dialog box appears asking you to enter a name for the copy.
- Step 3** Enter a unique name. See [Naming Guidelines, page B-1](#) for details.
- Step 4** Click **OK**. The Templates window refreshes and the new name appears in the Existing Templates table.
- Step 5** Click **Edit**. See [Editing a Template, page 5-3](#).
-

Editing a Template

Use this option to edit a configuration template.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Select the template you want to edit from the Existing Templates table, then click **Edit**. The window refreshes with Template Creation menu in the left pane and the Template Name dialog box in the right pane.
- Step 3** Select the choices in the Template Menu to create a configuration template. For a description, see [Template Choices, page 5-6](#).
-

Deleting a Template

Use this option to delete a configuration template.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Select the template you want to delete from the Existing Templates table, then click **Delete**. A window appears asking if you want to delete the template.

**Note**

You cannot delete a template if it is used in a scheduled job.

- Step 3** Click **OK** to delete it.

Importing a Template

Use this option to import a configuration to the WLSE, either from a file or from a device. You can import files from devices that are not managed by the WLSE.

When you import a configuration from an IOS access point, the imported configuration options are displayed in the Custom Values template screen.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Select IOS.
- Step 3** Click **Import**. The Import Template window appears and varies depending upon which type you selected.
- Step 4** Complete the following:

Field	Description
Template Name	If you are importing from a file, enter a new name for the template or leave the entry blank to use the imported template name. If you are importing from a device, you must enter a template name.
Description	Enter a description for the template. Do not click the Enter key at the end of the description; it will generate an error.

Field	Description
From file	Enter the template filename or browse to find the file, then click Import .
From device (IP Address)	Enter a device name or IP address, then click Import .
Non-IP-Identity	Select this option if you do not want to download identity parameters, such as IP address, from the access point. Some parameters are ignored using this type of import. The downloaded configuration parameters are not a full representation of the access point's configuration but an optimal representation.
Full	Select this option to import a full configuration from the access point. This type of import includes the access point's identity parameters, such as sysname, IP address, etc. When using this option, it is recommended you delete all the custom key values from the imported template before applying the template to any device.
Device Credentials	Select Telnet or SSH.
User Name	If the device is not managed by the WLSE, or if the device is managed but the credentials have not been set, enter the username on the access point.
User Password	If the device is not managed by the WLSE, enter the user password on the access point.

Step 5 To import another template, click **Back** and go to [Step 3](#).

Step 6 When you are finished, click **Done**.

Step 7 View the template you imported by selecting **Configure > Templates** and selecting it in the Existing Templates table.

Exporting a Template

Use this option to export a configuration template to your local drive.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Configure > Templates**. The Templates dialog box appears.

Step 2 Select a template name from Existing Templates, then click **Export**. The Export Template window appears.

Step 3 From the list, select the template you want to export, then click **Export**. The Export Template to Desktop window appears with the name of the template.

- Step 4** Right-click on the template name, select **Save As**, and enter the location to save the template.
-

Template Choices

When you create or edit an IOS configuration template, the following choices appear in the left pane of the Templates window:

1. **Template Name**—See [Naming the Template](#), page 5-7.

2. **Template Categories**



Note

Any or all of the template categories can be completed in any order.

- **Basic Settings**—See [Using Basic Settings](#), page 5-8.
 - **Basic Security**—See [Using Basic Security](#), page 5-12.
 - **Voice Express**—See [Configuring Voice Express](#), page 5-14
 - **Association**—See [Using Association](#), page 5-15.
 - **Network Interfaces**—See [Setting Up Network Interfaces](#), page 5-18.
 - **Security**—See [Defining Security Settings](#), page 5-33.
 - **Services**—See [Defining Services](#), page 5-65.
 - **Event Log**—See [Configuring the Event Log](#), page 5-94.
 - **Wireless Services**—See [Configuring Wireless Services](#), page 5-90.
 - **System Config**—See [System Config](#), page 5-96.
 - **Device Specific**—See [Configuring Device Specific Settings](#), page 5-98
 - **Custom Values**—See [Configuring Custom Values](#), page 5-98.
3. **Preview**—See [Previewing the Template](#), page 5-100.
 4. **Save**—See [Saving the Template](#), page 5-100.

Naming the Template

This option enables to you to name the template.

Procedure



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Step 1 Select **Template Name**. The Template Name dialog box appears:

Field	Description
Template Name	Enter a name for the template. See Naming Guidelines, page B-1 .
Description	Enter a description of the purpose of the template. See Naming Guidelines, page B-1 . Do not click the Enter key at the end of the description; it will generate an error.

Step 2 Select a template category. For additional information, see [2.Template Categories, page 5-6](#).

Using Basic Settings

Use this option if you need to set up an access point quickly with a simple configuration. This will allow you to enter all the access point's essential settings for basic operation.

Procedure

Step 1 Select **Basic Settings**. The Basic Settings dialog box displays in the right pane:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-1 Basic Settings

Field	Description
Configuration Server Protocol	Set this entry to match the network's method of IP address assignment. Select one of the following options: - DHCP—Use this setting if your network uses Dynamic Host Configuration Protocol, in which IP addresses are “leased” for predetermined periods of time. - Static IP—Use this setting if your network does has an automatic system for IP address assignment.
Default Gateway	Enter the IP address of your default Internet gateway. The entry 255.255.255.255 indicates no gateway.
Web Server	Select one of the following: Standard (HTTP) or Secure (HTTPS).
SNMP Community	- Enter the SNMP community name. - Select one of the following: Read-Only, Read-Write Note After a template job with this setting is successfully applied, the SNMP community string is displayed under Devices > Discover > Device Credentials > SNMP Communities.

Table 5-1 Basic Settings (continued)

Field	Description
Radio0-802.11B/G	
Role in Radio Network	Select one of the following: • Access Point Root—Use this setting for a root access point to become a repeater and associate to a nearby root access point when the wired connection is lost. • Repeater Non-Root—Use this setting if the access point is not connected to the wired LAN. Client data is transferred to the access point selected as the repeater parent. • Workgroup Bridge—Use this setting to specify that the device is a workgroup bridge. Access points and bridges normally treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges. • Bridge Root—Use this setting to designate one device in each group of bridges as the root bridge. A root bridge can only communicate with non-root bridges and other client devices and cannot associate with another root bridge. • Bridge Non-Root—Use this setting to specify that the bridge operates as a non-root bridge and must associate to a root bridge. • Install Mode—Use this setting to configure a bridge for installation mode. In installation mode, the bridge flashes its LEDs to indicate received signal strength (RSSI), which assists in antenna alignment. Click See detail to see for which device types or versions this setting is valid. • Scanner Access Point—Select to specify that the access point is a Scanning AP, which is used to guard certain air space from any potential intruders that operate on the same frequency band.
Optimize Radio Network for	Select one of the following: • Throughput—Use this setting to maximize the data volume handled by the access point; however, it might reduce the access point's range. • Range—Use this setting to maximize the access point's range; however, it might reduce throughput. • Default—Use this setting to set the data rates to factory default settings. This option is not supported on the 2.4-GHz, 802.11b radio.
Aironet Extensions	Select one of the following: • Enable—Use this setting to enable load balancing, Message Integrity Check (MIC), and WEP key hashing. • Disable—Use this setting to disable load balancing, Message Integrity Check (MIC), and WEP key hashing.

Table 5-1 Basic Settings (continued)

Field	Description
Radio0-802.11A	
Role in Radio Network	Select one of the following: • Access Point Root—Use this setting for a root access point to become a repeater and associate to a nearby root access point when the wired connection is lost. • Repeater Non-Root—Use this setting if the access point is not connected to the wired LAN. Client data is transferred to the access point selected as the repeater parent. • Workgroup Bridge—Use this setting to specify that the device is a workgroup bridge. Access points and bridges normally treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges. • Bridge Root—Use this setting to designate one device in each group of bridges as the root bridge. A root bridge can only communicate with non-root bridges and other client devices and cannot associate with another root bridge. • Bridge Non-Root—Use this setting to specify that the bridge operates as a non-root bridge and must associate to a root bridge. • Install Mode—Select to configure a bridge for installation mode. In installation mode, the bridge flashes its LEDs to indicate received signal strength (RSSI), which assists in antenna alignment. Click See detail to see for which device types or versions this setting is valid. • Scanner Access Point—Select to specify that the access point is a Scanning AP, which is used to guard certain air space from any potential intruders that operate on the same frequency band.

Table 5-1 Basic Settings (continued)

Field	Description
Optimize Radio Network for	Select one of the following: • Throughput—Use this setting to maximize the data volume handled by the access point; however, it might reduce the access point's range. • Range—Use this setting to maximize the access point's range; however, it might reduce throughput. • Default—Use this setting to specify the that the access point use settings entered for the Network Interfaces Settings.
Aironet Extensions	Select one of the following: • Enable—Use this setting to enable load balancing, Message Integrity Check (MIC), and WEP key hashing. • Disable—Use this setting to disables load balancing, Message Integrity Check (MIC), and WEP key hashing. Click See detail to see for which device types or versions this setting is valid.

Step 2 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
 - **Save** to save the template. See [Saving the Template, page 5-100](#).
 - Another template category to configure more options. See [2.Template Categories, page 5-6](#).
-

Using Basic Security

Use this option if you need to set up an access point quickly with a simple security configuration. This will allow you to enter all the access point's essential settings for basic operation.

Procedure

Step 1 Select **Basic Security**. The Basic Security dialog box displays in the right pane:

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-2 Basic Security

Field	Description
SSID Configuration	
Apply to	Select one of the following: - Radio B/G—Select this option for radio 802.11b/g. - Radio A—Select this option for radio 802.11a.
SSID	Select one of the following: - Enter any alphanumeric, case-sensitive string, from 1 to 32 characters long. - Select Broadcast SSID in Beacon to allow devices without a specified SSID to associate with this access point. Click for additional information.
VLAN	Select one of the following: - No VLAN—Use this setting to indicate there is no VLAN setting. - Enable VLAN ID—Use this setting to indicate there is a VLAN setting, then enter the VLAN identification number. - Native VLAN—Select to indicate that this is a Native VLAN. - Bridge-Group—Enter the bridge group. If you do not make an entry the VLAN number will used.
Security	Select one of the following: - No Security—Use this setting if you do not want to specify security options. Click for additional information. - Static WEP Key—Use this setting to specify WEP encryption. Click for additional information. 40-bit WEP keys, enter 10 hexadecimal digits (0-9, a-f, or A-F). 128-bit WEP keys, enter 26 hexadecimal digits (0-9, a-f, or A-F). - EAP Authentication—Use this setting to specify mandatory WEP, encryption open authentication + EAP, network EAP authentication, and no key management, RADIUS server authentication on port 1645. Click for additional information. - RADIUS Server—Enter the hostname or IP address of the RADIUS server you are either creating or deleting. - RADIUS Server Secret—Enter the server's shared secret. - WPA—Use this setting to specify encryption ciphers TKIP, open authentication + EAP, network EAP authentication, mandatory WPA key management, and RADIUS server authentication on port 1645. Click for additional information. - RADIUS Server—Enter the hostname or IP address of the RADIUS server you are either creating or deleting. - RADIUS Server Secret—Enter the server's shared secret.

Step 3 Click **Add** to add the SSID to the table.

To delete an SSID, select it from the table, then click **Delete**.

Step 4 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Voice Express

This option enables you to configure admission control for voice and video. You can also configure call admission control for SSID and enable the Gratuitous Probe Response feature.

Procedure

Step 1 Select **Voice Express**. The Voice Express dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-3 Voice Express

Field	Description
Voice Express	Select one of the following: • Enable—Use the setting to enable the voice express feature. • Disable—Use the setting to disable the voice express feature. Click See detail for information about which default values are populated when you select either enable or disable.
Admission Control for Voice and Video Category	
Video (User Priority 4-5)	Accept the defaults or enter a value for the following:
Voice (User Priority 6-7)	• Max Channel Capacity (%)—Enter the maximum channel capacity allowed. • Admission Control—Select to increase the number of voice calls that an access point can support by relieving congestion of voice packets over the wireless media. Note Admission control should not be enabled if your deployment includes softphone applications. If you are not deploying softphone applications on laptops, then use the default.

Table 5-3 *Voice Express (continued)*

Field	Description
Gratuitous Probe Response (GPR) 802.11a	Accept the default or select one of the following: • Enable—Use this setting to enable GPR. The Gratuitous Probe Response feature helps conserve battery power by providing a high rate packet on the order of 10ms. Note If you are not deploying the CN622 handset from Motorola, then GPR should be disabled. • Disable—Use this setting to disable this feature. Click See detail for additional information about these settings.
Low Latency Packet Rates 802.11a	Accept the defaults, or for each frequency, select one of the following: Nominal Rate, Allowed Rate, or Disable. Click See detail for additional information about these settings.
Traffic Stream Metrics	1. Accept the defaults or select one of the following: – Enable—Use this setting to have the access point report aggregated measurements to the WDS. – Disable—Use this setting to disable this feature. Click See detail for additional information about this setting. 2. Select for which radio these settings apply: Radio B/G and/or Radio A.
Voice for SSID	Allow or disallow Voice on selected SSIDs. • Allow Voice for SSID—Enter the Service Set ID and click >>>. The SSID and the text (Voice Allowed) appears in the selection box on the right. • Disallow Voice for SSID—Enter the Service Set ID and click >>>. The SSID and the text (Voice Disallowed) appears in the selection box on the right. To remove an SSID from the selection box, highlight the SSID and click Delete. Click See detail to see the versions for which this setting is valid and additional information.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Using Association

Use this option to configure the number of seconds that the access point tracks an inactive device.

Procedure

Step 1 Select **Association**. The Association: Activity Timeout dialog box displays in the right pane:

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-4 Association

Field	Description
Association: Activity Timeout	
These settings determine the number of seconds the access point continues to track an inactive device depending on its class. A setting of zero tells the access point to track a device indefinitely no matter how long it is inactive.	
Device Class • Bridge— A device that connects two wired networks together through a wireless network. • Client Station— A device that is connected to an access point or bridge. • Repeater—A device (typically another access point) that forwards data from a client station to another access point. • Workgroup Bridge—A device that provides wireless infrastructure connections for Ethernet-enabled devices. A device connected to a workgroup bridge communicates with the network infrastructure through Cisco access points. • Unknown—A non-Cisco device.	• Default—Specifies the activity timeout value that the access point uses when a device associates and either proposes a zero-refresh rate or does not propose a refresh rate. • Maximum—Specifies the maximum activity timeout allowed for a device regardless of the refresh rate proposed by a device when it associates.

Table 5-4 Association (continued)

Field	Description
Delete Activity Timeout	
These settings are used to remove existing timeout settings configured on the access point.	
Device Class • Bridge— A device that connects two wired networks together through a wireless network. • Client Station— A device that is connected to an access point or bridge. • Repeater—A device (typically another access point) that forwards data from a client station to another access point. • Workgroup Bridge—A device that provides wireless infrastructure connections for Ethernet-enabled devices. A device connected to a workgroup bridge communicates with the network infrastructure through Cisco access points. • Unknown—A non-Cisco device.	• Default—Specifies the activity timeout value that the access point uses when a device associates and either proposes a zero-refresh rate or does not propose a refresh rate. • Maximum—Specifies the maximum activity timeout allowed for a device regardless of the refresh rate proposed by a device when it associates.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
 - **Save** to save the template. See [Saving the Template, page 5-100](#).
 - Another template category to configure more options. See [2.Template Categories, page 5-6](#).
-

Setting Up Network Interfaces

Use this option to configure the device's network interface settings.

Procedure

Step 1 Select **Network Interfaces**. The menu expands and the Network Interfaces: FastEthernet Settings dialog box displays in the right pane.

Step 2 Select one of the following from the menu:

- FastEthernet—See [Configuring Fast Ethernet Settings, page 5-18](#).
 - Radio-802.11b/g—See [Configuring Radio-802.11b/g Settings, page 5-19](#).
 - Radio-802.11a—See [Configuring Radio-802.11a Settings, page 5-27](#)
-

Configuring Fast Ethernet Settings

Use this option to define the Fast Ethernet port settings.

Procedure

Step 1 Select **Network Interfaces > FastEthernet**. The Network Interfaces: FastEthernet Settings dialog box appears.

Step 2 Complete the following:



Note

Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-5 Fast Ethernet Settings

Field	Description
Enable Ethernet	Select one of the following: • Enable—Use this setting to enable Ethernet. • Disable—Use this setting to disable Ethernet.
Requested Duplex	Select one of the following: • Auto—Use this setting to allow the duplex setting to be automatically negotiated between the access point and the hub, switch, or router to which the access point is connected. • Half—Use this setting to allow operation in half-duplex mode. • Full—Use this setting to allow operation in full-duplex mode.
Requested Speed	Select one of the following: • Auto—Use this setting to allow the transmission speed to be automatically negotiated between the access point and the hub, switch, or router to which the access point is connected. • 100Mbps—Use this setting to allow a transmission speed of 100 Mbps. • 10Mbps—Use this setting to allow a transmission speed of 10 Mbps.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Radio-802.11b/g Settings

Use this option to configure the device's 802.11b and 802.11g radio.

Procedure

Step 1 Select **Network Interfaces > Radio-802.11b/g**. The Network Interfaces: Radio-802.11b/g dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-6 **Radio-802.11b/g Settings**

Field	Description
Configure Radio	Select the radio interface type: • Radio B • Radio G—Click See detail to see for which device types or versions this setting is valid.
Enable Radio	Select one of the following: • Enable—Use this setting to allow the access point to send packets through its radio interface and monitor when other devices use the radio interface to send packets. • Disable—Use this setting to change the administrative state of the radio from up to down.
Role in Radio Network (Fallback mode upon loss of Ethernet connection)	This setting is used to configure a fallback role for the access point. The access point automatically assumes the fallback role when its Ethernet port is disabled or disconnected from the wired LAN. Select one of the following: • Access Point Root (Fallback to Radio Island)—Use this setting to enable wireless clients to continue to associate even when there is no connection to the wired LAN. • Access Point Root (Fallback to Radio Shutdown)—Use this setting to force the clients to associate to another access point, if one is available, when the radio shuts down because the wired connection is lost. • Access Point Root (Fallback to Repeater)—Use this setting for a root access point to become a repeater and associate to a nearby root access point when the wired connection is lost. • Repeater Non-Root—Use this setting if the access point is not connected to the wired LAN. Client data is transferred to the access point selected as the repeater parent. • Scanner Access Point—Select to specify that the access point is a Scanning AP, which is used to guard certain air space from any potential intruders that operate on the same frequency band.

Table 5-6 **Radio-802.11b/g Settings (continued)**

Field	Description
	• Workgroup Bridge—Use this setting to specify that the device is a workgroup bridge. Access points and bridges normally treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges. • Bridge Root without Clients—Use this setting to designate one device in each group of bridges as the root bridge. A root bridge can only communicate with non-root bridges and other client devices and cannot associate with another root bridge. • Bridge Root with Clients—Use this setting to designate a device as the root bridge with clients. • Bridge Non-Root without Clients—Use this setting to specify that the bridge operates as a non-root bridge and must associate to a root bridge. • Bridge Non-Root with Clients—Use this setting to specify that the bridge operates as a non-root bridge with clients. • Install Mode—Select to configure a bridge for installation mode. In installation mode, the bridge flashes its LEDs to indicate received signal strength (RSSI), which assists in antenna alignment. Click See detail to see for which device types or versions this setting is valid.

Table 5-6 **Radio-802.11b/g Settings (continued)**

Field	Description
Data Rates	- Click one of the following to automatically set the data transmission rates: - Best Range—Use this setting to maximize the access point's range; however, it might reduce throughput. - Best Throughput—Use this setting to maximize the data volume handled by the access point; however, it might reduce the access point's range. - Default—Use this setting to compromise between range and throughput, providing good range and good throughput. Or - Select one of the following to manually set the data transmission rates: - Require—Use this setting to enable transmission at this rate for all packets, both unicast and multicast. At least one data rate must be set to Require. A client must support a required rate before it can associate. - Enable—Use this setting to enable transmission at this rate for unicast packets only. - Disable—Use this setting to not allow transmission at this rate.
Transmitter Power (mW)	Select the power level of the radio transmission. Note Government regulations define the highest allowable power level for radio devices. This setting must conform to established standards for the country in which you use the device. To reduce interference, limit the range of your access point, or conserve power, select a lower power setting.  Caution Do not use the 50mW or 10mW setting for Japanese channels. For a list of maximum power levels allowed in each regulatory domain refer to one of the following: - URL: http://www.cisco.com/en/US/products/hw/wireless/ps430/products_command_reference_chapter09186a0080147d8b.html#87443 - Cisco IOS Commands for Access in the <i>Cisco Aironet 1200 Series Access Point Command Reference</i>. Click See detail to see for which device types or versions this setting is valid. Click Power Translation Table mW/dBm to see the mapping values for transmitter power.

Table 5-6 Radio-802.11b/g Settings (continued)

Field	Description
CCK Transmitter Power (mW)	Use this setting on the 2.4-GHz, 802.11g radio to specify Complementary Code Keying (CCK) power levels in milliwatts. CCK modulation is supported by 802.11b and 802.11g devices. Click See detail to see for which device types or versions this setting is valid.
CCK Transmitter Power (dBm)	Use this setting on the 2.4-GHz, 802.11g radio to specify Complementary Code Keying (CCK) power levels in decibels below 1 milliwatt. CCK modulation is supported by 802.11b and 802.11g devices. Click See detail to see for which device types or versions this setting is valid.
OFDM Transmitter Power (mW)	Use this setting on the 2.4-GHz, 802.11g radio to specify Orthogonal Frequency Division Multiplexing (OFDM) power levels in milliwatts. OFDM modulation is supported by 802.11g and 802.11a devices. Click See detail to see for which device types or versions this setting is valid.
OFDM Transmitter Power (dBm)	Use this setting on the 2.4-GHz, 802.11g radio to specify Orthogonal Frequency Division Multiplexing (OFDM) power levels in decibels below 1 milliwatt. OFDM modulation is supported by 802.11g and 802.11a devices. Click See detail to see for which device types or versions this setting is valid.
Client Power Local	Use this setting to limit the power level on client devices that associate to the access point to the same setting as the AP's configured transmitter power. Note Setting the client's power level to the same as the AP transmitter power provides improved interference control in the WLAN. Note If you disable this option, you should use one of the Limit Client Power fields (see below) to set the client's power level to a specific value. Click See detail to see for which device types or versions this setting is valid.
Limit Client Power (mW)	Use this setting to limit the power level on client devices that associate to the access point in milliwatt. When a client device associates to the access point, the access point sends the maximum power level setting to the client.
Limit Client Power (dBm)	Use this setting to limit the power level on client devices that associate to the access point in decibel. When a client device associates to the access point, the access point sends the maximum power level setting to the client.

Table 5-6 **Radio-802.11b/g Settings (continued)**

Field	Description
Default Radio Channel	From the list, select the radio channel you want for a default. If you select Least Congested Frequency, the access point scans for the radio channel that is least busy and selects that channel for use. The device scans at power-up and when the radio settings are changed. Click See detail to verify which channels are applicable in your region.
Least Congested Channel Search	If you want to limit the channels the access point scans when the Default Radio Channel is set for Least Congested Frequency, select one or more channels from the list.
World Mode Multi-Domain Operation	Select one of the following: • Disable—Use this setting to not allow the access point to add channel carrier set information to its beacon. • Legacy—Use this setting to enable Cisco legacy world mode. • Dot11d—Use this setting to enable 802.11d world mode. When you use this setting, you must enter an ISO country code (for example, the ISO country code for the United States is US). You can find a list of ISO country codes at the ISO website.
Country Code (use only for Dot11d)	From the list, select the country code, then select either indoor or outdoor.
Radio Preamble	Select one of the following: • Short—Use this setting to improves throughput performance; Cisco Aironet's Wireless LAN Adapter supports short preambles. • Long—Use this setting to ensure compatibility between the access point and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A).
Receive Antenna	From the list, select one of the following: • Diversity—Use this setting if your access point has two fixed (non-removable) antennas; it tells the access point to use the antenna that receives the best signal. • Left—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's left connector. (When you look at the access point's back panel, the left antenna is on the left.) • Right—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's right connector. (When you look at the access point's back panel, the right antenna is on the right.)
Transmit Antenna	
External Antenna Configuration	Select one of the following: • Enable—Use this setting to configure the access point or bridge's antenna gain. • Disable—Use this setting to disable this feature.
Antenna Gain (dB)	Enter the desired antenna gain.

Table 5-6 Radio-802.11b/g Settings (continued)

Field	Description
Aironet Extensions	Select one of the following: • Enable—Use this setting to enable load balancing, Message Integrity Check (MIC), and WEP key hashing. • Disable—Use this setting to disable load balancing, Message Integrity Check (MIC), and WEP key hashing.
Ethernet Encapsulation Transform	Select one of the following: • RFC1042—Use this setting to ensure interoperability with non-Cisco Aironet wireless equipment. • 802.1H—Use this setting to provide optimum performance for Cisco Aironet wireless products.
Concatenation	Select one of the following: • Enable—Use this setting for packet concatenation on the bridge radio to combine multiple packets into one packet to reduce packet overhead and overall latency, and to increase transmission efficiency. • Disable—Use this setting to disable this feature. Click See detail to see for which device types or versions this setting is valid.
Max Length of Concatenation	Use this setting to specify a maximum size, in bytes, for concatenated packets.
Distance (Km)	Enter value between 0 and 99 that determines the length of the radio link propagation delay. Click See detail to see for which device types or versions this setting is valid.
Reliable Multicast to WGB	Select one of the following: • Disable—Use this setting to not allow reliable multicast to workgroup bridges. • Enable—Use this setting to allow reliable multicast to workgroup bridges.
Public Secure Packet Forwarding	Note Use this setting only if no VLAN is configured. If a VLAN is configured, then enable and disable PSPF by selecting Services > VLAN. Select one of the following: • Enable—Use this setting to enable use of the protected port for secure mode configuration. (No exchange of unicast, broadcast, or multicast traffic occurs between protected ports.) • Disable—Use this setting to disable the use of the port for secure mode configuration.

Table 5-6 **Radio-802.11b/g Settings (continued)**

Field	Description
Mobile Station	Select one of the following: • Enable—Use this setting to allow scanning by a mobile station for a better radio connection, which provides seamless roaming. • Disable—Use this setting to disable the feature.
Short Slot-Time	Select one of the following: • Enable—Use this setting to enable short slot time on the 802.11g, 2.4-GHz radio. Short slot time reduces the slot time from 20 microseconds to 9 microseconds, thereby increasing throughput. The access point uses short slot time only when all clients that are associated to the 802.11g radio can support short slot time. • Disable—Use this setting to disable this feature. Click See detail to see for which device types or versions this setting is valid.
Beacon Period	Enter the amount of time between beacons in kilomicroseconds. (One kilomicrosecond equals 1,024 microseconds.)
Data Beacon Rate (DTIM)	Enter the amount of time, always a multiple of the beacon period, to determine how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them. If the beacon period is set at 100, its default setting, and the data beacon rate is set at 2, its default setting, then the access point sends a beacon containing a DTIM every 200 kilomicrosecond.
Max. Data Retries	Enter the maximum number of attempts the access point makes to send a packet before giving up and dropping the packet.
RTS Max. Retries	Enter the maximum number of times the access point issues an RTS before stopping the attempt to send the packet through the radio.
Fragmentation Threshold	Enter a setting to 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. Click See detail for the maximum fragmentation threshold value for access points.
RTS Threshold	Enter a setting to determine the packet size at which the access point issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the access point, or in areas where the clients are far apart and can detect only the access point and not each other. Click See detail for the maximum RTS threshold value for access points.

Table 5-6 *Radio-802.11b/g Settings (continued)*

Field	Description
Repeater Parent AP Timeout	Enter a timeout value in seconds that determines how long the repeater attempts to associate to a parent access point before trying the next parent in the list.
Repeater Parent AP MAC1 through MAC 4	Enter the MAC address for the access point to which the repeater should associate. You can enter MAC addresses for up to four parent access points. The repeater attempts to associate to MAC address 1 first; if that access point does not respond, the repeater tries the next access point in its parent list.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Radio-802.11a Settings

Use this option to configure the device's 802.11a radio.

Procedure

Step 1 Select **Network Interfaces > Radio-802.11a**. The Network Interfaces: Radio-802.11a dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-7 *Radio-802.11a Settings*

Field	Description
Enable Radio	Select one of the following: • Enable—Use this setting to allow the access point to send packets through its 802.11a radio interface and monitor when other devices use the 802.11a radio interface to send packets. • Disable—Use this setting to change the administrative state of the radio from up to down.

Table 5-7 Radio-802.11a Settings (continued)

Field	Description
Role in Radio Network (Fallback mode upon loss of Ethernet connection)	This setting is used to configure a fallback role for the access point. The access point automatically assumes the fallback role when its Ethernet port is disabled or disconnected from the wired LAN. Select one of the following: - Access Point Root (Fallback to Radio Island)—Use this setting to enable wireless clients to continue to associate even when there is no connection to the wired LAN. - Access Point Root (Fallback to Radio Shutdown)—Use this setting to force the clients to associate to another access point, if one is available, when the radio shuts down because the wired connection is lost. - Access Point Root (Fallback to Repeater)—Use this setting for a root access point to become a repeater and associate to a nearby root access point when the wired connection is lost. - Repeater Non-Root—Use this setting if the access point is not connected to the wired LAN. Client data is transferred to the access point selected as the repeater parent. - Scanner Access Point—Select to specify that the access point is a Scanning AP, which is used to guard certain air space from any potential intruders that operate on the same frequency band. - Workgroup Bridge—Use this setting to specify that the device is a workgroup bridge. Access points and bridges normally treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges.
	- Bridge Root without Clients—Use this setting to designate one device in each group of bridges as the root bridge. A root bridge can only communicate with non-root bridges and other client devices and cannot associate with another root bridge. - Bridge Root with Clients—Use this setting to designate a device as the root bridge with clients. - Bridge Non-Root without Clients—Use this setting to specify that the bridge operates as a non-root bridge and must associate to a root bridge. - Bridge Root with Clients—Use this setting to designate a device as the root bridge with clients. - Install Mode—Select to configure a bridge for installation mode. In installation mode, the bridge flashes its LEDs to indicate received signal strength (RSSI), which assists in antenna alignment. Click See detail to see for which device types or versions this setting is valid.

Table 5-7 Radio-802.11a Settings (continued)

Field	Description
Data Rates	- Click one of the following to automatically set the data transmission rates: - Best Range—Use this setting to maximize the access point's range; however, it might reduce throughput. - Best Throughput—Use this setting to maximize the data volume handled by the access point; however, it might reduce the access point's range. - Default—Use this setting to compromise between range and throughput, providing good range and good throughput. Or - Select one of the following to manually set the data transmission rates: - Require—Use this setting to enable transmission at this rate for all packets, both unicast and multicast. At least one data rate must be set to Require. A client must support a required rate before it can associate. - Enable—Use this setting to enable transmission at this rate for unicast packets only. - Disable—Use this setting to not allow transmission at this rate.
Transmitter Power (mW)	Select the power level of the access point's radio transmission. Note Government regulations define the highest allowable power level for radio devices. This setting must conform to established standards for the country in which you use the device. To reduce interference, limit the range of your access point, or conserve power, select a lower power setting. For a list of maximum power levels allowed in each regulatory domain refer to one of the following: - URL: http://www.cisco.com/en/US/products/hw/wireless/ps430/products_command_reference_chapter09186a0080147d8b.html#87443 - Cisco IOS Commands for Access in the <i>Cisco Aironet 1200 Series Access Point Command Reference</i>. Click See detail to see for which device types or versions this setting is valid.
Transmitter Power (dBm)	Select the power level of the bridge's radio transmission: Maximum power is regulated by the regulatory agency in the country of operation and is set during manufacture of the bridge. Click See detail to see for which device types or versions this setting is valid. Click Power Translation Table mW/dBm to see the mapping values for transmitter power.

Table 5-7 Radio-802.11a Settings (continued)

Field	Description
Client Power Local	Use this setting to limit the power level on client devices that associate to the access point to the same setting as the AP's configured transmitter power. Note Setting the client's power level to the same as the AP transmitter power provides improved interference control in the WLAN. Note If you disable this option, you should use one of the Limit Client Power fields (see below) to set the client's power level to a specific value. Click See detail to see for which device types or versions this setting is valid.
Limit Client Power (mW)	Use this setting to limit the power level on client devices that associate to the access point. When a client device associates to the access point, the access point sends the maximum power level setting to the client. Click See detail to see for which device types or versions this setting is valid.
Limit Client Power (dBm)	Use this setting to limit the power level on client devices that associate to the access point. When a client device associates to the access point, the access point sends the maximum power level setting to the client. Click See detail to see for which device types or versions this setting is valid.
Default Radio Channel	From the list, select the radio channel you want for a default. If you select Least Congested Frequency, the access point scans for the radio channel that is least busy and selects that channel for use. The device scans at power-up and when the radio settings are changed. Click See detail for information on valid settings.
Least Congested Channel Search	If you want to limit the channels the access point scans when the Default Radio Channel is set for Least Congested Frequency, select one or more channels from the list.
World Mode Multi-Domain Operation	Select one of the following: • Disable—Use this setting to not allow the access point to add channel carrier set information to its beacon. • Legacy—Use this setting to enable Cisco legacy world mode. • Dot11d—Use this setting to enable 802.11d world mode. When you use this setting, you must enter an ISO country code (for example, the ISO country code for the United States is US). You can find a list of ISO country codes at the ISO website. Click See detail to see for which device types or versions this setting is valid.
Country Code (use only for Dot11d)	From the list, select the country code, then select one either Indoor or Outdoor.

Table 5-7 Radio-802.11a Settings (continued)

Field	Description
Receive Antenna	From the list, select one of the following:
Transmit Antenna	• Diversity—Use this setting if your access point has two fixed (non-removable) antennas; it tells the access point to use the antenna that receives the best signal. • Left—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's left connector. (When you look at the access point's back panel, the left antenna is on the left.) • Right—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's right connector. (When you look at the access point's back panel, the right antenna is on the right.) Click See detail to see for which device types or versions this setting is valid.
External Antenna Configuration	Select one of the following: • Enable—Use this setting to configure the access point or bridge's antenna gain. • Disable—Use this setting to disable this feature. Click See detail to see for which device types this setting is valid.
Antenna Gain (dB)	Enter the desired antenna gain.
Aironet Extensions	Select one of the following: • Enable—Use this setting to enable load balancing, Message Integrity Check (MIC), and WEP key hashing. • Disable—Use this setting to disable load balancing, Message Integrity Check (MIC), and WEP key hashing. Click See detail to see for which device types or versions this setting is valid.
Ethernet Encapsulation Transform	Select one of the following: • RFC1042—Use this setting to ensure interoperability with non-Cisco Aironet wireless equipment. • 802.1H—Use this setting to provide optimum performance for Cisco Aironet wireless products.
Concatenation	Select one of the following: • Enable—Use this setting for packet concatenation on the bridge radio to combine multiple packets into one packet to reduce packet overhead and overall latency, and to increase transmission efficiency. • Disable—Use this setting to disable this feature. Click See detail to see for which device types or versions this setting is valid.
Max Length of Concatenation	Use this setting to specify a maximum size, in bytes, for concatenated packets.

Table 5-7 **Radio-802.11a Settings (continued)**

Field	Description
Distance (Km)	Enter value between 0 and 99 that determines the length of the radio link propagation delay. Click See detail to see for which device types or versions this setting is valid.
Reliable Multicast to WGB	Select one of the following: • Enable—Use this setting to allow reliable multicast to workgroup bridges. • Disable—Use this setting to not allow reliable multicast to workgroup bridges. Click See detail to see for which device types or versions this setting is valid.
Public Secure Packet Forwarding	Note Use this setting only if no VLAN is configured. If a VLAN is configured, then enable and disable PSPF by selecting Services > VLAN. Select one of the following: • Enable—Use this setting to enable use of the protected port for secure mode configuration. (No exchange of unicast, broadcast, or multicast traffic occurs between protected ports.) • Disable—Use this setting to disable the use of the port for secure mode configuration. Click See detail to see for which device types or versions this setting is valid.
Beacon Period	Enter the amount of time between beacons in kilomicroseconds. (One kilomicrosecond equals 1,024 microseconds.)
Data Beacon Rate (DTIM)	Enter the amount of time, always a multiple of the beacon period, to determine how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them. If the beacon period is set to 100, its default setting, and the data beacon rate is set to 2, its default setting, then the access point sends a beacon containing a DTIM every 200 kilomicrosecond. Click See detail to see for which device types or versions this setting is valid.
Max. Data Retries	Enter the maximum number of attempts the access point makes to send a packet before giving up and dropping the packet.
RTS Max. Retries	Enter the maximum number of times the access point issues an RTS before stopping the attempt to send the packet through the radio.

Table 5-7 Radio-802.11a Settings (continued)

Field	Description
Fragmentation Threshold	Enter a setting to 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. Click See detail to see for which device types or versions this setting is valid.
RTS Threshold	Enter a setting to determine the packet size at which the access point issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the access point, or in areas where the clients are far apart and can detect only the access point and not each other. Click See detail to see for which device types or versions this setting is valid.
Repeater Parent AP Timeout	Enter a timeout value in seconds that determines how long the repeater attempts to associate to a parent access point before trying the next parent in the list. Click See detail to see for which device types or versions this setting is valid.
Repeater Parent AP MAC1 though MAC 4	Enter the MAC address for the access point to which the repeater should associate. You can enter MAC addresses for up to four parent access points. The repeater attempts to associate to MAC address 1 first; if that access point does not respond, the repeater tries the next access point in its parent list.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Defining Security Settings

Use this option to configure the device's security settings.

Procedure

- Step 1** Select **Security**. The menu expands and the Security: Admin Access dialog box displays in the right pane.
- Step 2** Select one of the following from the menu:
- Admin Access—See [Configuring Admin Access Settings, page 5-34](#).
 - SSID 802.11b/g—See [Configuring SSID 802.11b/g Settings, page 5-36](#).

- SSID 802.11a—See [Configuring SSID 802.11a Settings, page 5-43](#).
 - WEP 802.11b/g—See [Configuring WEP 802.11b/g Settings, page 5-49](#).
 - WEP 802.11a—See [Configuring WEP 802.11a Settings, page 5-51](#).
 - Server Manager—See [Configuring Server Manager Settings, page 5-55](#).
 - Advanced Security—See [Configuring Advanced Security, page 5-59](#).
 - Local Radius Server—See [Setting Up the Local RADIUS Server, page 5-62](#).
-

Configuring Admin Access Settings

Use this option to add users to the system, remove users from the system, and assign user capabilities.

Procedure

Step 1 Select **Security > Admin Access**. The Security: Admin Access dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-8 **Admin Access Settings**

Field	Description
Corporate Server	Select the type of server: RADIUS or TACACS+.

Table 5-8 Admin Access Settings (continued)

Field	Description
Administrator Authenticated by	Select one of the following: - Default Authentication (Global Password)—Use this setting to skip the username and enter only a password. You will need to enter the password in the Default Authentication (Global Password field below). - Local User List Only (Individual Password)—Use this setting to designate the local user list for authentication. You will need to have at least one Read-Write user in the Local User List on the access point or in the Local User List field below. - Authentication Server Only—Use this setting to designate the server for authentication. - Authentication Server if not found in Local List—Use this setting to designate the server for authentication if not in the local list. You will need to have at least one Read-Write user in the Local User List on the access point or in the Local User List field below. - Local List if no response from Authentication Server—Use this setting to designate the local list for authentication if there is no response from the server. - Enable Authentication Server Caching—Use this setting to enable AAA authentication caching. Click See detail to see for which versions this setting is valid.
Default Authentication (Global Password)	
Default Authentication Password	Enter the password to be used as the default.
Confirm Authentication Password	Reenter the password.
Local User List (Individual Passwords)	
User List	Lists the existing users. To delete a username from the list, select it, then click Delete.
Username	Enter the username.
Password	Enter the password
Confirm Password	Reenter the password
Capability Settings	Select one of the settings, then click Add .
Delete Users	
User ID	Enter the user identification, then click >>.
Users to Delete	Lists the users to be deleted. To remove users from the list, click <<

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).

- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring SSID 802.11b/g Settings

Use this option to configure SSID 802.11b and 802.11g settings.

Procedure

- Step 1** Select **Security > SSID 802.11b/g**. The Security: SSID Manager 802.11b/g dialog box appears.
- Step 2** Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-9 SSID 802.11b/g Settings

Field	Description
SSID List	Lists the currently configured SSIDs. To delete an SSID from the list, select it, then click Delete .
SSID	Enter any alphanumeric, case-sensitive string, from 1 to 32 characters long. The SSID is a unique identifier that clients use to associate with the radio.
VLAN	Enter the identification number or the name of the VLAN.
Network ID	Enter the network identification number.

Table 5-9 SSID 802.11b/g Settings (continued)

Field	Description
Authentication Methods Accepted	
Open Authentication	Select one of the following from the list: • MAC Authentication—Use this setting to specify that client devices that associate to the access point with open authentication, use MAC authentication. • EAP—Use this setting to specify that client devices that associate to the access point with open authentication, use EAP authentication. • MAC Authentication and EAP—Use this setting to allow client devices that associate to the access point using 802.11 open authentication to first attempt MAC authentication; if MAC authentication succeeds, the client device joins the network. If MAC authentication fails, the access point waits for the client device to attempt EAP authentication. • MAC Authentication or EAP—Use this setting to allow client devices that associate to the access point using open authentication to first attempt MAC authentication. If MAC authentication succeeds, the client device joins the network; if the client is also using EAP authentication, it attempts to authenticate using EAP. If MAC authentication fails, the access point waits for the client device to attempt EAP authentication. • Optional EAP—Use this setting to allow both Open clients and EAP clients to associate and become authenticated with either authentication method.
Shared Authentication	Select one of the following from the list: • MAC Authentication—Use this setting to specify that client devices that associate to the access point with shared authentication, use MAC authentication. • EAP—Use this setting to specify that client devices that associate to the access point with shared authentication, use EAP authentication. • MAC Authentication and EAP—Use this setting to specify that client devices that associate to the access point with shared authentication, use MAC and EAP authentication.
Network EAP	Select the following from the list: MAC Authentication—Use this setting to specify that client devices that associate to the access point with network EAP authentication, use MAC authentication.

Table 5-9 SSID 802.11b/g Settings (continued)

Field	Description
Server Priorities	
EAP Authentication Servers	Select one of the following: • Use Defaults—Use this setting to use the defaults. • Use Server Group—Use this setting to specify a server group then enter the group name. • Customize—Use this setting to create a new server group. • New Group Name—Enter a name for the new group. • Priority—Enter the server IP address or hostname. – Auth Port—Enter the authentication port. – Acct Port—Enter the accounting port. or – Select a name from the list.
MAC Authentication Servers	
Authenticated Key Management	From the list, select one of the following: • None—Use this setting to indicate you do not want to use authenticated key management. • Mandatory—Use this setting to indicate authenticated key management is mandatory. • Optional—Use this setting to indicate authenticated key management is optional.
CCKM	Note For 802.11b/g, you can select both CCKM and WPA. Select this option to use Cisco Centralized Key Management (CCKM). Using CCKM, authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network acts as a wireless domain services (WDM) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDM's cache of credentials reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point. Note To enable CCKM for an SSID, you must configure network-EAP authentication.
WPA	Note For 802.11b/g, you can select both CCKM and WPA. Select this option to use Wi-Fi Protected Access (WPA). The WPA key management uses a combination of encryption methods to protect communication between client devices and the access point. If authentication key management is WPA, the client and authentication server authenticate to each other using an EAP authentication method (e.g., EAP-TLS) and generate a Pairwise Master Key. Note To enable WPA for an SSID, you must also enable Open authentication and/or Network EAP.

Table 5-9 SSID 802.11b/g Settings (continued)

Field	Description
Authentication Methods Accepted	
Open Authentication	Select one of the following from the list: • MAC Authentication—Use this setting to specify that client devices that associate to the access point with open authentication, use MAC authentication. • EAP—Use this setting to specify that client devices that associate to the access point with open authentication, use EAP authentication. • MAC Authentication and EAP—Use this setting to allow client devices that associate to the access point using 802.11 open authentication to first attempt MAC authentication; if MAC authentication succeeds, the client device joins the network. If MAC authentication fails, the access point waits for the client device to attempt EAP authentication. • MAC Authentication or EAP—Use this setting to allow client devices that associate to the access point using open authentication to first attempt MAC authentication. If MAC authentication succeeds, the client device joins the network; if the client is also using EAP authentication, it attempts to authenticate using EAP. If MAC authentication fails, the access point waits for the client device to attempt EAP authentication. • Optional EAP—Use this setting to allow both Open clients and EAP clients to associate and become authenticated with either authentication method.
Shared Authentication	Select one of the following from the list: • MAC Authentication—Use this setting to specify that client devices that associate to the access point with shared authentication, use MAC authentication. • EAP—Use this setting to specify that client devices that associate to the access point with shared authentication, use EAP authentication. • MAC Authentication and EAP—Use this setting to specify that client devices that associate to the access point with shared authentication, use MAC and EAP authentication.
Network EAP	Select the following from the list: MAC Authentication—Use this setting to specify that client devices that associate to the access point with network EAP authentication, use MAC authentication.

Table 5-9 SSID 802.11b/g Settings (continued)

Field	Description
Server Priorities	
EAP Authentication Servers	Select one of the following: • Use Defaults—Use this setting to use the defaults. • Use Server Group—Use this setting to specify a server group then enter the group name. • Customize—Use this setting to create a new server group. • New Group Name—Enter a name for the new group. • Priority—Enter the server IP address or hostname. – Auth Port—Enter the authentication port. – Acct Port—Enter the accounting port. or – Select a name from the list.
MAC Authentication Servers	
Authenticated Key Management	From the list, select one of the following: • None—Use this setting to indicate you do not want to use authenticated key management. • Mandatory—Use this setting to indicate authenticated key management is mandatory. • Optional—Use this setting to indicate authenticated key management is optional.
CCKM	Note For 802.11b/g, you can select both CCKM and WPA. Select this option to use Cisco Centralized Key Management (CCKM). Using CCKM, authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network acts as a wireless domain services (WDM) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDM's cache of credentials reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point. Note To enable CCKM for an SSID, you must configure network-EAP authentication.
WPA	Note For 802.11b/g, you can select both CCKM and WPA. Select this option to use Wi-Fi Protected Access (WPA). The WPA key management uses a combination of encryption methods to protect communication between client devices and the access point. If authentication key management is WPA, the client and authentication server authenticate to each other using an EAP authentication method (e.g., EAP-TLS) and generate a Pairwise Master Key. Note To enable WPA for an SSID, you must also enable Open authentication and/or Network EAP.

Table 5-9 SSID 802.11b/g Settings (continued)

Field	Description
WPA Pre-shared Key	Enter a key for the access point to support client devices using WPA key management. For versions earlier than 12.2(11)JA, Enter a WEP key. For 40-bit encryption, enter 10 hexadecimal digits; for 128-bit encryption, enter 26 hexadecimal digits. Select either ASCII or Hexadecimal. If you use hexadecimal, you must enter 64 hexadecimal characters (unencrypted key) to complete the 256-bit key. If you use ASCII, you must enter a minimum of 8 letters, numbers, or symbols, and the access point expands the key for you. Up to 63 ASCII characters are allowed.
EAP Client	
Username	Enter the username used for EAP authentication when the repeater access point is associating with a parent access point.
Password	Enter the EAP client password.
Association Limit	Enter the maximum number of clients that may associate to a particular SSID. This limit prevents access points from getting overloaded and helps to provide an adequate level of service to associated clients.
Broadcast this SSID in Beacon (BSSID)	Select one of the following: • Enable—Use this option to enable BSSID. • Disable—Use this option to disable BSSID.
Multiple Beacon Rate (DTIM)	Enter the rate at which the beacon sends a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them. For example, if the beacon period is set at 100, and the data beacon rate is set at 1, then the access point sends a beacon containing a DTIM every 100 Kmsecs. One Kmsec equals 1,024 microseconds.
Accounting	From the list, select one of the following: • Enable—Use this setting to indicate whether you want this server to record usage data of clients associating with the access point. • Disable—Use this setting to turn off accounting for your wireless network

Table 5-9 SSID 802.11b/g Settings (continued)

Field	Description
Accounting Server Priorities	Select one of the following: • Use Defaults—Use this setting to select the defaults. • Use Server Group—Use this setting to specify a server group, then enter the name of the group. • Customize—Use this setting to create a new server group, then enter the name of the group. • Priority—Enter the server IP address or hostname. • Auth Port—Enter the authentication port. – Acct Port—Enter the accounting port. or – Select a name from the list.
Advertise Extended Capabilities of this SSID	Select to enable advertising SSIDL IE information (only extended capabilities) in beacon/probe response. Advertise Wireless Provisioning Services (WPS) Support—Use this option to set WPS flag in the extended capabilities. Advertise the SSID as a Secondary Broadcast SSID—Use this option to send SSID name and capabilities in the SSIDL IE.
Enable IP Redirection on this SSID	Use this setting to redirect all packets sent from client devices associated to the SSID to a specific IP address. This is used primarily on wireless LANs serving handheld devices that use a central software application and are statically configured to communicate with a specific IP address. • IP Address—Enter the IP address. • IP Filter—Enter a filter name or choose from an existing one.

Step 3 Click **Save**.

Step 4 Complete the following to set Beacon Mode/Infrastructure SSID:

Table 5-10 Setting Beacon Mode/Infrastructure SSID

Field	Description
Set Infrastructure SSID	Enter the SSID that other access points and workgroup bridges use to associate to this access point. If you do not designate an SSID as the infrastructure SSID, infrastructure devices can associate to the access point using any SSID. Click Force infrastructure devices to associate only to this SSID if you want to enforce it.
Set Beacon Mode	• Single Beacon SSID—Use this option to disable the MBSSID for this interface. Enter the SSID for Guest mode. • Multiple Beacon SSID—Use this option to enable MBSSID for this interface. Guest mode is disabled.

Step 5 Complete the following:

Table 5-11 Setting MBSSID 802.11b/g Global Properties

Field	Description
Multiple BSSID	• Enable—Use this option to enable MBSSID on all the interfaces that support it. • Disable—Use this option to disable MBSSID on all the interfaces that support it.

Step 6 Complete the following to delete an SSID:

Table 5-12 Deleting SSID 802.11b/g

Field	Description
SSID	Enter the SSID you want to delete, then click >>. The SSID is added to the SSID to Delete list.
Remove this SSID Globally	Select this option to delete the SSID globally.
SSID to Delete	Lists the SSIDs to delete. To remove an SSID from this list, click <<.

Step 7 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring SSID 802.11a Settings

Use this option to configure SSID 802.11a settings.

Procedure

Step 1 Select **Security > SSID 802.11a**. The Security: SSID Manager 802.11a dialog box appears.

Step 2 Complete the following:



Note

Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-13 SSID 802.11a Settings

Field	Description
SSID List	Lists the currently configured SSIDs. To delete an SSID from the list, select it, then click Delete .
SSID	Enter any alphanumeric, case-sensitive string, from 1 to 32 characters long. The SSID is a unique identifier that clients use to associate with the radio. Click See detail to see for which device types or versions this setting is valid.
VLAN	Enter the identification number or the name of the VLAN.
Network ID	Enter the network identification number.
Authentication Methods Accepted	Click See detail to see for which device types or versions this setting is valid.
Open Authentication	Select one of the following from the list: • MAC Authentication—Use this setting to specify that client devices that associate to the access point with open authentication, use MAC authentication. • EAP—Use this setting to specify that client devices that associate to the access point with open authentication, use EAP authentication. • MAC Authentication and EAP—Use this setting to allow client devices that associate to the access point using 802.11 open authentication to first attempt MAC authentication; if MAC authentication succeeds, the client device joins the network. If MAC authentication fails, the access point waits for the client device to attempt EAP authentication. • MAC Authentication or EAP—Use this setting to allow client devices that associate to the access point using open authentication to first attempt MAC authentication. If MAC authentication succeeds, the client device joins the network; if the client is also using EAP authentication, it attempts to authenticate using EAP. If MAC authentication fails, the access point waits for the client device to attempt EAP authentication. • Optional EAP—Use this setting to allow both Open clients and EAP clients to associate and become authenticated with either authentication method.
Shared Authentication	Select one of the following from the list: • MAC Authentication—Use this setting to specify that client devices that associate to the access point with shared authentication, use MAC authentication. • EAP—Use this setting to specify that client devices that associate to the access point with shared authentication, use EAP authentication. • MAC Authentication and EAP—Use this setting to specify that client devices that associate to the access point with shared authentication, use MAC and EAP authentication.

Table 5-13 SSID 802.11a Settings (continued)

Field	Description	
Network EAP	Select the following from the list: MAC Authentication—Use this setting to specify that client devices that associate to the access point with network EAP authentication, use MAC authentication.	
Server Priorities		
EAP Authentication Servers	Select one of the following: • Use Defaults—Use this setting to use the defaults. • Use Server Group—Use this setting to specify a server group then enter the group name. • Customize—Use this setting to create a new server group. • New Group Name—Enter a name for the new group. • Priority—Enter the server IP address or hostname. – Auth Port—Enter the authentication port. – Acct Port—Enter the accounting port. or – Select a name from the list.	
MAC Authentication Servers		
Click See detail to see for which device types or versions this setting is valid.		
Authenticated Key Management		
Authenticated Key Management	From the list, select one of the following: • None—Use this setting to indicate you do not want to use authenticated key management. • Mandatory—Use this setting to indicate authenticated key management is mandatory. • Optional—Use this setting to indicate authenticated key management is optional.	
CCKM	Note To enable CCKM for an SSID, you must configure network-EAP authentication. 1. Select this option to use Cisco Centralized Key Management (CCKM). Using CCKM, authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network acts as a wireless domain services (WDM) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDM's cache of credentials reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point. 2. From the list, select one of the following: • Mandatory—Use this setting to indicate authenticated key management is mandatory. • Optional—Use this setting to indicate authenticated key management is optional.	

Table 5-13 SSID 802.11a Settings (continued)

Field	Description
WPA	Note To enable WPA for an SSID, you must also enable Open authentication and/or Network EAP. 1. Select this option to use Wi-Fi Protected Access (WPA). The WPA key management uses a combination of encryption methods to protect communication between client devices and the access point. If authentication key management is WPA, the client and authentication server authenticate to each other using an EAP authentication method (e.g., EAP-TLS) and generate a Pairwise Master Key. 2. From the list, select one of the following: – Mandatory—Use this setting to indicate authenticated key management is mandatory. – Optional—Use this setting to indicate authenticated key management is optional.
WPA Pre-shared Key	Enter a key for the access point to support client devices using WPA key management. For versions earlier than 12.2(11)JA, Enter a WEP key. For 40-bit encryption, enter 10 hexadecimal digits; for 128-bit encryption, enter 26 hexadecimal digits. Select either ASCII or Hexadecimal. If you use hexadecimal, you must enter 64 hexadecimal characters (unencrypted key) to complete the 256-bit key. If you use ASCII, you must enter a minimum of 8 letters, numbers, or symbols, and the access point expands the key for you. Up to 63 ASCII characters are allowed. Click See detail to see for which device types or versions this setting is valid.
EAP Client Username	Enter the username used for EAP authentication when the repeater access point is associating with a parent access point.
Password	Enter the EAP client password.
Association Limit	Enter the maximum number of clients that may associate to a particular SSID. This limit prevents access points from getting overloaded and helps to provide an adequate level of service to associated clients.
Broadcast this SSID in Beacon (BSSID)	Select one of the following: • Enable—Use this option to enable BSSID. • Disable—Use this option to disable BSSID.
Multiple Beacon Rate (DTIM)	Enter the rate at which the beacon sends a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them. For example, if the beacon period is set at 100, and the data beacon rate is set at 1, then the access point sends a beacon containing a DTIM every 100 Kmsecs. One Kmsec equals 1,024 microseconds.

Table 5-13 SSID 802.11a Settings (continued)

Field	Description
Accounting	From the list, select one of the following: • Enable—Use this setting to indicate whether you want this server to record usage data of clients associating with the access point. • Disable—Use this setting to turn off accounting for your wireless network. Click See detail to see for which device types or versions this setting is valid.
Accounting Server Priorities	Select one of the following: • Use Defaults—Use this setting to select the defaults. • Use Server Group—Use this setting to specify a server group, then enter the name of the group. • Customize—Use this setting to create a new server group, then enter the name of the group. • Priority—Enter the server IP address or hostname. • Auth Port—Enter the authentication port. – Acct Port—Enter the accounting port. or – Select a name from the list.
Advertise Extended Capabilities of this SSID	Select to enable advertising SSIDL IE information (only extended capabilities) in beacon/probe response.
	Advertise Wireless Provisioning Services (WPS) Support—Use this option to set WPS flag in the extended capabilities.
	Advertise the SSID as a Secondary Broadcast SSID—Use this option to send SSID name and capabilities in the SSIDL IE.
Enable IP Redirection on this SSID	Use this setting to redirect all packets sent from client devices associated to the SSID to a specific IP address. This is used primarily on wireless LANs serving handheld devices that use a central software application and are statically configured to communicate with a specific IP address. • IP Address—Enter the IP address. • IP Filter—Enter a filter name or choose from an existing one.

Step 3 Click **Save**.

Step 4 Complete the following to set Beacon Mode/Infrastructure SSID:

Table 5-14 Setting Beacon Mode/Infrastructure SSID

Field	Description
Set Infrastructure SSID	Enter the SSID that other access points and workgroup bridges use to associate to this access point. If you do not designate an SSID as the infrastructure SSID, infrastructure devices can associate to the access point using any SSID. Click Force infrastructure devices to associate only to this SSID if you want to enforce it.
Set Beacon Mode	- Single Beacon SSID—Use this option to disable the MBSSID for this interface. Enter the SSID for Guest mode. - Multiple Beacon SSID—Use this option to enable MBSSID for this interface. Guest mode is disabled.

Step 5 Complete the following:

Table 5-15 Setting MBSSID 802.11a Global Properties

Field	Description
Multiple Beacon BSSID	- Enable—Use this option to enable BSSID. - Disable—Use this option to disable BSSID.

Step 6 Complete the following to delete an SSID:

Table 5-16 Deleting SSID 802.11a

Field	Description
SSID	Enter the SSID you want to delete, then click >>. The SSID is added to the SSID to Delete list.
Remove this SSID Globally	Select this option to delete the SSID globally.
SSID to Delete	Lists the SSIDs to delete. To remove an SSID from this list, click <<.

Step 7 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring WEP 802.11b/g Settings

Use this option to select authentication types for the access point. The WEP keys allow you to encrypt radio signals sent by the device and decrypt radio signals received by the device.

Procedure

- Step 1** Select **Security > WEP 802.11b/g**. The Security: WEP Key Manager 802.11b/g dialog box appears.
- Step 2** Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-17 **WEP 802.11b/g Settings**

Field	Description
Set Encryption Mode and Keys for VLAN	Enter the VLAN for which you want to set the encryption mode and keys. If you enter None, properties are applied globally.
VLAN List	Lists the currently configured VLANs. To remove a VLAN from the list, select it, then click Delete .
Encryption Modes	
None	Select this option if the device communicates only with client devices that are not using WEP.
WEP Encryption	Select this option if you want to use WEP key encryption.
	From the list, select one of the following: - Optional—Use this option to allow client devices to communicate with the access point either with or without WEP. - Mandatory—Use this option to require client devices to use WEP when communicating with the access point. Devices not using WEP are not allowed to communicate.
	Select one of the following: - Cisco Compliant TKIP Features—Use this option to enable Temporal Key Integrity Protocol (TKIP). When TKIP is enabled, all WEP-enabled client devices associated to the access point must support WEP key hashing, or they will not be able to communicate with the access point. - Enable MIC—Use this setting if you to enable Message Integrity Check (MIC). When you enable MIC, only MIC-capable client devices can communicate with the access point. - Enable Per Packet Keying—Use this option to enable MIC on both the access point and all associated client devices. A few bytes are added to each packet to make the packets tamper-proof.

Table 5-17 **WEP 802.11b/g Settings (continued)**

Field	Description
Cipher	Select this option to enable Wi-Fi Protected Access (WPA) or Cisco Centralized Key Management (CCKM). Cipher suites are sets of encryption and integrity algorithms designed to protect radio communication on your wireless LAN. From the list, select the one of the cipher suites. • WEP 128 bit—Use this option to specify that 128-bit WEP is included in the cipher suite. • WEP 40 bit—Use this option to specify that 40-bit WEP is included in the cipher suite. • TKIP—Temporal key integrity protocol is the most secured cipher suite. • CKIP—Cisco Key Integrity Protocol is Cisco's WEP key permutation technique based on an early algorithm. • CMIC—Cisco Message Integrity Check is Cisco's message integrity check mechanism designed to detect forgeries attracts. • CKIP + CMIC—See description for CKIP and CMIC. • TKIP+WEP 128 bit—See description for TKIP and WEP 128 bit. • TKIP+WEP 40 bit—See description for TKIP and WEP 40 bit. • AES CCMP—Advanced Encryption Standard of symmetric block cipher that encrypts and decrypt data using keys of 128, 192, and 256 bits.
	• AES CCMP+TKIP—See description for AES CCMP and TKIP. • AES CCMP+TKIP+WEP 128 bit—See description for AES CCMP, TKIP, and WEP 128 bit. • AES CCMP+TKIP+WEP 40 bit—See description for AES CCMP, TKIP, and WEP 40 bit.
WEP Keys	
Encryption Keys 1 through 4	
Transmit Key	Select to indicate this is the key you want to use to transmit packets. Only one key can be selected at a time.
Encryption Key	Enter the type of encryption key used: • For 40-bit WEP keys, enter as 10 hexadecimal digits (0-9, a-f, or A-F). • For 128-bit WEP keys, enter as 26 hexadecimal digits (0-9, a-f, or A-F).
Key Size	From the list, select one of the following: • 40 bit • 128 bit

Table 5-17 WEP 802.11b/g Settings (continued)

Field	Description
Broadcast Key Rotation Interval	Select one of the following: • Disable Rotation—Use this setting to disable broadcast key rotation. • Enable Rotation with Interval—Use this setting for the access point to provide a dynamic broadcast WEP key and to change it at the selected interval.
WPA Group Key Update	Select the appropriate checkbox to determine how frequently the access point changes and distributes the group key to WPA-enabled client devices. • Enable Group Key Update on Membership Termination—Select this setting if clients do not roam frequently among access points. The access point generates and distributes a new group key when any authenticated station disassociates from the access point. This option keeps the group key private to only currently active members. However, it may generate some overhead if clients in your network roam frequently. • Enable Group Key Update on Member's Capability Change—Use this setting, when in WPA migration mode, to improve the security of the key management capable clients when there are no legacy clients associated to the access point. The access point generates and distributes a dynamic group key when the last non-key management (static WEP) client disassociates, and it distributes the statically configured WEP key when the first non-key management (static WEP) client authenticates.

Step 3 Click **Save**. The VLAN is added to the list box.

Step 4 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring WEP 802.11a Settings

Use this option to select authentication types for the access point. The WEP keys allow you to encrypt radio signals sent by the device and decrypt radio signals received by the device.

Procedure

Step 1 Select **Security > WEP 802.11a**. The Security: WEP Key Manager 802.11a dialog box appears.

Step 2 Complete the following:

**Note**

Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-18 **WEP 802.11a Settings**

Field	Description
Set Encryption Mode and Keys for VLAN	Enter the VLAN for which you want to set the encryption mode and keys. If you enter None, properties are applied globally.
VLAN List	Lists the currently configured VLANs. To remove a VLAN from the list, select it, then click Delete .
Encryption Modes	
None	Select this option if the device communicates only with client devices that are not using WEP.
WEP Encryption	Select this option if you want to use WEP key encryption.
	From the list, select one of the following: - Optional—Use this option to allow client devices to communicate with the access point either with or without WEP. - Mandatory—Use this option to require client devices to use WEP when communicating with the access point. Devices not using WEP are not allowed to communicate.
	Select one of the following: - Cisco Compliant TKIP Features—Use this option to enable Temporal Key Integrity Protocol (TKIP). When TKIP is enabled, all WEP-enabled client devices associated to the access point must support WEP key hashing, or they will not be able to communicate with the access point. - Enable MIC—Use this setting if you to enable Message Integrity Check (MIC). When you enable MIC, only MIC-capable client devices can communicate with the access point. - Enable Per Packet Keying—Use this option to enable MIC on both the access point and all associated client devices. A few bytes are added to each packet to make the packets tamper-proof.

Table 5-18 WEP 802.11a Settings (continued)

Field	Description
Cipher	Select this option to enable Wi-Fi Protected Access (WPA) or Cisco Centralized Key Management (CCKM). Cipher suites are sets of encryption and integrity algorithms designed to protect radio communication on your wireless LAN. From the list, select the one of the cipher suites. • WEP 128 bit—Use this option to specify that 128-bit WEP is included in the cipher suite. • WEP 40 bit—Use this option to specify that 40-bit WEP is included in the cipher suite. • TKIP—Temporal key integrity protocol is the most secured cipher suite. • CKIP—Cisco Key Integrity Protocol is Cisco's WEP key permutation technique based on an early algorithm. • CMIC—Cisco Message Integrity Check is Cisco's message integrity check mechanism designed to detect forgeries attracts. • CKIP + CMIC—See description for CKIP and CMIC. • TKIP+WEP 128 bit—See description for TKIP and WEP 128 bit. • TKIP+WEP 40 bit—See description for TKIP and WEP 40 bit. • AES CCMP—Advanced Encryption Standard of symmetric block cipher that encrypts and decrypt data using keys of 128, 192, and 256 bits.
	• AES CCMP+TKIP—See description for AES CCMP and TKIP. • AES CCMP+TKIP+WEP 128 bit—See description for AES CCMP, TKIP, and WEP 128 bit. • AES CCMP+TKIP+WEP 40 bit—See description for AES CCMP, TKIP, and WEP 40 bit.
WEP Keys	
Encryption Keys 1 through 4	
Transmit Key	Select to indicate this is the key you want to use to transmit packets. Only one key can be selected at a time.
Encryption Key	Enter the type of encryption key used: • For 40-bit WEP keys, enter as 10 hexadecimal digits (0-9, a-f, or A-F). • For 128-bit WEP keys, enter as 26 hexadecimal digits (0-9, a-f, or A-F).
Key Size	From the list, select one of the following: • 40 bit • 128 bit

Table 5-18 **WEP 802.11a Settings (continued)**

Field	Description
Broadcast Key Rotation Interval	Select one of the following: • Disable Rotation—Use this setting to disable broadcast key rotation. Click See detail to see for which device types or versions this setting is valid. • Enable Rotation with Interval—Use this setting for the access point to provide a dynamic broadcast WEP key and to change it at the selected interval.
WPA Group Key Update	Select the appropriate checkbox to determine how frequently the access point changes and distributes the group key to WPA-enabled client devices. • Enable Group Key Update on Membership Termination—Select this setting if clients do not roam frequently among access points. The access point generates and distributes a new group key when any authenticated station disassociates from the access point. This option keeps the group key private to only currently active members. However, it may generate some overhead if clients in your network roam frequently. Click See detail to see for which device types or versions this setting is valid. • Enable Group Key Update on Member's Capability Change—Use this setting, when in WPA migration mode, to improve the security of the key management capable clients when there are no legacy clients associated to the access point. The access point generates and distributes a dynamic group key when the last non-key management (static WEP) client disassociates, and it distributes the statically configured WEP key when the first non-key management (static WEP) client authenticates.

Step 3 Click **Save**. The VLAN is added to the list box.

Step 4 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Server Manager Settings

Use this option to enter the authentication settings. The RADIUS server on the your network uses EAP to provide authentication service for wireless client devices.

Procedure

- Step 1** Select **Security > Server Manager**. The Security: Server Manager dialog box appears.
- Step 2** Complete the following to add a server to the list:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-19 Backup Radius Server

Field	Description
Backup Radius Server	Select one of the following:
Click See detail to see for which device types or versions this setting is valid.	- Create—Use this setting to create a backup RADIUS server. - Delete—Use this setting to delete a backup RADIUS server.
Backup Radius Server	Enter the hostname or IP address of the RADIUS server you are either creating or deleting.
Shared Secret	Enter the server's shared secret.
Corporate Servers	
Current Server List	Lists the servers that are currently configured. To remove a server from the list, select it, then click Delete .
RADIUS	Select this option if you are configuring settings for RADIUS.
TACACS+	Select this option if you are configuring settings for TACACS+.
Server	Enter the hostname or IP address for the selected server.
Shared Secret	Enter the shared secret used by your server.
Authentication Port	Enter the port number your server uses for authentication. Enter the port number the server uses for authentication.
Accounting Port	Enter the port number your server uses for accounting.

- Step 3** Click **Save**. The server appears on the list.
- Step 4** To delete a server from the list, select it from the list, then click **Delete**.

Step 5 Complete the following to set default server priorities:

Table 5-20 **Default Server Priority Settings**

Field	Description
EAP Authentication	• Priority—Enter the server IP address or hostname. • Auth Port—Enter the authentication port used by the server. • Acct Port—Enter the accounting port used by the server.
MAC Authentication	
Click See detail to see for which device types or versions this setting is valid.	
Accounting	
Click See detail to see for which device types or versions this setting is valid.	
Admin Authentication (RADIUS)	
Admin Authentication (TACACS+)	

Step 6 Complete the following to set global server properties:

Table 5-21 Global Server Properties

Field	Description
Accounting Update Interval	Enter the interval at which the accounting updates should be performed. The accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming.
TACACS+ Server Timeout	Enter the number of seconds the access point should wait before resending the request.
RADIUS Server Timeout	Enter the number of seconds the access point should wait before resending the request.
RADIUS Server Retransmit Retries	Enter the number of seconds the access point should wait before giving up contacting the server.
Dead RADIUS Server List	When a server is found to be unresponsive after numerous retransmissions and time-outs, it is assumed to be dead and is put in a dead server list. Select one of the following: • Disable—Use this setting to disable the feature. • Enable; Server remains on list for—Use this setting to enable the feature and to set the length of time for which the server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours).
RADIUS Calling/Called Station ID Format	Use this setting to indicate the format of the Called Station ID and Calling Station ID. field in the authentication packets sent to the RADIUS server. Select one of the following: • Default—Use this setting to implement the Cisco IOS MAC address format. • IETF—Use this setting to implement the standard recommended by the IETF document. • Unformatted— Use this setting to implement the MAC address format used in non-IOS access points.
RADIUS Attributes	
Remove Existing WISPr Location-ID	Select to remove the existing location identification configured on the access point, which is sent with authentication and account requests, and use the ISO and E.164 country codes, and E.164 area code instead.
ISO Country Code	Enter a unique two-letter code. Information about the ISO 3166 country codes can be found at the following URL: http://www.iso.ch/iso/en/prods-services/iso3166ma/index.html

Table 5-21 Global Server Properties (continued)

Field	Description
E.164 Country Code	Enter a three-digit code for special uses. Information about the ISO 3166 country codes can be found at the following URL: http://www.iso.ch/iso/en/prods-services/iso3166ma/index.html .
E.164 Area Code	Enter a three-digit code based on the International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T) recommendations. Information about ITU-T can be found at the following URL: http://www.itu.int/ITU-T/

Step 7 Complete the following to delete RADIUS servers:

Table 5-22 Deleting Servers and Server Groups

Field	Description
Servers to Delete	Lists the servers to delete. To delete a server from the list, select it, then click Delete .
Delete Server	Enter the server you want to delete, then select either RADIUS or TACACS+.
Authentication Port	Enter the port number your RADIUS/TACACS+ server uses for authentication.
Accounting Port	Enter the port number your RADIUS/TACACS+ server uses for accounting.
From Group	Enter the name of the group from which you want to delete the server.
Delete Server also?	If you want to delete the server from the group and delete the server itself.. Click Add Server to Delete List and the server name is added to the Servers to Delete.

Step 8 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Advanced Security

Use this option to set up the access point to authenticate client devices using a combination of MAC-based and EAP authentication.

When you enable this feature, client devices that associate to the access point using 802.11 open authentication first attempt MAC authentication. If MAC authentication succeeds, the client device joins the network. If the client is also using EAP authentication, it attempts to authenticate using EAP. If MAC authentication fails, the access point waits for the client device to attempt EAP authentication.

Procedure

Step 1 Select **Security > Advanced Security**. The Security: Advanced Security dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-23 *Advanced Security*

Field	Description
MAC Address Authentication	
Click See detail to see for which device types or versions this setting is valid.	
MAC Addresses Authenticated by	Select one of the following: - Local List Only—Use this setting if you want the authentication to be stored on the access point, and enter MAC addresses. - Authentication Server Only—Use this setting if you want the authentication to be stored on the server. - Authentication Server if not found in Local List—Use this setting if you want to try MAC authentication list first and then automatically try the Authentication server list.
Local MAC Address List	
Click See detail to see for which device types or versions this setting is valid.	
Local List	The local MAC address list is displayed in this listbox. To delete an entry from the list, select it, then click Delete .
New MAC Address	Enter the MAC address, then click Add . Click Add MAC Address from file to open a window that allows you to browse for a file of MAC addresses, if you have created one. To see an example of a file, click Sample File . After you have located the sample file containing the MAC addresses, click OK .

Table 5-23 Advanced Security (continued)

Field	Description
Radio0-802.11B/G EAP Authentication	
EAP Reauthentication Interval	Select one of the following: • Disable Reauthentication—Use this setting to disable reauthentication. • Enable Reauthentication with Interval—Use this setting to enter the interval in seconds that the access point waits before forcing an authenticated client to reauthenticate. • Enable Reauthentication with Interval given by Authentication Server—Use this setting to use the reauthentication period specified by the authentication server.
EAP Client Timeout	Enter the number of seconds the access point should wait for a reply from a client attempting to authenticate before the authentication fails.
TKIP MIC Failure Holdoff Time	Select one of the following: • Disable Holdoff—Use this setting to disable the TKIP MIC failure holdoff feature. • Enable Holdoff with Interval—Use this setting to enable the TKIP MIC failure hold time. The number of seconds you enter specifies the amount of time the access point blocks all TKIP clients on the interface.
Radio0-802.11A EAP Authentication	
EAP Reauthentication Interval	Select one of the following: • Disable Reauthentication—Use this setting to disable reauthentication. • Enable Reauthentication with Interval—Use this setting to enter the interval in seconds that the access point waits before forcing an authenticated client to reauthenticate. • Enable Reauthentication with Interval given by Authentication Server—Use this setting to use the reauthentication period specified by the authentication server.
EAP Client Timeout	Enter the number of seconds the access point should wait for a reply from a client attempting to authenticate before the authentication fails.
TKIP MIC Failure Holdoff Time	Select one of the following: • Disable Holdoff—Use this setting to disable the TKIP MIC failure holdoff feature. • Enable Holdoff with Interval—Use this setting to enable the TKIP MIC failure hold time. The number of seconds you enter specifies the amount of time the access point blocks all TKIP clients on the interface.

Table 5-23 Advanced Security (continued)

Field	Description
Global Client Properties	
Click See detail to see for which device types or versions this setting is valid.	
Client Holdoff Time	Select one of the following: • Disable Holdoff--Use this setting to disable the client holdoff feature. • Enable Holdoff with Interval--Use this setting to specify the number of seconds a client device must wait before it can reattempt to authenticate following a failed authentication.
Association Access List	
Click See detail to see for which device types or versions this setting is valid.	
Filter client association with MAC address access list	Select one of the following: • Enable— Use this setting to enable a MAC address filter for clients who are trying to associate with the access point. • Disable—Use this setting to prevent clients from associating based on their MAC addresses.
Filter	Enter the MAC address filter or select one from the list.

- Step 3** Complete the following to delete local MAC addresses:
- Click **See detail** to see for which device types or versions this setting is valid.

Table 5-24 Deleting Local MAC Addresses

Field	Description
Delete Local MAC Addresses	
Click See detail to see for which device types or versions this setting is valid.	
MAC Address	Enter the address you want to delete, then click >>. The address is added to the MAC Addresses to Delete list.
MAC Addresses to Delete	Lists the MAC dress to delete. To remove an address from the list, select it, then click <<.

- Step 4** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
 - **Save** to save the template. See [Saving the Template, page 5-100](#).
 - Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Setting Up the Local RADIUS Server

Use this option to configure local server settings.

Procedure

- Step 1** Select **Security > Local Radius Server**. The Security: Local Radius Server - General Set-Up dialog box appears.



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

- Step 2** Complete the following:

Table 5-25 **Local Radius Server**

Field	Description
Local Radius Server Authentication Settings	
EAP-FAST	Select one of the following: • Enable—Use this option to enable authentication settings for this local Radius server. • Disable—Use this option to disable settings for this local Radius server.
LEAP	
MAC	
Network Access Server	
Click See detail to see for which device types or versions this setting is valid.	
Current Network Access Servers	Lists the network access servers. To remove a server from the list, select it, then click Delete .
Network Access Server	Enter the IP address of the RADIUS server.
Shared Secret	Enter the shared secret text string used between the access point and the RADIUS server.
User Groups	
Current User Group	Lists the user groups. To remove a group from the list, select it, then click Delete .
Group Name	Enter a name for the a new group.
Session Timeout	Use this setting to specify the maximum number of seconds of service to be provided to the user before the session terminates.
Number of Failed Authentications	Enter the number of times a user assigned to this group can provide an incorrect password; when the user fails this number of authentication attempts, the access point locks out the user. This setting helps prevent or delay password “dictionary” attacks.

Table 5-25 Local Radius Server (continued)

Field	Description
Lockout	Select one of the following: • Infinite—Use this setting to manually unlock any locked-out users. • Interval—Use this setting to specify the length of time that the access point locks out a user before the user can reattempt authentication.
VLAN ID	Enter the identification number of the VLAN.
SSID	Enter the SSID (any alphanumeric, case-sensitive string, from 1 to 32 characters long), then click Add .
SSID List	Lists all the SSIDs. To delete an SSID from the list, select it, then click Delete .
Individual User	
Current User List	Lists the current usernames. To remove a user from the list, select it, then click Delete .
Username	Enter the username.
Password	Enter the password, then select Text or NT Hash.
Confirm Password	Reenter the password.
Group Name	From the list, select the group name or None if the user does not belong to any group.
	MAC Authentication Only—Select to enable.
	Click Save to add the name to the current user list.
PAC Encryption Keys—Before a client can authenticate with an access point that is functioning as local RADIUS server, it needs a provision called PAC (Protected Access Credential).	
Primary Key	Enter a key to use for encryption or select Generate Random to have the system generate an encryption key.
Secondary Key	Enter a secondary key to use for encryption or click Copy from Primary .
PAC Content	
Authority Info	Enter information describing the authority information.
Authority ID	Enter an authority identification number for the access server.
Automatic PAC Provisioning—Use this setting when the client is auto-provision capable and is issued a PAC.	
Current User Group	Lists the current user groups.
User Group Name	Enter a user group name.
PAC Expiration	Enter the amount of time for which the issued PAC is valid.
PAC Grace Period	Enter the amount of time for a grace period after the PAC has expired. (The PAC can be used after it has expired as long as it is within the configured grace period.)
Out-of-Band PAC Generation—Use this setting when the client, using an IP address, accesses a machine in which PAC is stored.	

Table 5-25 Local Radius Server (continued)

Field	Description
Current User List	Lists the current usernames for out-of-band PAC generation.
User Name	Enter the user name.
TFTP File Server	Enter the IP address of the server in which PAC is stored.
PAC File Name	Enter the file name that contains the PAC information.
PAC Encryption Password	Enter the password to use to encrypt the PAC information.
PAC Expiration	Enter the time after which PAC becomes invalid, then click Generate PAC .
Delete Servers, Groups, and Users	
Server	Enter the server you want to delete, then click Add . The server name is added to the Servers to Delete list.
Servers to Delete	Select the server to delete from the list, then click Delete .
Group	Enter the group you want to delete, then click Add . The group name is added to the Groups to Delete list.
Groups to Delete	Select the group to delete from the list, then click Delete .
User	Enter the user you want to delete, then click Add . The user name is added to the Servers to Delete list.
Users to Delete	Select the user to delete from the list, then click Delete .
Delete PAC Encryption Keys, PAC Content	
Primary Key	Select an option to remove it.
Secondary Key	
Authority ID	
Authority Info	

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
 - **Save** to save the template. See [Saving the Template, page 5-100](#).
 - Another template category to configure more options. See [2.Template Categories, page 5-6](#).
-

Defining Services

Use this option to configure various system features and support services on the device.

Procedure

Step 1 Select **Services**. The menu expands and the Security: Telnet/SSH dialog box displays in the right pane.

Step 2 Select one of the following from the menu:

- Telnet/SSH—See [Configuring Telnet/SSH, page 5-65](#).
- Hot Standby—See [Configuring Hot Standby, page 5-67](#).
- CDP—See [Configuring CDP, page 5-68](#).
- DNS—See [Configuring DNS, page 5-69](#).
- MAC address filters—See [Configuring MAC Address Filters, page 5-70](#).
- IP filters—See [Configuring IP Filters, page 5-72](#).
- Ethertype filters—See [Configuring Ethertype Filters, page 5-75](#).
- HTTP—See [Configuring HTTP, page 5-77](#).
- QoS policies—See [Configuring QoS Policies, page 5-77](#).
- QoS radio 802.11b/g—See [Configuring QoS Radio 802.11b/g, page 5-81](#).
- QoS radio 802.11a—See [Configuring QoS Radio 802.11a, page 5-82](#).
- SNMP—See [Configuring SNMP, page 5-82](#).
- SNTP—See [Configuring SNTP, page 5-85](#).
- VLAN—See [Configuring VLAN, page 5-85](#).
- ARP Cache—See [Configuring ARP Cache, page 5-87](#).
- STP—See [Configuring STP, page 5-88](#).
- Packet Handle 802.11a—[Configuring Packet Handling 802.11a, page 5-90](#).

Configuring Telnet/SSH

Use this option to configure the access point to work through Telnet or SSH.

Procedure

Step 1 Select **Services > Telnet/SSH**. The Services: Telnet/SSH dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-26 *Telnet/SSH*

Field	Description
Telnet	Select one of the following: • Enable—Use this setting to enable Telnet access to the management system. • Disable—Use this setting to disable Telnet access to the management system.
Terminal Type	Select one of the following: • Teletype—Use this setting if your terminal emulator does not support ANSI. • ANSI—Use this setting to offer graphic features such as reverse video buttons and underlined links.
Columns	Enter a number to define the width of the terminal emulator display within the range of 64 characters to 132 characters.
Lines	Enter a number to define the height of the terminal emulator display within the range of 16 characters to 50 characters. Note For versions 12.3(8)JA and later, the default number of lines is reduced from 16 to 5. Therefore, this option generates a configuration for lines 0 to 4. To enable additional lines, use the Custom Values option to configure them.
Secure Shell Configuration	
Secure Shell	Select one of the following: • Enable—Use this setting to enable secure shell. Note You must enter values in the System Name and Domain Name fields to enable SSH. If you do not enter an RSA key size, it will default to 512. • Disable—Use this setting to disable secure shell. • Modify—Use this setting to modify secure shell.
System Name	Enter a system name for your access point.
Domain Name	Enter a domain name for your access point.
RSA Key Size	Enter the additional bits used for authentication. Note For SSH, you must enter a key size or it will remain disabled.
Authentication Timeout	Enter the timeout in seconds, not to exceed 120 seconds for the length of time for authentication to take place.
Authentication Retries	Enter the number of authentication retries.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Hot Standby

Use this option to configure an access point for hot standby mode. Hot standby mode designates an access point as a backup for another access point.

The standby access point is placed near the access point it monitors, and is configured exactly the same as the monitored access point.

The standby access point associates with the monitored access point as a client and queries the monitored access point regularly through both the Ethernet and the radio ports. If the monitored access point fails to respond, the standby access point comes online and takes the monitored access point's place in the network.

Procedure

Step 1 Select **Services > Hot Standby**. The Services: Hot Standby dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-27 Hot Standby

Field	Description
Hot Standby Mode	Select one of the following: • Enable—Use this setting to enable hot standby mode on the access point. • Disable—Use this setting to disable hot standby mode on the access point. • Modify—Use this setting to modify the hot standby mode. Click See detail to see for which device types or versions this setting is valid.
MAC Address for the Monitored 802.11b/g Radio	Enter the MAC address of the access point to be monitored.
MAC Address for the Monitored 802.11a Radio	
Polling Interval	Enter the number of seconds between queries that the access point sends to the monitored access point's radio and Ethernet ports.

Table 5-27 Hot Standby (continued)

Field	Description
Timeout for Each Polling	Enter the number of seconds the access point waits for a response from the monitored access point before it assumes that the monitored access point has malfunctioned.
Shutdown Primary Radios on Failover	Select one of the following: Yes—Use this setting to shut down the primary radios on failover. No—Use this setting to not shut down the primary radios on failover.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring CDP

Use this option to enable, disable, or adjust the access point's CDP settings.

Procedure

Step 1 Select **Services > CDP**. The Services: CDP-Cisco Discovery Protocol dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-28 CDP Settings

Field	Description
Cisco Discovery Protocol (CDP)	Select one of the following: • Enabled—Use this setting to enable CDP on the access point. • Disabled—Use this setting to disable CDP on the access point.
Packet Hold Time	Enter the number of seconds other CDP-enabled devices should consider the access point's CDP information valid.
Packets Sent Every	Enter the number of seconds between each CDP packet the access point sends. This value should always be less than the packet hold time.

Table 5-28 CDP Settings (continued)

Field	Description
Individual Port Enable	
Ethernet	Select one of the following: - Enabled—Use this option to enable CDP on the Ethernet port. - Disabled—Use this option to disable CDP on the Ethernet port.
Radio-802.11B/G	Select one of the following: - Enabled—Use this option to enable CDP on the radio port. - Disabled—Use this option to disable CDP on the radio port.
Radio-802.11A	Select one of the following: - Enabled—Use this option to enable CDP on the radio port. - Disabled—Use this option to disable CDP on the radio port.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring DNS

Use this option to configure the access point to work with your network's Domain Name System (DNS) server.

Procedure

Step 1 Select **Services > DNS**. The Services: DNS-Domain Name Service dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-29 DNS Settings

Field	Description
Domain Name System (DNS)	Select one of the following: - Enabled—Use this setting if your network uses DNS. - Disabled—Use this setting if you network does not use DNS.
Domain Name (optional)	Enter the domain name.

Table 5-29 **DNS Settings (continued)**

Field	Description
Name Server IP Addresses	Enter the IP addresses of up to three domain name servers on your network.
Delete Name Servers	
Server	Enter the server you want to delete, then click >>. The server name is added to the Servers to Delete list.
Servers to Delete	Select the server to delete, then click <<.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring MAC Address Filters

Use this option to configure MAC address filters.

MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses except those you specify.

Procedure

Step 1 Select **Services > MAC address filters**. The Services: Filters - MAC Address Filters dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-30 **MAC Address Filters**

Field	Description
Create and Apply	Select this option to create and apply MAC address filters.
Create Only	Select this option to create MAC address filters, but not apply them.
Apply Only	Select this option to apply the MAC address filters.
Filters List	Lists the currently configured filters. To delete a filter from the list, select it, then click Delete Filter .

Table 5-30 MAC Address Filters (continued)

Field	Description
Filter Index	Enter a number from 700 to 799. The number you assign creates an access control list (ACL) for the filter. ACLs applied from the WLSE have a cumulative effect on the device. If you want to modify the ACLs, delete the existing ACL using a template and then regenerate it using the WLSE. This way you are guaranteed that the ACL is applied in the correct order. For example, If an ACL has the following lines: <pre>access-list 700 permit 0040.1111.1111 0000.0000.0000 access-list 700 permit 0040.2222.2222 0000.0000.0000 access-list 700 deny 0.0.0 ffff.ffff.ffff</pre> and you would like to add the following at the beginning of the list: <pre>access-list 700 permit 0040.3333.3333 0000.0000.0000</pre> Then you need to delete the ACL and reapply it. Otherwise, the line you added will show up at the end of the list, not at the beginning where you intended it.
Add MAC Address	Enter the MAC address.
Mask	Enter the subnet mask.
Action	From the list, select one of the following actions: - Forward—Use this setting to forward the MAC addresses. - Block—Use this setting to block the MAC addresses.
Load MAC Address	Click to open a window that allows you to browse for a file of MAC addresses, if you have created one. To see an example of a file, click Sample File. After you have located the sample file containing the MAC addresses, click OK.
VLAN ID	Enter the VLAN identification number then click >>. To remove a VLAN ID from the list, select it, then click <<.
Bridge-Group	Enter a valid bridge group number used by the interface for which you want to create or delete filters.
Apply Filter to	
FastEthernet	Select one of the following:
Radio0-802.11B/G	Incoming—Use this option to apply the filter to the incoming packets.
Radio0-802.11A	Outgoing—Use this option to apply the filter to the outgoing packets. Click AddFilter.

Table 5-30 **MAC Address Filters (continued)**

Field	Description
Default Action	Select one of the following: - Block All - Forward All then click Update. The filter's default action must be the opposite of the action for at least one of the addresses in the filter. For example, if you enter several addresses and you select Block as the action for all of them, you must choose Forward All as the filter's default action.
Filters Classes	Lists MAC addresses. To remove the MAC address from the Filters Classes list, select it, then click Delete.
Delete Filters	
Filters	To delete a filter, select it from the list, then click Delete .
Filter Index	Enter the filter index number.
VLAN ID	Enter the VLAN identification number, then click >> to add it to the list. To delete a VLAN ID from the list, click <<.
Bridge-Group	Enter a valid bridge group number.
Remove Filter from	
FastEthernet	Select one of the following: - Incoming—Use this option to remove the filter from the incoming packets. - Outgoing—Use this option to remove the filter from the outgoing packets. Click AddFilter.
Radio0-802.11B/G	
Radio0-802.11A	

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring IP Filters

Use this option to create IP filters that prevent or allow the use of IP address(es), IP protocols, and TCP/UDP ports through the access point's Ethernet and radio ports.

Procedure

Step 1 Select **Services > IP Filters**. The Services: Filters - IP Filters dialog box appears.

Step 2 Complete the following:



Note

Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-31 *IP Filters*

Field	Description
Create and Apply	Select this option to create and apply IP address filters.
Create Only	Select this option to create IP address filters, but not apply them.
Apply Only	Select this option to apply the IP address filters.
Filter Name List	List the currently configured filters. To delete a filter from the list, select it, then click Delete Filter .
Filter Name	Enter a name for the filter.
Default Action	From the list, select one of the following: - Block All—Use this setting to block all IP addresses. - Forward All—Use this setting to forward all IP addresses. then click Update .
IP Address	
Destination Address	Enter the IP address that you want to filter.
Mask	Enter the mask for the destination IP address. Enter the mask with periods separating the three groups of four characters (255.255.255.240, for example). If you enter 255.255.255.255 as the mask, the access point accepts any IP address. If you enter 0.0.0.0, the access point looks for an exact match with the IP address you entered. The mask you enter in this field behaves the same way that a mask behaves when you enter it in the CLI.
Source Address	Enter the IP address you want to filter.
Mask	Enter the mask for the source IP address. Enter the mask with periods separating the three groups of four characters (255.255.255.240, for example). The method for entering the mask depends on the release. Entering 255.255.255.255 as the mask causes the access point to accept any IP address. If you enter 0.0.0.0, the access point looks for an exact match with the IP address you entered in the IP Address field.
Action	From the list, select one of the following: - Forward —Use this setting to forward the IP address. - Block —Use this setting to block the IP address. Click Add .

Table 5-31 *IP Filters (continued)*

Field	Description
IP Protocol	
IP Protocol	Do one of the following: - Click the existing protocol list, then select a protocol. - Click Custom, then enter a custom protocol.
Action	From the list, select one of the following: - Forward —Use this setting to forward the IP protocol. - Block —Use this setting to block the IP protocol. Click Add .
UDP/TCP Port	
TCP Port	Do one of the following: - Click the TCP Port list, then select one port from the list. - Click Custom, then enter a custom port.
Action	From the list, select one of the following: - Forward —Use this setting to forward the TCP port. - Block —Use this setting to block the IP TCP port. Click Add .
UDP Port	Do one of the following: - Click the UDP Port list, then select one port from the list. - Click Custom, then enter a custom port.
Action	From the list, select one of the following: - Forward —Use this setting to forward the UDP port. - Block —Use this setting to block the IP UDP port. Click Add .
VLAN ID	Enter the VLAN identification number then click >>. To remove a VLAN ID from the list, select it, then click <<.
Apply Filter	
FastEthernet	Select one of the following: - Incoming—Use this option to apply the filter to the incoming packets. - Outgoing—Use this option to apply the filter to the outgoing packets. Click Apply .
Radio0-802.11B/G	
Radio0-802.11A	
Filters Classes	Lists the currently configured filters. To delete a filter from the list, select it, then click Delete.
Delete Filters	
Filters	To delete a filter from the list, select it from the list, then click Delete .
Filter Name	Enter the filter name.

Table 5-31 *IP Filters (continued)*

Field	Description
VLAN ID	Enter the VLAN identification number, then click >> to add it to the list. To remove a VLAN ID from the list, click <<.
VLAN List	Lists the VLANs.
Remove Filter	
FastEthernet	Select one of the following: - Incoming—Use this option to remove the filter from the incoming packets. - Outgoing—Use this option to remove the filter from the outgoing packets. Click AddFilter .
Radio0-802.11B/G	
Radio0-802.11A	

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Ethertype Filters

Use this option to configure Ethertype filters to prevent or allow the use of specific L3 protocols through the access point's Ethernet and radio ports.

Procedure

Step 1 Select **Services > Ethertype Filters**. The Services: Filters - Ethertype Filters dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-32 *Ethertype Filters*

Field	Description
Create and Apply	Select this option to create and apply Ethertype filters.
Create Only	Select this option to create Ethertype filters, but not apply them.
Apply Only	Select this option to apply the Ethertype filters.
Filters List	Lists the currently configured filters. To remove a filter from the list, select it, then click Delete Filter .

Table 5-32 **Ethertype Filters (continued)**

Field	Description
Filter Index	Enter a number from 200 to 299. The number you assign creates an access control list (ACL) for the filter.
Add EtherType	Enter an EtherType number.
Mask	Enter the mask for the EtherType.
Action	From the list, select one of the following: - Forward —Use this setting to forward the traffic. - Block —Use this setting to block the traffic.
VLAN ID	Enter the VLAN identification number then click >>. To remove a VLAN ID from the list, select it, then click <<.
Bridge-Group	Enter a valid bridge group number used by the interface for which you want to create or delete filters.
Apply Filter to	
FastEthernet	Select one of the following:
Radio0-802.11B/G	- Incoming—Use this option to apply the filter to the incoming packets. - Outgoing—Use this option to apply the filter to the outgoing packets. Click Apply .
Radio0-802.11A	
Default Action	From the list, select one of the following: - Block All—Use this setting to block all. - Forward All—Use this setting to forward all. then click Update .
Filters Classes	Lists the currently configured filters. To delete a filter from the list, select it, then click Delete.
Delete Filters	
Filters	To delete a filter from the list, select it from the list, then click Delete .
Filter Index	Enter the filter index.
VLAN ID	Enter the VLAN identification number, then click >> to add it to the list. To delete a VLAN ID from the list, click <<
Bridge-Group	Enter a valid bridge group number.
Remove Filter	
FastEthernet	Select one of the following:
Radio0-802.11B/G	- Incoming—Use this option to remove the filter from the incoming packets. - Outgoing—Use this option to remove the filter from the outgoing packets. Click AddFilter .
Radio0-802.11A	

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring HTTP

Use this option to configure HTTP settings for the access point.

Procedure

- Step 1** Select **Services > HTTP**. The Services: HTTP-Web Server dialog box appears.
- Step 2** Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-33 HTTP

Field	Description
Web-based Configuration Management	Select one of the following: • Enable Standard (HTTP) Browsing—Use this setting to allow web-based browsing to the management system. • Enable Secure (HTTPS) Browsing—Use this setting to allow secure web-based browsing to the management system. • Disable Web-based Management—Use this setting to disallow web-based browsing to the management system.
HTTP Port	Enter the port through which the access point provides web access.
HTTPS Port	Enter the port through which the access point provides secure web access.
Default Help Root URL	Enter the URL where the device can locate help files.

- Step 3** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
 - **Save** to save the template. See [Saving the Template, page 5-100](#).
 - Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring QoS Policies

Use this option to configure quality of service policies.

If you know the applications used by wireless client devices, the applications' sensitivity to delay, and the amount of traffic associated with the applications, you can configure QoS to improve performance.

Procedure

Step 1 Select **Services > QoS Policies**. The Services: QoS Policies dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** in the upper right side of the screen removes all the entries you have made so far and returns you to the Template Name page.

Clicking **Clear** in the lower right side of the screen only removes entries you have made on this page.

Clicking **Reset** clears the entries you have made on the page and restores the defaults, if any were set.

Table 5-34 QoS Policies

Field	Description
Create and Apply	Select this option to create and apply QoS policies.
Create Only	Select this option to create QoS policies., but not apply them.
Apply Only	Select this option to apply the QoS policies.
QoS Element for Wireless Phones	Select one of the following: • Enable—Use this setting to specify that wireless phone clients' traffic has a higher priority than the rest of the clients. • Disable—Use this setting to disable this feature. • Dot11e—Select to enable for.11e. Click See detail to see for which device types or versions this setting is valid.
IGMP Snooping Helper	Select one of the following: • Enable—Use this setting to enable Internet Group Membership Protocol (IGMP) snooping. When this feature is enabled, the access point sends a general IGMP query to the network infrastructure on behalf of the client every time the client associates or reassociates to the access point. By doing so, the multicast stream is maintained for the client as it roams. • Disable—Use this setting to disable this feature. Click See detail to see for which device types or versions this setting is valid.

Table 5-34 QoS Policies (continued)

Field	Description
Map Ethernet Packets with CoS 5 to CoS 6 (AVVID Priority Mapping)	Select one of the following: • Yes—Use this setting if your network is based on the Cisco AVVID specification. This setting will prioritize voice packets coming with priority 5 (video). • No—Use this setting if your network is not based on the Cisco AVVID specification. Click See detail to see for which device types or versions this setting is valid.
WiFi Multimedia	Click See detail to see for which device types or versions this setting is valid. For each radio interface select one the following: • Enable—Select this option to enable WME support. • Disable—Select this option to disable the feature.
Policy List	Lists the names of the existing policies. To remove a name from the list, select it, then click Delete Policy.
Policy Name	Enter a name for the policy.
Classifications	Lists the classifications assigned to that policy. To delete a classification from the list, select it, then click Delete.
Match Classifications	
Precedence	If the packets that you need to prioritize contain IP precedence information select an IP precedence classification from the list.
Apply Class of Service	From the list, select the class of service that the access point will apply to packets of the type that you selected from the Precedence list, then click Add .
IP DSCP	If the packets that you need to prioritize contain IP DSCP information, select an IP DSCP classification from the list or create a new one.
Apply Class of Service	From the list, select the class of service that the access point will apply to packets of the type that you selected from the IP DSCP list, then click Add .
IP Protocol 119	If you need to prioritize the packets from Spectralink on your wireless LAN, select the class of service the access point will apply to the phone packets, then click Add .
Apply Class of Service	Click See detail to see for which device types or versions this setting is valid.
Filter	If you need to assign a priority to filtered packets, from the list, select the filter to include in the policy or create a new one.
Apply Class of Service	From the list, select the class of service that the access point will apply to packets that match the filter that you selected or entered, then click Add .
Default Classification for Packets on the VLAN	If you want to set a default classification for all packets on a VLAN, select the class of service that the access point will apply to packets on a VLAN, then click Add .

Table 5-34 QoS Policies (continued)

Field	Description
VLAN ID	Enter the VLAN identification number, then click >> to add it to the list.
VLAN ID List	To delete a VLAN ID from the list, click <<.
Apply Policy to	
FastEthernet	Select one of the following: • Incoming—Use this option to apply the filter to the incoming packets. • Outgoing—Use this option to apply the filter to the outgoing packets. Click ApplyPolicy .
Radio0-802.11B/G	
Radio0-802.11A	
Remove Policy from Interface/VLANs	
Policy List	To delete a policy from the list, select it from the list, then click Delete .
Policy Name	Enter the name of the policy.
VLAN ID	Enter the VLAN identification number, then click >> to add it to the list.
VLAN ID List	To delete a VLAN ID from the list, click <<.
Remove Policy from	
FastEthernet	Select one of the following: • Incoming—Use this option to remove the filter from the incoming packets. • Outgoing—Use this option to remove the filter from the outgoing packets. Click AddPolicy .
Radio0-802.11B/G	
Radio0-802.11A	
Remove Policy Map and Class Map	
Policy List	Lists the policies. Select the policy to remove from the list, then click Delete .
Policy Name	Enter the policy name, then click Add Policy . The name appears in the Policy List.
Class Name	Enter the class name. Click >> to add it to the Class Name List
Class Name List	Click << to remove the class name from the list.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring QoS Radio 802.11b/g

Use this option to define traffic class QoS policies. The access point uses the radio traffic class definitions to calculate backoff times for each packet.

Procedure

Step 1 Select **Services > QoS Radio 802.11b/g**. The Services: QoS Policies - Traffic Class Definition dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-35 QoS Radio 802.11b/g Traffic Class Definition

Field	Description
802.11e 4 Level QoS	Select QoS for version 12.3(2)JA and above.
802.11e 4 Level QoS with WMM	Select QoS with Wi-Fi multimedia for version 12.3(2)JA and above.
Background	Enter values for AP and Client for the following access categories: - Min Contention Window—Enter the minimum contention window value. The access point computes Contention Window values. - Max Contention Window—Enter the maximum contention window value. The access point computes Contention Window values. - Fixed Slot Time—Enter a value for a fixed slot time. - Admission Control—Not applicable for this release. Used for 802.11e 4 Level QoS with WMM to specify that admission control is mandatory for this class.
Best Effort	
Video	
Voice	
	Transmit Opportunity—Not applicable for this release. Used for 802.11e 4 Level QoS with WMM to specify the value in microseconds during which transmitters that are qualified to transmit through the normal back-off procedure are allowed to send a set of pending packets during the configured transmit opportunity.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring QoS Radio 802.11a

Use this option to define traffic class QoS policies. The access point uses the radio traffic class definitions to calculate backoff times for each packet.

Procedure

Step 1 Select **Services > QoS Radio 802.11a**. The Services: QoS Policies - Traffic Class Definition dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-36 QoS Radio 802.11a Traffic Class Definition

Field	Description
Background	Enter a Local and a Cell value for each access category, or set the values automatically by clicking Optimized Voice or WFA Default. Note Only Local values for Max Contention Window, Min Contention Window, Fixed Slot Time, and Transmit Opportunity will be applied to devices with versions earlier than 12.3(8)JA. To clear the table of values, click Clear.
Best Effort	
Video	
Voice	
Admission Control	Select this option to specify that admission control is mandatory for this class. Note Admission control should not be enabled if your deployment includes softphone applications. If you are not deploying softphone applications on laptops, then use the default.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring SNMP

Use this option to configure settings for notifications to be sent to an SNMP server.

This option also enables you to send SNMP traps to this WLSE. Enabling this option allows faster fault processing of policies because the access point is reporting directly to the WLSE instead of the WLSE periodically polling the access point. For additional information, see [Setting RF Port Status Threshold, page 3-34](#) and [Setting RF Port AdminStatus Threshold, page 3-35](#).

Procedure

Step 1 Select **Services > SNMP**. The Services: SNMP- Simple Network Management Protocol dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-37 *SNMP*

Field	Description
Simple Network Management Protocol (SNMP)	Select one of the following: - Enabled—Use this setting to allow event notifications to be sent to an SNMP server. - Disabled—Use this setting to disallow event notifications to be sent to an SNMP server.
System Name	Enter the name of the access point. The name in this field is reported to your SNMP's management station as the name of the device when you use SNMP to communicate with the access point.
System Location	Enter a description of the access point's physical location, such as the building or room in which it is installed.
System Contact	Enter the name the system administrator responsible for the access point.
SNMP Request Communities	
Current Community Strings	Lists the current community strings. To delete an entry from the list, select it, then click Delete. To edit an entry, select it.
Edit Community Strings	- SNMP Community—The SNMP Community value for the selected community string displays. SNMP community strings authenticate access to MIB objects and function as embedded passwords. - Object Identifier —The Object Identifier value for the selected community string displays. Enter a new object identifier for the community string. The object identifier limits the scope of the SNMP MIB object that the user can access through the community string. For example, if you enter iso as the Object Identifier value for the public string, then only users using the public string can access the OID that is represented by the SNMP variable name iso, including all the variables that come under this variable starting at this point. (This is the MIB family view to which the community has access.) - Select one of the following one of the following: Read-Only or Read-Write.

Table 5-37 **SNMP (continued)**

Field	Description
SNMP Traps	
Send all traps to this WLSE	Select one of the following: • Enable—Use this setting to enable the access point to send traps to this WLSE. (The WLSE's address is added as an SNMP trap destination.) Enabling this setting allows faster processing of faults. (See Ports Hosted by the WLSE, page C-2 for correct port setting.) • Disable—Use this setting to disallow traps being sent to this WLSE. Using the setting does not disable traps; it removes this WLSE's address as an SNMP trap destination.
SNMP Trap Destination	1. Enter the IP address or the host name of the server running the SNMP Management software. 2. Select one of the following: – Enable All Trap Notifications—Use this setting to enable all traps. – Enable Specific Traps—Use this setting to select one or more of the displayed trap types. Click See detail to see for which device types or versions the particular settings are valid. 3. Click Save.
Delete Communities and SNMP Trap Destinations	
Community	Enter the community to delete, then click >>.
Communities to Delete	Lists the communities to be deleted. To delete a community, select it, then click <<.
SNMP Trap	Enter the IP address or the host name of the server to delete.
Communities	Enter the community associated with the SNMP trap, then click >>.
Destinations to Delete	Lists the SNMP trap destinations to be deleted. To delete a destination, select it, then click <<.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).



Note The WLSE's address appears as "%thiswlse%" in the displayed IOS commands. This is because the address is not known until the template is applied to an access point.

- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring SNTP

This option allows you to configure the date and time on using SNTP (Simple Network Time Protocol).

Procedure

Step 1 Select **Services > SNTP**. The Services: NTP - Network Time Protocol dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-38 SNTP

Field	Description
SNTP Server	
Click See detail for information about NTP support.	
Simple Network Time Protocol (SNTP)	Select one of the following: - Enabled—Use this setting to use of NTP. - Disabled—Use this setting to disallow the use NTP.
Time Server	Enter the server's IP address.
Time Settings	
GMT Offset	From the list, select one of the options.
Use Daylight Savings Time	Select one of the following: - Yes—Use this setting to use daylight savings time. - No—Use this setting if you are not going to use daylight savings time.
Manually Set Date	Use this setting to manually set the date.
Manually Set Time	Use this setting to manually set the time.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring VLAN

Using this option, you can configure VLANs on the access point.

Procedure

Step 1 Select **Services > VLAN**. The Services: VLAN dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-39 VLAN

Field	Description
Global VLAN Properties	
Set Native VLAN	From the list, select a VLAN for the default.
Assigned VLANs	
Current VLAN List	Lists the current VLANs. To delete a VLAN from the list, select it, then click Delete .
Create VLAN	
VLAN ID	Enter a VLAN ID.
VLAN Name	Enter a name for the VLAN.
Bridge-Group	Enter the bridge group number. - If the VLAN ID you entered is less than 255, and you do not enter a value in this field, then the same number for the bridge group is automatically assigned. - If the VLAN ID you entered is 255 or greater you will need to know what bridge group numbers are unused on the access point and enter one of them. When a VLAN is created directly on the access point, the access point dynamically assigns a bridge group to the VLAN. So, if you create a VLAN ID of 123, then the bridge group is 123. If the VLAN is larger than 255, the access point starts at 255 and decrements the count until it gets to an unused bridge group number. So, if you create a VLAN ID of 500, the access point assigns a bridge group of 255 if that number is unused. If it is used, it will then try 254, and so on until it finds an unused number for the bridge group.
Enable Public Secure Packet Forwarding	Select to enable public secure packet forwarding (PSPF). With PSPF enabled, client devices cannot communicate with other client devices on the wireless network. This feature is useful for public wireless networks like those installed in airports or on college campuses. Click See detail to see for which device types or versions this setting is valid.
Associate SSIDs with VLAN Name	Select to enable association of the VLAN name with the SSID.

Table 5-39 VLAN (continued)

Field	Description
Radio0-802.11B/G	Select the appropriate radio, if desired. This setting is not enforced.
Radio0-802.11A	For Radio0-802.11A, click See detail to see for which device types or versions this setting is valid.
SSID	Enter an SSID, then click Add .
STP	Select one of the following: • Enable—Use this setting to enable Spanning Tree Protocol (bridges only). • Disable—Use this setting to disable the feature. then click Add .
Workgroup Bridge Ethernet Client VLAN	
Add	Click to configure a client VLAN when the workgroup bridge's clients are on a non-native VLAN, then enter the VLAN ID.
Delete	Click to delete the client, then enter the VLAN ID.
Delete VLANs	
VLANs to Delete	Lists the VLANs to delete. To delete VLAN from the list, select it, then click Delete .
VLAN ID	Enter the identification number of the VLAN you want to add to the VLANs to Delete list.
VLAN Name	Enter the VLAN name.
Associate SSIDs with VLAN Name	Select to associate the SSIDs with the VLAN name.
Radio0-802.11B/G	Select the appropriate radio.
Radio1-802.11A	
SSID	Enter the SSID, then click Add . The VLAN appears in the VLANs to Delete list.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring ARP Cache

Address resolution protocol (ARP) is used to find the MAC address that corresponds to a particular IP address. Using this option, the access point remembers the IP addresses of its clients and will not send ARP requests to them.

This feature helps improve performance because it reduces traffic load over the wireless link. If all client IP address are not known, the access point drops the ARP request, and caching is prevented.

Procedure

Step 1 Select **Services > ARP Cache**. The Services: Client ARP Caching dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-40 ARP Cache

Field	Description
Client ARP Caching	Select one of the following: - Enabled—Use this setting to allow ARP caching. - Disabled—Use this setting to disable the feature. Click See detail to see for which device types or versions this setting is valid.
Forward ARP Requests To Radio Interfaces When Not All Client IP Addresses Are Known	Select when all client IP address are not known, so that the access point forwards the ARP request to all its clients, and caching is prevented

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring STP

This option enables to you to configure spanning tree protocol.

Procedure

Step 1 Select **Services > STP**. The Spanning Tree Protocol dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-41 STP

Field	Description
STP Properties	
Click See detail to see for which device types or versions this setting is valid.	
Per VLAN Spanning Tree List	Lists the current STPs. To remove an STP from the list, select it, then click Delete .
VLAN ID	Enter the VLAN identification number.
Bridge Group	Enter the name of the bridge group.
Root Configuration	
Priority	Enter the spanning tree priority (STP) for the bridge. STP uses the bridge priority to select the spanning tree root. The lower the priority, the more likely it is that the bridge will become the spanning tree root.
Max Age	Enter the interval that the bridge waits to hear BPDUs from the spanning tree root. If the bridge does not hear bridge protocol data units (BPDUs) from the spanning tree root within this specified interval, it assumes that the network has changed and recomputes the spanning-tree topology.
Hello Time	Enter the interval between hello bridge protocol data units (BPDUs).
Forward Delay	Enter the forward delay interval on the bridge.
Port Configuration	These settings apply to individual ports on the bridge. Use these settings to adjust the status of individual ports i.e. Ethernet or Radio port on the bridge.
Ethernet	Complete the following: • Path Cost—Use this setting to specify the relative efficiency of the port's network link. A port with a high path cost is less likely to become a bridge's root port. • Priority—Use this setting to influence whether STP designates a port as a root port. A port with a low priority setting is more likely to become a root port.
Root Radio 802.11b/g	
Root Radio 802.11a	
Spanning Tree without VLAN	
STP for Radio 802.11b/g	Select one of the following: Enable or Disable.
STP for Radio 802.11a	Select one of the following: Enable or Disable.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Packet Handling 802.11a

Use this option to define packet retry policies.

Procedure

- Step 1** Select **Services > Packet Handling 802.11a**. The Stream-Packet Handling Radio 802.11a dialog box appears.
- Step 2** Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-42 *Packet Handling 802.11a*

Field	Description
General Packet Handling	Click See detail to see the versions for which this setting is valid.
Packet Handling per User Priority:	
User Priority	Lists the Class of Service (COS) for which you can set packet handling and maximum number of retries before the packet is discarded.
Packet Handling	Select one of the following: • None—Use this setting to disable packet handling. • Reliable—Use this setting to disable the max-retry option of packets. • Low Latency—Use this setting to enable the max-retry option of packets.
Max Retries for Packet Discard	This option specifies the packet retries before dropping a packet if the first fail-threshold not reached. It is disabled if Packet Handling is set to None. For Reliable and Low Latency packet handling settings, accept the default or specify a different number of maximum retries.

- Step 3** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
 - **Save** to save the template. See [Saving the Template, page 5-100](#).
 - Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Wireless Services

This option provides context control to the nodes by maintaining a cache of all client contexts within a given subnet.

Procedure

- Step 1** Select **Wireless Services**. The menu expands and the Wireless Services: AP dialog box displays in the right pane.
- Step 2** Select one of the following from the menu:
- AP Configuration—See [Configuring the AP, page 5-91](#).
 - WDS—See [Configuring WDS, page 5-92](#).

Configuring the AP

Use this option to configure the access point to interact with wireless services.

Procedure

- Step 1** Select **Wireless Services > AP Configuration**. The Wireless Services: AP dialog box appears.
- Step 2** Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-43 *AP Configuration*

Field	Description
Use Wizard Configuration	Select one of the following: • Enable—Use this setting to employ the configuration defined with the Deployment Wizard. The fields on this page are grayed out when this setting is selected. • Disable—Use this setting to disable the Deployment Wizard configuration, and to use this page to configure the AP.
Participate in SWAN Infrastructure	Select one of the following; • Enable—Use this setting indicate that the access point is participating in the Cisco Structured Wireless Aware Network (SWAN). • Disable—Use this setting to indicate that the access point is not participating in SWAN. Click See detail to see for which device types or versions this setting is valid.
WDS Discovery	Select one of the following: • Auto Discovery—Use this setting to search for any WDS access point. • Specified Discovery—Use this setting to search for a particular WDS access point, then enter the IP address for that access point.

Table 5-43 *AP Configuration (continued)*

Field	Description
Username	Enter a username.
Password	Enter a password.
Confirm Password	Reenter the password.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring WDS

Use this option to configure wireless domain services and to set its priority.

Procedure

Step 1 Select **Wireless Services > WDS**. The Wireless Services: WDS - Wireless Domain Services - Settings dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-44 *WDS Settings*

Field	Description
Use Wizard Configuration	Select one of the following: • Enable—Use this setting to employ the configuration defined with the Deployment Wizard. The fields on this page are grayed out when this setting is selected. • Disable—Use this setting to disable the Deployment Wizard configuration, and to use this page to configure WDS.

Table 5-44 WDS Settings (continued)

Field	Description
Global Properties	
Click See detail to see for which device types or versions this setting is valid.	
Use this AP as Wireless Domain Services	Select one of the following: • Enable—Use this setting to enable the access point to provide Wireless Domain Services. • Disable—Use this setting to disable the access point to provide Wireless Domain Services. • Modify—Use this setting to modify the Wireless Domain Services on the access point.
Wireless Domain Services Priority	Enter a number between 1 and 255 to indicate the priority. The priority is structured so that a WDS will not replace an active WDS with the same priority value, even it has a higher node ID.
Wireless Network Manager Address	Enter the access point's IP address or hostname.
Use Local MAC List for Client Authentication	Select one of the following: • Enable—Use this setting to use the local MAC address list for authentication. • Disable—Use this setting to disable the local MAC address list for authentication.
Server Groups	
Server Group List	Lists the configured servers. To delete a server from the list, select it, then click Delete .
Server Group Name	Enter the name of the server group then complete the following: • Priority—Enter the server IP address or hostname. • Auth Port—Enter the authentication port. • Acct Port—Enter the accounting port. or • Select a name from the list.
Use Group for	Select one of the following: • Infrastructure Authentication—Use this setting to initiate infrastructure authentication by sending a path initialization request message to its WDS, which acts as the IN authenticator. • Client Authentication—Use this setting to provide client authentication services, then under Authentication Settings, select one of the types of client authentication.
SSID	Enter the SSID or leave blank to apply to all SSIDs, then click >> to add to the SSID List. Click Save .

Table 5-44 WDS Settings (continued)

Field	Description
SSID List	Lists the current SSIDs. To remove an SSID from the list, select it, then click <<.
Delete Server Group	
Server Group Name	Enter the server group to delete.
Server Group List to Delete	Lists the server groups to delete. To remove a group from the list, select it, then click <<.
Use Group For	Select one of the following: - Infrastructure Authentication—Use this setting to initiate infrastructure authentication by sending a path initialization request message to its WDS, which acts as the IN authenticator. - Client Authentication—Use this setting to provide client authentication services. Select the type of client authentication. Then, click >> to add to the Server Group List to Delete.

Step 3 Click **Save**. The server is added to the Authentication Server List.

Step 4 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring the Event Log

This option enables to you to customize the display of access point events.

Procedure

Step 1 Select **Event Log**. The menu expands and the Event Log: Configuration Options dialog box displays in the right pane.

Step 2 Select one of the following from the menu:

- Configuration Options—See [Setting Configuration Options, page 5-95](#).
- Notification Options—See [Setting Notification Options, page 5-96](#).

Setting Configuration Options

Procedure

Step 1 Select **Event Log > Configuration Options**. The Event Log: Configuration Options dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-45 Configuration Options

Field	Description
Disposition of Events (by Severity Level)	
Emergency	Check one or more of the following for each of the events: • Display on Event Log • Notify via SNMP/Syslog Trap • Record for SNMP/Syslog History Table • Display on Telnet/SSH Monitor
Alert	
Critical	
Error	
Warning	
Notification	
Information	
Debugging	
Time Stamp Format for Future Events	Select one of the following: • System Uptime—Use this setting to use the system uptime in the timestamp. • Global Standard Time—Use this setting to use the global standard time in the timestamp. • Local Time—Use this setting to use the local time in the timestamp.
Event Log Size	Enter the maximum size of the event log.
History Table Size	Enter the maximum number of messages in the history table.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Setting Notification Options

Procedure

Step 1 Select **Event Log > Notification Options**. The Event Log: Notification Options dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-46 Notification Options

Field	Description
Events Generate Syslog Messages	Select one of the following: • Enable—Use this setting to allow events to generate syslog messages. • Disable—Use this setting to disable the feature.
Syslog Server Hostname or IP Address	Enter the hostname or IP address of the syslog server.
Syslog Facility	From the list, select the syslog facility.
Delete Syslog Server	
Server Hostname or IP Address to remove	Enter the Syslog server hostname or IP address to be deleted.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

System Config

This option allows you to do two different things: reload a device and negotiate power settings.

Reload Settings

Before you reload, you can chose either to save the configuration to NVRAM or not to save the configuration to NVRAM.



Note If custom commands have been configured, they will be applied before a Reload command; the Reload command is always applied last.

Power Option Settings

These settings allow the access point to negotiate its power settings when it powers on. It negotiates the power settings as follows:

- If the access point is powered from an AC adaptor, no configuration is necessary.
- If the access point is connected to an inline switch that supports power negotiation, the access point will negotiate its power settings with the switch.
- If the access point is powered from a 15W inline switch that does not support power negotiation, “Pre-standard Compatibility Mode” is required.
- If the access point is powered from a 6W inline switch, a power injector is required. The “Power Injector” is required with a MAC address that matches the one on the Ethernet port where the injector is connected.
- If the access point is powered from a non-Cisco 802.3(af) switch, no additional configuration is required.
- If the access point is unable to verify a 15W inline power source, then the access point will stay in a low power state.

Procedure

Step 1 Select **System Config**. The System Config dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-47 **System Config**

Field	Description
System Config	
Reload Device	Select one of the following: • Without Writing NVRAM—Select this option to write the configuration to NVRAM. • With Writing NVRAM—Select this option if you do not want the configuration written to NVRAM. Click See detail for caution.

Table 5-47 **System Config (continued)**

Field	Description
Power Settings	
Power Settings	Select one of the following: • Power Negotiation—Use this setting to allow a device to negotiate inline power with the switch. • Pre-standard Compatibility—Use this setting if the access point is powered from a 15W inline switch that does not support power negotiation. Click See detail to see for which device types or versions this setting is valid.
Power Injector	Select one of the following: • Enable installed on Port with MAC Address—Use this setting if the access point is powered from a 6W inline switch and requires a power injector. that matches the one on the Ethernet port where the injector is connected. • Disable—Use this setting to disable the use of the power injector.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
- **Save** to save the template. See [Saving the Template, page 5-100](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Device Specific Settings

This option enables you to create a template with specific settings. Unlike other template options, these commands are not validated when the template is saved.

For information on importing, exporting, and viewing device settings, see [Managing Device Specific Configurations, page 8-47](#).

Procedure

- Step 1** Select **Device Specific**. The Device Specific Settings dialog box appears.
- Step 2** Select **Enable Device Specific Settings for this Template** to use the settings specified in the CSV file.

Configuring Custom Values



Note

This option should be used only by advanced users.

This option enables you to enter custom values that might not be available in the Template Menu. It also allows you to quickly enter a value, if you know the exact value you want to change, instead of going through the menu.

Important Notes

- Any custom values you configure are applied to the device only after all the other template configurations have been applied.
- Custom values are not validated. However, if a configuration contains a combination of custom values and values entered using the templates, the values entered using the templates are validated; only the values entered with the custom configuration are not.
- If the custom value you enter is the same as an existing one in the Template Menu, the custom value will override the value in the menu.
- If you use the `username` command with the password encryption option (i.e 7), for example:

```
username Cisco1 privilege 15 password 7 062506324F4158
```

then after applying the command through the config job, the credentials will not be updated in the WLSE. The WLSE cannot decrypt the IOS-encrypted password.

Procedure

Step 1 Select **Configure > Templates > Custom Values**. The Custom IOS Values dialog box appears.



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Step 2 Enter the IOS commands.



Note Do not use either the `exit` or `end` commands

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-100](#).
 - **Save** to save the template. See [Saving the Template, page 5-100](#).
 - Another template category to configure more options. See [2.Template Categories, page 5-6](#).
-

Previewing the Template

Procedure

-
- Step 1** Click **Preview**. A Command Preview window displays the configuration choices you have made to the template.
- (See [In What Order are the Template Configurations Applied to the Devices?](#), page 8-8 for information about the order in which the template choices are applied.)
- Step 2** Click **Save**. See [Saving the Template](#), page 5-100.
-

Saving the Template

When you save a template, the WLSE first validates the template and displays the valid Device Type, Interface, and the corresponding Device Version(s) for that template.

An access point with an 802.11g radio, supports different commands from a similar access point with an 802.11b radio. The same is true for a 1310 wireless bridge in bridge mode versus a 1310 wireless bridge in access point mode or in a workgroup bridge mode.

If the Interface column displays 802.11g/a, it means that the template is applicable to an access point with a and g radio. If the Interface column displays 802.11b/a, it means that the template is applicable to an access point with a and b radio.

Similarly, if the Device Type column displays BR1310, it means that the configuration template is applicable to a 1310 wireless bridge which is in bridge mode. If the Device Type column displays an AP1310, it means the template is applicable to a 1310 wireless bridge in access point mode.

Procedure

-
- Step 1** Click **Save** in the left pane to complete creating a template. The Save dialog box appears in the right pane.
- Step 2** Click **Save** to create the template.
- Step 3** Do one of the following:
- Click **Yes** if you want to save the template then schedule a configuration job.
The window refreshes to the Job Creation window and a job is automatically created for you using the template name and a random number. See [Selecting Devices](#), page 8-14.
 - Click **No** if you want to save the template only.
 - Click **Cancel** to cancel the operation and then display the previous screen.
-



Using WLSM Templates

The WLSE allows you to view, create, copy, edit, and delete WLSM (Wireless LAN Services Module) configuration templates and apply them.

The topics covered are:

- [What is a Configuration Template?, page 6-1](#)
- [Viewing the Existing Templates, page 6-2](#)
- [Creating a Template, page 6-2](#)
- [Copying a Template, page 6-2](#)
- [Editing a Template, page 6-3](#)
- [Deleting a Template, page 6-3](#)
- [Importing a Template, page 6-4](#)
- [Exporting a Template, page 6-5](#)
- [Template Choices, page 6-6](#)

Related Topics

- [Using Wizard Templates, page 7-1](#)
- [Managing Configuration Jobs, page 8-7](#)

What is a Configuration Template?

You can think of a configuration template as a configuration update file for an WLSM. This file might contain the update for only one parameter or a complete configuration.

WLSM-based templates are stored as text files containing IOS commands.

You can use the **Configure > Templates** option to:

- View existing templates—See [Viewing the Existing Templates, page 6-2](#)
- Create a configuration template—See [Creating a Template, page 6-2](#)
- Copy an existing template—See [Copying a Template, page 6-2](#)
- Edit an existing template—See [Editing a Template, page 6-3](#)
- Delete a template—See [Deleting a Template, page 6-3](#)
- Import a template—See [Importing a Template, page 6-4](#)

- Export a template—[Exporting a Template, page 6-5](#)

Viewing the Existing Templates

Use this option to create a configuration template.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** From the list, select the type of templates you want to display, then click Filter.
- Step 3** The selected template types are displayed in the Existing Templates table.

Creating a Template

Use this option to create a configuration template.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** From the list, select **WLSM**.
- Step 3** Enter a unique name. See [Naming Guidelines, page B-1](#) for details.
- Step 4** Click **New**. The window refreshes with the Template Creation menu in the left pane and the Template Name dialog box in the right pane.
- Step 5** Select the choices in the left pane to create a configuration template. For a description, see [Template Choices, page 6-6](#).

Copying a Template

Use this option to copy a configuration template that you can use as a base for another template.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Select the template you want to copy from the Existing Templates table, then click **Copy**. A dialog box appears asking you to enter a name for the copy.
- Step 3** Enter a unique name. See [Naming Guidelines, page B-1](#) for details.
- Step 4** Click **OK**. The Templates window refreshes and the new name appears in the Existing Templates table.
- Step 5** Select the template, then click **Edit**. See [Editing a Template, page 6-3](#).
-

Editing a Template

Use this option to edit a configuration template.



Note

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Select the template you want to edit from the Existing Templates table, then click **Edit**. The window refreshes with Template Creation menu in the left pane and the Template Name dialog box in the right pane.
- Step 3** Select the choices in the Template Menu to create a configuration template. For a description, see [Template Choices, page 6-6](#).
-

Deleting a Template

Use this option to delete a configuration template.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Select the template you want to delete from the Existing Templates table, then click **Delete**. A window appears asking if you want to delete the template.



Note You cannot delete a template if it used in a scheduled job.

- Step 3** Click **OK** to delete it.

Importing a Template

Use this option to import a configuration to the WLSE, either from a file or from a device. You can import files from devices that are not managed by the WLSE.

When you import a configuration from a WLSM, the imported configuration options are displayed in the Custom Values template screen.



Note Your login determines whether you can use this option.

Procedure

- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Click **Import**. The Import Template window appears and varies depending upon which type you selected.
- Step 3** Complete the following:

Field	Description
Template Name	If you are importing from a file, enter a new name for the template or leave the entry blank to use the imported template name. If you are importing from a device, you must enter a template name.
Description	Enter a description for the template. Do not click the Enter key at the end of the description; it will generate an error.
From file	Enter the template filename or browse to find the file, then click Import .
From device (IP Address)	Enter a device name or IP address, then click Import .

Field	Description
Non-IP-Identity	Select this option if you do not want to download identity parameters, such as IP address. Some parameters are ignored using this type of import. The downloaded configuration parameters are not a full representation of the configuration but an optimal representation.
Full	Select this option to import a full configuration from the WLSM. This type of import includes the identity parameters, such as sysname, IP address, etc. When using this option, it is recommended you delete all the custom key values from the imported template before applying the template to any device.
Device HTTP Credentials	
User Name	If the device is not managed by the WLSE, or if the device is managed but the credentials have not been set, enter the username on the WLSM.
User Password	If the device is not managed by the WLSE, enter the user password on the WLSM.

Step 4 To import another template, click **Back** and go to [Step 2](#).

Step 5 When you are finished, click **Done**.

Step 6 View the template you imported by selecting **Configure > Templates** and selecting it in the Existing Templates table.

Exporting a Template

Use this option to export a configuration template to your local drive.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Configure > Templates**. The Templates dialog box appears.

Step 2 Select a template name from Existing Templates, then click **Export**. The Export Template window appears.

Step 3 From the list, select the template you want to export, then click **Export**. The Export Template to Desktop window appears with the name of the template.

- Step 4** Right-click on the template name, select **Save As**, and enter the location to save the template.
- Step 5** Click **Done**.
-

Template Choices

When you create or edit a WLSM configuration template, the following choices appear in the left pane of the Templates window:

1. **Template Name**—See [Naming the Template, page 6-6](#).
2. **Template Categories**



Note Any or all of the template categories can be completed in any order.

- **Server Manager**—See [Using the Server Manager, page 6-7](#).
 - **Custom Values**—See [Configuring Custom Values, page 6-10](#).
3. **Preview**—See [Previewing the Template, page 6-11](#).
 4. **Save**—See [Saving the Template, page 6-11](#).

Naming the Template

This option enables to you to name the template.

Procedure

Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Step 1 Select **Template Name**. The Template Name dialog box appears:

Field	Description
Template Name	Enter a name for the template. See Naming Guidelines, page B-1 .
Description	Enter a description of the purpose of the template. See Naming Guidelines, page B-1 . Do not click the Enter key at the end of the description; it will generate an error.

Step 2 Select a template category. For additional information, see [2.Template Categories, page 6-6](#).

Using the Server Manager

Use this option to enter authentication settings. The RADIUS server on our network uses EAP to provide authentication service for wireless client devices.

You can:

- Add a server manager—See [Adding a Server Manager, page 6-7](#).
- Delete a server manager—See [Deleting a Server Manager, page 6-9](#).

Adding a Server Manager

Procedure

Step 1 Select **Server Manager**. The Server Manager dialog box displays in the right pane:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Step 2 Complete the following:

Table 6-1 **Adding Server Manager**

Field	Description
Radius Servers	
Current Server List	Lists the servers that are currently configured. To delete a server from the list, select it, then click Delete .
Server	Enter the hostname or IP address for the RADIUS server.
Authentication Port	Enter the port number your server uses for authentication.
Accounting Port	Enter the port number your server uses for accounting.
Shared Secret	Enter the shared secret used by your server.

Step 3 Click **Save**. The server is added to the Current Server List.

Step 4 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-11](#).
- **Save** to save the template. See [Saving the Template, page 6-11](#).
- Another template category to configure more options. See [2.Template Categories, page 6-6](#).

Deleting a Server Manager

Step 1 Complete the following:

Table 6-2 *Deleting Server Manager*

Field	Description
Delete Servers	
Delete Server List	Lists the servers to be deleted. To remove a server from the list, select it, then click Delete .
Delete Server	Enter the hostname or IP address for the RADIUS server to be deleted.
Authentication Port	Enter the port number the server uses for authentication.
Accounting Port	Enter the port number the server uses for accounting.

Step 2 Click **Add Server to Delete List**. The server appears in the Delete Server List.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-11](#).
 - **Save** to save the template. See [Saving the Template, page 6-11](#).
 - Another template category to configure more options. See [2.Template Categories, page 6-6](#).
-

Configuring Custom Values

This option enables you to enter custom values that might not be available in the Template Menu. It also allows you to quickly enter a value, if you know the exact value you want to change, instead of going through the menu.



Note

Any custom values you configure, are applied to the device only after all the other template configurations have been applied.



Note

This option should be used only by advanced users.

Custom values are not validated. However, if a configuration contains a combination of custom values and values entered using the templates, the values entered using the templates are validated; only the values entered with the custom configuration are not.

Procedure

Step 1 Select **Custom Values**. The Custom IOS Commands dialog box appears.



Note

Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.



Note

If the custom value you enter is the same as an existing one in the Template Menu, the custom value will override the value in the menu.

Step 2 Enter the IOS commands.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-11](#).
 - **Save** to save the template. See [Saving the Template, page 6-11](#).
 - Another template category to configure more options. See [2.Template Categories, page 6-6](#).
-

Previewing the Template

Procedure

-
Step 1	Click Preview . A Command Preview window displays the configuration choices you have made to the template.
Step 2	Click Save. See Saving the Template, page 6-11 .
-

Saving the Template

When you save a template, the WLSE first validates the template and displays the valid Device Type (WLSM), and the corresponding Device Version(s) for that template.

Procedure

-
Step 1	Click Save in the left pane to complete creating a template. The Save dialog box appears in the right pane.
Step 2	Click Save to create the template.
Step 3	Do one of the following: • Click Yes if you want to save the template then schedule a configuration job. The window refreshes to the Job Creation window and a job is automatically created for you using the template name and a random number. See Selecting Devices, page 8-14. • Click No if you want to save the template only. • Click Cancel to cancel the operation and then display the previous screen.
-



Using Wizard Templates

The WLSE allows you to view, copy, delete, and export Wizard configuration templates.

The topics covered are:

- [What is a Configuration Template?, page 7-1](#)
- [Viewing the Existing Templates, page 7-2](#)
- [Creating a Template, page 7-2](#)
- [Copying a Template, page 7-2](#)
- [Deleting a Template, page 7-3](#)
- [Exporting a Template, page 7-4](#)

Related Topics

- [Using IOS Templates, page 5-1](#)
- [Managing Configuration Jobs, page 8-7](#)

What is a Configuration Template?

You can think of a configuration template as a configuration update file that you can apply to large numbers of devices at a time. This file might contain the update for only one parameter or a complete access point configuration.

You can use the **Configure > Templates** option to:

- View existing templates—See [Viewing the Existing Templates, page 7-2](#).
- Create a template—See [Creating a Template, page 7-2](#).
- Copy an existing template—See [Copying a Template, page 7-2](#).
- Delete a template—See [Deleting a Template, page 7-3](#).
- Export a template—[Exporting a Template, page 7-4](#).



Note

You cannot edit a Wizard template. However, you can copy a Wizard template to an IOS template, then use the IOS template choices to edit it.

Viewing the Existing Templates

Use this option to view a configuration template.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** From the list, select the type of templates you want to display, then click Filter
- Step 3** The selected template types are displayed in the Existing Templates table.
-

Creating a Template

Use this option to create a configuration template.

**Tip**

It is strongly recommended that you not use multiple templates to configure the same access point. While you can create multiple templates to configure different groups of access points, it is good practice to use the same template to configure the same access point every time.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** From the list, select **Wizard**.
- Step 3** Click **New**. This launches the Deployment Wizard (see [Using the Deployment Wizard, page 2-1](#)).
- Step 4** Follow the steps in the Deployment Wizard to create a template.
-

Copying a Template

Use this option to copy a configuration template that you can use as a base for another template.

When you copy a Wizard template, the new template appears as an IOS template in the Type column of the Existing Templates table.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Select the template you want to copy from the Existing Templates table, then click **Copy**. A dialog box appears asking you to enter a name for the copy.
- Step 3** Enter a unique name. See [Naming Guidelines, page B-1](#) for details.
- Step 4** Click **OK**. The Templates window refreshes and the new name appears in the Existing Templates table.
- Step 5** Select the template, then click **Edit**. See [Editing a Template, page 7-3](#).
-

Editing a Template

Use this option to edit a *copied* Wizard configuration template. You cannot edit a Wizard template; you can only edit a copy of one.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Select the template you want to edit from the Existing Templates table, then click **Edit**. The window refreshes with Template Creation menu in the left pane and the Template Name dialog box in the right pane.
- Step 3** Select the choices in the Template Menu to create a configuration template.
-

Deleting a Template

Use this option to delete a configuration template.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Select the template you want to delete from the Existing Templates table, then click **Delete**. A window appears asking if you want to delete the template.

**Note**

You cannot delete a template if it is used in a scheduled job.

- Step 3** Click **OK** to delete it.
- Step 4** To import another template, click **Back** and go to [Step 2](#).
- Step 5** When you are finished, click **Done**.
- Step 6** View the template you imported by selecting **Configure > Templates** and selecting it in the Existing Templates table.
-

Exporting a Template

Use this option to export a configuration template to your local drive.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Select a template name from Existing Templates, then click **Export**. The Export Template window appears.
- Step 3** From the list, select the template you want to export, then click **Export**. The Export Template to Desktop window appears with the name of the template.
- Step 4** Right-click on the template name, select Save As, and enter the location to save the template.
- Step 5** Click **Done**.
-



Managing Device Configurations

The WLSE allows you to create templates, schedule and check on the status of configuration jobs, manage configuration archives, and automate configurations.

Following are the subtabs under Configure:

- **Templates**—See [Using IOS Templates, page 5-1](#), [Using WLSM Templates, page 6-1](#), or [Using Wizard Templates, page 7-1](#).
- **Archives**—See [Managing Configuration Archives, page 8-1](#).
- **Jobs**—See [Managing Jobs, page 8-7](#).
- **Auto Update**—See [Automating Configurations, page 8-39](#).
- **Device Specific**—See [Managing Device Specific Configurations, page 8-47](#)

Managing Configuration Archives

As WLAN networks become larger, configuration management becomes more difficult. Each group of devices may have distinct configuration parameters that are difficult to track and maintain manually. The configuration archive feature allows you to easily restore or troubleshoot a failing device by applying the previously stored configuration. It also enables you to archive the last 4 distinct configurations for a device, which you can restore if needed.



Note

Your login determines whether you can use this option.

The topics covered in this section are:

- Viewing, editing, deleting, comparing, and exporting configuration archives—See [Viewing Archived Configurations, page 8-1](#).
- Scheduling a configuration archive job—[Scheduling an Archive Collection, page 8-3](#).
- Viewing the status of a configuration archive job—[Viewing Archive Status, page 8-3](#).

Viewing Archived Configurations

Use this option to view, edit, delete, compare, and export an archived configuration. You can also allow or disallow a configuration archive to be overwritten.

Before You Begin

Before you can view any archived configurations, you must have run an archive job. See [Scheduling an Archive Collection, page 8-3](#) for information on creating and running an archive job.

Procedure

Step 1 Select **Configure > Archives**.

Step 2 Search for a device or select the device for which you want to view a configuration archive from the device selector in the left pane.



Note The icons in the device selector indicate the current status of the access points, not the archive status.

For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).

Step 3 Click the device group or device name and the following table appears:

Field	Description
Device Name	The name of the device.
Archive Name	The name of the archived configuration. Click the Archive Name to view the configuration. A window appears displaying the configuration file for the selected archive.
Date	The date the configuration was archived.
Type	The type of configuration archive.
Overwrite	Indicates if the configuration has been marked as Overwrite. Yes indicates that the configuration is available to be overwritten; No indicates it will not be overwritten.
Edit	Click the icon to edit the information. The Archive Details Window appears. See Editing the Archive, page 8-4 .

Step 4 By selecting the archives in this table you can do any of the following:

- Allow or disallow overwriting—See [Selecting Overwrite Settings, page 8-4](#).
- Delete an archived configuration—See [Applying an Archived Configuration to a Device, page 8-5](#).
- Apply an archived configuration to a device—See [Applying an Archived Configuration to a Device, page 8-5](#).
- Compare configurations—See [Comparing Configurations, page 8-5](#).
- Export a configuration to a file—See [Exporting a Configuration to a File, page 8-5](#)
- Export a configuration to a template—See [Exporting a Configuration to a Template, page 8-6](#)

Scheduling an Archive Collection

Procedure

- Step 1** Select **Configure > Archives**.
- Step 2** Click **Schedule Archive Collection**. The window for creating an archive job appears. See [Archive Job Choices, page 8-28](#).
- Step 3** After scheduling a job, click **View Archives** to return to the **Configure > Archives** window.
-

Viewing Archive Status

Procedure

- Step 1** Select **Configure > Archives**.
- Step 2** Click **View Archive Status**. The window for creating and archive job appears. See [Viewing Archive Job Status, page 8-33](#).
- Step 3** After viewing the archive status, click **View Archives** to return to the **Configure > Archives** window.
-

Editing the Archive

Procedure

Step 1 To edit the archive, complete the following:



Note None of the fields under Details are editable; they are informational only.

Field	Description
Archive Name	Enter a name for the archived configuration.
Overwrite	Select one of the following: Yes—Use this setting to indicate that the configuration archive is available to be overwritten. No—Use this setting to indicate that it will not be overwritten.
Description	Enter a description for the archived configuration.
Details	
Save Time	The date and time the configuration archive was saved.
Type	The type of configuration archive.
Device Name	The name of the device.

Step 2 Click **Save Changes**.

Selecting Overwrite Settings

Use this option to allow an archive to be overwritten or to disallow overwriting it.

Procedure

Step 1 Select a configuration archive configuration.

Step 2 Click one of the following:

- Overwrite—to allow the configuration archive to be overwritten.
- Do Not Overwrite—to make sure the configuration archive is not overwritten.

Deleting Archived Configurations

Use this option to delete an archived configuration from the database. You cannot retrieve a deleted configuration archive.

Procedure

-
- Step 1** Select a configuration from the table.
- Step 2** Click **Delete**.
-

Applying an Archived Configuration to a Device

Use this option to apply an archived configuration to the device.

Procedure

-
- Step 1** Select a configuration from the table.
- Step 2** Click **Apply to Device**.
- A confirmation box displays asking if you are sure you want to apply the configuration.
- Step 3** Click **Yes** to continue. The configuration is applied.
-

Comparing Configurations

Use this option to compare archived configurations.



Tip

You can compare archived configurations for devices that are in different groups by creating a new group, then putting the devices you want to compare into that group.

Procedure

-
- Step 1** Select any two archived configurations you want to compare from the table.
- Step 2** Click **Compare**. A window opens with the selected configurations.
- Differences between the configurations are shown in red; information that is one configuration but not the other are shown in orange.
-

Exporting a Configuration to a File

Use this option to export an archived configuration to a file.

Procedure

-
- Step 1** Select a configuration you want to from the table.
- Step 2** Click **Export to File**. You will be prompted for a location to export the configuration.
-

Exporting a Configuration to a Template

Use this option to export an archived configuration to a template.

Procedure

-
Step 1	Select a configuration you want to from the table.
Step 2	Click Export to Template . The configuration is exported to a template.
Step 3	To view the exported template, select Configure > Templates and it is listed in the Existing Templates window.
-

Managing Jobs

There are two types of jobs you can manage in this window:

- Configuration Jobs—See [Managing Configuration Jobs, page 8-7](#).
- Archive Jobs—[Managing Archive Jobs, page 8-25](#).

Managing Configuration Jobs

This window allows you to view a list of configuration jobs. It also allows you to create, edit, undo, and perform other operations on configuration jobs.

The configuration job types include:

- Config Regular—Jobs created to apply template configurations to devices.
- Config Auto—Jobs created using the Auto Update option.
- Archive Regular—Jobs created using the Schedule Archive Collection option.

The topics covered in this section are:

- [How Do WLSE Configuration Jobs Work?, page 8-8](#)
- [In What Order are the Template Configurations Applied to the Devices?, page 8-8](#)
- [Recommendations For Running Configuration Jobs, page 8-9](#)
- [Creating a Configuration Job, page 8-18](#)
- [Viewing Configuration Job Status, page 8-18](#)
 - [Filtering a Configuration Job, page 8-22](#)
 - [Editing a Configuration Job, page 8-23](#)
 - [Running a Configuration Job Again, page 8-23](#)
 - [Deleting a Configuration Job, page 8-24](#)
 - [Copying a Configuration Job, page 8-24](#)
 - [Viewing the Job Run Details Tables, page 8-24](#)

Related Topics

- [Using IOS Templates, page 5-1](#)

How Do WLSE Configuration Jobs Work?

Access points use jobs created by the **Configure > Jobs** option to make configuration updates.

When the WLSE configures access points, it pushes raw IOS CLI commands to the access points over a telnet or SSH connection.

To update the configuration, therefore, the WLSE requires only the telnet or SSH user name and password access point credentials.

Related Topics

- [Recommendations For Running Configuration Jobs, page 8-9](#)
- [Creating a Configuration Job, page 8-18](#)

In What Order are the Template Configurations Applied to the Devices?

When you create a template using several categories (Association, Services > CDP, etc.) the commands associated with each category are applied sequentially to the device, but the order in which each category is applied is random.

For example, if you create an IOS template made up of two categories, Basic Security and SecurityManager > SSID 802.11 b/g, all the commands generated by the Basic Security category are applied in order. However, the commands associated with the Security Manager > SSID 802.11b/g might be applied before the commands generated for Basic Security.

Any custom values you configure, are applied to the device only after all the other template configurations have been applied. Any device specific values are applied to the device only after all other template configurations and custom values have been applied.

For Config Regular and Config Auto Jobs, the following template order is maintained:

1. Security: Server Manager
2. Services: VLAN
3. Services: Filters - IP Filters
4. Services: Filters - MAC Address Filters
5. Security: Admin Access
6. Security: Local Radius Server - General Set-Up
7. Security : WEP Key Manager 802.11b/g
8. Security : WEP Key Manager 802.11a
9. Basic Security
10. Security : SSID Manager 802.11b/g
11. Security : SSID Manager 802.11a
12. Security : Advanced Security
13. Services: Telnet/SSH
14. Services: Hot Standby
15. Services: CDP-Cisco Discovery Protocol
16. Services: DNS - Domain Name Service
17. Services: Filters - EtherType Filters

18. Services: HTTP- Web Server
19. Voice Express
20. Services: QoS Policies
21. Services: QoS Policies 11b/g - Traffic Class Definition
22. Services: QoS Policies 11a - Traffic Class Definition
23. Stream - Packet Handling Radio 802.11a
24. Services: SNMP- Simple Network Management Protocol
25. Services: NTP- Network Time Protocol
26. Services: ARP Caching
27. Services: Spanning Tree Protocol
28. Basic Settings
29. Network Interfaces: FastEthernet Settings
30. Network Interfaces: Radio-802.11b/g
31. Network Interfaces: Radio-802.11a
32. Wireless Services: AP
33. Wireless Services: WDS - Wireless Domain Services - Settings
34. Association: Activity Timeout
35. Event Log: Configuration Options
36. Event Log: Notification Options
37. Custom Values: Custom IOS Commands
38. Device Specific: Device Specific Settings
39. System Config

Recommendations For Running Configuration Jobs

There are two interrelated questions you should consider when you use the WLSE configuration feature:

- How many devices should be included in the job?
- How much time should be allotted for the job?

How Many Devices?

Because the WLSE configuration feature is multi-threaded with up to 20 allotted threads, it can configure as many as twenty access points simultaneously. For example, a configuration job with 100 devices will begin by configuring twenty devices, one thread per device. When a device configuration completes, its thread will start on a new device immediately, even if the other configuration tasks are in progress. However, the maximum limit of devices can be configured in single job is 500.

How Much Time?

When calculating the amount of time it takes to configure an access point, the factors to consider are:

- How long does it take to download the template via TFTP or push IOS CLI commands to the access point?

TFTP download and IOS CLI command pushes are highly dependent on network performance. The WLSE has an internal configuration parameter that specifies a timeout value for configuration jobs. If the WLSE is unable to complete the job within the timeout period, it will declare the job as a failure. A timeout value that is set too low may cause the WLSE to prematurely abort configuration jobs or improperly report a device configuration failure. So if you have high latency issues or a congested network, increase the configuration timeout setting.

- How long does it take for the access point to reboot if required by the configuration change?

The amount of time to reboot and load new firmware is usually constant. However, if the access point uses DHCP to get an IP address or retrieve a configuration file when it comes up after a reboot, this time is also affected by network performance. This may cause issues with the configuration job timeout, so you may need to increase the timeout.

Here are some other factors that might influence configuration times:

- Configuration jobs sometimes fail due to configuration parameter dependencies on the access points. Consult the access point documentation to understand if there are any configuration dependencies if you have issues with configuration jobs failing.
- Large templates take longer to apply and are more prone to issues with parameter dependencies. If you are applying a large template and seeing configuration failures, it may be useful to break the template into multiple templates and run multiple configuration jobs.

For example, configuration tasks can be greatly simplified by using the WLSE device grouping feature. Suppose a WLSE administrator has created a group for the access points in Site A, sub-groups for Channels 1, 6, and 11, and moved the appropriate access points into the channel groups. Now, the administrator can create three separate templates to set the Channel IDs to Channels 1, 6, and 11. Then to set the access points to the correct channel, three configuration jobs can be created to map the correct template to the corresponding channel group.

Calculating the Estimated Change Window

Configuration jobs should be kept to a reasonable size. Typically, a job with 100 devices is a reasonably sized job, but that can vary. A configuration job should be able to complete within a change window. To calculate this window, use a formula similar to the one recommended for firmware:

$$T = (n / 10) * t + s$$

where:

- T is the total time for the change window
- n is the number of devices in the configuration job
- t is the estimated time to configure a single device
- s is the safety factor.

In this formula, T is often a constant defined by IT policies. For example, many campuses allow for a change window of no more than two hours. If you determine that it will take more than T to configure the access points, plan the upgrades in phases, each of which can be completed well within the change window. It is always a good idea to plan configuration changes conservatively. One conservative way to use this formula is to use the configuration timeout setting as your value for t.

Configuration Job Choices

When you create or edit a configuration job, the following choices appear in the left pane of the Jobs window:

**Caution**

Clicking on another Configure subtab before you have saved your entries in this window will cause the window to reset and you will lose all the information you entered.

1. **Job Name**—See [Naming the Configuration Job](#), page 8-11.
2. **Select Template**—See [Selecting a Template](#), page 8-12.
3. **Select Devices**—See [Selecting Devices](#), page 8-14.
4. **Schedule Job**—See [Scheduling a Configuration Job](#), page 8-15.
5. **Options**—See [Setting Configuration Job Options](#), page 8-15.
6. **Save**—See [Saving the Configuration Job](#), page 8-17.

Before you Begin

Before you schedule a job, make sure you have done the following:

- Ensure all devices of the same device type in the network or within the group of selected devices have the same firmware version. If not, schedule firmware jobs to upgrade the images.
- If device specific settings are configured on the WLSE, ensure that **Enable Device Specific for this Template** is enabled on the template. (See **Configure > Templates > IOS > Device Specific**.)
- Create templates based on device type or on a set of similar device types. For example, do not include a bridge AP with regular AP in the same group. Create different templates for each.
- Assign a template to a group of devices that share similar deployment characteristics, such as same device type and also similar operational characteristics such as data rates, SSID configuration, beacon intervals etc.
- Enable SSH across all devices in the network for secure configuration. Include these settings in the template.
- Ensure that the same template is associated with the AP when it is configured as a job or through the Auto-Config option.
- If DHCP is configured to obtain the configuration from the TFTP server, ensure the same template is associated with a specific AP.
- Ensure the template is complete, including proper SNMP, SSH (or Telnet) credentials, and that AAA configured correctly. Also ensure the native VLAN is configured correctly to maintain connectivity. If the AP configuration succeeds, the WLSE automatically updates the access credentials from those specified in the template.

Naming the Configuration Job**Procedure**

- Step 1** Click **Job Name**. The Job Name dialog box appears.
- Step 2** Complete the following:

**Note**

Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Table 8-1 **Job Name**

Field	Description
Job Name	Enter a name for the job. See Naming Guidelines, page B-1 .
Description	Enter a description of the job. See Naming Guidelines, page B-1 .

- Step 3** From the menu in the left pane, go to the next step, Select Template. For additional information, see [Selecting a Template, page 8-12](#).

Selecting a Template

Procedure

- Step 1** Click **Select Template**. The Select Template window appears.

- Step 2** Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Table 8-2 **Select Template**

Field	Description
Configuration Template	From the list, select the template which you want to apply to the devices.
Name	Displays the name of the selected template.
Device Types	Displays the device types that are valid for the selected template.

Table 8-2 **Select Template (continued)**

Field	Description
Device Versions	Displays the device versions for the device types listed in the Device Type field. Each device type's valid versions are displayed in sequence and grouped using parentheses. If the template is applicable to an access point with an 802.11g radio, it cannot be applied to an access point with an 802.11b radio. A template that is valid for a 1310 wireless bridge in AP mode cannot be applied to 1310 wireless bridge that is in bridge mode, and vice versa. If a 1310 wireless bridge is in workgroup bridge mode, the job will fail because the WLSE does not support configurations on workgroup bridges. which will be noted in the job run log.
Description	Displays the template description.
Version Check Enabled	Indicates whether the version check is enabled.

Step 3 From the menu in the left pane, go to the next step, Select Devices. For additional information, see [Selecting Devices, page 8-14](#).

Selecting Devices

The maximum number of devices that can be configured in a single job is 500.

Procedure

Step 1 Click **Select Devices**. The Select window appears.



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Step 2 From the device selector, click the folder from which you want to build a device list.

- Clicking the folder displays the folder's contents in the Available Devices list box.
- Repeat this step as many times as necessary to select devices from the folder in which they reside.

Step 3 From the Available Devices list, select folders or individual devices, then click >>. The devices appear in the Selected Devices list box.



Note If you select a folder, the template will be applied to all of the devices in that folder. If a device is subsequently added to the folder, the template is applied to that device.

Step 4 To remove devices, select them from the Selected Devices list, then click <<.

Step 5 From the menu in the left pane, go to the next step, Select Template. For additional information, see [Scheduling a Configuration Job, page 8-15](#).

Scheduling a Configuration Job

Procedure

Step 1 Click **Schedule Job**. The Schedule Job dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Table 8-3 **Schedule Job**

Field	Description
Run Now	Click to run the job. Note This option ignores any dates you have entered in Start Date and Start Time.
Start Date	From the lists, select the month, day, and year you want your job to run.
Start Time	From the list, select the hour and minutes of the day you want your job to run.
Repeat	
Enable	Check to run the job repeatedly.
Every	Indicate how often you want the job to repeat by entering a numerical value, then selecting an interval of time: Hours, Days, Months, or Years.

Step 3 From the menu in the left pane, go to the next step, Options. For additional information, see [Saving the Configuration Job, page 8-17](#).

Setting Configuration Job Options

Procedure

Step 1 Click **Options** in the left pane to complete creating a job. The Options dialog box appears in the right pane.

Table 8-4 **IOS Template Job**

Field	Description
Email Settings	
On completion, email to	Enter a comma-separated list of email addresses to be notified when the job completes.

Table 8-4 IOS Template Job

Field	Description
Email only if job fails	Select this checkbox if you want recipients to be notified only if the job fails.
Apply Template to Running Configuration Click See detail to see for additional information about this option.	Select this checkbox if you want to apply the template to the running configuration, then specify the method: Telnet or SSH.
Copy Running Configuration to Startup Configuration (Write NVRAM on Success)	Select this checkbox if you want this template, after the job has succeeded, to be used by the access point in the event of a reload.
Apply Template To Startup Configuration Click See detail to see for additional information about this option.	 Caution This option is recommended for advanced users only. Use it when you are sure that the new template is a complete configuration which can replace the existing configuration on the device(s), and when you are sure that the device(s) can be safely rebooted. Select this checkbox to overwrite the existing configuration on the device with the selected configuration template, then specify the method: Telnet or SCP. Click See detail to see for additional information about using the SCP method.

**Tip**

If email notification is not working, you may need to configure the mailroute by selecting **Admin > Appliance > Configure Mailroute**.

- Step 2** From the menu in the left pane, go to the next step, Save. For additional information, see [Saving the Configuration Job](#), page 8-17.

Saving the Configuration Job

When you run a configuration job, the jobs are validated to make sure that the configuration template you selected is applicable to the devices you selected.

If the job encounters validation problems, a window displays the found errors or warnings.

- **Warnings**—They are issued when there are version mismatches and are not critical. You can still force the template on the devices despite the warnings. Warnings are caused by one of the following reasons:
 - The selected device is running a software version that is not currently supported.
 - The selected device version does not match the device versions supported by the selected template.
- **Errors**—They are issued based on device type mismatches and are critical. You cannot force a configuration template on a device with job errors; you must correct the problem.

Procedure

-
- Step 1** Click **Save** in the left pane to complete creating a job. The Save dialog box appears in the right pane with the job details.



Note If a warning message appears saying that WLSE server is ahead of or behind your local time, see [Understanding Time Discrepancy Problems in Job Scheduling, page 1-11](#).

- Step 2** Click **Save**. A window displays comments to indicate whether the job has passed the validation tests.
-

Creating a Configuration Job

Using this option, you can create a configuration job.

If you are creating a job that includes device specific settings, make sure that you enabled them under **Configure > Templates > IOS > Device Specific**.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Configure > Jobs**.
- Step 2** Click **Config Job**. The Jobs Window appears.
- Step 3** Select the numbered choices in the left pane to create a job. For a description, see [Configuration Job Choices](#), page 8-10.
-

Viewing Configuration Job Status

This window allows you to view job status. It also allows you to filter a job, edit a job, and view details about the job.

Device data is polled every 15 minutes by default, and the duration that job data is retained is 30 days. To change either default, see [Managing Polling Parameters](#), page 4-66.

The topics covered in this section are:

- [Creating a Configuration Job](#), page 8-18
- [Viewing the Configuration Job](#), page 8-18
- [Filtering a Configuration Job](#), page 8-22
- [Editing a Configuration Job](#), page 8-23
- [Running a Configuration Job Again](#), page 8-23
- [Deleting a Configuration Job](#), page 8-24
- [Copying a Configuration Job](#), page 8-24
- [Viewing the Job Run Details Tables](#), page 8-24

**Note**

Your login determines whether you can use this option.

Related Topics

- [Using IOS Templates](#), page 5-1

Viewing the Configuration Job

Procedure

-
- Step 1** Select the status of the job you want to view from the Job State list.

Step 2 Select the type of job you want to view from the Job Type list.

If you select Config Auto, the User field always displays WLSE as the user.

Step 3 Click **Apply**. The window refreshes and the jobs are displayed.

The tables vary depending on the type of Job State and Job Type you selected: •[Scheduled and Unscheduled](#), •[Running](#), or •[All](#).

- Scheduled and Unscheduled

Field	Description
Job Name	The job name.
Recurring	Whether the job recurs.
Next Schedule	For scheduled jobs, this indicates the next time the job will run. For completed jobs, this is last time the job ran.
Last Run Status	The status of the last run. Note Jobs that cause an access point to reboot are listed as Unverified.
User	The user who created the job. Note If you upgrade from a previous release to Release 2.9, and have scheduled a recurring job, the user will appear as WLSE after the upgrade.

- Running

Field	Description
Job Name	The job name.
Recurring	Whether the job recurs.
Job Start Time	The time the job started.
Percent Complete	The percent of the job that has completed running.
Next Schedule	The next time the job is scheduled to run.
User	The user who created the job. Note If you upgrade from a previous release to Release 2.9, and have scheduled a recurring job, the user will appear as WLSE after the upgrade.

- All

Field	Description
Job Name	The job name.
Recurring	Whether the job recurs.
Job State	The state of the job (Completed, Scheduled, etc.)
Next Schedule	For scheduled jobs, this indicates the next time the job will run. For completed jobs, this is last time the job ran.
Last Run Status	The status of the job the last time it ran. For more information, see Understanding Job Status Information, page 8-21 .
User	The user who created the job. Note If you upgrade from a previous release to Release 2.9, and have scheduled a recurring job, the user will appear as WLSE after the upgrade.

Step 4 To sort table data, click on the column heading by which you want to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 5 Do any of the following:



Note If the option is not available for the job type, the buttons are grayed.

- Filter the job—See [Filtering a Configuration Job](#), page 8-22.
- Edit the job—See [Editing a Configuration Job](#), page 8-23.
- Run the job again—See [Running a Configuration Job Again](#), page 8-23.
- Delete the job—See [Deleting a Configuration Job](#), page 8-24.
- Copy a job—See [Copying a Configuration Job](#), page 8-24.
- View the run details—See [Viewing the Job Run Details Tables](#), page 8-24.
- Refresh the screen—Click **Refresh**.

Understanding Job Status Information

[Table 8-5 on page 8-21](#) describes the status of the job.

Table 8-5 **Job Status**

Status	Meaning
Success	The configuration job for all devices was successful..
Failed	The configuration job for all devices failed. Rerun the job by clicking Job Run Details , then click one of the options to rerun the job. See Viewing Job Run Details , page 8-37.
Partial Success	The configuration job failed for some of the devices, not all. Rerun the job by clicking Job Run Details , then click one of the options to rerun the job. See Viewing Job Run Details , page 8-37.
Success (no backup)	The configuration update succeeded but a backup could not be performed.
Aborted	This job status can be caused by one of the following: • An unexpected failure occurred and the configuration job did not complete. Select the job, and click Run Again. • A user stopped the configuration job before it completed.
Not verified	The job status cannot be verified, whether the job completed or not. For example, if the configuration job caused a device to reboot, the WLSE may not be able to verify whether the job succeeded.
Running	The job is running.
Not run	The job does not have any devices on which to run the job.
Waiting	The job has just entered the queue to run.

Filtering a Configuration Job

Use this option to filter jobs from the displayed list. Filtering this way allows you to display a limited set of jobs, making it easier to search for a particular job if you know the name.

Procedure

-
- Step 1** Click **Filter Job**. The Filter Job dialog box appears.
- Step 2** Enter the name, or part of the a name, on which to filter. Use % as a wildcard to filter jobs. For example, entering %name% will filter all the jobs that contain “name.”
- Step 3** Click **Apply filter**. The Job window refreshes and the matching jobs are displayed on the Jobs list.



Note The filter is applied only until the page is refreshed.

Editing a Configuration Job

Use this option to edit jobs from the displayed list of jobs.

Procedure

-
- Step 1** Select the job from the list which you would like to edit.
- Step 2** Click **Edit Job**. The Job Name dialog box appears.
- Step 3** Select the choices in the Template Menu to create a configuration template. For a description, see [Configuration Job Choices, page 8-10](#).
-

Running a Configuration Job Again

Use this option to run jobs again from the displayed list of jobs.



Note This option works only for Run Now jobs.

Procedure

-
- Step 1** Select the job or jobs from the list which you would like to re-run.
- Step 2** Click **Run Again**. A confirmation box appears verifying the job was run.
-

Deleting a Configuration Job

Use this option to delete jobs from the displayed list of jobs. Jobs that are scheduled, unscheduled, completed and did not start can be deleted. Jobs that are running cannot be deleted.

Procedure

-
- Step 1** Select the job from the list which you would like to delete.
- Step 2** Click **Delete Job**.
-

Copying a Configuration Job

Use this option to copy unscheduled jobs from the displayed list of jobs, which can be run later on demand.

Procedure

-
- Step 1** Select the job from the list which you would like to copy.
- Step 2** Click **Copy Job**. A dialog box appears.
- Step 3** Enter a name for the job, then click **OK**. The screen refreshes and the job is listed.
-

Viewing the Job Run Details Tables

The Job Runs Details the following tables display:

Table 8-6 **Job Runs**

Field	Description
Job StartTime	The time the job started.
Job End Time	The time the job ended.
Job Status	The status of the job. For more information, see Understanding Job Status Information , page 8-21.
Percent Complete	The percent of the job that has completed.

Select any of the jobs, in the Job Runs table, then you can click the following options:

- **Show Run Details**—The information for the selected job is displayed in [Table 8-7](#).

- **Job Run Log**—A window displays the job log information.
- **Refresh**—The screen refreshes.

Table 8-7 **Job Run Details**

Field	Description
Device Name	The name of the device.
Start Time	The time the job started.
End Time	The time the job ended.
Status	The status of the job. For more information, see Understanding Job Status Information, page 8-21 .

You can click the following options:

- **Select All**—Selects all the jobs listed.
- **DeSelect All**—Deselects all the jobs listed.



Note If you have multiple screens, you must Select All or DeSelect All one screen at a time.

- **Rerun for All Failed Devices**—Re-runs all failed jobs.
- **Rerun for All Selected Devices**—Re-runs all selected jobs.

Managing Archive Jobs

This window allows you to view a list of archive jobs. It also allows you to create, edit, and perform other operations on archive jobs.

The topics covered in this section are:

- [How Do Configuration Archive Jobs Work?, page 8-26](#)
- [Recommendations For Using Configuration Archives, page 8-27](#)
- [Creating an Archive Job, page 8-33](#)
- [Viewing Archive Job Status, page 8-33](#)
 - [Filtering an Archive Job, page 8-35](#)
 - [Editing an Archive Job, page 8-36](#)
 - [Running an Archive Job Again, page 8-37](#)
 - [Deleting an Archive Job, page 8-37](#)
 - [Copying an Archive Job, page 8-37](#)
 - [Viewing the Job Run Details Table, page 8-38](#)

How Do Configuration Archive Jobs Work?

The **Configure > Archive** feature allows you to set up a job that will archive an access point configuration. When a configuration archive job runs, the WLSE uses TFTP to download the configuration from the access point. If the configuration is identical to the previous archived configuration, the new configuration is not saved. If the new configuration is different from the previous archive, a new archived configuration is saved as a file on the WLSE.

The feature can archive a maximum four different configurations. By default, archived configurations can be overwritten after the maximum number of configurations has been reached. You can, however, mark an archived configuration as protected, so that it cannot be overwritten. If the maximum numbers of configurations are archived and all of the files are protected against overwrites, the WLSE will not create a new configuration archive.

Using this option, you can also:

- View existing archived configurations.
- Compare any two archived configurations within a WLSE device group.
- Export archived configurations to a file or to a WLSE configuration template.

Related Topics

- [Recommendations For Using Configuration Archives, page 8-27](#)
- [Scheduling an Archive Collection, page 8-3](#)

Recommendations For Using Configuration Archives

There are several issues to consider when using the Configuration Archive feature:

- Q.** When should archive jobs be run?
 - A.** Configurations are downloaded from access points to the WLSE using TFTP, which means that configuration archival is potentially sensitive to network congestion and oversubscription. Therefore, due to the potential sensitivity to network conditions and because configuration archival is a low-priority background task that can be affected by higher priority processes, archive jobs should be run during off-hours.
- Q.** How many devices should I include in an archive job?
 - A.** The number of devices assigned to a configuration archive job will vary depending on network congestion and WLSE performance factors. Some WLSE users have successfully archived hundreds of configurations in a single job, while others have had difficulty with less than one hundred.

Arriving at a good number for an archive job may be a trial-and-error process. For example, you could start with twenty-five devices. If that is successful, try fifty. Keep adding more devices until configurations are no longer archived satisfactorily.
- Q.** How often should I archive configurations?
 - A.** The recommended frequency of configuration archival varies with deployment and operational requirements and WLSE performance capabilities. Typically, device configurations do not change much after a network becomes stable. Therefore, after archiving the initial baseline configurations, you might need to run configuration archive jobs as monthly recurring jobs or only after known changes have been made to network configurations.
- Q.** What should be protected from overwrites?
 - A.** After archiving baseline configurations for the network devices, you should protect these official configurations. For additional protection, export the archive to a file and to a configuration template. A configuration template can be used if a roll-back is required.
- Q.** How can I take advantage of the WLSE grouping feature?
 - A.** The WLSE grouping feature is especially useful when configuring configuration archive jobs. Each configuration archive job should operate on a logical grouping of devices. For example, it might make sense to archive configurations per campus or per building. See [Recommendations For Running Configuration Jobs, page 8-9](#), for details on organizing the managed WLAN with the WLSE grouping feature.
- Q.** How can I use the compare feature effectively?
 - A.** The configuration archive compare feature allows you to compare any archived file with any other archived file within a device group. The comparison feature is really most relevant for examining the difference between two configuration archives from access points of the same type or access points that are deployed identically to other access points.
- Q.** What should I do when some configuration archives fail?
 - A.** Because WLSE configuration archive jobs download configurations using TFTP, some devices might fail during the archive job. The job run log files typically contain information about why the configuration archival for a device might have failed. Typically, rerunning an archive job for any devices that have failed is all that is necessary.

If the entire configuration archive job fails, verify that the WLSE is configured with the correct device credentials. If the WLSE has the correct credentials, there are probably network issues to resolve.

Related Topics

- [Managing Archive Jobs, page 8-25](#)

Archive Job Choices

When you create or edit an archive job, the following choices appear in the left pane of the Jobs window:

1. **Job Name**—See [Naming the Archive Job, page 8-29](#).
2. **Select Devices**—See [Selecting Devices, page 8-29](#).
3. **Schedule Job**—See [Scheduling an Archive Job, page 8-31](#).
4. **Finish**—See [Finishing the Archive Job, page 8-31](#).

**Note**

All these steps, except Schedule Job, must be completed, but do not have to be done in order.

Related Topics

[Recommendations For Using Configuration Archives, page 8-27](#)

Naming the Archive Job

Procedure

Step 1 Click **Job Name**. The Job Name dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Table 8-8 **Job Name**

Field	Description
Job Name	Enter a name for the job. See Naming Guidelines, page B-1 .
Description	Enter a description of the job. See Naming Guidelines, page B-1 .

Step 3 From the menu in the left pane, go to the next step, Select Devices. For additional information, see [Selecting Devices, page 8-14](#).

Selecting Devices

The maximum number of devices that can configured in single job is 500.

Procedure

Step 1 Click **Select Devices**. The Select window appears.



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

- Step 2** From the device selector, click the folder from which you want to build a device list.
- Clicking the folder displays the folder's contents in the Available Devices list box.
 - Repeat this step as many times as necessary to select devices from the folder in which they reside.



Note The icons in the device selector indicate the current status of the access points, not the archive status.

- Step 3** From the Available Devices list, select folders or individual devices, then click >>. The devices appear in the Selected Devices list box.



Note If you select a folder, the template will be applied to all of the devices in that folder. If a device is subsequently added to the folder, the template is applied to that device.

- Step 4** To remove devices, select them from the Selected Devices list, then click <<.

- Step 5** From the menu in the left pane, go to the next step, Schedule Job. For additional information, see [Scheduling a Configuration Job, page 8-15](#).
-

Scheduling an Archive Job

Procedure

Step 1 Click **Schedule Job**. The Schedule Job dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Table 8-9 **Schedule Job**

Field	Description
Run Now	Click to run the job. Note This option ignores any dates you have entered in Start Date and Start Time.
Start Date	From the lists, select the month, day, and year you want your job to run.
Start Time	From the list, select the hour and minutes of the day you want your job to run.
Repeat	
Enable	Check to run the job repeatedly.
Every	Indicate how often you want the job to repeat by entering a numerical value, then selecting an interval of time: Hours, Days, Months, or Years.

Step 3 From the menu in the left pane, go to the next step, Finish. For additional information, see [Finishing the Archive Job, page 8-31](#).

Finishing the Archive Job

Procedure

Step 1 Click **Finish** in the left pane to complete creating a job. The Finish dialog box appears in the right pane.

Step 2 Complete the following:

Field	Description
On completion, email to	Enter a comma-separated list of email addresses to be notified when the job completes.
Email only if job fails	Select this checkbox if you want recipients to be notified only if the job fails.
Configuration Type	Select the type of configuration.

**Tip**

If email notification is not working, you may need to configure the mailroute by selecting **Admin > Appliance > Configure Mailroute**.

Step 3 Click **Save**. A confirmation window appears with the job summary.

Creating an Archive Job

Using this option, you can create an archive job.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Configure > Jobs**.
- Step 2** Click **Archive Job**. The Jobs Window appears.
- Step 3** Select the numbered choices in the left pane to create a job. For a description, see [Archive Job Choices, page 8-28](#).
-

Related Topics

[Recommendations For Using Configuration Archives, page 8-27](#)

Viewing Archive Job Status

This window allows you to view job status. It also allows you to filter a job, edit a job, and view details about the job.

The topics covered in this section are:

- [Viewing the Archive Job, page 8-33](#)
- [Filtering an Archive Job, page 8-35](#)
- [Editing an Archive Job, page 8-36](#)
- [Running an Archive Job Again, page 8-37](#)
- [Deleting an Archive Job, page 8-37](#)
- [Copying an Archive Job, page 8-37](#)
- [Viewing the Job Run Details Table, page 8-38](#)

**Note**

Your login determines whether you can use this option.

Viewing the Archive Job

Procedure

-
- Step 1** Select the status of the job you want to view from the Job State list.
- Step 2** Select Archive Regular from the Job Type list.
- Step 3** Click **Apply**. The window refreshes and the jobs are displayed.
- The tables vary depending on the type of Job State and Job Type you selected: •[Scheduled and Unscheduled](#), •[Running](#), or •[All](#).
- Scheduled and Unscheduled

Field	Description
Job Name	The job name.
Recurring	Whether the job recurs.
Next Schedule	For scheduled jobs, this indicates the next time the job will run. For completed jobs, this is last time the job ran.
Last Run Status	The status of the last run.
User	The user who created the job. Note If you upgrade from a previous release to Release 2.9, and have scheduled a recurring job, the user will appear as WLSE after the upgrade.

- Running

Field	Description
Job Name	The job name.
Recurring	Whether the job recurs.
Job Start Time	The time the job started.
Percent Complete	The percent of the job that has completed running.
Next Schedule	The next time the job is scheduled to run.
User	The user who created the job. Note If you upgrade from a previous release to Release 2.9, and have scheduled a recurring job, the user will appear as WLSE after the upgrade.

- All

Field	Description
Job Name	The job name.
Recurring	Whether the job recurs.
Job State	The state of the job.
Next Schedule	For scheduled jobs, this indicates the next time the job will run. For completed jobs, this is last time the job ran.

Field	Description
Last Run Status	The status of the job the last time it ran.
User	The user who created the job. Note If you upgrade from a previous release to Release 2.9, and have scheduled a recurring job, the user will appear as WLSE after the upgrade.

Step 4 To sort table data, click on the column heading by which you want to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 5 You can do the following:



Note If the option is not available for the job type, the buttons are grayed.

- Filter the job—See [Filtering an Archive Job](#), page 8-35.
- Edit the job—See [Editing an Archive Job](#), page 8-36.
- Delete the job—See [Deleting an Archive Job](#), page 8-37.
- Run the job again—See [Running an Archive Job Again](#), page 8-37.
- Copy a job—See [Copying an Archive Job](#), page 8-37.
- View the run details—See [Viewing Job Run Details](#), page 8-37.
- Refresh the screen—Click **Refresh**.

Filtering an Archive Job

Use this option to filter jobs from the displayed list. Filtering this way allows you to display a limited set of jobs, making it easier to search for a particular job if you know the name.

Procedure

- Step 1** Click **Filter Job**. The Filter Job dialog box appears.
- Step 2** Enter the name, or part of the a name, on which to filter. Use % as a wildcard to filter jobs. For example, entering %name% will filter all the jobs that contain “name.”
- Step 3** Click **Apply filter**. The Job window refreshes and the matching jobs are displayed on the Jobs list.



Note The filter is only applied until the page is refreshed.

Editing an Archive Job

Use this option to edit jobs from the displayed list of jobs.

Procedure

- Step 1** Select the job from the list which you would like to edit.
 - Step 2** Click **Edit Job**. The Job Name dialog box appears.
 - Step 3** Select the choices in the Archive Job Menu to edit the job. For a description, see [Archive Job Choices](#), page 8-28.
-

Running an Archive Job Again

Use this option to run jobs again from the displayed list of jobs.

**Note**

This option works only for Run Now jobs.

Procedure

-
- Step 1** Select the job or jobs from the list which you would like to re-run.
- Step 2** Click **Run Again**. A confirmation box appears verifying the job was run.
-

Deleting an Archive Job

Use this option to delete jobs from the displayed list of jobs. Jobs that are scheduled, unscheduled, completed and did not start can be deleted. Jobs that are running cannot be deleted.

Procedure

-
- Step 1** Select the job from the list which you would like to delete.
- Step 2** Click **Delete Job**.
-

Copying an Archive Job

Use this option to copy unscheduled jobs from the displayed list of jobs, which can be run later on demand.

Procedure

-
- Step 1** Select the job from the list which you would like to copy.
- Step 2** Click **Copy Job**. A dialog box appears.
- Step 3** Enter a name for the job, then click **OK**. The screen refreshes and the job is listed.
-

Viewing Job Run Details

Use this option to view details about a job.

Procedure

-
- Step 1** From the table displayed in **Configure > Jobs** window, select a job for which you would like to see details, then click **Job Run Detail**.
- Step 2** The details window appears with the Job Runs table:

Field	Description
Select Run	Used to select a job for which you want to see more details.
Job Start Time	The time the job started.
Job End Time	The time the job ended.
Job Status	The status of the job.
Percent Complete	The percent of the job that completed.

Step 3 Do any of the following:

- To view details for a particular job run, select the job, then click **Show Run Details**. The Job Run details table displays the information. See [Viewing the Job Run Details Table, page 8-38](#).
- To view the job run log, click **Job Run Log**. A window displays all the details for the selected job number.
- To refresh the table, click **Refresh**.

Viewing the Job Run Details Table

The Job Runs Details table displays the following information:

Field	Description
Device Name	The name of the device.
Start Time	The time the job started.
End Time	The time the job ended.
Status	The status of the job.

- To sort table data, click on the column heading by which you want to sort the data:
 - A triangle indicates ascending order.
 - An upside-down triangle indicates descending order.
 - No triangle indicates that the data is not sorted.

Automating Configurations

This window allows you to automatically upload configuration templates to access points and bridges. Use this feature to:

- Apply startup templates through the DHCP server to newly installed devices with manufacturer-default configurations.
- Apply a common template to devices the first time they are discovered, auto managed, and the WLSE has their inventory information.

The topics covered in this section are:

- [Creating a Startup Configuration Template, page 8-39](#)
- [Assigning a Startup Configuration, page 8-41](#)
- [Assigning an Auto-Managed Configuration, page 8-43](#)

Creating a Startup Configuration Template

The startup configuration is used to bootstrap a device to allow the WLSE to discover it.

**Caution**

The startup configuration template is placed in tftpboot directory and anyone who knows the file name can access it. This template should contain only minimal feature settings.

To create a startup template select **Configure > Templates**. (To configure the access point manually without using a startup configuration, see [Getting Started with Device Management, page 4-1](#).)

**Caution**

Do not use the Reload command in a startup configuration.

Use the following table to guide you in creating a startup configuration template for IOS devices:

(See [In What Order are the Template Configurations Applied to the Devices?](#), page 8-8 for information about the order in which the template choices are applied.)

Tasks	Template Choice	Notes
Enable Cisco Discovery Protocol (CDP)	Select Services > CDP .	CDP is required for the WLSE to discover devices on the network.
Enable Telnet	Select Services > Telnet/ .	Select Enable for Telnet.

Tasks	Template Choice	Notes
Enable SSH	Select Services > Telnet/SSH.	Do the following: 1. Select Enabled for Secure Shell. 2. Enter the system name, where the system name is the host name of the IOS access point. For a factory- default IOS access points, this name is by default set to ap. 3. Enter the domain name. For example, cisco.com. Note For any version earlier than 12.2(11)JA, you will have to manage the access points, then create and upload a template that enables SSH on those access points.
Enable SNMP	Select Services > SNMP.	SNMP is required for the WLSE to discover and manage the device. Select Enabled for Simple Network Management Protocol (SNMP).
Create a Read community string	Select Services > SNMP.	Do the following: 1. Enter a community string in the SNMP Community field. 2. Select Read-Only. Note The read community string must be specified under Devices > Discover > Device Credentials > SNMP Communities.
Create a Write community string	Select Services > SNMP.	Do the following: 1. Enter a community string in the SNMP Community field. 2. Select Write-Only. Note The write community string must be specified under Admin > Device Credentials.

**Note**

Access points come with a factory default username, password, and SSID. If you do not want the defaults, apply a custom template to remove them.

Assigning a Startup Configuration

The startup configuration is used for newly-installed devices that have a manufacturer-default configuration. After the devices are powered on and receive an IP address from a DHCP server, the startup configuration will be automatically uploaded to the devices.

**Tip**

After the access point is powered on and the startup configuration is applied, you may want to prevent the startup configuration from being uploaded to devices again if for some reason the access points reboot.

For access points with Version 12.2(13)JA or later: Prevent the initial configuration from being uploaded to devices after a reboot by using the IOS config command **no boot upgrade**. Enter this command in the Custom Value template.

Before You Begin

1. Create a template for the startup configuration. See [Creating a Startup Configuration Template, page 8-39](#).
2. Make sure that the AP SNMP strings are setup correctly by selecting **Devices > Discover > Device Credentials > SNMP Communities**.
3. If you are configuring
 - A DHCP server, go to step 5.
 - A router as a DHCP server, go to step 4.
4. To configure a router as a DHCP server, enter the following commands:

```
ip dhcp pool (name)
network (network address) (subnet mask)
bootfile (startup file)
next-server (WLSE IP address)
default-router (default router)
domain-name (domain name)
dns-server (DNS IP address)
```

In this example, use the **next-server** command instead of option 66 or option 150.

5. To configure a DHCP server, do the following:
 - a. Return the WLSE's address. This is done by entering the <IP address of the WLSE> in the **Boot Server Host Name** field (option number 066) on the DHCP server.
 - b. Return the name of the initial template file in the DHCP reply message. This is done by entering <startup file name> in the **BootfileName** field (option number 067) on the DHCP server.

For example, if you had a WLSE with the IP address 10.10.11.12 and an associated startup template with Bootfile Name "newap1200.ini", you would do the following:

- a. On the DHCP server, select **Scope > Scope Options**.
- b. Set Scope option 066 (TFTP boot server name or IP address) with **10.10.11.12** (the WLSE's IP address).
- c. Set Scope option 067 (Bootfile Name) with **newap1200.ini** (the new Bootfile Name associated with the startup template file.)

Related Topics

- [Creating a Startup Configuration Template, page 8-39](#)
- [Assigning an Auto-Managed Configuration, page 8-43](#)

Procedure

Step 1 Select **Configure > Auto Update > Startup Configuration**. The Startup Configuration Template dialog box appears.

Step 2 Complete the following:

Field	Description
Startup Templates	Lists the startup templates that have been created.
Bootfile Name	Enter the configuration file name that appears on the DHCP server.
Description	Enter a description for the configuration.
Configuration Template	From the list select the startup template to assign to the configuration file. Click Details to see the device types and device versions for which the template is valid.
Copy Running Configuration to Startup Configuration (Save Configuration to NVRAM)	Select the checkbox to save the auto-managed configuration to NVRAM.

Step 3 Click **Save** to save the template. Click **Delete** to delete the template.

Step 4 Modify the periodic discovery or run an immediate discovery to get the APs discovered by selecting **Devices > Discover > Discovery Wizard**.

Assigning an Auto-Managed Configuration

Use this option to automatically apply a configuration template to devices the first time they are discovered, auto managed, and the WLSE has their inventory information.

The following topics are covered in this section:

- Assigning an Auto-Managed Configuration Template—See [Assigning Auto-Managed Configuration Templates, page 8-43](#)
- Emailing the Configuration Job Results—See [Using Auto-Managed Options, page 8-47](#)

Assigning Auto-Managed Configuration Templates

When a template is to be applied, the WLSE tries to find a template based on the selected matching criteria. The template with the first matching criteria is applied to the device. The order in which the WLSE searches for matches is as follows:

- MAC Address
- Serial Number
- Device Type + Device Version + Subnet
- Device Type + Device Version
- Device Type + Subnet
- Device Type
- Device Version + Subnet
- Device Version
- Subnet

Before you Begin

Make sure that for IOS APs, the Telnet/SSH credentials are entered correctly in the WLSE by selecting **Devices > Device Credentials > Telnet/SSH User /Password**.

Procedure

-
- Step 1** Select **Configure > Auto Update > Auto-Managed Configuration > Assign Templates**. The Auto-Managed Configuration Templates dialog box appears with the names of the groups for which you can apply an automated template.
- Step 2** Complete the following:

Table 8-10 *Auto-Managed Configuration Templates*

Field	Description
Auto-Managed Templates	Lists the auto-managed templates that have already been created.
Enable	Select the checkbox to automatically apply a configuration template to the devices, after they are auto managed, that matches the criteria below.
Name	Enter a name for the auto-managed configuration.

Table 8-10 **Auto-Managed Configuration Templates (continued)**

Field	Description
Description	Enter a description for the configuration.
Configuration Template	From the list select the template to assign to the configuration file. Click Details to see the device types and device versions for which the template is valid.
Matching Criteria	
MAC Address	1. Select the checkbox to enable the MAC address matching. 2. Enter a MAC address, or select an existing one from the list, then click >> to add it to the list of valid MAC addresses for that template  Note The existing MAC addresses list is populated by enabling filtering for auto managed devices under Devices > Discover > Discover > Advanced Options. 3. To remove a MAC address from the list, select it, then click Remove.
Serial Number	1. Select the checkbox to enable the serial number matching. 2. Enter the device serial number (top assembly serial number), then click >> to add it to the list of valid serial numbers for that template. 3. To remove a serial number from the list, select it, then click Remove.

Table 8-10 **Auto-Managed Configuration Templates (continued)**

Field	Description
Description	Enter a description for the configuration.
Configuration Template	From the list select the template to assign to the configuration file. Click Details to see the device types and device versions for which the template is valid.
Matching Criteria	
MAC Address	1. Select the checkbox to enable the MAC address matching. 2. Enter a MAC address, or select an existing one from the list, then click >> to add it to the list of valid MAC addresses for that template  Note The existing MAC addresses list is populated by enabling filtering for auto managed devices under Devices > Discover > Discover > Advanced Options. 3. To remove a MAC address from the list, select it, then click Remove.
Serial Number	1. Select the checkbox to enable the serial number matching. 2. Enter the device serial number (top assembly serial number), then click >> to add it to the list of valid serial numbers for that template. 3. To remove a serial number from the list, select it, then click Remove.

Table 8-10 **Auto-Managed Configuration Templates (continued)**

Field	Description
Device Types	1. Select the checkbox to enable the device type matching. 2. Enter the device type, or select an existing one from the list, then click >> to add it to the list of valid devices for that template. Note the following: – AP350—Auto-managed templates for AP 350s are applied to 350 bridges; you cannot assign a different template for bridges based on device type alone. If the bridges are running a different software version than the AP350s, use a different template for bridges and set the appropriate version numbers. – AP1210—For 1210 access points with dual radios (11a and 11g), use device type 1210. For 1210 access points with a single radio (11g) use device type AP1210-SR. 3. To remove devices from the list, select it, then click Remove.
Device Versions	1. Select the checkbox to enable the device version matching. 2. Enter the version numbers if they are not in the list, or from the list, select the version number, then click >> to add it to the list of valid versions for that template. 3. To remove a version number, select it from the list, then click Remove.
Subnet	1. Select the checkbox to enable subnet matching. 2. Enter the subnet if it is not in the list, or from the list, select the subnet then click >> to add it to the list of valid subnets for that template. 3. To remove a subnet, select it from the list, then click Remove.
Copy Running Configuration to Startup Configuration (Save Configuration to NVRAM.	Select the checkbox to save the auto-managed configuration to NVRAM. Click See detail to see for additional information about this option.
Apply Template to Startup Configuration	Select this checkbox to overwrite the existing configuration on the device with the selected configuration template. Click See detail to see for additional information about this option.

- Step 3** Click **Save** to save the template.
- Step 4** To delete a template, select it from the Auto-Managed Templates listbox, then click **Delete**.
-

Using Auto-Managed Options

This option allows you to email the results of your auto-managed configuration job.

Procedure

- Step 1** Select **Configure > Auto Update > Auto-Managed Configuration > Auto-Managed Options**. The Auto-Managed Configuration Options dialog box appears.
- Step 2** Select the protocol to use: SSH or Telnet. Click **See detail** to see for additional information about using the SSH option.
- Step 3** Select the checkbox to enable email notification, then enter the email addresses.
- Step 4** Enter the email address for the recipients of the notification.



Tip If email notification is not working, you may need to configure the mailroute by selecting **Admin > Appliance > Configure Mailroute**.

- Step 5** Click **Save**.
-

Managing Device Specific Configurations

This window enables you to import, export, and view specific access point settings, such as channel, power, and hostname. You can create a configuration template with these settings and apply them to access points in your network. For information on creating templates with device specific settings, see [Configuring Device Specific Settings, page 5-98](#).



Note Device specific settings are applied after custom configurations.

Using this option, you can:

- Import settings from the desktop—See [Importing Device Specific Configurations, page 8-48](#).
- Export settings to the desktop—See [Exporting Device Specific Configurations, page 8-50](#).
- View current configuration—See [Viewing Device Specific Configurations, page 8-51](#).
- View a report about devices set up with device specific configurations—See [Validating a Device Specific Configuration, page 8-52](#).

Importing Device Specific Configurations

This option allows you to import device settings from a local CSV file on your desktop. (See [About the Device Specific CSV File, page 8-48](#).) The WLSE checks each setting in the file. Invalid settings are discarded and reported in a pop-up window.

You cannot edit the file with the settings using the WLSE. If you need to change the settings, export the file, and use a text editor. When you are finished, re-import the file with the edited settings to the WLSE.

**Note**

When a new access point is installed in the network, its settings and identity number must be imported to the WLSE. Otherwise, it will not receive the specific settings when a periodic configuration job is run.

To ensure that access points are receiving the specific settings, create a periodic configuration job. See **Configure > Jobs > Create Config Job**.

**Tip**

To create device-specific settings for a large group of access points, instead of typing the MAC addresses manually for each device, you can export the Group Identity Report in a CSV format under **Reports > Current**, and obtain all the MAC addresses for that group of access points.

Procedure

Step 1 Select **Configure > Device Specific > Import**. The Import dialog box appears.

**Note**

Click **Learn about the Device Specific Import File** for specific information, or see [About the Device Specific CSV File, page 8-48](#).

Step 2 Complete the following:

Table 8-11 *Import Device Specific Settings*

Field	Description
File Location	Click Browse to locate and select the CSV file containing the specific access point settings.
Remove current entries before importing	Select to remove all the existing settings from the WLSE before importing. If you do not select this option, existing settings remain in the file, matching settings are unchanged, and new settings are added.

Step 3 Click **Import**. The settings are imported.

About the Device Specific CSV File

The file used to import specific settings is an ASCII CSV (comma-separated values) file. Create and edit the CSV file with a text editor.

The following are ignored:

- Fields that are not in the first row of the CSV file.
- Empty values in the CSV file (,,).

Following is a sample:

```
000ff7507295, sjc14-ap27.cisco.com, SJ, ECS, 36, 95, 10, mW, 6, 95, 50, 50, mW, snmp-server community
public RW
000b46faff02, sjc14-ap36.cisco.com, SJ, ECS, 44, 92, 10, mW, 11, 92, 20, 20, dBm, snmp-server community
public RW; snmp-server community private RO
```

The CSV file can contain the following information:

Table 8-12 **Device Specific CSV File**

CSV Column	Description	CLI Command Generated
identity	The access point's Ethernet MAC address. Note This is the only required field; all others are optional.	Not applicable.
hostname	The name configured as the hostname on the access point.	hostname <i>value from CSV column</i>
syslocation	The location configured on the access point.	snmp-server location <i>value from CSV column</i>
syscontact	The name configured as the contact on the access point.	snmp-server contact <i>value from CSV column</i>
radioa_channel	The channel configuration for radio A.	Interface dot11radio 1 channel <i>value from CSV column</i>
radioa_beacon	The beacon interval for radio A.	interface dot11radio 0 beacon period <i>value from CSV column</i>
radioa_power	The power configuration for radio A.	Interface dot11radio 1 power local <i>value from CSV column</i>
powera_unit	The unit for radio A power.	Not applicable.
radiobg_channel	The channel configuration for radios B and G.	Interface dot11radio 0 channel <i>value from CSV column</i>
radiobg_beacon	The beacon interval for radios B and G.	interface dot11radio 0 beacon period <i>value from CSV column</i>
radiob_power_ckk	The CCK power configuration for radios B and G.	Interface dot11radio 0 power local <i>value from CSV column</i>
radiobg_power_ofdm	The OFDM power configuration for radios G.	Interface dot11radio 0 power local ofdm <i>value from CSV column</i>
powerbg_unit	The power unit for radios B and G.	Not applicable.
ap_cli command	The custom CLI command for a particular access point. For multi-line commands, separate each command with a semicolon(;). The maximum length of this field is restricted to 255 characters.	An example of a sample CLI entry in the CSV file is as follows: Interface dot11radio 0;ssid tsunami;authentication open

Exporting Device Specific Configurations

This option allows you to export device settings to a local CSV file on your desktop.

Procedure

-
Step 1	Select Configure > Device Specific > Export . The Export dialog box appears.
Step 2	Click Download CSV file to desktop .
-

Viewing Device Specific Configurations

This option allows you to view the current device settings.

Procedure

- Step 1** Select **Configure > Device Specific > View**. The following settings are displayed:.

Table 8-13 Viewing Device Specific Settings

Field	Description
Identity	The access point's Ethernet MAC address. This address is found at the back of the access point.
Host Name	The configured hostname on the access point, which is not the same as the DNS name. If you have configured the access point with a static IP and DNS is not configured, then this setting is recommended.
Location	The location of the access point.
Contact	A contact name.
Channel A	The access point's A radio. (Applicable only if the access point has an A radio).
Beacon A (ms)	The beacon interval in milliseconds.
Power A	The channel's power setting.
Power A unit	The channel power unit: either mW or dBm
Channel B/G	The access point's B/G radio.
Beacon B/G (ms)	The beacon interval in milliseconds.
CCK Power B/G	The CCKM power configuration for radios B and G.
OFDM Power G	The OFDM power configuration for radios B and G.
Power B/G unit	The channel power unit: either mW or dBm.
CLI Command	CLI command specific to the access point.
Last Modified	The last time the access point settings were modified.

To delete

- All the entries in the table, click **Show All** at the bottom of the table, then select the checkbox in the table heading and click **Delete**.
- All the entries on a page, select the checkbox in the table heading and click **Delete**.
- A single entry, select the checkbox next to the row you want to remove, then click **Delete**.

Validating a Device Specific Configuration

This option allows you view a report about:

- Devices for which specific settings have been set up and which are currently managed
- Devices for which specific settings have been set up but are currently not managed.

Procedure

Step 1 Select **Configure > Device Specific > Validation**.

Step 2 From the drop down list select one of the following:

Step 3 **Managed or Unmanaged.**

Depending upon which you select, the following tables are displayed:

- Managed—See [Viewing a Device Specific Report for Managed Devices](#).
- Unmanage—See [Viewing a Device Specific Report for Unmanaged Devices](#).

Table 8-14 *Viewing a Device Specific Report for Managed Devices*

Field	Description
Identity	The access point's Ethernet MAC address. This address is found at the back of the access point.
IP Address	The IP address of the access point.
Host Name	The configured hostname on the access point, which is not the same as the DNS name. If you have configured the access point with a static IP and DNS is not configured, then this setting is recommended.

Table 8-15 *Viewing a Device Specific Report for Unmanaged Devices*

Field	Description
Identity	The access point's Ethernet MAC address. This address is found at the back of the access point.
IP Address	The IP address of the access point.
Host Name	The configured hostname on the access point, which is not the same as the DNS name. If you have configured the access point with a static IP and DNS is not configured, then this setting is recommended.
State	Indicates the current state of the access point.



Upgrading Device Firmware



Note

The firmware subtabs may not be visible to some users. Your login determines whether you can use firmware options.

You can use the WLSE to upgrade the firmware on multiple access points. Upgrading firmware involves:

- Downloading software images to the WLSE or to a remote TFTP server—See [Managing Firmware Images, page 9-3](#).
- Running firmware jobs—See [Managing Firmware Jobs, page 9-11](#).
- Setting firmware parameters, if required—See [Setting Advanced Parameters, page 9-9](#)

You can also view and update the firmware versions supported by the WLSE—See [Viewing and Updating Firmware Versions Supported by the WLSE, page 9-10](#).

About Firmware Upgrades

The topics covered in this section are:

- [How Firmware Upgrades Work, page 9-1](#)
- [Recommendations For Running Firmware Upgrades, page 9-2](#)

How Firmware Upgrades Work

To use the firmware upgrade feature, you must:

1. Download the firmware image to the desktop and import it to the WLSE or import the image directly from Cisco.com to the WLSE. You can also download images to a remote TFTP server.
2. Configure the upgrade job.
3. Schedule the upgrade job or run it immediately.

Usually when a firmware job runs, the WLSE instructs each access point in the upgrade job to download the new firmware from the WLSE. You may want to initiate a TFTP download from a server other than the WLSE if your access points are located remotely.

After an access point downloads new firmware, it reboots. The WLSE tries to contact the access point periodically after the reboot until it verifies that the device has resumed normal operation. The WLSE assumes the upgrade is successful if the access point reboots successfully.

For IOS access points, the WLSE usually initiates the download by using an SNMP set operation, then the access point is rebooted using Telnet/SSH.

Recommendations For Running Firmware Upgrades

For information about the number of devices to include in firmware jobs and the amount of time it takes to run a job, see:

- [Number of Devices in a Job, page 9-2](#)
- [How Much Time to Allocate, page 9-2](#)
- [Calculating the Estimated Time, page 9-2](#)

Number of Devices in a Job

Because the WLSE firmware upgrade feature is multi-threaded with up to 20 allotted threads, it can upgrade as many as twenty access points simultaneously. For example, a firmware upgrade job with 100 devices will begin by upgrading twenty devices, one thread per device. When a device upgrade completes, that thread will start on a new device immediately, even if the other firmware upgrade tasks are in progress.

How Much Time to Allocate

When calculating the amount of time it takes to upgrade an access point, the factors to consider are:

- How long does it take to download the firmware via TFTP?

TFTP download is dependent on network performance. If you have high latency issues or a congested network, allow extra time for the download.

- How long does it take for the access point to reboot and load the new firmware?

The amount of time to reboot and load new firmware is usually constant. However, if the access point uses DHCP to get an IP address or retrieve a configuration file when it comes up after a reboot, this time is affected by network performance.

Here are some other factors that might influence firmware upgrade times:

- In some cases, you may need to change the WLSE firmware upgrade timeout setting to get accurate upgrade job status (see the *FAQ and Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13*). The default setting is usually adequate, but in cases where there are congested and high latency links, the timeout usually needs to be increased.
- If you have access points deployed remotely, consider using the TFTP staging server option, especially if the remote site is at the other end of a slow WAN link or behind a firewall. When you configure the WLSE upgrade job, you select the remote TFTP server option and input the remote TFTP server address.

Calculating the Estimated Time

Assume that a WLAN administrator plans to upgrade 200 AP1100 access points. Preliminary testing has revealed that it takes approximately 5 minutes over a 100 Mbps Ethernet network to upgrade one access point. In this example, 100 Mbps is the slowest connection that the upgrade process will need to traverse; and because the upgrade will be done late at night, network congestion will probably not cause delays in the upgrade. Therefore, a rough estimate of the amount of time needed for the upgrade might be:

$(200 \text{ APs} / 20 \text{ threads}) * 5 \text{ minutes per AP} = 50 \text{ minutes}$

Consider adding a safety factor into the equation. In this example, the WLAN administrator might want to add an additional 45 minutes, in case one device rejects the new firmware and a separate upgrade needs to be started after the first upgrade job completes.

The estimated change window formula can be calculated as follows:

$$T = (n / 20) * t + s$$

where:

- T is the total time for the change window
- n is the number of devices in the upgrade job
- t is the estimated time to upgrade a single device
- s is the safety factor.

In this formula, T is often a constant defined by IT policies. For example, many campuses allow for a change window of no more than two hours. If you determine that it will take more than T to upgrade the access points, plan the upgrades in phases, each of which can be completed well within the change window. It is always a good idea to plan upgrades conservatively. One conservative way to use this formula is to use the firmware upgrade timeout setting as your value for t.

Managing Firmware Images

The options under the Images subtab allow you to:

- Download images to the WLSE—See [Importing Images to the WLSE](#), page 9-6.
- View images downloaded to the WLSE—See [Viewing Images Downloaded to the WLSE](#), page 9-3.
- Edit images on the WLSE—See [Editing Image Details on the WLSE](#), page 9-4.
- Delete images from the WLSE—See [Deleting Images from the WLSE](#), page 9-5.
- Download images to a remote TFTP server if you are updating devices that are located remotely—See [Using a Remote TFTP Server for Updating Devices](#), page 9-9.

Related Topics

- [Managing Firmware Jobs](#), page 9-11
- [About Firmware Upgrades](#), page 9-1

Viewing Images Downloaded to the WLSE



Note

Your login determines whether you can use this option.

You can view the list of images stored on the WLSE and view image details.

Procedure

- Step 1** Select **Firmware > Images**. The Imported Firmware Images selector shows the images that have been imported into the WLSE.

Step 2 To view the list of available images for a type of device, expand its folder.



Note Images that you download to the WLSE are automatically listed in the Firmware Images selector.

Step 3 To view details, select an image. The Image Details window shows the image name, image version, image size, and a description.

Related Topics

[Editing Image Details on the WLSE, page 9-4](#)

Editing Image Details on the WLSE



Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Firmware > Images**.

Step 2 Expand the folder that contains the image you want to edit, then select the image.

Step 3 You can edit the image name, image version, device type, and description as described in [Table 9-1 on page 9-4](#).

Table 9-1 *Image Details*

Field	Description
Name	By default, the name of the image file. Note The image name should be in the following format: *-tar or *-tar.* , where * (asterisk) is any word.
Device Type	The device type to which the firmware applies. Be careful when changing the version; proper uploading of firmware to devices requires accurate version information. You can enter the version in uppercase or lowercase characters. If you change the device type of an image, the image is removed from the former device type folder and added to the new one. For example, if you change the device type from AP340 to AP350, the image is removed from the AP340 folder and added to the AP350 folder.

Table 9-1 *Image Details (continued)*

Field	Description
Version	The image version. Be careful when editing the version; proper uploading of firmware to devices requires accurate version information. You can enter the version in uppercase or lowercase characters. Note To prevent errors when importing, do not rename IOS images. There are several valid formats for image version. You must retain all of the digits and letters and the first decimal point. For example: • Official format—12.2(4)JA1 • Cisco.com format—12.2.4-JA1
Size	Size of the image (read-only field).
Description	An optional description. This field is blank by default.

- Step 4** When you finish editing, click **Save**.
Click **Reset** to cancel your edits.

Related Topics

- [Deleting Images from the WLSE, page 9-5](#)
- [Viewing and Updating Firmware Versions Supported by the WLSE, page 9-10](#)

Deleting Images from the WLSE

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Firmware > Images**.
- Step 2** Expand the folder that contains the image you want to delete, then select the image.
- Step 3** Click **Delete**, then click **OK**.
- Result: The image is deleted from the list of images in the folder and deleted from the WLSE.

Related Topics

- [Viewing Images Downloaded to the WLSE, page 9-3](#)
- [Editing Image Details on the WLSE, page 9-4](#)

Importing Images to the WLSE

This option allows you to:

- Download images to the WLSE from the desktop—see [Importing Images from the Client System Desktop to the WLSE](#), page 9-6.
- Download images to the WLSE directly from Cisco.com—see [Importing Images Directly from Cisco.com to the WLSE](#), page 9-7.

Related Topics

- [Viewing Images Downloaded to the WLSE](#), page 9-3
- [Editing Image Details on the WLSE](#), page 9-4

Importing Images from the Client System Desktop to the WLSE



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Download the desired firmware images to your client system from Cisco.com. You can download firmware images from the following URL:
- <http://tools.cisco.com/support/downloads/pub/MDFTree.x?butype=wireless>
- For information about supported versions of images, see the Supported Devices Table on Cisco.com and the Firmware Supported Versions table in **Administration > System > Firmware Supported Versions**.
- Step 2** Select **Firmware > Images > Import > From Desktop**. Enter information as described in [Table 9-2 on page 9-6](#).

Table 9-2 *Desktop Import Window*

Field	Description
Device Type	Select the device type from the list. Note If you have an AP 1231 or AP1232, select AP1210.
Version	Enter the image version. Be careful when entering the version; proper uploading of firmware to devices requires accurate version information. You can enter the version in uppercase or lowercase characters. Note To prevent errors when importing, do not rename IOS images. There are several valid formats for image version. You must retain all of the digits and letters and the first decimal point must be present. For example: • Official format—12.2(4)JA1 • Cisco.com format—12.2.4-JA1

Table 9-2 Desktop Import Window (continued)

Field	Description
File Location	Enter the path to the image on the desktop or click Browse . Images for Cisco Aironet 350 wireless bridges may be named as images for access points (that is, names begin with <i>AP</i>). To avoid confusion, you can rename these images. See Editing Image Details on the WLSE, page 9-4 .
Overwrite Existing Image	Select this if you are importing an image that is already stored on the WLSE. Otherwise, the image import will fail if the same image is already stored on the WLSE.

Step 3 Click **Import**. *Do not close the popup window until you receive a message that the import was successful or the import failed.*

If the import is successful, a confirmation message appears and the image is saved on the WLSE.

If the import fails, an error message appears. The import may fail for one of the following reasons:

- The image you are trying to import is not valid. An error message appears.
- There is insufficient space on the WLSE to store images.
- You specified an image that already exists in the image library and you did not select the Overwrite Existing Image checkbox in Step 2.
- For an IOS image, you renamed the file or the file is not recognized.

Step 4 Repeat Steps 2 and 3 to import more images.

Step 5 For information on uploading firmware to access points and bridges, see [Managing Firmware Jobs, page 9-11](#).

Importing Images Directly from Cisco.com to the WLSE



Note

Your login determines whether you can use this option.

The first time you attempt to download firmware for IOS access points from Cisco.com, an error message is displayed and you must acknowledge that you have the required cryptography permissions. See the following procedure for the text of the message.

Procedure

Step 1 Select **Firmware > Images > Import > From Cisco.com**. Complete the following:

Table 9-3 Cisco.com Import Window

Field	Description
Cisco.com Username	Your Cisco.com username.
Cisco.com Password	Your Cisco.com password

Table 9-3 Cisco.com Import Window (continued)

Field	Description
Proxy IP/Hostname ¹	The IP address of the proxy server used to mediate between the web browser and Cisco.com. The proxy port used by the proxy server (if required on your network).
Proxy Port	
Proxy Username	The username and password for contacting the proxy server (if required on your network).
Proxy Password	

1. Some proxy server software does not work properly while importing firmware from Cisco.com. If you have problems using your proxy server with this feature, download the firmware image to your desktop from Cisco.com and import the image from the desktop (see [Importing Images from the Client System Desktop to the WLSE](#), page 9-6).

Step 2 To clear all of your entries in the window, click **Clear**.

Step 3 To proceed with image download, click **Login**. The Import window changes to allow you to select the device type.

- If the following message appears under Image Details and you are downloading IOS images, log in to Cisco.com and provide the required information. After that, you can proceed to download IOS images.

```
Error while selecting or displaying image details.
Please log into cisco.com at
http://www.cisco.com/cgi-bin/Software/Crypto/crypto_main.pl
and make sure your username has acknowledged cryptography
permissions for downloading IOS Aironet images.
```

- If a “connectivity failed” message appears, make sure that domain name service (DNS) is configured on the WLSE and DNS can resolve the cisco.com domain name.

Step 4 Click the device type; the firmware versions available on Cisco.com are displayed. Select a firmware version; the image details are displayed.



Note If you have an AP1231 or AP1232, select AP1210.



Note Images for Cisco Aironet 350 bridges are listed in the Import window as Cisco Aironet 350 access point images (that is, the names begin with *AP*). To avoid confusion, you can rename these images after importing them. For more information, see [Editing Image Details on the WLSE](#), page 9-4.

Step 5 To add the image to the Selected Images list, click **Add**.

Step 6 Repeat steps 4 and 5 to add more images.

Step 7 To remove an image from the Selected Images list, click **Remove**.

Step 8 Select **Overwrite Existing Images** if you are importing an image version that is already stored on the WLSE. Otherwise, the image import will fail if the same version is already stored on the WLSE.

Step 9 Click **Import**. The Import Status window appears. *Do not close this window until you receive a message that either says the import was successful or the import failed.*

If the import is successful, a confirmation message appears and the image is saved on the WLSE.

If the import fails, an error message appears. The import may fail for one of the following reasons:

- The image you are trying to import is not valid. In that case, an error message appears.
- There is insufficient space on the WLSE to store images.
- You specified an image that already exists in the image library and you did not select **Overwrite Existing Image** in Step 7.
- This is the first time you have tried to download software that has cryptographic features. You will be directed to log into Cisco.com and fill out a form to provide more information about your organization.

Step 10 Click **Refresh** to refresh the Import Status window; click **Close** to close it.

Step 11 For information on uploading firmware to access points and bridges, see [Managing Firmware Jobs, page 9-11](#).

Using a Remote TFTP Server for Updating Devices

You can download firmware images to a TFTP server and then upload them to access points and bridges. This method of uploading may be quicker than uploading from the WLSE if you have a slow link between the WLSE and the access points and bridges in your network.

To download firmware images from Cisco.com, go to the following URL:

<http://www.cisco.com/public/sw-center/sw-wireless.shtml>

The image file must reside in the main directory for TFTP access on the server (usually the /tftpboot directory).

To make sure you are downloading a supported firmware release, see the list of supported devices and firmware versions at **Administration > System > Firmware Supported Versions**.

Use the normal procedure for creating firmware jobs described in [Managing Firmware Jobs, page 9-11](#). You specify the TFTP server and provide the filename when you specify job options (for more information, see [5. Set Options, page 9-14](#)).

Setting Advanced Parameters

If a firmware job times out before completion, you can increase the values in [Table 9-4 on page 9-10](#) to extend the job timeout and allow the upgrade to complete. The values to use for these parameters depend on:

- How fast the image is pushed to the access point
- The size of the firmware image
- Network latency
- Size of the access point configuration

The default values should suffice for a network in which devices are connected by fast links. Users who have access points in remote locations or branch offices might be familiar with the time it takes to upgrade a single access point without using the WLSE and can increase the timeout values accordingly.

**Note**

Your login determines whether you can use this option.

To set timing parameters for firmware jobs:

Procedure

Step 1 Select **Firmware > Advanced Parameters**.

Firmware Job parameters apply to all firmware jobs.

Step 2 Set the desired parameters as explained in [Table 9-4 on page 9-10](#).

Table 9-4 Advanced Firmware Parameters

Field	Range and Default	Description
Firmware Jobs		
Per device job operation timeout	Default: 7200 seconds	How much time to allow for each device in a firmware job before declaring a job timeout. You should increase this value if: • Devices are in remote locations such as branch offices. • Devices are connected through slow network links.
Device reboot wait timeout	Default: 360 seconds	After a new firmware image is installed, the device is rebooted. This parameter indicates how much time to wait for a device to reboot before attempting to contact it again.
Job confirmation retries	Default: 3 tries	How many times the WLSE attempts to contact a device and confirm the newly installed firmware version.

Step 3 Select **Save** to save your settings.

Step 4 Select **Refresh** to clear any changes you have made but not saved, and restore the settings that were previously saved.

Step 5 Select **Job Status Check** to view firmware job status.

Viewing and Updating Firmware Versions Supported by the WLSE

The WLSE maintains an internal list of officially supported firmware versions. You can view version support by selecting **Admin > System > Firmware Supported Versions**. See [Managing Firmware Version Support](#), page 16-49.

Managing Firmware Jobs

The Jobs subtab allows you to:

- Create firmware jobs—See [Creating and Running a Firmware Job](#), page 9-11.
- View a list of firmware jobs—See [Viewing Job Status Information](#), page 9-20.
- Filter the list of firmware jobs—See [Filtering Jobs](#), page 9-22.
- Edit firmware jobs—See [Editing a Job](#), page 9-22.
- Copy firmware jobs—see [Copying a Job](#), page 9-23.
- Delete firmware jobs—See [Deleting a Job](#), page 9-23.
- View firmware jobs details—See [Viewing Job Run Details and Rerunning/Reverifying Jobs](#), page 9-24.

Related Topics

[Managing Firmware Images](#), page 9-3

Creating and Running a Firmware Job



Note

After a new image is downloaded to an access point, the access point will automatically reboot.

Use the following procedure to create firmware jobs for routine upgrades of the firmware on access points.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Firmware > Jobs**.

Step 2 Enter a name for the job and click **Create Job**.



Note

Job names must be unique. Do not use the same job name for firmware jobs and other jobs (such as configuration and radio management jobs).

For other guidelines on job names, see [Appendix B, “Naming Guidelines.”](#)

Step 3 The window refreshes with the Job Creation menu in the left pane and the Job Name dialog box in the right pane.

Step 4 Select the numbered choices in the left pane to create and run a firmware job. For information on these choices, see [Job Creation Tasks](#), page 9-12.

Job Creation Tasks

When you create or edit a firmware upload job, the following tasks appear in the left pane of the Jobs window. All tasks must be completed whether you are uploading images from the WLSE or from a remote TFTP server. You can omit scheduling the job and edit the job later to provide a schedule. You can complete tasks 1 through 5 in any order.

It is recommended that you download the latest version support file before beginning a firmware job. If the image is not recognized; however, you can still proceed by ignoring the warnings that are displayed in Step 6, Save the Job. For information about versions currently supported by the WLSE and downloading the support file to update the supported versions, see [Managing Firmware Version Support, page 16-49](#).

1. **Job Name**—See [1. Name the Job, page 9-12](#).
2. **Select Image**—See [2. Select the Image, page 9-13](#).
3. **Select Devices**—See [3. Select Devices, page 9-13](#).
4. **Schedule Job**—See [4. Schedule the Job, page 9-14](#).
5. **Options**—See [5. Set Options, page 9-14](#).
6. **Save the Job and Finish**—After completing tasks 1 through 5, you can save the job. After you save the job, it will run if it is an immediate job. If it is scheduled for a later time, it will be added to the schedule of jobs—See [6. Save the Job and Finish, page 9-15](#).



Caution

Clicking on a any subtab (for example, Jobs or Images) before you have saved your entries in the Jobs window will cause the window to reset and you will lose all the information you entered.

1. Name the Job

Procedure

- Step 1** Select **JOB NAME** from the left pane.



Note

Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

- Step 2** Enter the data described in [Table 9-5 on page 9-12](#).

Table 9-5 Job Name Parameters

Field	Description
Job Name	Enter a name for the job. For guidelines on naming jobs, see Appendix B, “Naming Guidelines.” Note Job names must be unique. Do not use the same job name for firmware jobs and other jobs (such as configuration and radio management jobs).
Description	Enter a description of the job. For guidelines on entering descriptions, see Appendix B, “Naming Guidelines.”

- Step 3** Go to the next step, Select Image. See [2. Select the Image, page 9-13](#).
-

2. Select the Image

Procedure

- Step 1** Select **SELECT IMAGE** from the left pane.
- Step 2** Expand the device folder and select the image you want to upload. The Image Detail window opens.
If the desired image does not appear in the tree, you must import it to the WLSE unless the image is located on a remote TFTP server. For more information, see [Importing Images to the WLSE, page 9-6](#).
- Step 3** From the menu in the left pane, go to the next step, Select Devices. See [3. Select Devices, page 9-13](#).
-

3. Select Devices

The maximum number of devices that can configured in single job is 500.

Procedure

- Step 1** Select **SELECT DEVICES** from the left pane. All managed devices are listed in the Device selector in the middle pane.



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

- Step 2** Select devices from the device selector or use Search. For information on using the device selector or search, see [Using the Device Selector, page 1-12](#).
- Step 3** Expand the folder for the group that contains the devices you want to include in the job. Then click the group folder. The group and all its devices are added to the Available Devices list.
For more information on device grouping, see [Managing Groups, page 4-74](#).
- Step 4** From the Available Devices list, select the group or individual devices, then click >>.
- The devices you selected are moved to the Selected Devices list.



Note Device that are moved to the Selected list are removed from the Available Devices list. You can repopulate the Selected list by clicking on the group again.

- The devices in the Selected Devices list box will receive the image you selected.
- Step 5** To add devices from other groups, repeat steps 3 and 4.
- Step 6** To remove devices, select them from the Selected Devices list, then click <<.
- Step 7** Go to the next step, Schedule Job. See [4. Schedule the Job, page 9-14](#).
-

Related Topics

[Managing Groups, page 4-74](#)

4. Schedule the Job

When scheduling a firmware job, you can select **Run Now** to start the job in 2 minutes, or you can schedule the job for a future date and time.

**Note**

You can save a job without scheduling it. You can edit the job later to add the scheduling information. To edit a job, select **Firmware > Jobs**; then select the job from the list and click **Edit Job**.

Procedure

Step 1 Select **SCHEDULE JOB** from the left pane.

**Note**

Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows until now.

Step 2 Schedule the job as follows:

- To run the job now, select the **Run Now** checkbox. The job will begin running immediately.

**Note**

Selecting this option ignores any date and time that you enter from the Start Date and Start Time lists.

- To schedule the job for a later date and time, select the month, day, and year from the Start Date lists and select the hour and minutes from the Start Time lists.

Step 3 Go to the next task, Set Options. See [5. Set Options, page 9-14](#).

5. Set Options

In this task, you can select email notification (optional) and specify the remote server (if you are uploading the image from a remote TFTP server instead of uploading from the WLSE).

Procedure

Step 1 Select **OPTIONS** in the left pane.

Step 2 **Email settings**

If you want to be notified by email when the job finishes, enter the following information in this section.

Table 9-6 *Email Notification Settings for Firmware Jobs*

Field	Description
On completion, mail to	Enter a comma-separated list of email addresses to be notified when the job completes.
Email only if job fails	Select this checkbox if you want recipients to be notified only if the job fails.

**Tip**

If email notification is not working, you may need to set up the mail route by specifying an SMTP server. See [Configuring the Mail Route, page 16-45](#).

Step 3 **Remote server settings section**

If images will be uploaded to devices from a remote TFTP server (instead of being uploaded from the WLSE), enter the information described in [Table 9-7 on page 9-15](#). For information about storing images on the remote TFTP server, see [Using a Remote TFTP Server for Updating Devices, page 9-9](#).

**Note**

When you use this option, the access point might report an Invalid checksum error or Unknown failure. If this happens verify that the image filename entered in the job matches the image filename on the remote TFTP server.

Table 9-7 *Remote TFTP Server Settings for Firmware Jobs*

Field	Description
Use remote server	Select this checkbox to upload the image from a TFTP server. The remote server must have a tftp server running.
Remote server IP address	Enter the IP address of the TFTP server or select a server from the list of recently used servers. Every time you enter a remote server IP address, the address will be added to the Recently used servers list.
Remote server firmware image filename	The filename of the firmware image file on a remote server. The image file must reside in the main directory for TFTP access on the server (usually the /tftpboot directory).

Step 4 Go to the last task, [6. Save the Job and Finish, page 9-15](#).

6. Save the Job and Finish

Procedure

Step 1 Select **SAVE** from the left pane.

**Note**

If a warning message appears saying that WLSE server is ahead of or behind your local time, see [Understanding Time Discrepancy Problems in Job Scheduling, page 1-11](#).

The Save window shows information about the job and the results of the validation tests that the WLSE runs on all firmware jobs. The window may contain warnings or errors:

- A warning usually indicates one of the following problems. You can go back and edit your job choices or choose to proceed in spite of warnings.
 - The action is not advisable; for example, you are downgrading the image version on the devices.
 - You selected an image version that is unknown to the WLSE.

For information about versions currently supported by the WLSE or updating the versions supported by the WLSE, see [Managing Firmware Version Support, page 16-49](#).

- Errors indicate that the job will always fail for those devices.

**Note**

For more information about the messages in the Save window, see [About the Save Window, page 9-18](#).

Step 2 Click **Save**.

- If there are no errors or warnings, the job runs or is scheduled and the Job Summary window appears. Go to Step 3 for more information.
- If there are uncorrected errors or warnings, the Save Confirmation window appears. Proceed as follows, according to whether there are errors or warnings:

**Note**

To remove all of your settings for the job, click **Clear**.

- **If there are only warnings:**

Desired Action	Steps
Apply image to all devices, including those with warnings.	Click Yes . The Job Summary window appears.
Skip devices with warnings and only apply image to devices without warnings.	Click No . The Job Summary window appears.
Correct warnings before proceeding.	1. Click Cancel. The Save window appears. 2. Return to job choices, make corrections, and save job again.

- **If there are warnings and errors:**

Desired Action	Steps
Skip devices with errors. Apply image to all other devices, including those with warnings.	Click Yes. The Job Summary window appears. Note Image will <i>not</i> be applied to devices with errors.

Skip devices with warnings or errors. Apply image to all other devices.	Click No . The Job Summary window appears. Note Image will <i>not</i> be applied to devices with errors.
Correct warnings or errors before proceeding.	1. Click Cancel. The Save window appears. 2. Return to the job choices, make corrections, and save the job again.

– If there are only errors:

Desired Action	Steps
Skip devices with errors. Apply image to all other devices.	Click OK . The Job Summary window appears. Note Image will <i>not</i> be applied to devices with errors.
Correct errors before proceeding.	1. Click Cancel. The Save window appears. 2. Return to job choices, make corrections, and save job again.

- Step 3** When the job is ready to run, the Job Summary window displays the following information and the main Jobs window appears. All new jobs are added to the list of jobs, and immediate jobs start running. For more information about the main Jobs window, see [Viewing Job Status Information, page 9-20](#).

Table 9-8 Save Summary Window

Field	Description
Name	Name of the job.
Description	Job description, if any.
Image	Name of the image selected for the job.
Devices	Names of the devices selected for the job.
Groups	Names of groups selected for the job.
Schedule	Scheduled date and time for the job, or <i>No Schedule</i> if the job has not been scheduled.

- Step 4** After the image is downloaded to the device, the device will be rebooted using SSH. If the attempt to reboot by using SSH fails, the device will be rebooted using Telnet.
- Step 5** For information about job status, see [Viewing Job Status Information, page 9-20](#).

To view the status of jobs at any time, select **Firmware > Jobs**.

Related Topics

- [Deleting a Job, page 9-23](#)
- [Viewing Job Status Information, page 9-20](#)
- [Viewing Job Run Details and Rerunning/Reverifying Jobs, page 9-24](#)

About the Save Window

The Save window shows information on the firmware job, including errors and warnings. Messages indicate whether the job has passed the validation tests. For the meaning of the messages, see [Table 9-10 on page 9-18](#).

Table 9-9 **Save Window**

Information type	Description
Image selected, Version, and Device type	Image name, image version, and device type that you selected when creating the job. Usage notes about this image version may also appear.
Duration estimate	Maximum amount of time required to complete the job is indicated by the following message: <i>This job can take as long as xx minutes to complete.</i>
Image version validation	Whether the image version is valid for the selected device type. This field is marked <i>Warning</i> if the image is not recognized. For information on supported firmware versions and viewing information on versions supported by the WLSE, see Managing Firmware Version Support, page 16-49 .
Image known bugs validation	Any major caveats for this image.
Device-Image validation	Whether the selected image is valid for this device: • <i>Error</i> if the image is not valid for the selected device type. • <i>Warning</i> if the image is not recognized by the WLSE. • <i>Information</i> if the same image is already installed on the devices.

Messages in the Save window show the status of each item that is tested by the job validation process:

Table 9-10 **Messages in the Save Window**

Message Type	Description and Solution
<i>Passed</i>	No problems were found.
<i>Information</i>	No problems were found, but there is information you might want to know. For example, the image version you selected is already installed on the device.

Table 9-10 *Messages in the Save Window (continued)*

Message Type	Description and Solution
<i>Warning</i>	The operation is permitted but may not be advisable; for example, downgrading to an earlier image. The image will not be applied to devices that have warnings, unless you choose to ignore warnings. A popup window will be displayed after you click Save in this window and you can decide whether to ignore warnings. The warning messages are: • Device is running a software version that is not currently supported by WLSE—The WLSE does not recognize this software version. You can click Yes when prompted to ignore warnings. • Selected image version has an older version the one currently existing on the device—You are attempting to downgrade the device firmware. You can click Yes when prompted to ignore warnings. • Selected firmware image version is the same as the image running on the device—You can click Yes when prompted to ignore warnings.
<i>Error</i>	The operation is not permitted. The image will not be applied to devices that have errors associated with them. It is recommended that you eliminate the errors before saving the job. If you save a job with errors, the corresponding devices will be ignored during the job run. • Selected image may not valid for device type—The image is not valid for the type of device you selected; for example, you are trying to apply an AP1100 image to an AP350. Remove this device from the job or verify that the image was imported as the appropriate device type. • Select image may not be valid for device type, not supported—Firmware upgrade is not supported for this type of device; for example, the device is a switch. Remove the device from the job. • SNMP protocol not supported for firmware upload on device—Remove the device from the job. • Telnet/SSH credentials are not provided to reboot this device during upgrade, please add them to WLSE before creating the job—An IOS device's Telnet or SSH credentials were not added to the WLSE; therefore, the device cannot be rebooted after the upgrade. You must add the credentials under Devices > Discover > Device Credentials before you can upgrade this device. For more information, see Enter Telnet/SSH Usernames and Passwords—Access Points, page 4-10.

Using the Functions in the Main Jobs Window

To check job status, view job details, filter the job list, edit jobs, copy jobs, or delete jobs, select **Firmware > Jobs**. The main jobs window appears.

Job data is retained for 6 months; this parameter is not configurable.

- To check the status of jobs, see [Viewing Job Status Information, page 9-20](#).
- To filter the list of jobs, see [Filtering Jobs, page 9-22](#).
- To edit a job, see [Editing a Job, page 9-22](#).
- To delete a job, see [Deleting a Job, page 9-23](#).
- To see the details of a job, see [Viewing Job Run Details and Rerunning/Reverifying Jobs, page 9-24](#).

Related Topics

[Creating and Running a Firmware Job, page 9-11](#)

Viewing Job Status Information

For information about specific job states, see [Understanding Job Status Information and Job Run Log Messages, page 9-25](#).

Job data is retained for six months, then purged; this parameter is not configurable.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Firmware > Jobs**.

Step 2 From the Job State list, select the type of job whose status you want to check. The window refreshes and the jobs are displayed.

The information displayed depends on which Job State you selected: **Scheduled**, **Unscheduled**, **Running**, or **All**.

- Scheduled

Field	Description
Job Name	The job name.
Next Schedule	For scheduled jobs, this indicates when the job will run. For completed jobs, this is the time the job ran.
Last Run Status	The status of the last run.
User	The user who created the job.

- **Unscheduled**

Field	Description
Job Name	The job name.
Next Schedule	For scheduled jobs, this indicates when the job will run. For completed jobs, this is the time the job ran.
Last Run Status	The status of the last run.
User	The user who created the job.

- **Running**

Field	Description
Job Name	The job name.
Job Start Time	The time the job started.
Percent Complete	The percent of the job that has completed running.
Next Schedule	Firmware jobs are not recurring.
User	The user who created the job.

- **All**

Field	Description
Job Name	The job name.
Job State	The state of the job. Note A job in the DidNotStart state must be rescheduled.
Next Schedule	For scheduled jobs, this indicates when the job will run. For completed jobs, this is when the job ran.
Last Run Status	The status of the job the last time it ran.
As Of	The time the WLSE polled information from the device.
User	The user who created the job.

Step 3 The following options are provided:

- Filter jobs—See [Filtering Jobs](#), page 9-22.
- Edit a job—See [Editing a Job](#), page 9-22.
- Delete a job—See [Deleting a Job](#), page 9-23.
- Copy a job—See [Table 9-10 on page 9-23](#).
- View job run details—See [Viewing Job Run Details and Rerunning/Reverifying Jobs](#), page 9-24.

Step 4 To refresh the screen, click **Refresh**.

Related Topics

[Using the Functions in the Main Jobs Window, page 9-20](#)

Filtering Jobs

Use this option to display a limited set of jobs, making it easier to search for a particular job by name.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Firmware > Jobs**.
- Step 2** Click **Filter Job**.
- Step 3** Enter the name, or part of the name. You can use % as a wildcard: for example, entering %name% displays all the jobs that contain the word “name.”
- Step 4** Click **Apply filter**. The Job window refreshes and the matching jobs are displayed in the Jobs list.

**Note**

The filter remains in effect until the page is refreshed.

Related Topics

[Using the Functions in the Main Jobs Window, page 9-20](#)

Editing a Job

Use this option to edit jobs from the displayed list of jobs.

**Note**

If you have deleted the image that was associated with the job you are editing, the job will show that no image has been selected.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Firmware > Jobs**.
- Step 2** From the list of jobs, select the job that you want to edit.
- Step 3** Click **Edit Job**.
- Step 4** Select choices in the Job Creation Menu. For descriptions of the choices, see [Job Creation Tasks, page 9-12](#).
-

Related Topics

[Using the Functions in the Main Jobs Window, page 9-20](#)

Deleting a Job

Use this option to delete jobs from the displayed list of jobs. Jobs that are scheduled, unscheduled, completed, or did not start can be deleted. Jobs that are running cannot be deleted.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Firmware > Jobs**.
 - Step 2** From the list of jobs, select the job that you want to delete.
 - Step 3** Click **Delete Job**.
 - Step 4** Click **OK** in the popup windows.
-

Related Topics

[Using the Functions in the Main Jobs Window, page 9-20](#)

Copying a Job

Use this option to copy a job.

**Note**

If you have deleted the image associated with the job that you want to copy, the job will show that no image has been selected.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Firmware > Jobs**.
 - Step 2** From the list of jobs, select the job that you want to copy.
 - Step 3** Click **Copy Job**.
 - Step 4** Enter a name for the job in the popup window. The copy will be unscheduled. To schedule it, select the job and click Edit Job.
-

Related Topics

[Using the Functions in the Main Jobs Window, page 9-20](#)

Viewing Job Run Details and Rerunning/Reverifying Jobs

Use this option to view details about a job.

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **Firmware > Jobs**.

Step 2 From the All Jobs table displayed in the **Firmware > Jobs** window, select a job, then click **Job Run Detail**.

Step 3 The details window shows the following:

Field	Description
Select Run	Select a job to see its details.
Job Start Time	The time the job started.
Job End Time	The time the job ended.
Job Status	The status of the job. For more information, see Understanding Job Status Information and Job Run Log Messages, page 9-25 .
Percent Complete	The percent of the job that completed.

Step 4 Select a job and click the following options:

- **Show Run Details**—Displays the following details for the selected job run: device name, start and end times, and status.
- **Job Run Log**—Displays the job run log in a separate window for the selected job run. For information on the messages in the job run log, see [Understanding Job Status Information and Job Run Log Messages, page 9-25](#). This information is retained 30 days by default. To modify the number of days job run logs are retained, select **Devices > Discover > Inventory > Polling**.
- **Refresh**—Refreshes the screen.
- **Rerun for all Failed Devices**—Re-runs all failed jobs.
- **Rerun for all Selected Devices**—Re-runs selected jobs.
- **Reverify for Not Verified Devices**—Re-verifies jobs that ended with “not verified” status.

Related Topics

[Using the Functions in the Main Jobs Window, page 9-20](#)

Understanding Job Status Information and Job Run Log Messages

This section provides information about:

- [Job Status, page 9-25](#)
- [Job Run Log Messages, page 9-26](#)

Job Status

[Table 9-11 on page 9-25](#) describes the jobs status states for each device in the job and for the overall firmware job.

Table 9-11 Job Status

Status	Meaning
Status for individual devices	
Success	Device was upgraded successfully.
Failed	Upgrade failed.
Not verified	The firmware image was pushed to the device, but the WLSE may have timed out before verifying whether the job succeeded. See Understanding “Not Verified” Job Status, page 9-25 .
Aborted	An unexpected failure occurred and the upgrade did not succeed.
Status for overall firmware job	
Success	All devices in the job were upgraded successfully.
Failed	Upgrade failed for all devices in the job.
Partial Success	Upgrade failed for some devices in the job or ended as “not verified” for some devices in the job. See Understanding “Not Verified” Job Status, page 9-25 .
Not verified	For all devices in the job, the firmware was pushed to the devices, but the WLSE may have timed out before verifying whether the job succeeded. See Understanding “Not Verified” Job Status, page 9-25 .
Aborted	The job aborted because of some unexpected failure.

Understanding “Not Verified” Job Status



Note

A status of “not verified” may not mean that the job failed. The WLSE may have timed out before verifying whether the job succeeded.

If a job ends with the status “not verified,” or fails because of timeouts caused by slow links, you can:

- Use the Reverify option. See [Viewing Job Run Details and Rerunning/Reverifying Jobs, page 9-24](#).
- Rerun the job. See [Viewing Job Run Details and Rerunning/Reverifying Jobs, page 9-24](#).
- Change the values of the job properties parameters in the WLSE, as described below and then rerun the job.

To change job properties parameters that affect timeouts, select **Firmware > Advanced Parameters**.

- If the job ended as “not verified” and the job failed, increase the value of the **Device Reboot Wait Timeout** parameter and run the job again.
- If the job is timing out and failing because the access point and WLSE are connected through a slow link (less than 1.544 Mbps), first increase the value of the **Per device job operation timeout** parameter. For example, for a 56 kbps link, the recommended value is 2400 seconds (40 minutes). For a 128 kbps link, the recommended value is 1200 seconds (20 minutes). Then, run the job again.

Job Run Log Messages

For a normal, successful firmware upgrade, the job run log contains messages similar to the following:

```
Device: 110.80.cisco.com Initiating firmware upgrade.
Device: 110.80.cisco.com Uploading new firmware image, please wait.
Device:110.80.cisco.com Upload completed, proceeding to reboot AccessPoint.
Device: 110.80.cisco.com Waiting for firmware update confirmation.
Device: 110.80.cisco.com Attempting to confirm version installed.
Device: 110.80.cisco.com Actual version is 12.2(11)JA1, expected version is 1.2.211-JA1.
Device: 110.80.cisco.com Firmware update completed successfully.
```

The following error messages may appear in the job run log:

Table 9-12 Error Messages—Firmware Job Run Log

Message	Meaning
SNMP error while initiating firmware upgrade. SNMP write community string was not provided or is incorrect.	The job failed. Enter the correct write community string for the device in Devices > Device Credentials . For more information about the required community strings, see the <i>Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine, 2.12</i> on Cisco.com.
SNMP error while confirming version for <i>access_point</i> . Device could have been rebooting. See the documentation on how to increase the Job Timeout Properties.	The job may or may not have failed. See job status. Also, see the job timeout information in Job Status, page 9-25 .



Using Reports

The Reports tab displays information about your devices. You can save and email reports. You can also set specific times for emailed reports to be run and sent automatically.

The reports available are dependent on the groups of devices and individual devices you choose from the selector in the left pane.



Note

Some of the subtabs may not be visible to some users.

The following topics discuss the reports provided by WLSE:

- [Using the Basic Report Features, page 10-1](#)
- [Using the Device Center, page 10-7](#)
- [Displaying Radio Manager Reports, page 10-15](#)
- [Displaying Voice Reports, page 10-24](#)
- [Displaying Wireless Client Reports, page 10-37](#)
- [Displaying Current Reports, page 10-45](#)
- [Displaying Trends, page 10-83](#)
- [Displaying Real-Time Reports, page 10-97](#)
- [Displaying Intrusion Detection System Reports, page 10-103](#)

Using the Basic Report Features

The WLSE reports share several common features. The following topics describe these features:

- [Using the Device Selector, page 10-2](#)
- [Sorting Table Data, page 10-2](#)
- [Exporting a Report, page 10-2](#)
- [Exporting URL-Based Report Data, page 10-2](#)
- [Emailing a Report, page 10-3](#)
- [Scheduling Email Jobs, page 10-5](#)

Using the Device Selector

The WLSE contains a device selector and Search that can be used to select a group or devices or an individual device. For information about how to use the device selector, see [Using the Device Selector, page 1-12](#)

The search results, as well as the folders in the device selector, display icons indicating the alarm status of the devices. For an explanation of the icons, see [Understanding the Icons, page 1-12](#).

For information about the folders for device groups in the device selector, see [System-Defined Groups, page 4-75](#).

Sorting Table Data

For information on how to sort table data, see [Sorting Table Data, page 1-13](#).

Exporting a Report

Procedure

-
- Step 1** Click **Export**. An Export window appears.
 - Step 2** From the Output Format list, select the format in which you want the file exported: CSV, PDF, or XML.
 - Step 3** Click Submit. A window opens and you are prompted to open or save the output in the chosen format. If you select Open, the output opens in the selected application, for example a CSV file opens in an Microsoft Office Excel spreadsheet. If you select Save, the output is saved to the specified location and can be opened with any application.
-

Exporting URL-Based Report Data

The WLSE provides a feature that allows the system administrator to manually enter a URL in the WLSE to export report data, rather than using the UI export function.



Note

This procedure can only be performed by the system administrator with the username admin.

Procedure

-
- Step 1** After you have logged in to the WLSE, enter the following URL in your browser:

```
http://{WLSE name:port /  
ipaddress:port}/servlet/com.cisco.nm.wlse.util.WLSEReportsExportServlet?{parameters}
```

The parameters are as follows and are case sensitive:

 - reporttype**= { Wireless Client | group | device }
 - id**= { group name | client macaddress | device name | device ip address }

family= {Router | Switch | IOSAccessPoint | Wireless Client | EAP | RADIUS | PEAP | EAP-MD5 | group}

reportName = {name} Enter the name of the report.

filetype= {csv | xml | pdf}

reportcategory={current | trends}

tzOffset={time} The time zone offset in minutes for GMT/UTC. Add a + (plus) or - (minus) as appropriate. For example, -300 minutes means 5 hours.

For trend reports, you must add the following parameters:

startdate={YYYY-MM-DD-hh-mm-ss}

enddate={YYYY-MM-DD-hh-mm-ss}



Note The start date and end date are interpreted relative to the time zone offset provided.

topNVal This is required only to display Top N Reports.

DataFrequency={Hourly | Weekly | Daily | Monthly}

save = { yes | no } When exporting data, enter yes to provide a dialog box to open or save the report in the selected format, or enter no to open the report in the same window.

Following is an example of a URL to generate XML output for Group Performance Report: RF Utilization:

```
http://172.19.28.139:1741/servlet/com.cisco.nm.wlse.reports.util.WLSEReportsExportServlet?
id=AP%201100&reporttype=group&family=group&reportName=Group%20Performance%20Report%203A%2
0RF%20Utilization&tzOffset=330&filetype=xml&reportcategory=trends&startdate=2005-6-21-00-00-0
0&enddate=2006-8-21-23-59-59&DataFrequency=Hourly&save=no
```

Emailing a Report

All reports can be exported via email. These reports can be mailed on-demand, as one-time scheduled jobs, or at recurring intervals. Although IT policies vary depending on the deployment environment, consider scheduling weekly email exports of trending reports and exporting inventory reports as needed. For example, some of the security configuration inventory reports might be exported on a monthly basis as part of an ongoing security audit.

Before You Begin

Configure the mailroute so that the WLSE knows where to send the e-mails. Enter the mail server hostname or IP address by selecting **Administration > Appliance > Configure Mailroute**.

Procedure

- Step 1** Click **Email Report**. A the right pane refreshes with an Email properties dialog box.

Step 2 Enter the following:



Tip

If email notification is not working, you may need to configure the mailroute by selecting **Administration > Appliance > Configure Mailroute**.

Field	Description
To	Enter the email address of the person to whom you want to send the report. An entry in this field is required.
Cc	Enter email addresses of persons that you want to copy on the email.
Subject	Enter a subject for the email.
Attachment Type	From the list, select the format in which you would like the report sent: CSV, PDF, or XML. CSV and XML formats are designed to be used by automated tools.
Message	Enter any message you would like to send.

Step 3 To cancel the email, click **Cancel**.

Step 4 To send the email immediately, click **Send Now**.

Step 5 To schedule the email for later:

- a. Click **Schedule**. The schedule job dialog box appears.
- b. Enter the following:

Field	Description
Job Name	Enter a name for the job. For more information, see Naming Guidelines, page B-1 .
Report Data for Last	From the list, select the number of days, weeks, or months for which you want the hourly/daily, weekly, or monthly report data emailed. Note This entry is applicable to Trends reports only.
Start Date	From the list, select the date you would like to send the email.
Start Time	From the list, select the time you would like to send the email.
Repeat	
Enable	Check if you want to set up a scheduled job that periodically sends email.
Every	From the list, select the period of time you would like the email sent.

Step 6 Do one of the following:

- Click **Cancel** to cancel the schedule.
- Click **Finish** to complete scheduling. You receive a confirmation message that your email has been scheduled.

Step 7 To view, delete, or edit the scheduled email jobs, see [Scheduling Email Jobs, page 10-5](#)

Scheduling Email Jobs

This window allows you to view information about email jobs you have scheduled. It also allows you to delete them and edit them.


Note

For information about creating an email job, see [Emailing a Report, page 10-3](#).

The length of time job data is retained is 30 days by default. To change the default setting, select **Devices > Discover > Inventory > Polling**.


Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Reports > Scheduled Email Jobs**. The Email Jobs window appears.

Field	Description
Job Name	The name of the job. For more information, see Naming Guidelines, page B-1 .
Recurring	Indicates whether it is a recurring job.
Next Schedule	Indicates when the job runs again.

Step 2 To delete a job, select it, then click **Delete Email Job**.

Step 3 To view an email job, select it, then click **View Email Job**. See [Viewing Email Job Details, page 10-5](#).

Step 4 To edit a job, select it, then click **Edit Email Job**. See [Editing an Email Job, page 10-6](#).

Viewing Email Job Details

The following tables are displayed in a window when you select a job in **Reports > Scheduled Email Jobs**, then click **View Email Job**.

Report Properties

Column	Description
User Name	The name of the user who scheduled the job.
Report Type	The report type.
Report Name	The report name.

Email Properties

Column	Description
To	The username of the person to whom the report is being emailed.
Cc	The username of the person to whom the report is being copied.
Subject	The email subject.
Email Format	The format in which the report is being emailed.
Body	The text entered into the body of the email.

Schedule Properties

Column	Description
Email Job Name	The name of the email job.
Start Date	The date the report is emailed.
Frequency	The frequency with which the report is to be emailed.

Editing an Email Job

Procedure

Step 1 Click **Edit Email Report**. The selected email job is displayed.

Step 2 Change any of the following email properties:

Field	Description
To	Edit the email address of the person to whom you want to send the report. An entry in this field is required.
Cc	Edit email addresses of persons that you want to copy on the email.
Subject	Edit the subject for the email.
Attachment Type	From the list, select the format in which you would like the report sent: CSV, PDF, or XML.
Message	Edit any message you would like to send.



Tip

If email notification is not working, you may need to configure the mailroute by selecting **Administration > Appliance > Configure Mailroute**.

Step 3 Change any part of the following email schedule:

Field	Description
Start Date	Edit the date the report is emailed.
Start Time	Edit the time the report is emailed.
Repeat	Change the setting for scheduling a recurring job by deselecting or selecting the checkbox.
Every	Change the period of time you want the email sent.

Step 4 Click **Save** to save your edits, or **Cancel** to discard them.

Using the Device Center

The device center enables you to quickly access various types of reports for a particular device.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Reports > Device Center**. The Device Center appears above the device selector in the left pane.

Step 2 Search for a device or select the device for which you want a report from the device selector in the left pane. See [Using the Device Selector, page 1-12](#).



Note

Device information might not display properly if you are viewing the reports with a Firefox browser; it does not support line breaks or long text (maximum 50 characters).

Step 3 Click for different report types:

- [Access Points and Bridges, page 10-7](#)
- [WDS-WLSM, page 10-8](#)
- [WDS-AP, page 10-8](#)
- [Switches, page 10-8](#)
- [Routers, page 10-8](#)
- [Servers, page 10-9](#)

Access Points and Bridges

- Summary Report—See [Displaying an AP Summary Report, page 10-65](#)
- Detailed Report—See [Displaying a Detailed Report, page 10-67](#)
- Fault Status—See [Viewing the Fault Status Report, page 10-13](#)
- Device History—See [Viewing Device History, page 10-13](#)
- Config History—See [Viewing Config History, page 10-14](#)

- Firmware History—See [Viewing Firmware History, page 10-14](#)
- AP Web Page—Opens up a browser window to the AP Summary Status.

**Tip**

The HTTP port on access points must be set to 80 for this link to work. For information on setting up the HTTP port, see [Enter HTTP/HTTPS Port Settings—Access Points, page 4-13](#).

- AP Config—Displays the access point's current configuration.
- Auto Config Retry—[Viewing the Auto Config Retry Report, page 10-15](#).

WDS-WLSM

- WDS Summary Report—See [Viewing the WDS Summary Report, page 10-10](#).
- Fault Status—See [Viewing the Fault Status Report, page 10-13](#)
- Device History—See [Viewing Device History, page 10-13](#)
- WDS Registered APs—[Viewing the WDS Registered APs Report, page 10-12](#).
- WDS Mobility Groups—[Displaying a Mobility Groups Report, page 10-82](#)
- WDS Mobility ID Report—[Displaying a Mobility ID Report, page 10-82](#)

WDS-AP

- Summary Report—See [Displaying an AP Summary Report, page 10-65](#)
- Detailed Report—See [Displaying a Detailed Report, page 10-67](#)
- WDS Summary Report—See [Viewing the WDS Summary Report, page 10-10](#).
- WDS Registered APs—[Viewing the WDS Registered APs Report, page 10-12](#).
- Fault Status—See [Viewing the Fault Status Report, page 10-13](#)
- Device History—See [Viewing Device History, page 10-13](#)
- Config History—See [Viewing Config History, page 10-14](#)
- Firmware History—See [Viewing Firmware History, page 10-14](#)
- AP Web Page—Opens up a browser window to the AP Summary Status.

**Tip**

The HTTP port on access points must be set to 80 for this link to work. For information on setting up the HTTP port, see [Enter HTTP/HTTPS Port Settings—Access Points, page 4-13](#).

- AP Config—Displays the access point's current configuration.
- Auto Config Retry—[Viewing the Auto Config Retry Report, page 10-15](#).

Switches

- Summary report—See [Displaying a Switch Summary Report, page 10-77](#)
- Fault Status—See [Viewing the Fault Status Report, page 10-13](#)
- Device History—See [Viewing Device History, page 10-13](#)

Routers

- Summary Report—See [Displaying a Router Summary Report, page 10-79](#)
- Fault Status—See [Viewing the Fault Status Report, page 10-13](#)

- Device History—See [Viewing Device History, page 10-13](#)

Servers

Summary Report—See [Displaying a Server Summary Report, page 10-80](#).

Viewing the WDS Summary Report

The following reports are displayed for the device's wireless domain services (WDS) summary:

- AP-WDS Report—See [AP-WDS Summary Report](#).
- WLSM-WDS Report—See [WLSM-WDS Summary Report](#)

Table 10-1 *AP-WDS Summary Report*

Column	Description
Name	The access point name.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays , page 1-10
MAC Address	The MAC address of the access point.
IP Address	The IP address of the access point. Click to open a browser window to the AP Summary Status. Tip The HTTP port on access points must be set to 80 for this link to work. For information on setting up the HTTP port, see Enter HTTP/HTTPS Port Settings—Access Points , page 4-13.
Status	The operational status of the device: • Admin standalone—Configured as the WDS but with no other devices participating. • Active—The WDS is actively performing as the WDS on the subnet. • Backup—The WDS is acting as a backup to the main WDS. • Candidate—The device is configured as a WDS candidate.
WDS Priority	The access point's assigned WDS priority number.
Subnet Address	The access point's subnet address.
Subnet Mask	The access point's subnet mask.
Active WDS IP Address	The IP address of the active WDS.
Last WDS Election Time	The last time this access point was elected as a WDS.
Number of Infrastructure Nodes Registered with WDS	The number of access points registered with the WDS.
WLSE to WDS Authentication Status	The status of the authentication of the WLSE with the WDS.
WLSE IP Address Configured at WDS	The IP address of the WLSE.

Table 10-2 WLSM-WDS Summary Report

Column	Description
Name	The access point name.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10
MAC Address	The MAC address of the WLSM.
IP Address	The IP address of the WLSM.
Subnet Address	The WLSM subnet address.
Subnet Mask	The WLSM subnet mask.
Number of Infrastructure Nodes Registered with WDS	The number of access points registered with the WDS.
WLSE to WDS Authentication Status	The status of the authentication of the WLSE with the WDS.
WLSE IP Address Configured at WDS	The IP address of the WLSE.
Switch containing the WLSM	The IP address of the switch that contains the WLSM.
HSRP Redundant Status	The status of the hot standby router interface.
HSRP Virtual IP Address	The virtual IP address of the hot standby router interface.

Viewing the WDS Registered APs Report

The following table provides information about the access points that are registered with the WDS.

Table 10-3 *WDS Registered APs Report*

Column	Description
AP Name	The access point name.
AP IP Address	The IP address of the access point.
Subnet Address	The access point's subnet address.
Subnet Mask	The access point's subnet mask.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Viewing the Fault Status Report

The following table is displayed for the device's fault status:

Table 10-4 **Device Fault Status**

Column	Description
Type	The fault type.
Description	A description of the fault. Click to see fault details. See Viewing Fault Details, page 3-7 .
Severity	The fault severity level.
State	The current state of the fault.
Timestamp	The time the fault was reported. Click to see fault details. See Viewing Fault Details, page 3-7 . For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Viewing Device History

The following table is displayed for the device's history:

Table 10-5 **Device History**

Column	Description
Timestamp	The time the device's state last changed. For more information, see Understanding WLSE Time Displays, page 1-10 .
Device Name	The name of the device.
IP Address	The IP address of the device.
State	The current state of the device.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Viewing Config History

The following table is displayed for the device's configuration history:

Table 10-6 *Device Configuration History*

Column	Description
Start Time	The start time for the device's configuration.
End Time	The end time for the device's configuration.
Job Status	The state of the configuration job.
Template Name	The name of the configuration template used. An asterisk (*) indicates that the template has been modified since it was applied to the device.
Job Name	The name of the configuration job.
Job Type	The type of configuration job.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Viewing Firmware History

The following table is displayed for the device's firmware history:

Table 10-7 *Device Firmware History*

Column	Description
Start Time	The start time for the device's firmware upgrade job.
End Time	The end time for the device's firmware upgrade job.
Job Status	The state of the firmware job.
Image Name	The name of the firmware image.
Image Version	The version of the firmware.
Image Device Type	The device type.
Job Protocol	The protocol used for the firmware job.
Job Name	The name of the firmware job.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Viewing the Auto Config Retry Report

This report provides information about retries in uploading auto-configuration templates that are deployed using the Deployment Wizard.

Table 10-8 *Auto Config Retry*

Column	Description
Name	The device name.
Device IP	The IP address of the device.
Status	The device status, which is one of the following Deployment Wizard phases: • Error • Initial Startup Config • Initial Discovery Phase • Initial Inventory Phase • Auto Config Job Scheduled • Successfully Configured • Operation Aborted
Boot Time	The time the device booted up.
Template Name	The name of the template designated as the auto config template.
Retry Number	The number of times the WLSE has attempted to upload the template to the device.
Retry Time	The time the auto config job will re-run.
Description	The status description
As Of	The time the status was last updated. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying Radio Manager Reports



Note

If Radio Management has been disabled, the **Reports > Radio Manager** subtab will *not* be displayed. To reenable Radio Management, see [Enabling and Disabling Radio Management Features, page 11-4](#).

The Radio Manager reports allow you to view radio management information.

- Configured Radio Parameters Report—See [Viewing the Radio Configuration Parameters, page 10-16](#)
- Path Loss Between Managed APs Report—See [Viewing Current Path Loss Results, page 10-17](#)

- Path Loss Historical Report—See [Viewing Historical Path Loss Results, page 10-19](#)
- Channel Loading Report—See [Viewing Current Channel Load Results, page 10-19](#)
- Channel Loading Historical Report—See [Viewing Historical Channel Load Results, page 10-21](#)
- Radar Detection Report—See [Viewing Current Radar Detection Events, page 10-21](#)
- Radar Detection Historical Report—See [Viewing Historical Radar Detection Events, page 10-23](#)

Viewing the Radio Configuration Parameters

Use the **Configured Radio Parameters** report to display the radio configuration parameters for a selected access point.

Typical Scenarios and FAQs

- How can I display the current radio configuration parameters for an access point?



Note

Your login determines whether you can use this option.

Before You Begin

- Perform an AP Radio Scan (see [Using AP Radio Scans to Collect RM Data, page 13-43](#))
- Configure the radio parameters by running either:
 - RM Assisted Configuration (see [Using Assisted Configuration, page 13-71](#))
 - Assisted Site Survey Wizard (see [Using the Location Manager Assisted Site Survey Wizard, page 13-17](#))

Procedure

- Step 1** Select **Reports > Radio Manager**. The window refreshes with a device selector in the left pane.
- Step 2** From the device selector, click to expand the folder and select an access point or a folder. The right pane refreshes.
- Step 3** From the Report Name list, select **Configured Radio Parameters Report**.
- Step 4** Click **View**. The Configured Radio Parameters report displays the following information:

Table 10-9 **Configured Radio Parameters Report**

Column	Description
AP Name	The name of the access point.
Interface Name	The name of the radio interface.
MAC Address	The MAC address of the access point.
PHY	The physical interface type (11a, 11b, or 11g) of the radio interface.
Channel	The radio channel used.
Transmit Power	The power level of the radio transmission (in milliwatts).
Data Rate	The data rates supported by this interface (in Mbps).

Table 10-9 *Configured Radio Parameters Report (continued)*

Column	Description
Beacon	The amount of time between beacons (in kilo microseconds). Note This is the configured beacon interval. The fact that the port status is up or down does not change the fact that the beacon interval is set to a certain value.
Admin Status	The administrative status of the access point. For more information about the radio interface port's administrative status values, see Setting RF Port AdminStatus Threshold, page 3-35 .
Operational Status	The operational status of the access point. For an explanation of the possible operational status values, see Viewing the WDS Summary Report, page 10-10 .
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

- [Displaying Radio Manager Reports, page 10-15](#)
- [Using the Basic Report Features, page 10-1](#)
- [Generating Radio Parameters, page 13-66](#)

Viewing Current Path Loss Results

Use the **Path Loss Between Managed APs** report to:

- View the calculated path-loss data after you run AP Radio Scan.
- Periodically to check whether your WLAN radio environment has changed. If the changes are significant, you can use Auto Re-Site Survey (see [Evaluating AP Radio Performance, page 12-6](#)) to automatically trigger an alarm if the changes significantly degrade the network performance or capacity.

For a selected access point, this report displays:

- The surrounding access points that can hear the selected AP.
- The path loss (in decibels) between the selected AP and each of the surrounding APs.

Typical Scenarios and FAQs

- I have just finished running an AP Radio Scan. How can I view the calculated path loss data?
- I have not run an AP Radio Scan recently. How can I check to see if my WLAN radio network has changed?

**Note**

Your login determines whether you can use this option.

Before You Begin

- Perform an AP Radio Scan (see [Using AP Radio Scans to Collect RM Data, page 13-43](#)).
- Be sure that Radio Monitoring is enabled. Radio Monitoring is enabled by default; if it has been disabled, you must re-enable it (see [Using Radio Monitoring to Collect RM Data, page 12-1](#)).

Procedure

- Step 1** Select **Reports > Radio Manager**. The window refreshes with a device selector in the left pane.
- Step 2** From the device selector, click to expand the folder and select an access point or a folder. The right pane refreshes.
- Step 3** From the Report Name list, select **Path Loss Between Managed APs Report**.
- Step 4** Click **View**. The report displays the following data for the selected access points:

Table 10-10 *Path Loss Between Managed APs Report*

Column	Description
AP Name	The name of the access point.
Interface Name	The name of the radio interface.
PHY	The physical interface type (11a, 11b, or 11g) of the radio interface.
Channel	The radio channel used.
Neighbor AP Name	The name of the neighbor access point.
Neighbor Interface Name	The interface name of the neighbor access point.
Path Loss	The amount in decibels of path loss between the two access points.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

- [Viewing Historical Path Loss Results, page 10-19](#)
- [Displaying Radio Manager Reports, page 10-15](#)
- [Using the Basic Report Features, page 10-1](#)

Viewing Historical Path Loss Results

The historical path loss report displays the previous path loss information for selected a AP (or group). The information is collected every 15 minutes and saved to the path loss historical table. The data in the historical table is trimmed every 60 minutes.

**Note**

Your login determines whether you can use this option.

Before You Begin

- Perform an AP Radio Scan (see [Using AP Radio Scans to Collect RM Data, page 13-43](#))
- Be sure that Radio Monitoring is enabled. Radio Monitoring is enabled by default; if it has been disabled, you must re-enable it (see [Using Radio Monitoring to Collect RM Data, page 12-1](#)).

Procedure

- Step 1** Select **Reports > Radio Manager**. The window refreshes with a device selector in the left pane.
- Step 2** From the device selector, click to expand the folder and select an access point or a folder. The right pane refreshes.
- Step 3** From the Report Name list, select **Path Loss Historical Report**.
- Step 4** Click **View**. The report displays the previous path loss data for the selected access points. For more information about path loss data, see [Viewing Current Path Loss Results, page 10-17](#).

Related Topics

- [Viewing Current Path Loss Results, page 10-17](#)
- [Displaying Radio Manager Reports, page 10-15](#)
- [Using the Basic Report Features, page 10-1](#)

Viewing Current Channel Load Results

Radio measurement data, the Clear Channel Assessment (CCA) measurement in particular, provides information about how heavily a channel is loaded. For a selected access point, you can use the **Channel Loading** report to display the percentage of time a channel is being used.

**Note**

This type of report has very little use in case of an isolated office building, but can be very useful in crowded spaces (such as among New York high rise buildings with many WLANs from neighboring companies).

The Channel Loading report shows the background loading of each AP—in particular, how often the channel is busy due to traffic that is not generated by the reporting AP radio. This information is useful even before running AP Radio Scan just to see how busy the environment is before deploying new sets of access points. You can also run this same report from time to time just to see whether this environment has changed.

**Note**

Channel load information is collected only from access points on the Radio Monitoring list.

Typical Scenarios and FAQs

- How can I determine the current channel loads for the existing access points in my network?
- How can I determine if the channel loads for the access points in my WLAN radio environment have changed?

**Note**

Your login determines whether you can use this option.

Before You Begin

- Perform an AP Radio Scan (see [Using AP Radio Scans to Collect RM Data, page 13-43](#)).
- Be sure that Radio Monitoring is enabled. Radio Monitoring is enabled by default; if it has been disabled, you must re-enable it (see [Using Radio Monitoring to Collect RM Data, page 12-1](#)).

Procedure

- Step 1** Select **Reports > Radio Manager**. The window refreshes with a device selector in the left pane.
- Step 2** From the device selector, click to expand the folder and select an access point or a folder. The right pane refreshes.
- Step 3** From the Report Name list, select **Channel Loading Report**.
- Step 4** Click **View**. The report displays the following data for the selected access points:

Table 10-11 **Channel Loading Report**

Column	Description
AP Name	The name of the access point.
PHY	The physical interface type (11a, 11b, or 11g) of the radio interface.
Channel	The radio channel used.
Average Near (%)	The average (of 15 minutes) channel loading detected by the access point from the nearest clients.
Average Far (%)	The average (of 15 minutes) channel loading detected by the access point from the farthest clients.
Peak Near (%)	The average (of 15 minutes) peak value detected by the access point from the nearest clients.
Peak Far (%)	The average (of 15 minutes) peak value detected by the access point from the farthest clients.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

- [Viewing Historical Channel Load Results, page 10-21](#)
- [Displaying Radio Manager Reports, page 10-15](#)
- [Using the Basic Report Features, page 10-1](#)

Viewing Historical Channel Load Results

The historical channel load report displays the previous channel load information for selected a AP (or group). The information is collected every 15 minutes and saved to the channel load historical table. The data in the historical table is trimmed every 60 minutes.

**Note**

Your login determines whether you can use this option.

Before You Begin

- Perform an AP Radio Scan (see [Using AP Radio Scans to Collect RM Data, page 13-43](#)).
- Be sure that Radio Monitoring is enabled. Radio Monitoring is enabled by default; if it has been disabled, you must re-enable it (see [Using Radio Monitoring to Collect RM Data, page 12-1](#)).

Procedure

-
- Step 1** Select **Reports > Radio Manager**. The window refreshes with a device selector in the left pane.
- Step 2** From the device selector, click to expand the folder and select an access point or a folder. The right pane refreshes.
- Step 3** From the Report Name list, select **Channel Loading Historical Report**.
- Step 4** Click **View**. The report displays the previous channel load data for the selected access points. For more information about channel load data, see [Viewing Current Channel Load Results, page 10-19](#).
-

Related Topics

- [Viewing Current Channel Load Results, page 10-19](#)
- [Displaying Radio Manager Reports, page 10-15](#)
- [Using the Basic Report Features, page 10-1](#)

Viewing Current Radar Detection Events

This report provides information about all currently-active radar detection events.

**Note**

Because DFS only applies to 802.11a radios (the 5GHz band), this report has no relevance to 11b or 11g radios because they operate in the 2.4GHz band.

**Note**

Your login determines whether you can use this option.

Before You Begin

- Configure your network for radio management (see [Getting Started with Radio Manager, page 12-1](#)).
- Be sure that Radio Monitoring is enabled. Radio Monitoring is enabled by default; if it has been disabled, you must re-enable it (see [Using Radio Monitoring to Collect RM Data, page 12-1](#)).
- Set the threshold condition for radar detection (**Faults > Manage Fault Settings > Radio 802.11a Policies > Dynamic Frequency Selection**).

Procedure

- Step 1** Select **Reports > Radio Manager**. The window refreshes with a device selector in the left pane.
- Step 2** From the device selector, click to expand the folder and select an access point or a folder. The right pane refreshes.
- Step 3** From the Report Name list, select **Radar Detection Event Report**.
- Step 4** Click **View**. The report displays the following data for the selected access points:

Table 10-12 *Radar Detection Event Report*

Column	Description
AP Name	The identity of the AP that detected radar.
PHY	The identity of the specific radio interface that detected radar contention.
Radar Detect Channel	The channel on which radar was originally detected.
Radar Detect Time	The time at which radar was originally detected.

Related Topics

- [Viewing Historical Radar Detection Events, page 10-23](#)
- [Displaying Radio Manager Reports, page 10-15](#)
- [Using the Basic Report Features, page 10-1](#)

Viewing Historical Radar Detection Events

This report provides information about all recorded radar detection events.

**Note**

Because DFS only applies to 802.11a radios (the 5GHz band), this report has no relevance to 11b or 11g radios because they operate in the 2.4GHz band.

**Note**

Your login determines whether you can use this option.

Before You Begin

- Configure your network for radio management (see [Getting Started with Radio Manager, page 12-1](#)).
- Be sure that Radio Monitoring is enabled. Radio Monitoring is enabled by default; if it has been disabled, you must re-enable it (see [Using Radio Monitoring to Collect RM Data, page 12-1](#)).
- Set the threshold condition for radar detection (**Faults > Manage Fault Settings > Radio 802.11a Policies > Dynamic Frequency Selection**).

Procedure

- Step 1** Select **Reports > Radio Manager**. The window refreshes with a device selector in the left pane.
- Step 2** From the device selector, click to expand the folder and select an access point or a folder. The right pane refreshes.
- Step 3** From the Report Name list, select **Radar Detection Event Historical Report**.
- Step 4** Click **View**. The report displays the following data for the selected access points:

Table 10-13 *Radar Detection Event Historical Report*

Column	Description
AP Name	The identity of the AP that detected radar.
PHY	The identity of the specific radio interface that detected radar contention.
Radar Detect Channel	The channel on which radar was originally detected.
Radar Detect Time	The time at which radar was originally detected.
New Channel	The channel to which the radio interface switched operation or an indicator that the first channel-switch attempt failed.
Channel Switch Time	The time at which the channel-switch was performed (if applicable).

Related Topics

- [Viewing Current Radar Detection Events, page 10-21](#)
- [Displaying Radio Manager Reports, page 10-15](#)

- [Using the Basic Report Features, page 10-1](#)

Displaying Voice Reports

The **Reports > Voice** option displays voice call information about the devices in your network. This information can be shown for an AP, a single floor, or the entire network. You can view, export, and email the reports. Using this option, you can view, export, and email the following report types:

- Group Reports:
 - [AP Group Call Summary: Current, page 10-24](#)
 - [AP Group Metrics Summary: Current, page 10-25](#)
- Access Point Reports:
 - [AP Detail: Current, page 10-27](#)
 - [AP Detail: Last Hour, page 10-29](#)
 - [Voice Queuing Delay, page 10-30](#)
 - [Voice Packet Loss, page 10-31](#)
 - [Voice Roaming, page 10-33](#)
 - [Bandwidth In Use, page 10-34](#)
 - [Voice Streams In Progress, page 10-35](#)
 - [Rejected Voice Streams, page 10-36](#)

AP Group Call Summary: Current

The AP Group Call Summary: Current report allows you to view the current status of a group of APs.



Note

Your login determines whether you can use this option.

Before You Begin

Satisfy the voice prerequisites (see [Guidelines for Using Voice, page 15-5](#)).

Procedure

- Step 1** Select **Reports > Voice**.
- Step 2** Select an AP group (that has voice capability) from the device selector.
- Step 3** From the Report Name list, select **AP Group Call Summary: Current**.

This report displays the following information:

Column	Description
Time	The time (month, day, hour, and minute) the WLSE polled information from the device (MM-DD-hh-mm). For more information, see Understanding WLSE Time Displays, page 1-10 .
AP Name	The name of the access point.
Percent Bandwidth Allocated	The percentage of the channel allocated for voice traffic.
Percent of Allocated Bandwidth in Use	The percentage of the configured bandwidth that is currently being used by voice traffic.
Voice Streams in Progress	The number of voice streams in progress on the AP. Each client participating in a call counts as one voice stream. There are at least two voice streams, one from each client, per call. For a conference call, the number of voice streams is equal to the number of clients participating in that call.
Additional Voice Streams	The AP's estimate of the number of voice streams it can admit, minus the roaming reserve.
Calls Rejected Due to Insufficient Bandwidth	Number of TSPEC requests denied due to insufficient bandwidth.
Calls Rejected Due to Other Reason	Number of TSPEC requests denied for other reasons.

Step 4 Use the buttons to the right of the Report Name list to export, email, or refresh this report.

AP Group Metrics Summary: Current

The AP Group Metrics Summary: Current report displays the consolidated metrics of all the clients collected in the current 90 second report.



Note This report displays the metrics for clients only.

You can use this report to highlight different information about the displayed APs. For example:

- Sort on the QOS to display the APs grouped into three QOS categories: Degraded (red), Fair (yellow) and Normal (green).
- Use a descending sort on the PLR (packet loss ratio) column to display the APs with the most errors.

**Note**

Your login determines whether you can use this option.

Before You Begin

Satisfy the voice prerequisites (see [Guidelines for Using Voice](#), page 15-5).

Procedure

- Step 1** Select **Reports > Voice**.
- Step 2** Select an AP group (that has voice capability) from the device selector.
- Step 3** From the Report Name list, select **AP Group Metrics Summary: Current**.

This report displays the following information:

Column	Description
Time	The time (month, day, hour, and minute) the WLSE polled information from the device (MM-DD-hh-mm). For more information, see Understanding WLSE Time Displays , page 1-10.
AP Name	The name of the access point.
Interface Name	The name of the radio interface.
QOS	An indicator bar that shows whether the packet latency and packet loss rates are within normal limits. - Green: The AP can admit both originating and roaming-in calls. - Yellow: The AP can only accept roaming-in calls. - Red: The AP is completely full and cannot accept any more calls. This data comes from the Traffic Stream Metrics (see Understanding Voice Packet Latency, Jitter, and Loss , page 15-3).
% PLR (Downlink)	The percentage of packets lost per traffic stream (from the AP to the client).
% PLR (Uplink)	The percentage of packets lost per traffic stream (from the client to the AP).
Ave Queuing Delay (ms) (Downlink)	The average delay (in milliseconds) from the time a packet was queued in the AP's driver queue to the time the acknowledgement was received by the AP's driver from the client.
Ave Queuing Delay (ms) (Uplink)	The average delay (in milliseconds) from the time a packet was queued in the client's driver queue to the time the acknowledgement was received by the client's driver from the AP.
% Packets > 40ms Queuing Delay	The percentage of packets that experience more than 40 ms delay per cell.
% Packets > 20ms Queuing Delay	The percentage of packets that experience less than or equal to 40 ms and more than 20 ms delay per cell.

Column	Description
Client(s) Using U-APSD	Whether the AP's clients are using U-APSD (unsolicited automatic power save delivery).
Roaming Delay (ms)	The time (in milliseconds) between the last RTP packet seen on the old AP and the first RTP packet seen on the new AP.

Step 4 Use the buttons to the right of the Report Name list to export, email, or refresh this report.

Related Topics

[Understanding Voice Packet Latency, Jitter, and Loss, page 15-3](#)

AP Detail: Current

The AP Detail: Current report highlights information about the associated clients for the last 90 second interval. For example:

- Choosing a descending sort on a Packet Count column displays the busiest clients in the last 90 second interval.
- Choosing a descending sort on the Roaming Count column displays the clients with the most roams.
- Sorting on the Roaming Delay column displays the clients with the longest average roaming delays.



Note

Your login determines whether you can use this option.

Before You Begin

Satisfy the voice prerequisites (see [Guidelines for Using Voice, page 15-5](#)).

Procedure

- Step 1** Select **Reports > Voice**.
- Step 2** Select an AP (that has voice capability) from the device selector.
- Step 3** From the Report Name list, select **AP Detail: Current**.

The AP Detail: Current report displays the following information:

Column	Description
Time	The time (month, day, hour, and minute) the WLSE polled information from the device (MM-DD-hh-mm). For more information, see Understanding WLSE Time Displays, page 1-10 .
Client MAC	The client's MAC address.
Interface Name	The name of the radio interface.

Column	Description
QOS	An indicator bar that shows whether the packet latency and packet loss rates are within normal limits. - Green indicates that the AP can admit both originating and roaming-in calls. - Yellow indicates that the AP can only accept roaming-in calls. - Red indicates that the AP is completely full and cannot accept any more calls. This data comes from the Traffic Stream Metrics.
Packet Count (Downlink)	The total number of packets counted per traffic stream (from the AP to the client).
Packet Count (Uplink)	The total number of packets counted per traffic stream (from the client to the AP).
% PLR (Downlink)	The percentage of packets lost per traffic stream (from the AP to the client).
% PLR (Uplink)	The percentage of packets lost per traffic stream (from the client to the AP).
Ave Queuing Delay (ms) (Downlink)	The average delay (in milliseconds) from the time a packet was queued in the AP's driver queue to the time the acknowledgement was received by the AP's driver from the client.
Ave Queuing Delay (ms) (Uplink)	The average delay (in milliseconds) from the time a packet was queued in the client's driver queue to the time the acknowledgement was received by the client's driver from the AP.
% Packets > 40ms Queuing Delay	The percentage of packets that experience more than 40 ms delay per cell.
% Packets > 20ms Queuing Delay	The percentage of packets that experience less than or equal to 40 ms and more than 20 ms delay per cell.
Using U-APSD	Whether the AP's clients are using U-APSD (unsolicited automatic power save delivery).
Roaming Delay (ms)	The time (in milliseconds) it takes for a roaming call's association process to complete.
Roaming Count	The number of times a client has roamed to this AP.

Step 4 Use the buttons to the right of the Report Name list to export, email, or refresh this report.

Related Topics

- [AP Detail: Last Hour, page 10-29](#)
- [Understanding Voice Packet Latency, Jitter, and Loss, page 15-3](#)
- [Using the Basic Report Features, page 10-1](#)

AP Detail: Last Hour

The AP Detail: Last Hour report highlights information about the associated clients for the last hour. For example:

- Choosing a descending sort on a Packet Count column displays the busiest clients in the last hour.
- Sorting on the Roaming Delay column displays the clients with the longest average roaming delays.



Note

Your login determines whether you can use this option.

Before You Begin

Satisfy the voice prerequisites (see [Guidelines for Using Voice, page 15-5](#)).

Procedure

- Step 1** Select **Reports > Voice**.
- Step 2** Select an AP (that has voice capability) from the device selector.
- Step 3** From the Report Name list, select **AP Detail: Last Hour**.
- The AP Detail: Last Hour report displays the following information:

Column	Description
Time	The time (month, day, hour, and minute) the WLSE polled information from the device (MM-DD-hh-mm). For more information, see Understanding WLSE Time Displays, page 1-10 .
Interface Name	The name of the radio interface.
QOS	An indicator bar that shows whether the packet latency and packet loss rates are within normal limits. • Green indicates that the AP can admit both originating and roaming-in calls. • Yellow indicates that the AP can only accept roaming-in calls. • Red indicates that the AP is completely full and cannot accept any more calls. This data comes from the Traffic Stream Metrics.
% PLR (Downlink)	The percentage of packets lost per traffic stream (from the AP to the client).
% PLR (Uplink)	The percentage of packets lost per traffic stream (from the client to the AP).
Ave Queuing Delay (ms) (Downlink)	The average delay (in milliseconds) from the time a packet was queued in the AP's driver queue to the time the acknowledgement was received by the AP's driver from the client.
Ave Queuing Delay (ms) (Uplink)	The average delay (in milliseconds) from the time a packet was queued in the client's driver queue to the time the acknowledgement was received by the client's driver from the AP.

Column	Description
% Packets > 40ms Queuing Delay	The percentage of packets that experience more than 40 ms delay per cell.
% Packets > 20ms Queuing Delay	The percentage of packets that experience less than or equal to 40 ms and more than 20 ms delay per cell.
Client(s) Using U-APSD	Whether the AP's clients are using U-APSD (unsolicited automatic power save delivery).
Roaming Delay (ms)	The time (in milliseconds) it takes for a roaming call's association process to complete.

Step 4 Use the buttons to the right of the Report Name list to export, email, or refresh this report.

Related Topics

- [AP Detail: Current, page 10-27](#)
- [Understanding Voice Packet Latency, Jitter, and Loss, page 15-3](#)
- [Using the Basic Report Features, page 10-1](#)

Voice Queuing Delay

This graph displays:

- The average delay (in milliseconds) from the time a packet was queued in the AP's driver queue to the time the acknowledgement was received by the AP's driver from the client during the last hour.
- The average delay (in milliseconds) from the time a packet was queued in the client's driver queue to the time the acknowledgement was received by the client's driver from the AP during the last hour.



Note

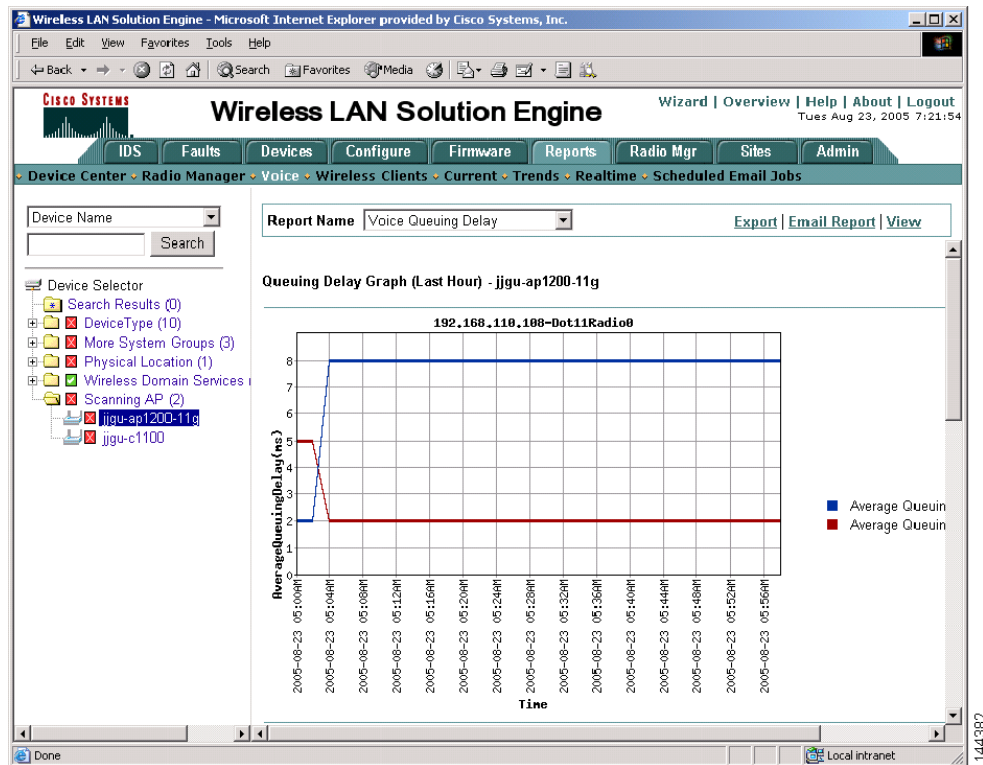
Your login determines whether you can use this option.

Before You Begin

Satisfy the voice prerequisites (see [Guidelines for Using Voice, page 15-5](#)).

Procedure

- Step 1** Select **Reports > Voice**.
- Step 2** Select an AP (that has voice capability) from the device selector.
- Step 3** From the Report Name list, select **Voice Queuing Delay**.



Step 4 Use the buttons to the right of the Report Name list to export, email, or refresh this report.

Related Topics

[Understanding Radio Management for VoWLAN, page 15-1](#)

Voice Packet Loss

This graph displays:

- The total number of packets counted per traffic stream from the AP to the client during the last hour.
- The total number of packets counted per traffic stream from the client to the AP during the last hour.

Tracking the packet count is important for these reasons:

- If **VAD** (voice activity detection) is enabled, not all packets expected in the measurement interval might be transmitted by an endpoint due to talker silence during that interval. Therefore, by including the packet count, the actual packet loss rate (PLR) can be computed.
- Because different codecs employ different packetization intervals (typically 20 or 30ms), there can be a different number of packets transmitted by the different endpoints in the measurement interval.



Note

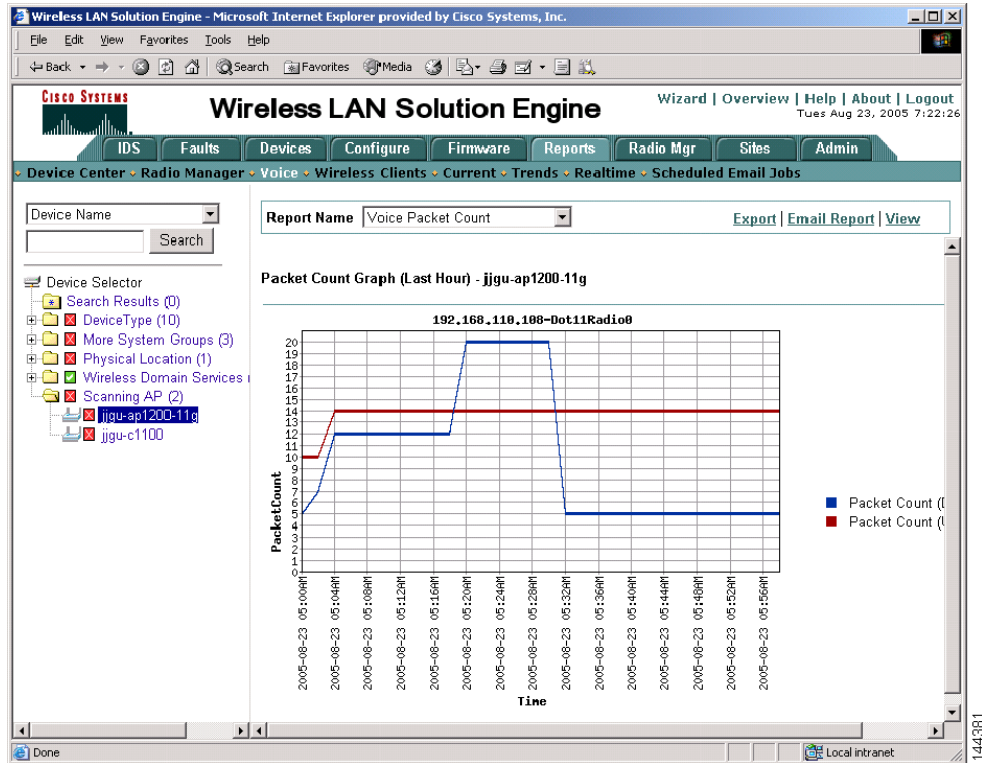
Your login determines whether you can use this option.

Before You Begin

Satisfy the voice prerequisites (see [Guidelines for Using Voice](#), page 15-5).

Procedure

- Step 1** Select **Reports > Voice**.
- Step 2** Select an AP (that has voice capability) from the device selector.
- Step 3** From the Report Name list, select **Voice Packet Loss**.



- Step 4** Use the buttons to the right of the Report Name list to export, email, or refresh this report.

Related Topics

[Understanding Radio Management for VoWLAN](#), page 15-1

Voice Roaming

This graph displays:

- The roaming delay (in milliseconds) from the AP to the client during the last hour.
- The roaming delay (in milliseconds) from the client to the AP during the last hour.



Note

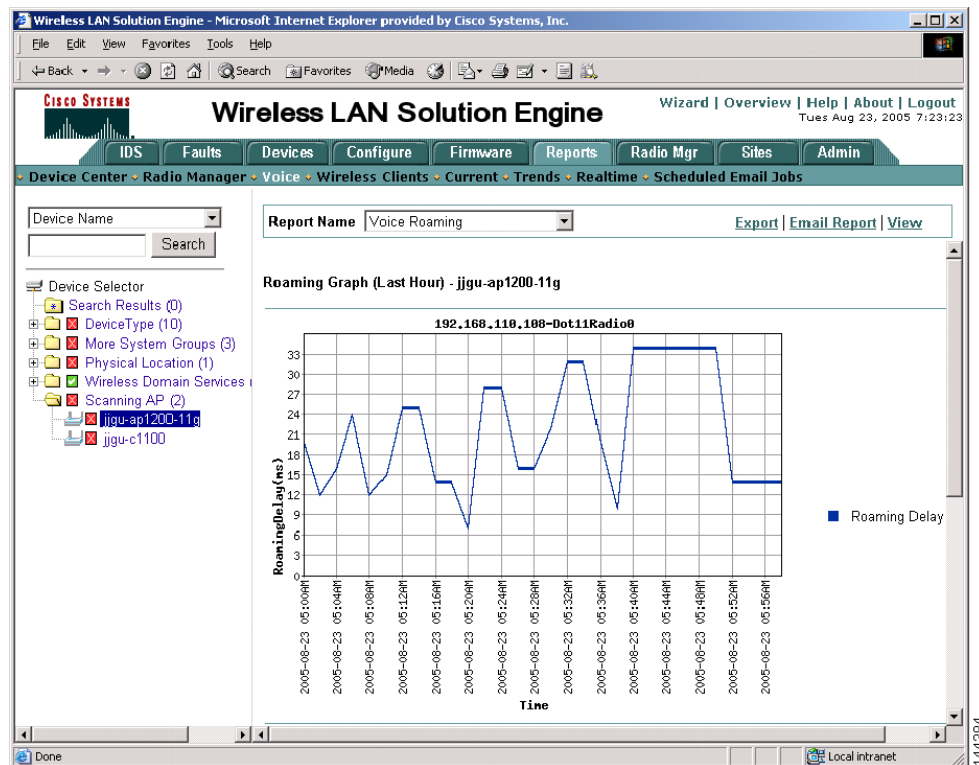
Your login determines whether you can use this option.

Before You Begin

Satisfy the voice prerequisites (see [Guidelines for Using Voice](#), page 15-5).

Procedure

- Step 1** Select **Reports > Voice**.
- Step 2** Select an AP (that has voice capability) from the device selector.
- Step 3** From the Report Name list, select **Voice Roaming**.



- Step 4** Use the buttons to the right of the Report Name list to export, email, or refresh this report.

Related Topics

[Understanding Roaming](#), page 15-3

Bandwidth In Use

This graph displays the percentage of allowed bandwidth that has been used by the AP during the last hour.



Note

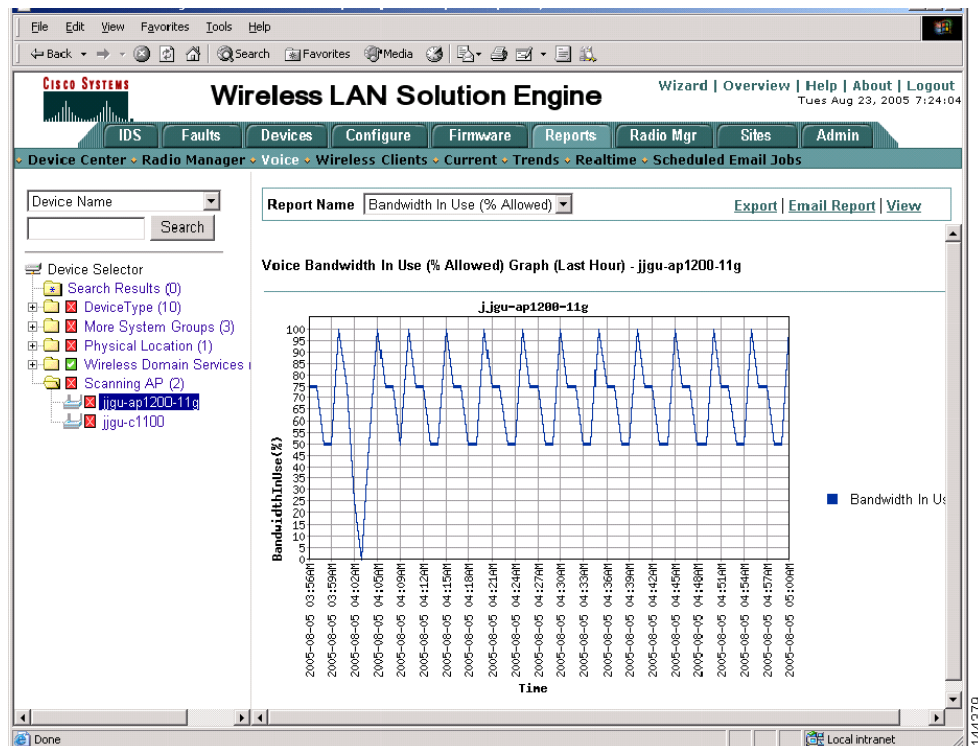
Your login determines whether you can use this option.

Before You Begin

Satisfy the voice prerequisites (see [Guidelines for Using Voice](#), page 15-5).

Procedure

- Step 1** Select **Reports > Voice**.
- Step 2** Select an AP (that has voice capability) from the device selector.
- Step 3** From the Report Name list, select **Bandwidth in Use (% Allowed)**.



- Step 4** Use the buttons to the right of the Report Name list to export, email, or refresh this report.

Related Topics

[Understanding Radio Management for VoWLAN](#), page 15-1

Voice Streams In Progress

This graph displays the number of voice streams in progress on the AP during the last hour.

Each client participating in a call counts as one voice stream. There are at least two voice streams, one from each client, per call. For a conference call, the number of voice streams is equal to the number of clients participating in that call.



Note

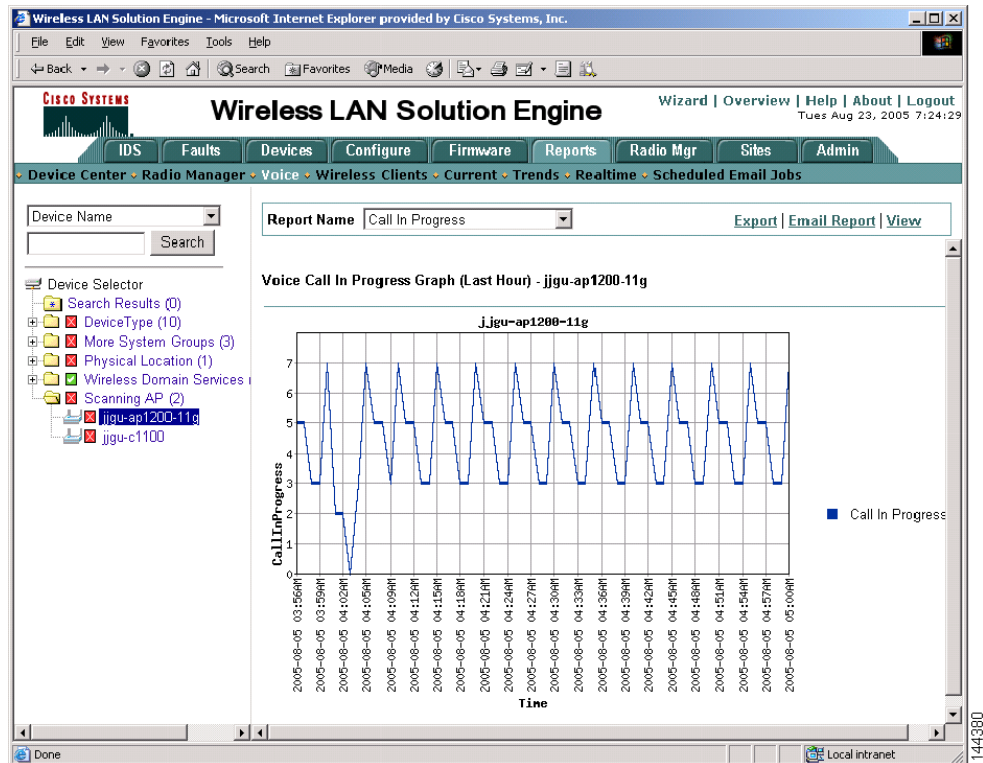
Your login determines whether you can use this option.

Before You Begin

Satisfy the voice prerequisites (see [Guidelines for Using Voice](#), page 15-5).

Procedure

- Step 1** Select **Reports > Voice**.
- Step 2** Select an AP (that has voice capability) from the device selector.
- Step 3** From the Report Name list, select **Voice Streams In Progress**.



- Step 4** Use the buttons to the right of the Report Name list to export, email, or refresh this report.

Related Topics

[Understanding Radio Management for VoWLAN](#), page 15-1

Rejected Voice Streams

This graph displays the number of voice streams rejected by the AP during the last hour.

Each client participating in a call counts as one voice stream. There are at least two voice streams, one from each client, per call. For a conference call, the number of voice streams is equal to the number of clients participating in that call.



Note

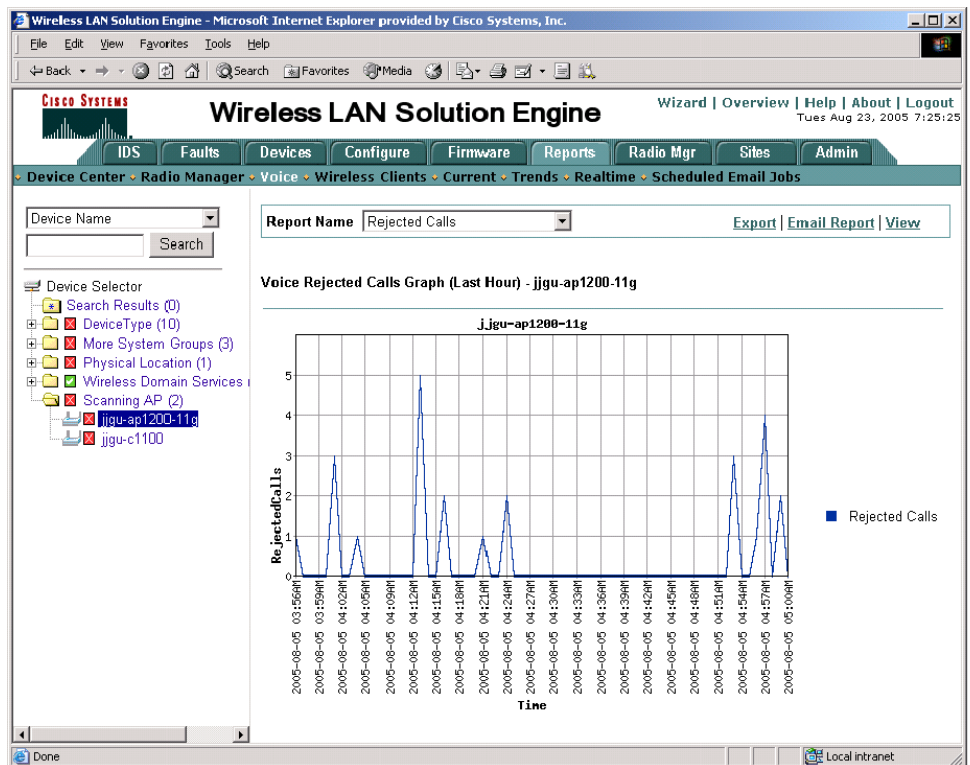
Your login determines whether you can use this option.

Before You Begin

Satisfy the voice prerequisites (see [Guidelines for Using Voice](#), page 15-5).

Procedure

- Step 1** Select **Reports > Voice**.
- Step 2** Select an AP (that has voice capability) from the device selector.
- Step 3** From the Report Name list, select **Rejected Voice Streams**.



- Step 4** Use the buttons to the right of the Report Name list to export, email, or refresh this report.

Related Topics

[Understanding Radio Management for VoWLAN](#), page 15-1

Displaying Wireless Client Reports

Wireless client reports provide information about:

- The type of client that is associating with an access point.
- How much bandwidth the client is using.
- A history of which access points the client has been associated with.
- The type of client activity.

Wireless client reports are not real-time reports. The information displayed in the reports is gathered by client polling and, for particular versions of firmware, client tracking. To understand more about wireless client reports and how the information for them is gathered, see [Client Tracking vs. Client Polling](#), page 4-21.

**Note**

Your login determines whether you can use this option.

You can view the following the report types:

- Client Detail Report—See [Displaying a Client Detail Report](#), page 10-37
- Client Statistics Report—See [Displaying a Client Statistics Report](#), page 10-39
- Client Historical Association Report—See [Displaying a Client Historical Association Report](#), page 10-40
- Client Access Failure—See [Displaying a Client Access Failure Report](#), page 10-42
- Voice Client Details: Last Hour—See [Voice Client Detail: Last Hour](#), page 10-43

Displaying a Client Detail Report

Wireless client polling frequency is set to 51 minutes by default. To increase the accuracy of this report, increase the polling frequency. To change the default setting, select **Devices > Discover > Inventory > Polling**.

**Caution**

Increasing the polling frequency could have an effect on performance.

In some instances, report data may be missing for clients that are associated with access points in which client tracking is turned on for their corresponding WDS devices. This happens because the WDS does not include all the information displayed in the report when it sends notifications about client activity events to the WLSE. The missing data may be obtained by selecting **Devices > Discover > Inventory > Run Inventory** on the associated access point.

Procedure

- Step 1** Select **Reports > Wireless Clients**. The Wireless Clients selector appears in the left pane.
- Step 2** From the list, select the method you want to use to search for clients.
- Step 3** Enter the Client EAP User Name, Client MAC Address, or Client based on Mobility ID. (To search based on mobility ID, client tracking must be enabled.) You can use an asterisk (*) as a wild card to denote numbers and letters.



Note The MAC address must be entered in hexadecimal, for example 0070eb37c90.

Step 4 Click **Search**. A list appears in the left pane.

Step 5 Click the username, MAC address, or mobility ID number. (To search based on mobility ID, client tracking must be enabled.) The right pane refreshes and displays the Client Detail Report, which is the default report.



Note You cannot specify start and end dates for this report.

Table 10-14 *Client Detail Report*

Column	Description
Name	The client name. Note This field is empty for Cisco 7920 phones.
IP Address	The client IP address.
EAP User Name	The client used for EAP authentication.
Mobility ID	The client mobility identification number. Note Mobility IDs are only available when client tracking is enabled.
Client Type	The type of client. For example Workgroup Bridge, 350 Series, Ethernet AP, etc. Note Cisco 7920 phones will display in this field if they are running version 1.08 and associate to an AP running version 12.3(2) JA or later.
Connected to	The name or IP address of the AP. Click on this link to view the AP Detail Report and the Fault Summary. For more information, see Displaying a Detailed Report, page 10-67
Role	The role of the wireless device. For example, client station, repeater, root bridge, etc. Note This field is empty for Cisco 7920 phones.
Radio Type	The type of radio model of the wireless device. For example, Cisco 3500, 3000, 4500, 340, or 350 radios.
State	The current state of the authentication and association process between the client and the access point or bridge.
Time last seen	The time the client was last seen by the system.
Software Version	The IOS version if the client is an access point, bridge or repeater. Otherwise, it is the firmware version of the client card. Note This field is empty for Cisco 7920 phones.
MAC Address	The MAC address of the client.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Client Statistics Report

Wireless client polling frequency is set to 51 minutes by default. If 0 (zero) values are displayed in the report or if you want to increase the accuracy of the report, increase the polling frequency. To change the default setting, select **Devices > Discover > Inventory > Polling**.

**Caution**

Increasing the polling frequency could have an effect on performance.

Procedure

- Step 1** Select **Reports > Wireless Clients**. The Wireless Clients selector appears in the left pane.
- Step 2** From the list, select the method you want to use to search for clients.
- Step 3** Enter the Client EAP User Name, Client MAC Address, or Client based on Mobility ID. (To search based on mobility ID, client tracking must be enabled.) You can use an asterisk (*) as a wild card to denote numbers and letters.
- Step 4** Click **Search**. A list appears in the left pane.
- Step 5** Click the username, MAC address, or mobility ID number. The right pane refreshes.
- Step 6** From the Report Name list, select **Client Statistics Report**.
- Step 7** Click **View**. You cannot specify start and end dates for this report.

Table 10-15 **Client Statistics Report**

Column	Description
Name	The client name.
IP Address	The client IP address.
EAP User Name	The username used for EAP authentication.
MAC Address	The client MAC address.
Time last seen	The time the wireless client was last seen by the system.
Packets Transmitted	The number of packets transmitted.
Octets Transmitted	The number of octets transmitted.
Packets Received	The number of packets received.
Octets Received	The number of octets received.
Latest Received Signal Strength	A tally of the received signal power.
Latest Signal Quality	The current index of radio signal quality.
Received WEP errors	The number of WEP errors received.
Packet Errors	The number of packet errors received.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Client Historical Association Report

Wireless client polling frequency is set to 51 minutes by default. To increase the accuracy of this report, increase the polling frequency. To change the default setting, select **Devices > Discover > Inventory > Polling**.

**Caution**

Increasing the polling frequency could have an effect on performance.

Client tracking is available on all access points with firmware release 12.2(15)JA or later, and with WDS service enabled. To enable client tracking, select **Devices > Discover > Client Tracking**. (See [Prerequisites for Enhanced Client Tracking, page 4-20](#))

Procedure

- Step 1** Select **Reports > Wireless Clients**. The Wireless Clients selector appears in the left pane.
- Step 2** From the list, select the method you want to use to search for clients.
- Step 3** Enter the Client EAP User Name, Client MAC Address, or Client based on Mobility ID. (To search based on mobility ID, client tracking must be enabled.) You can use an asterisk (*) as a wild card to denote numbers and letters.
- Step 4** Click **Search**. A list appears in the left pane.
- Step 5** Click the username, MAC address, or mobility ID number. The right pane refreshes.
- Step 6** From the Report Name list, select **Client Historical Association Report**.
- Step 7** From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.
- Step 8** Click **View**. The Client Historical Association Report displays in the right pane with the following information:

Table 10-16 *Client Historical Association Report*

Column	Description
AP Name	The name of the access point.
AP IP Address	The IP address of the access point.

Table 10-16 **Client Historical Association Report (continued)**

Column	Description
EAP User Name	The RADIUS username used for EAP authentication. (Usernames are not available for non-EAP authentications.) Note Data for this column is only available when the client tracking feature is enabled, and only for WDS access points with firmware version 12.2(15)JA or later. Otherwise, it is blank. The RADIUS username is generally available in all EAP authentication cases, except for PEAP and EAP-TTLS. In these instances, the availability of the information is dependent on vendor support.
Authentication Type	The authentication type used.
Event Type	The type of event that occurred: • Refresh—This event occurs whenever the WLSE syncs up with the WDS. It is a start up phase during which the WLSE learns about all the registered clients within a WDS domain. This can happen when the WLSE reboots and the WDS to WLSE management link is established or restored after being lost. • Registered with WDS—This event occurs when a client successfully registers with the WDS for the first time. • Detach from WDS—This event occurs when the access point indicates that a client has become inactive, or when the WDS performs a clean up of stale clients. • Roam—This event occurs when a client roams to another access point within the same WDS domain. • Access Failure—This event occurs during EAP authentication when client access to the AP fails. • IP Address Change—This event occurs when a client's IP address changes, and the change is detected at the AP to which the client is registered. The IP address change is sent from the WDS to the WLSE. An example of when an IP Address Change event is generated is when a DHCP server initially assigns an IP address to a client.
MAC Address	The client MAC address.
WDS Address	The IP address of the WDS.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10.
Event Time	The time the event occurred.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Client Access Failure Report

Wireless client polling frequency is set to 51 minutes by default. To increase the accuracy of this report, increase the polling frequency. To change the default setting, select **Devices > Discover > Inventory > Polling**.



Caution

Increasing the polling frequency could have an effect on performance.

Client tracking is available on all access points with firmware release 12.2(15)JA or later, and with WDS service enabled. To enable client tracking, select **Devices > Discover > Client Tracking**. (See [Prerequisites for Enhanced Client Tracking, page 4-20](#))

Procedure

- Step 1** Select **Reports > Wireless Clients**. The Wireless Clients selector appears in the left pane.
- Step 2** From the list, select the method you want to use to search for clients.
- Step 3** Enter the Client EAP User Name, Client MAC Address, or Client based on Mobility ID. (To search based on mobility ID, client tracking must be enabled.) You can use an asterisk (*) as a wild card to denote numbers and letters.
- Step 4** Click **Search**. A list appears in the left pane.
- Step 5** Click the username, MAC address, or mobility ID number. The right pane refreshes.
- Step 6** From the Report Name list, select **Client Access Failure Report**.
- Step 7** From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.
- Step 8** Click **View**. The Client Access Failure Report displays in the right pane with the following information:

Table 10-17 **Client Access Failure Report**

Column	Description
AP Name	The name of the access point.
AP IP Address	The IP address of the access point.
Client MAC Address	The MAC address of the client.
EAP User Name	The RADIUS username used for EAP authentication. (Usernames are not available for non-EAP authentications.) Note Data for this column is only available when the client tracking feature is enabled, and only for WDS access points with firmware version 12.2(15)JA or later. Otherwise, it is blank. The RADIUS username is generally available in all EAP authentication cases, except for PEAP and EAP-TTLS. In these instances, the availability of the information is dependent on vendor support.
Authentication Type	The authentication type used.

Table 10-17 *Client Access Failure Report (continued)*

Column	Description
Event Type	The type of event that occurred: • Refresh—This event occurs whenever the WLSE syncs up with the WDS. It is a start up phase during which the WLSE learns about all the registered clients within a WDS domain. • This can happen when the WLSE reboots and the WDS to WLSE management link is established or restored after being lost. • Registered with WDS—This event occurs when a client successfully registers with the WDS for the first time. • Detach from WDS—This event occurs when the access point indicates that a client has become inactive, or when the WDS performs a clean up of stale clients. • Roam—This event occurs when a client roams to another access point within the same WDS domain. • Access Failure—This event occurs during EAP authentication when client access to the AP fails.
WDS Address	The IP address of the WDS.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10.
Event Time	The time this event occurred.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Voice Client Detail: Last Hour

The Voice Client Detail: Last Hour report highlights the voice metrics of a specific client for the last hour.

**Note**

Your login determines whether you can use this option.

Before You Begin

Satisfy the voice prerequisites (see [Guidelines for Using Voice, page 15-5](#)).

Procedure

- Step 1** Select **Reports > Wireless Clients**. The Wireless Clients selector appears in the left pane.
- Step 2** From the list, select the method you want to use to search for clients.

- Step 3** Enter the Client EAP User Name, Client MAC Address, or Client based on Mobility ID. (To search based on mobility ID, client tracking must be enabled.) You can use an asterisk (*) as a wild card to denote numbers and letters.
- Step 4** Click **Search**. A list appears in the left pane.
- Step 5** Click the username, MAC address, or mobility ID number. The right pane refreshes.
- Step 6** From the Report Name list, select **Voice Client Detail: Last Hour**.
- Step 7** Click **View**. The Voice Client Details: Last Hour report displays the following information:

Column	Description
Time	The time (month, day, hour, and minute) the WLSE polled information from the device (MM-DD-hh-mm). For more information, see Understanding WLSE Time Displays, page 1-10 .
QOS	An indicator bar that shows whether the packet latency and packet loss rates are within normal limits. - Green indicates that the AP can admit both originating and roaming-in calls. - Yellow indicates that the AP can only accept roaming-in calls. - Red indicates that the AP is completely full and cannot accept any more calls. This data comes from the Traffic Stream Metrics.
AP Name	The name of the access point.
Interface Name	The name of the radio interface.
Packet Count (Downlink)	The total number of packets counted per traffic stream (from the AP to the client).
Packet Count (Uplink)	The total number of packets counted per traffic stream (from the client to the AP).
% PLR (Downlink)	The percentage of packets lost per traffic stream from the AP to the client)
% PLR (Uplink)	The percentage of packets lost per traffic stream from the client to the AP.
Ave Queuing Delay (ms) (Downlink)	The average delay (in milliseconds) from the time a packet was queued in the AP's driver queue to the time the acknowledgement was received by the AP's driver from the client.
Ave Queuing Delay (ms) (Uplink)	The average delay (in milliseconds) from the time a packet was queued in the client's driver queue to the time the acknowledgement was received by the client's driver from the AP.
% Packets > 40ms Queuing Delay	The percentage of packets that experience greater than 40 milliseconds delay per cell.
% Packets > 20ms Queuing Delay	The percentage of packets that experience less than or equal to 40 milliseconds and greater than 20 milliseconds delay per cell.
Using U-APSD	Whether the client is using U-APSD (unsolicited automatic power save delivery).

Column	Description
Roaming Delay (ms)	The time it takes (in milliseconds) for a roaming call's association process to complete.
Roaming Count	The number of times a client has roamed to this AP.

Step 8 Use the buttons to the right of the Report Name list to export, email, or refresh this report.

Related Topics

- [AP Detail: Current, page 10-27](#)
- [Understanding Voice Packet Latency, Jitter, and Loss, page 15-3](#)
- [Using the Basic Report Features, page 10-1](#)

Displaying Current Reports

This window allows you to view current information about the monitored devices in your network. You can view, export, and email the reports.

The frequency with which configuration data is collected from the devices is 12 hours by default. To change the default setting, select **Devices > Discover > Inventory > Polling**.

Using this option, you can view the following types of current reports:

- Group Reports:
 - [Group Reports for APs, page 10-45](#)
 - [Group Reports for 1300 Wireless Bridges, page 10-46](#)
 - [Group Reports for 1400 Wireless Bridges, page 10-46](#)
 - [Group Reports for AP1100 and AP1200 in Workgroup Bridge Mode, page 10-47](#)
 - [Group Report for WLSM: Displaying a Group Mobility ID Report, page 10-62](#)
- [Access Point Reports, page 10-47](#)
- Bridge Reports:
 - [Wireless Bridge Reports \(BR1310 and BR1410\), page 10-47](#)
 - [Workgroup Bridge Reports \(AP1100 and AP1200 in WGB Mode\), page 10-48](#)
- [Switch Reports, page 10-48](#)
- [Router Reports, page 10-48](#)
- [Server Reports, page 10-48](#)
- [WLSM Reports, page 10-48](#)



Note

Your login determines whether you can use this option.

Group Reports for APs

- Group Client Association—See [Displaying a Group Client Association Report, page 10-48](#)

- Group Security Report—See [Displaying a Group Security Report](#), page 10-50
- Group SSID Report—See [Displaying a Group SSID Report](#), page 10-52
- Group MBSSID Report—See [Displaying a Group MBSSID Report](#), page 10-53
- Group VLAN Report—See [Displaying a Group VLAN Report](#), page 10-54
- Per VLAN Client Report—See [Displaying a Per VLAN Client Report](#), page 10-55
- Group Client Report—See [Displaying a Group Client Report](#), page 10-56
- Group Identity Report—See [Displaying a Group Identity Report](#), page 10-57
- Group Serial Number Report—See [Displaying a Group Serial Number Report](#), page 10-58
- Group Security Violation Report—See [Displaying a Group Security Violation Report](#), page 10-59
- Group CDP Inline Power Report—See [Displaying a Group CDP Inline Power Report](#), page 10-59
- Group Inventory Report—See [Displaying a Group Inventory Report](#), page 10-60
- Group LBS Report—See [Displaying a Group LBS Report](#), page 10-61
- Group Version Summary Report—See [Displaying a Group Version Summary Report](#), page 10-62
- Group Auto Config Retry Report—See [Displaying a Group Auto Config Retry Report](#), page 10-63

Group Reports for 1300 Wireless Bridges

- Group Client Association—See [Displaying a Group Client Association Report](#), page 10-48
- Group Security Report—See [Displaying a Group Security Report](#), page 10-50
- Group SSID Report—See [Displaying a Group SSID Report](#), page 10-52
- Group MBSSID Report—See [Displaying a Group MBSSID Report](#), page 10-53
- Group VLAN Report—See [Displaying a Group VLAN Report](#), page 10-54
- Per VLAN Client Report—See [Displaying a Per VLAN Client Report](#), page 10-55
- Group Client Report—See [Displaying a Group Client Report](#), page 10-56
- Group Identity Report—See [Displaying a Group Identity Report](#), page 10-57
- Group Serial Number Report—See [Displaying a Group Serial Number Report](#), page 10-58
- Group Security Violation Report—See [Displaying a Group Security Violation Report](#), page 10-59
- Group CDP Inline Power Report—See [Displaying a Group CDP Inline Power Report](#), page 10-59
- Group Inventory Report—See [Displaying a Group Inventory Report](#), page 10-60
- Group LBS Report—See [Displaying a Group LBS Report](#), page 10-61
- Group Version Summary Report—See [Displaying a Group Version Summary Report](#), page 10-62
- Group Auto Config Retry Report—See [Displaying a Group Auto Config Retry Report](#), page 10-63

Group Reports for 1400 Wireless Bridges

- Group Security Report—See [Displaying a Group Security Report](#), page 10-50
- Group SSID Report—See [Displaying a Group SSID Report](#), page 10-52
- Group MBSSID Report—See [Displaying a Group MBSSID Report](#), page 10-53
- Group VLAN Report—See [Displaying a Group VLAN Report](#), page 10-54
- Group Identity Report—See [Displaying a Group Identity Report](#), page 10-57
- Group Serial Number Report—See [Displaying a Group Serial Number Report](#), page 10-58

- Group Inventory Report—See [Displaying a Group Inventory Report, page 10-60](#)
- Group LBS Report—See [Displaying a Group LBS Report, page 10-61](#)

Group Reports for AP1100 and AP1200 in Workgroup Bridge Mode

- Group Security Report—See [Displaying a Group Security Report, page 10-50](#)
- Group SSID Report—See [Displaying a Group SSID Report, page 10-52](#)
- Group VLAN Report—See [Displaying a Group VLAN Report, page 10-54](#)
- Group Identity Report—See [Displaying a Group Identity Report, page 10-57](#)
- Group Serial Number Report—See [Displaying a Group Serial Number Report, page 10-58](#)
- Group Inventory Report—See [Displaying a Group Inventory Report, page 10-60](#)
- Group LBS Report—See [Displaying a Group LBS Report, page 10-61](#)

Access Point Reports



Note

These reports can be used for 1310 Wireless Bridges that are in AP mode.

- Summary Report—See [Displaying an AP Summary Report, page 10-65](#)
- Detailed Report—See [Displaying a Detailed Report, page 10-67](#)
- Associations—See [Displaying an Associations Report, page 10-69](#)
- RADIUS Authentication Report—See [Displaying a RADIUS Authentication Report, page 10-69](#)
- QoS Report—[Displaying an QoS Report, page 10-70](#)
- SSID Report—[Displaying an SSID Report, page 10-71](#)
- MBSSID Report—[Displaying an MBSSID Report, page 10-72](#)
- VLAN Report—[Displaying a VLAN Report, page 10-73](#)
- Per VLAN Client Report—[Displaying a Per VLAN Client Report, page 10-73](#)
- Hot Standby Report—[Displaying a Hot Standby Report, page 10-74](#)
- EAP and MAC Failed Authentication Report—[Table 10-45EAP and MAC Failed Authentication Report, page 10-75](#)
- Failed Authentication and Login Attempt per AP—[Displaying a Failed Authentication and Login Attempt per AP Report, page 10-76](#)

Wireless Bridge Reports (BR1310 and BR1410)

- Summary Report—See [Displaying an AP Summary Report, page 10-65](#)
- Detailed Report—See [Displaying a Detailed Report, page 10-67](#)
- VLAN Report—See [Displaying a VLAN Report, page 10-73](#)
- SSID Report—See [Displaying an SSID Report, page 10-71](#)
- QoS Report—See [Displaying an QoS Report, page 10-70](#)
- RADIUS Authentication Report—See [Displaying a RADIUS Authentication Report, page 10-69](#)
- MBSSID Report—See [Displaying an MBSSID Report, page 10-72](#)

Workgroup Bridge Reports (AP1100 and AP1200 in WGB Mode)

- Summary Report—See [Displaying an AP Summary Report](#), page 10-65
- Detailed Report—See [Displaying a Detailed Report](#), page 10-67
- VLAN Report—[Displaying a VLAN Report](#), page 10-73
- SSID Report—[Displaying an SSID Report](#), page 10-71
- QoS Report—[Displaying an QoS Report](#), page 10-70
- RADIUS Authentication Report—See [Displaying a RADIUS Authentication Report](#), page 10-69
- MBSSID Report—See [Displaying an MBSSID Report](#), page 10-72

Switch Reports

- Switch Summary Report—See [Displaying a Switch Summary Report](#), page 10-77
- AP and Bridge Connected to Switch Report—See [Displaying an AP and Bridge Connected to Switch Report](#), page 10-78
- WLSM Modules Report—See [Displaying an WLSM Modules Report](#), page 10-78

Router Reports

- Router Summary Report—See [Displaying a Router Summary Report](#), page 10-79
- AP and Bridge Connected to Router Report—See [Displaying an AP and Bridge Connected to Router Report](#), page 10-80

Server Reports

- Server Summary Report—See [Displaying a Server Summary Report](#), page 10-80
- AP Usage Report—See [Displaying an AP Usage Report](#), page 10-81

WLSM Reports

- WDS Summary Report—See [Viewing the WDS Summary Report](#), page 10-10
- WDS Registered APs—See [Viewing the WDS Registered APs Report](#), page 10-12
- WDS Mobility Groups—See [Displaying a Mobility Groups Report](#), page 10-82
- Mobility ID Report—See [Displaying a Mobility ID Report](#), page 10-82

Displaying a Group Client Association Report

Procedure

-
- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
 - Step 2** From the device selector in the left pane, click to expand the folder for the group reports you want to view. The right pane refreshes.
 - Step 3** From the Report Name list, select **Group Client Association Report**.

Table 10-18 **Group Client Association Report**

Column	Description
Number of Clients Associated with this Group	The total number of clients associated with the group of access points or bridges.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .
AP Name	The name of the access point. Click to view the following: - Detailed Report—See Displaying a Detailed Report, page 10-67. - Fault Summary—See Viewing the Fault Status Report, page 10-13. - RADIUS Authentication Report—See Displaying a RADIUS Authentication Report, page 10-69.
AP IP Address	The IP address of the access point. Click to open a browser window to the AP Summary Status. Tip The HTTP port on access points must be set to 80 for this link to work. For information on setting up the HTTP port, see Enter HTTP/HTTPS Port Settings—Access Points, page 4-13 .
RF Interface	The radio interface name.
Number of Clients Connected	The number of wireless clients connected to the device.
Number of Bridges Connected	The number of bridges connected to the access point.
Number of AP-Repeaters Connected	The number of repeaters connected to the access point.
Status (Fault)	Click to view the Fault Summary. For more information, see Viewing the Fault Status Report, page 10-13 .
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Group Security Report

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** From the device selector in the left pane, click to expand the folder for the group security reports you want to view.
- Step 3** From the Report Name list, select **Group Security Report**.

Table 10-19 *Group SSID Security Report*

Column	Description
AP Name	The name of the device. Click to view the following: - Detailed Report—Displaying a Detailed Report, page 10-67. - Fault Summary—Viewing the Fault Status Report, page 10-13. - RADIUS Authentication Report—Displaying a RADIUS Authentication Report, page 10-69.
AP IP Address	The IP address of the device. Click to open a browser window to the AP Summary Status. Tip The HTTP port on access points must be set to 80 for this link to work. For information on setting up the HTTP port, see Enter HTTP/HTTPS Port Settings—Access Points, page 4-13.
RF Interface	The radio interface name.
SSID	The service set identifier name.
Authentication Type - Open System	Indicates whether the SSID is configured for open authentication.
Authentication Type - Shared Key	Indicates whether the SSID is configured for shared authentication.
Authentication Type - Cisco EAP	Indicates whether the SSID is configured for Cisco EAP authentication.
As Of	The time the fault was reported. For more information, see Understanding WLSE Time Displays, page 1-10.

Table 10-20 Group VLAN Security Report

Column	Description
AP Name	The name of the device. Click to view the following: - Detailed Report—Displaying a Detailed Report, page 10-67. - Fault Summary—Viewing the Fault Status Report, page 10-13. - RADIUS Authentication Report—Displaying a RADIUS Authentication Report, page 10-69.
AP IP Address	The IP address of the device. Click to open a browser window to the AP Summary Status. Tip The HTTP port on access points must be set to 80 for this link to work. For information on setting up the HTTP port, see Enter HTTP/HTTPS Port Settings—Access Points, page 4-13.
VLAN ID	The VLAN identification number.
VLAN Name	The name of the VLAN.
RF Interface	The radio interface type. - For devices with Version 12.3 or above, it will be 11a, 11b, and 11g. - For devices with version 12.2(15) or below, it will display as N/A.
Length of WEP Key 1	The length of the WEP key.
Length of WEP Key 2	
Length of WEP Key 3	
Length of WEP Key 4	
Encryption Mode	The encryption mode: None, WEP Encryption, or Cipher.
Cipher Type	The cipher type, which could be any combination of the following: AESCCM, CKIP, CMIC, TKIP, WEP 128, and WEP 40.
As Of	The time the fault was reported. For more information, see Understanding WLSE Time Displays, page 1-10.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Group SSID Report

This report displays all the configured SSIDs (both primary and auxiliary) and their corresponding properties in all the devices in the group.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane. From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.
- Step 2** From the Report Name list, select **Group SSID Report**.

Table 10-21 *Group SSID Report*

Column	Description
SSID	The unique identifier the client device uses to associate with the access point.
AP Name	The name of the access point. Click to view the following: - Detailed Report—See Displaying a Detailed Report, page 10-67. - Fault Summary—See Viewing the Fault Status Report, page 10-13. - RADIUS Authentication Report—See Displaying a RADIUS Authentication Report, page 10-69.
AP IP Address	The IP address of the access point. Click to open a browser window to the AP Summary Status. Tip The HTTP port on access points must be set to 80 for this link to work. For information on setting up the HTTP port, see Enter HTTP/HTTPS Port Settings—Access Points, page 4-13.
RF Interface	The radio interface name.
Guest Mode Status	Indicates whether the SSID guest mode is enabled or disabled.
SSIDL Information Element	What is it? - For devices with versions 12.3 and above a combination of any of the following displays: SSIDL, WPS, Advertisements. - For devices with versions below 12.3, N/A is displayed.
VLAN ID	The identification number of the VLAN.
VLAN Name	The name of the VLAN.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Group MBSSID Report

This report displays all the configured MBSSIDs and their corresponding properties in all the devices in the group.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane. From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.
- Step 2** From the Report Name list, select **Group MBSSID Report**.

Table 10-22 *Group MBSSID Report*

Column	Description
SSID	The unique identifier the client device uses to associate with the access point.
BSSID	The unique Basic Service Set Identifier that is associated with the SSID.
AP Name	The name of the access point. Click to view the following: - Detailed Report—See Displaying a Detailed Report, page 10-67. - Fault Summary—See Viewing the Fault Status Report, page 10-13. - RADIUS Authentication Report—See Displaying a RADIUS Authentication Report, page 10-69.
AP IP Address	The IP address of the access point. Click to open a browser window to the AP Summary Status. Tip The HTTP port on access points must be set to 80 for this link to work. For information on setting up the HTTP port, see Enter HTTP/HTTPS Port Settings—Access Points, page 4-13 .
RF Interface	The radio interface name.
Guest Mode Status	Indicates whether the SSID guest mode is enabled or disabled.
MBSSID Status	Indicates whether MBSSID is enabled or disabled.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Group VLAN Report

This report displays all the configured VLANs and their corresponding properties in the group.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane. From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.
- Step 2** From the Report Name list, select **Group VLAN Report**.



Note VLAN information might not be displayed if the WEP keys have not been configured in each VLAN. When the WEP keys are configured in the access points, VLAN information is accessible by SNMP.

Table 10-23 *Group VLAN Report*

Column	Description
VLAN ID	The identification number of the VLAN.
VLAN Name	The name of the VLAN.
AP Name	The name of the access point. Click to view the following: - Detailed Report—See Displaying a Detailed Report, page 10-67. - Fault Summary—See Viewing the Fault Status Report, page 10-13. - RADIUS Authentication Report—See Displaying a RADIUS Authentication Report, page 10-69.
AP IP Address	The IP address of the access point. Click to open a browser window to the AP Summary Status. Tip The HTTP port on access points must be set to 80 for this link to work. For information on setting up the HTTP port, see Enter HTTP/HTTPS Port Settings—Access Points, page 4-13 .
RF Interface	The radio interface name.
Class of Service	The configured class of service.
SSID	The unique identifier the client device uses to associate with the access point.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Per VLAN Client Report

Wireless client polling frequency is set to 51 minutes by default. To increase the accuracy of this report, increase the polling frequency. To change the default setting, select **Devices > Discover > Inventory > Polling**.

**Caution**

Increasing the polling frequency could have an effect on performance.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane. From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.
- Step 2** From the Report Name list, select **Per VLAN Client Report**.

Table 10-24 *Per VLAN Client Report*

Column	Description
VLAN ID	The identification number of the VLAN.
VLAN Name	The name of the VLAN.
RF Interface	The radio interface name.
SSID	The unique identifier the client device uses to associate with the access point.
Client MAC Address	The MAC address of the client.
User Name	The name of the user.
Client Name	The name of the client.
Client IP Address	The IP address of the client.
ClientType	The type of client.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Group Client Report

This report lists the clients configured on each of the access points in this group.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane. From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.
- Step 2** From the Report Name list, select **Group Client Report**. The following report displays:

Table 10-25 *Group Client Report*

Column	Description
AP Name	The name of the access point. Click to view the following: - Detailed Report—See Displaying a Detailed Report, page 10-67. - Fault Summary—See Viewing the Fault Status Report, page 10-13. - RADIUS Authentication Report—See Displaying a RADIUS Authentication Report, page 10-69.
AP IP Address	The IP address of the access point. Click to open a browser window to the AP Summary Status.
RF Interface	The radio interface name.
SSID	The unique identifier the client device uses to associate with the access point.
Client MAC Address	The MAC address of the client.
Client Name	The name of the client.
EAP User Name	The username used for authentication.
Client IP Address	The IP address of the client.
Role	The role of the client.
Client Type	The type of client.
Time last seen	The time the client was last seen by the system.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Group Identity Report

This report lists information about the access points in the group such as their serial number, the switch to which they are connected, and other identifying features.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane. From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.
- Step 2** From the Report Name list, select **Group Identity Report**. The following report displays:

Table 10-26 **Group Identity Report**

Column	Description
AP Name	The name of the access point. Click to view the following: - Detailed Report—See Displaying a Detailed Report, page 10-67. - Fault Summary—See Viewing the Fault Status Report, page 10-13. - RADIUS Authentication Report—See Displaying a RADIUS Authentication Report, page 10-69.
Version	The device version.
SSID	The .11 SSID configured on the interface.
Channel	The channel number configured in the radio interface.
AP IP Address	The IP address of the access point. Click to open a browser window to the AP Summary Status.
MAC Address (Ethernet)	The Ethernet MAC address.
MAC Address (Radio B/G)	The base MAC Address of the radio interface, if MBSSID is enabled in the AP.
MAC Address (Radio A)	The .11a radio MAC address. Note This field is empty for 350 access points that do not have an A radio.
Serial Number	The serial number of the access point.

Table 10-26 *Group Identity Report (continued)*

Column	Description
Switch IP Address	The IP address of the switch to which the access point is connected.
Switch Port	The port of the switch to which the access point is connected.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays , page 1-10.

Related Topics[Using the Basic Report Features](#), page 10-1

Displaying a Group Serial Number Report

This report lists the top assembly serial number on the access point.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane. From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.
- Step 2** From the Report Name list, select **Group Serial Number Report**. The following report displays:

Table 10-27 *Group Serial Number Report*

Column	Description
AP Name	The name of the device.
AP IP Address	The IP address of the access point. Click to open a browser window to the AP Summary Status.
Description	The description of the access point.
Serial Number	The top assembly serial number.

Related Topics[Using the Basic Report Features](#), page 10-1

Displaying a Group Security Violation Report

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane. From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.
- Step 2** From the Report Name list, select **Group Security Violation Report**. The following report displays:

Table 10-28 *Group Security Violation Report*

Column	Description
AP Name	The name of the device.
AP IP Address	The IP address of the access point. Click to open a browser window to the AP Summary Status.
RF Interface	The name of the interface.
Client MAC Address	The MAC address of the client.
Local MIC Failures	The number of MIC failures encountered on the radio interface.
Remote MIC Failures	The number of MIC failures reported by the client's radio interface.
TKIP Counter Measures Invoked	The number of TKIP counter measures invoked on this interface.
TKIP Replay Errors Detected	The number of TKIP replay errors detected on this interface.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Group CDP Inline Power Report

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane. From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.
- Step 2** From the Report Name list, select **Group CDP Inline Power Report**. The following report displays:

Table 10-29 **Group CDP Inline Power Report**

Column	Description
AP Name	The name of the device.
AP IP Address	The IP address of the access point. Click to open a browser window to the AP Summary Status.
Power Source Type	Indicates the type of power source.
Current Power Value (mW)	Indicates, in milliwatts, the power value.
Current Power Mode	Indicates the power mode.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics[Using the Basic Report Features, page 10-1](#)

Displaying a Group Inventory Report

This report lists the top assembly serial number on the access point.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane. From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.
- Step 2** From the Report Name list, select **Group Inventory Report**.

Table 10-30 **Group Inventory Report**

Column	Description
AP Name	The name of the device.
AP IP Address	The IP address of the access point. Click to open a browser window to the AP Summary Status.
Radios Installed	The radios installed in the device.
Serial Number	The top assembly serial number.
Software Version	The software version running on the device.

Table 10-30 *Group Inventory Report (continued)*

Column	Description
Free Processor Memory (Bytes)	The amount, in bytes, of free processor memory available.
Used Processor Memory (Bytes)	The amount, in bytes, of used processor memory.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Group LBS Report

This report is for access points and bridges running version 12.3(4)JA and above.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane. From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.
- Step 2** From the Report Name list, select **Group LBS Report**. The following report displays:

Table 10-31 *Group LBS Report*

Column	Description
AP Name	The name of the device.
AP IP Address	The IP address of the access point. Click to open a browser window to the AP Summary Status.
Radio Interface	The radio interface name.
LBS Profile Name	The profile name configured in the AP.
LBS Position Server	The IP address of the positioning server configured in the AP.
LBS Track Method	The track method (RSSI).
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Group Mobility ID Report

This report lists the mobility identification numbers configured on the WLSM. For Mobility ID to be displayed, a Network ID must be configured on the access point, and a client must associate to an access point using the SSID with which the MobilityID (or Network ID on the access point) is configured.

**Note**

Data is displayed only when the client tracking is enabled in the WLSE for the WLSM.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane. From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.
- Step 2** From the Report Name list, select **Group Mobility ID Report**. The following report displays:

Table 10-32 **Group Mobility ID Report**

Column	Description
WLSM IP Address	The IP address of the WLSM.
Mobility ID	The mobility ID configured on the WLSM. Note Mobility IDs are only available when client tracking is enabled.
Client MAC Address	The client's MAC address.
SSID	The unique identifier the client device uses to associate with the access point.
Associated AP IP Address	The associated access point's IP address.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Group Version Summary Report

This report provides a summary of the versions for the devices in the group.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane. From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.

Step 2 From the Report Name list, select **Group Version Summary Report**. The following report displays:

Table 10-33 Group Version Summary Report

Column	Description
Device Version	The software version.
Count of Devices	The number of devices with that version.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Group Auto Config Retry Report

This report provides information about retries in uploading auto-configuration templates that are deployed using the Deployment Wizard.

Procedure

Step 1 Select **Reports > Current**. The window refreshes with a device selector in the left pane. From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.

Step 2 From the Report Name list, select **Group Auto Config Retry Report**. The following report displays:

Table 10-34 Group Auto Config Retry Report

Column	Description
Name	The device name.
Device IP	The IP address of the device.
Status	The device status, which is one of the following Deployment Wizard phases: • Error • Initial Startup Config • Initial Discovery Phase • Initial Inventory Phase • Auto Config Job Scheduled • Successfully Configured • Operation Aborted
Boot Time	The time the device booted up.
Template Name	The name of the template designated as the auto config template.
Retry Number	The number of times the WLSE has attempted to upload the template to the device.

Table 10-34 *Group Auto Config Retry Report (continued)*

Column	Description
Retry Time	The time the auto config job will re-run.
Description	The status description
As Of	The time the status was last updated.
	For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying an AP Summary Report

Procedure

- Step 1** Select **Reports > Current** or **Reports > Device Center**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **Summary Report**.



Note If the selected device has dual interfaces, information for each is displayed, one for each interface.

Table 10-35 **Summary Report**

Column	Description
Full Name	The name for the device as entered in the Name Form field under Devices > Discover > Discover > Advanced Options.
MAC Address	The device's MAC address.
IP Address	The device's IP address. Click to open a browser window to the AP Summary Status. Tip The HTTP port on access points must be set to 80 for this link to work. For information on setting up the HTTP port, see Enter HTTP/HTTPS Port Settings—Access Points, page 4-13 .
Description	A description of the device.
SysName	The system name.
Serial Number	The serial number of the access point.
Parent WDS for the Access Point Note This entry displays only on the Device Center summary report for WDS.	The access point that provides Wireless Domain Services.
Software Version	The IOS version on the device.
Model	The model number of the device.
Radio Port Note Displays only when the selected device has dual interfaces, and does not display for bridges.	The radio port.
Radio Type	The radio interface type used.
Radio MAC Address	The MAC address for the radio interface.

Table 10-35 Summary Report (continued)

Column	Description
MBSSID Status	Indicates whether the MBSSID is enabled or disabled.
Number of Clients Connected	The number of wireless clients connected to the device.
Number of Bridges Connected	The number of wireless bridges connected to the device.
Number of AP-Repeaters Connected	The number of AP repeaters connected to the device.
Desired SSID	The unique identifier the client device uses to associate with the access point.
Guest Mode SSID	A list of all the SSIDs that have a guest mode enabled for the interface.
Current Operating Frequency Channel	The radio channel being used.
Link to the Detailed Report	Click to see details.
Note This entry displays only under Current > Summary Report.	For more information, see Displaying a Detailed Report, page 10-67 .
Link to the Association Report	Click to see associations.
Note This entry displays only under Current > Summary Report.	For more information, see Displaying an Associations Report, page 10-69 .
Link to the Access Point Web Page	Click to open a browser window to the AP Summary Status.
Note This entry displays only under Current > Summary Report.	Please note: - The HTTP port on access points must be set to 80 for this link to work. - Access points with version 12.3 and above use HTTPS. The allowed port numbers for HTTPS are 443 (default) and port numbers greater than 1024. You can In addition, the device must be configured to use the HTTPS server. For information on setting up the HTTP and HTTPS ports, see Enter HTTP/HTTPS Port Settings—Access Points, page 4-13.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10.

To view information about the Fault Summary, see [Viewing the Fault Status Report, page 10-13](#)

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Detailed Report

Procedure

- Step 1** Select **Reports > Current** or **Reports > Device Center**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **Detailed Report**.
- If viewing from the Device Center tab, only the Detailed Report is displayed.
 - If viewing from the Current tab, the Detailed Report, the Fault Summary, and the EAP Authentication Report are displayed.



Note If the selected device has dual interfaces, two summary reports are displayed, one for each interface.

Table 10-36 Detailed Report

Column	Description
Full Name	The system name for the device as entered in the Name Form field under Devices > Discover > Discover > Advanced Options.
MAC Address	The device's MAC address.
IP Address	The device's IP address. Click to open a browser window to the AP Summary Status. Tip The HTTP port on access points must be set to 80 for this link to work. For information on setting up the HTTP port, see Enter HTTP/HTTPS Port Settings—Access Points, page 4-13 .
Description	A description of the device.
Software Version	The IOS version on the device.
Model	Model number of the device.
Subnet Mask	The subnet mask.
Hot StandBy	Indicates whether the hot standby unit is in monitoring mode. If true, the current unit is in monitoring mode.
Switch IP (attached to this AP, requires CDP)	The IP address of the switch to which this access point is attached. Note CDP must be enabled for the switch information to be collected for this report.
Switch Name ((attached to this AP, requires CDP)	The name of the switch to which this access point is attached. Note CDP must be enabled for the switch information to be collected for this report.

Table 10-36 *Detailed Report (continued)*

Column	Description
Switch Port	The port number of the switch to which the access point is connected.
Device Uptime	The time since the device last rebooted per the last inventory poll.
SysName	The system name.
Radio Port	The radio port.
Note Displays only when the selected device has dual interfaces.	
Radio Type	The radio interface type used.
Radio MAC Address	The MAC address of the radio interface.
MBSSID Status	Indicates whether the MBSSID is enabled or disabled.
Number of Clients Connected	The number of wireless clients connected to the device.
Desired SSID	The unique identifier the client device uses to associate with the access point.
Guest Mode SSID	A list of all the SSIDs that have a guest mode enabled for the interface.
SSID Associated to the Native Vlan	The SSID that is mapped to the native VLAN.
Radio Cell Role	Indicates the role of the device.
Transmit Power	The access point's transmission power setting in milliwatts.
Authentication Type - Open System	Indicates whether any device, regardless of its WEP keys, can authenticate and attempt to associate.
Authentication Type - Shared Key	Indicates whether an access point sends a query to any device attempting to associate with the access point.
Authentication Type-Cisco EAP	Indicates whether a device using EAP can authenticate and attempt to associate with the access point.
Active MAC Addresses	Click to view the list of all active MAC addresses. Active MAC addresses are shown only when the MBSSID mode is enabled in the AP.
Link to the Access Point Web Page	Click to open a browser window to the AP Summary Status.
Note This entry displays only under Current > Detailed Report.	Tip The HTTP port on access points must be set to 80 for this link to work. For information on setting up the HTTP port, see Enter HTTP/HTTPS Port Settings—Access Points, page 4-13 .
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

- [Viewing the Fault Status Report, page 10-13](#)
- [Displaying a RADIUS Authentication Report, page 10-69](#)
- [Using the Basic Report Features, page 10-1](#)

Displaying an Associations Report

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **Associations Report**.

Table 10-37 Associations Report

Column	Description
Name	The wireless client's name.
IP Address	The wireless client's IP address.
MAC Address	The wireless client's MAC address.
Device Type	The wireless client device type.
Role	The role of the client device in the network.
Radio Type	The type of client radio.
As Of	The time the client was last seen by the system. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a RADIUS Authentication Report

This device report lists all the authentication servers that are configured for the device.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.

- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **RADIUS Authentication Report**.

Table 10-38 *RADIUS Authentication Report*

Column	Description
Server IP Address	The IP address of the authentication server.
Server Protocol	The protocol used by the server.
Server Priority	The priority of the server when multiple servers are configured for the same service.
Authentication Port	The port setting used by the access point and the server for authentication.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying an QoS Report

This device report displays the configured QoS parameters on access points.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **QoS Report**. The following report is displayed:

Table 10-39 QoS Report

Column	Description
RF Interface	The radio interface name.
Class of Service	The configured class of service.
Min Contention Window	The minimum contention window value.
Max Contention Window	The maximum contention window value.
Fixed Time Slot	The configured time slot.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying an SSID Report

This device report displays all the configured SSIDs (both primary and auxiliary) and their corresponding properties.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **SSID Report**.

Table 10-40 SSID Report

Column	Description
SSID	The unique identifier the client device uses to associate with the access point.
RF Interface	The radio interface name.
SSIDL Information Element	What is it? - For devices with versions 12.3 and above a combination of any of the following displays: SSIDL, WPS, Advertisements. - For devices with versions below 12.3, N/A is displayed.
Guest Mode Status	Indicates whether the guest mode is enabled or disabled for the interface.
VLAN ID	The VLAN identification number.

Table 10-40 SSID Report (continued)

Column	Description
VLAN Name	The name of the VLAN.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying an MBSSID Report

This device report displays all the configured MBSSIDs.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **MBSSID Report**. The following report appears:

Table 10-41 MBSSID Report

Column	Description
SSID	The unique identifier the client device uses to associate with the access point.
RF Interface	The radio interface name.
MAC Address	The MAC address of the access point.
Guest Mode Status	Indicates whether the SSID guest mode is enabled or disabled.
MBSSID Status	Indicates whether MBSSID is enabled or disabled.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a VLAN Report

This device report displays all the configured VLANs and their corresponding properties.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **VLAN Report**.



Note VLAN information might not be displayed if the WEP keys have not been configured in each VLAN. When the WEP keys are configured in the access points, VLAN information is accessible by SNMP.

Table 10-42 **VLAN Report**

Column	Description
VLAN ID	The identification number of the VLAN.
VLAN Name	The name of the VLAN.
Class of Service	Lists the class of service.
RF Interface	The radio interface name.
SSID	The unique identifier the client device uses to associate with the access point.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Per VLAN Client Report

Wireless client polling frequency is set to 51 minutes by default. To increase the accuracy of this report, increase the polling frequency. To change the default setting, select **Devices > Discover > Inventory > Polling**.



Caution

Increasing the polling frequency could have an effect on performance.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **Per VLAN Client Report**. The report is displayed.

Table 10-43 Per VLAN Client Report

Column	Description
VLAN ID	The identification number of the VLAN.
VLAN Name	The name of the VLAN.
RF Interface	The radio interface name.
SSID	The unique identifier the client device uses to associate with the access point.
Client MAC Address	The MAC address of the client.
Client Name	The name of the client.
Client IP Address	The IP address of the client.
Client Type	The type of client associated to the access point.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Hot Standby Report

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **HotStandby Report**.

Table 10-44 Hot Standby Report

Column	Description
AP Hot Standby	Indicates whether the access is enabled for hot standby.
Monitored AP MAC Address	The MAC address of the access point this access point is monitoring. Note This field displays the value 000000000000 when the MAC Address has not been configured on the access point.
Monitored AP IP Address	The IP address of the access point this access point is monitoring. Note This field is empty if the monitored device is not in the list of devices discovered by the WLSE.
Monitored AP Name	The name of the access point this access point is monitoring. Note This field is empty if the monitored device is not in the list of devices discovered by the WLSE.
Polling Frequency	The frequency with which this access point is polling the monitored access point in seconds.
Polling Timeout	The amount of time in seconds that this access point waits for a response from the monitored access point before it assumes the monitored access point has malfunctioned.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying an EAP and MAC Failed Authentication Report

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **EAP and MAC Failed Authentication Report**. The following report is displayed:

Table 10-45 EAP and MAC Failed Authentication Report

Column	Description
AP Name	The name of the access point.
AP IP Address	The IP address of the access point.
Client IP Address	The IP address of the client.
EAP Username	Username used for authentication.

Table 10-45 *EAP and MAC Failed Authentication Report (continued)*

Column	Description
Authentication Type	The authentication type used.
Event Type	The type of event that failed.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Failed Authentication and Login Attempt per AP Report

This report provides information about authentication and login failures for devices that are deployed using the Deployment Wizard.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **Failed Authentication and Login Attempt per AP Report**. The report is displayed.

Table 10-46 *Failed Authentication and Login Attempt per AP Report*

Column	Description
AP Name	The name of the access point.
AP IP Address	The IP address of the access point.
Server Address	The IP address of the access server.
Server Type	The type of server (either RADIUS or TACACS).
Authentication Failures	The number of authentication failures.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Switch Summary Report

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **Switch Summary Report**.
The group report is displayed with the following headings:

Table 10-47 **Switch Summary Report**

Column	Description
System Name	The switch name.
IP Address	The switch IP address or hostname.
System Description	A description of the system.
Location	A description of the switch location.
Product Type	The switch type.
System Version	The software version on the switch.
Link to the AP and Bridge Connected	Click for details. For more information, see Displaying an AP and Bridge Connected to Switch Report, page 10-78 .
Link to the WLSM Modules Contained	The WLSM Modules report displays with the following information - Name—The name of the WLSM. - IP Address—The IP address of the WLSM. - Version—The version of the WLSM. - Redundant Status—The redundant status of the WLSM. - Virtual IP Address—The virtual IP address of the WLSM.

Related Topics

- [Viewing the Fault Status Report, page 10-13](#)
- [Using the Basic Report Features, page 10-1](#)

Displaying an AP and Bridge Connected to Switch Report

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **AP and Bridge Connected to Switch Report**.
The report is displayed with the following headings:

Table 10-48 *AP and Bridge Connected to Switch Report*

Column	Description
Device Port	The device port.
AP Name	The name of the access point or bridge connected to the switch.
AP IP Address	The IP address of the access point or bridge connected to the switch.
Status (Fault)	The fault status. Click for details. For more information, see Viewing the Fault Status Report, page 10-13 .
Reset Power	Click to begin a switch power cycle which will reload the access point. Note For switches with inline power only. For this feature to work properly, you must run discovery from Administration > Discover > DISCOVER on the switch if the connectivity of access point has changed in any way. This includes activities such as swapping access points between ports. In addition, if you change the DHCP address for the access points, you must delete the access points from the WLSE, then re-discover them for this feature to work.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying an WLSM Modules Report

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **WLSM Modules Report**.

The report is displayed with the following headings:

Table 10-49 **WLSM Modules Report**

Column	Description
Name	The hostname of the WLSM.
IP Address	The IP address of the WLSM.
Version	The WLSM version number.
Redundant Status	The HSRP status of the WLSM.
Virtual IP Address	The HSRP virtual IP address of the WLSM.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Router Summary Report

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **Router Summary Report**.
- Step 4** Click **View**. The group report is displayed with the following headings:

Table 10-50 **Router Summary Report**

Column	Description
System Name	The router name.
IP Address	The router IP address.
System Description	A description of the router.
Location	The location of the router.
Product Type	The router hardware type.
System Version	The router version.

Related Topics

- [Viewing the Fault Status Report, page 10-13](#)
- [Using the Basic Report Features, page 10-1](#)

Displaying an AP and Bridge Connected to Router Report

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **AP and Bridge Connected to Router Report**.
- Step 4** Click **View**. The report is displayed with the following headings:

Table 10-51 *AP and Bridge Connected to Router Report*

Column	Description
Device Port	The device port.
AP Name	The name of the access point or bridge connected to the router.
AP IP Address	The IP address of the access point or bridge connected to the router.
Status (Fault)	The fault status. Click for details. For more information, see Viewing the Fault Status Report, page 10-13 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Server Summary Report

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **Summary Report** for the server.
- Step 4** Click **View**.
The report is displayed with the following headings:

Table 10-52 Summary Report

Column	Description
Server Name	The name of the server.
Port	The port number used for authentication.
User Name	The user name used for authentication.

Related Topics

- [Viewing the Fault Status Report, page 10-13](#)
- [Using the Basic Report Features, page 10-1](#)

Displaying an AP Usage Report

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **AP Usage Report**.
- Step 4** Click **View**. The report is displayed with the following headings:

Table 10-53 AP Usage Report

Column	Description
AP Name	The name of the access point.
AP IP Address	The IP address of the access point.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Mobility Groups Report

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **Mobility Groups**.
- Step 4** Click **View**. The report is displayed with the following headings:

Table 10-54 *Mobility Groups Report*

Column	Description
Network ID	The mobility network ID configured on the WLSM to uniquely identify the mobility group.
Tunnel IP Address	The IP address of the tunnel configured for the mobility group.
No. of Clients	The number of client associated with the mobility group as of given time.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Mobility ID Report

For Mobility ID to be displayed, a Network ID must be configured on the access point, and a client must associate to an access point using the SSID with which the MobilityID (or Network ID on the access point) is configured.



Note

Data is displayed only when the client tracking is enabled in the WLSE for the WLSM.

Procedure

- Step 1** Select **Reports > Current**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **Mobility ID Report**.
- Step 4** Click **View**. The report is displayed with the following headings:

Table 10-55 **Mobility ID Report**

Column	Description
WLSM IP Address	The IP address of the WLSM.
Mobility ID	The mobility network ID with which the client associates.
Client MAC Address	The client MAC address.
SSID	The service set identifier name.
Associated AP IP Address	The IP address of the associated access point.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying Trends

The trending reports allow you to view performance and error rates over periods of time, which you can use to analyze peak network utilization periods (see [Using Trend Reports For Capacity Planning, page 10-85](#)). You can view trends about the monitored access points, bridges, and servers in your network, as well as view, export, and email the reports.

**Note**

Trending reports are not shown for routers or switches.

The frequency with which performance data is aggregated can be selected at the time you run the report. To change the default setting for the length of time the data is saved, **Devices > Discover > Inventory > Polling**.

There may be instances in which the data points on a graph do not appear at the interval you set. This occurs because the graph's contents are summarized when the space needed to show all the data is not available in the specified graph size. For example for a given date range, if there are 100 data points and only 25 can be plotted, the x-axis will be plotted for every 4th point.

Using this option, you can view the following types of trend reports:

- Group Reports for Access Points and Bridges
 - Group Performance Report: RF Utilization—[Displaying a Group Performance Report: RF Utilization, page 10-85](#)
 - Group Performance Report: Ethernet Utilization—See [Displaying a Group Performance Report: Ethernet Utilization, page 10-86](#)
 - Top N Number of Associations: Table—See [Displaying a Top N Number of Associations: Tabular Report, page 10-87](#)

- Top N Number of Associations: Graph—See [Displaying a Top N Number of Associations: Graph Report, page 10-88](#)
 - Top N Percentage Errors—See [Displaying a Top N Percentage Errors Report, page 10-88](#)
- Group Reports for the AP1100 in Workgroup Bridge Mode
 - Group Performance Report: RF Utilization—[Displaying a Group Performance Report: RF Utilization, page 10-85](#)
 - Group Performance Report: Ethernet Utilization—See [Displaying a Group Performance Report: Ethernet Utilization, page 10-86](#)
- Access Point and Bridge Reports
 - RF Transmission Statistics—See [Displaying an RF Transmission Statistics Report, page 10-89](#)
 - Ethernet Transmission Statistics—See [Displaying an Ethernet Transmission Statistics Report, page 10-91](#)
 - RF and Ethernet Utilization: Graph—See [Displaying an RF and Ethernet Utilization Graph, page 10-92](#)
 - RF and Ethernet Utilization: Tabular—See [Displaying an RF and Ethernet Utilization: Tabular Report, page 10-92](#)
 - Top N Busiest Clients—See [Displaying Top N Busiest Clients, page 10-93](#)
 - Top N Client Error Rate—See [Displaying Top N Client MIC Error Rate, page 10-94](#)
- AP1100 in Workgroup Bridge Mode
 - RF Transmission Statistics—See [Displaying an RF Transmission Statistics Report, page 10-89](#)
 - Ethernet Transmission Statistics—See [Displaying an Ethernet Transmission Statistics Report, page 10-91](#)
 - RF and Ethernet Utilization: Graph—See [Displaying an RF and Ethernet Utilization Graph, page 10-92](#)
 - RF and Ethernet Utilization: Tabular—See [Displaying an RF and Ethernet Utilization: Tabular Report, page 10-92](#)
- Server Report
 - Server Response Time Graph—See [Displaying a Server Response Time Graph, page 10-95](#)
 - WLSM Report

**Note**

Your login determines whether you can use this option.

Related Topics

- [Using Trend Reports For Capacity Planning, page 10-85](#)
- [Using the Basic Report Features, page 10-1](#)

Using Trend Reports For Capacity Planning

Trend reports can help you analyze when peak network utilization occurs and make intelligent decisions about whether or not the network is supporting these peak utilizations adequately. If you see that there are a high number of errors during peak periods, or the peak periods correlate with many complaints about performance, you can take steps to improve the WLAN experience, perhaps by deploying more access points.

You can use trend reports to see which access points are most utilized, which are most underutilized, and which have the most errors. These data are useful for making intelligent decisions about the WLAN. Why is the WLAN most utilized in some areas and underutilized in others? Is it simply the location or is there another reason?

For example, in some retail and manufacturing deployments, WLAN administrators have used the WLSE trending reports to determine where the WLAN was underutilized. Using these data, they determined that the employees in these areas were inadequately trained on mobile applications. After this problem was identified and more training supplied to the employees, the WLAN administrators used the WLSE trend reports to validate that the WLAN usage patterns were consistent with expectations. This helped to maximize the return on investment of both the WLAN infrastructure and the wireless applications.

Displaying a Group Performance Report: RF Utilization

Procedure

- Step 1** Select **Reports > Trends**. The window refreshes with a device selector in the left pane.
- Step 2** From the device selector in the left pane, click the group folder for which you want a report. The right pane refreshes.



Note This report can be used for 1310 and 1410 Wireless Bridges.

- Step 3** From the Report Name list, select **Group Performance Report: RF Utilization**.
- Step 4** From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.
- Step 5** From the Frequency list, select the frequency with which you want the performance data aggregated. For example, if you choose hourly, the information displayed will be one hour's aggregation of data.

The following table is displayed:

Table 10-56 Group Performance Report: RF Utilization

Column	Description
AP Name	The name of the access point.
AP IP Address	The IP address of the access point.
RF Interface	The radio interface name.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .
RF Utilization (%)	The percentage of radio frequency utilization.
Number of Associations	Shows the number of associations with clients.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Group Performance Report: Ethernet Utilization

Procedure

- Step 1** Select **Reports > Trends**. The window refreshes with a device selector in the left pane.
- Step 2** From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.



Note This report can be used for 1310 and 1410 Wireless Bridges.

- Step 3** From the Report Name list, select **Group Performance Report: Ethernet Utilization**.
- Step 4** From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.
- Step 5** From the Frequency list, select the frequency with which you want the performance data aggregated. For example, if you choose hourly, the information displayed will be one hour's aggregation of data.

The following table is displayed:

Table 10-57 Group Performance Report: Ethernet Utilization

Column	Description
AP Name	The name of the access point.
AP IP Address	The IP address of the access point.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .

Table 10-57 Group Performance Report: Ethernet Utilization

Column	Description
Ethernet Utilization (%)	The percentage of Ethernet utilization.
Number of Associations	Shows the number of associations with clients.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Top N Number of Associations: Tabular Report

This report lists the top number of access points which have the highest average number of associations over the selected period of time. The minimum and maximum number of associations are also displayed.

Procedure

- Step 1** Select **Reports > Trends**. The window refreshes with a device selector in the left pane.
- Step 2** From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.
- Step 3** From the Report Name list, select **Top N Number of Associations: Tabular**.
- Step 4** From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.
- Step 5** From the Frequency list, select the frequency with which you want the performance data aggregated. For example, if you choose hourly, the information displayed will be one hour's aggregation of data.
- Step 6** In the N Value text box, enter the top number of associations you want to view.

The following table is displayed:

Table 10-58 Top N Number of Associations: Tabular

Column	Description
AP Name	The name of the access point.
AP IP Address	The IP address of the access point.
Number of Clients Connected (Avg)	The average number of clients connected to the access point.
Number of Clients Connected (Min)	The minimum number of clients connected to the access point.
Number of Clients Connected (Max)	The maximum number of clients connected to the access point.

Related Topics[Using the Basic Report Features, page 10-1](#)

Displaying a Top N Number of Associations: Graph Report

This report lists the top number of access points which have the highest average number of associations over the selected period of time.

Procedure

- Step 1** Select **Reports > Trends**. The window refreshes with a device selector in the left pane.
- Step 2** From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.
- Step 3** From the Report Name list, select **Top N Number of Associations: Tabular**.
- Step 4** From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.
- Step 5** From the Frequency list, select the frequency with which you want the performance data aggregated. For example, if you choose hourly, the information displayed will be one hour's aggregation of data.
- Step 6** In the N Value text box, enter the top number of associations you want to view.

The following graph is displayed:

Table 10-59 *Top N Number of Associations: Graph*

Column	Description
Number of Clients Connected	The x-axis displays the time intervals. The y-axis displays the average number of clients connected

Related Topics[Using the Basic Report Features, page 10-1](#)

Displaying a Top N Percentage Errors Report

This report lists the top number of access points which have the highest average percentage of errors. The minimum and maximum percentage of errors during the selected period of time are also displayed.

Procedure

- Step 1** Select **Reports > Trends**. The window refreshes with a device selector in the left pane.
- Step 2** From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.
- Step 3** From the Report Name list, select **Top N Percentage Errors**.

- Step 4** From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.
- Step 5** From the Frequency list, select the frequency with which you want the performance data aggregated. For example, if you choose hourly, the information displayed will be one hour's aggregation of data.
- Step 6** In the N Value text box, enter the top number of errors you want to view. The following table is displayed:

Table 10-60 **Top N Percentage Errors**

Column	Description
AP Name	The name of the access point.
AP IP Address	The IP address of the access point.
RF Interface	The radio interface name.
Packet Errors (Avg) (%)	The average percentage of error packets.
Packet Errors (Min) (%)	The minimum percentage of error packets.
Packet Errors (Max) (%)	The maximum percentage of error packets.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying an RF Transmission Statistics Report

This report displays the transmit and receive rates overlaid in a graph.

Procedure

- Step 1** Select **Reports > Trends**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **RF Transmission Statistics**.
- Step 4** From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.
- Step 5** From the Frequency list, select the frequency with which you want the performance data aggregated. For example, if you choose hourly, the information displayed will be one hour's aggregation of data. The following graphs are displayed:

he following graphs are displayed:

Table 10-61 *RF Transmission Statistics in Packets*

Column	Description
Transmit Rate	The x-axis displays the time intervals. The y-axis displays the number of packets transmitted per second.
Receive Rate	The x-axis displays the time intervals. The y-axis displays the number of packets received per second.

Table 10-62 *RF Transmission Statistics in Bytes*

Column	Description
Transmit Rate	The x-axis displays the time intervals. The y-axis displays the number of bytes transmitted per second.
Receive Rate	The x-axis displays the time intervals. The y-axis displays the number of bytes received per second.

Table 10-63 *RF Transmission Statistics Packet Errors*

Column	Description
Packet Errors	The x-axis displays the time intervals. The y-axis displays the percent of error packets per number of packets.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying an Ethernet Transmission Statistics Report

This report displays the transmit and receive rates overlaid in a graph.

Procedure

- Step 1** Select **Reports > Trends**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **Ethernet Transmission Statistics**.
- Step 4** From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.
- Step 5** From the Frequency list, select the frequency with which you want the performance data aggregated. For example, if you choose hourly, the information displayed will be one hour's aggregation of data.

The following graphs are displayed:

Table 10-64 Ethernet Transmission Statistics in Packets

Column	Description
Transmit Rate	The x-axis displays the time intervals. The y-axis displays the number of packets transmitted per second.
Receive Rate	The x-axis displays the time intervals. The y-axis displays the number of packets received per second.

Table 10-65 Ethernet Transmission Statistics in Bytes

Column	Description
Transmit Rate	The x-axis displays the time intervals. The y-axis displays the number of bytes transmitted per second.
Receive Rate	The x-axis displays the time intervals. The y-axis displays the number of bytes received per second.

Table 10-66 Ethernet Transmission Statistics Packet Errors

Column	Description
Packet Errors	The x-axis displays the time intervals. The y-axis displays the percent of error packets per number of packets.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying an RF and Ethernet Utilization Graph

This report displays the Ethernet utilization and RF utilization overlaid in a graph.

Procedure

- Step 1** Select **Reports > Trends**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **RF and Ethernet Utilization Graph**.
- Step 4** From the Start Date list, select the start date for the graph, and from the For a period of list, select the number of days.
- Step 5** From the Frequency list, select the frequency with which you want the performance data aggregated. For example, if you choose hourly, the information displayed will be one hour's aggregation of data. The following graphs are displayed:

Table 10-67 *RF and Ethernet Utilization Graph*

Column	Description
Ethernet Utilization	The x-axis displays the time intervals. The y-axis displays the percent of Ethernet utilization.
RF Utilization	The x-axis displays the time intervals. The y-axis displays the percent of radio frequency utilization.

Table 10-68 *Number of Associations Graph*

Column	Description
Number of Associations	The x-axis displays the time intervals. The y-axis displays the number of client associations

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying an RF and Ethernet Utilization: Tabular Report

Procedure

- Step 1** Select **Reports > Trends**. The window refreshes with a device selector in the left pane.

- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **RF and Ethernet Utilization: Tabular**.
- Step 4** From the Start Date list, select the start date for the graph, and from the For a period of list, select the number of days.
- Step 5** From the Frequency list, select the frequency with which you want the performance data aggregated. For example, if you choose hourly, the information displayed will be one hour's aggregation of data. The following table is displayed:

Table 10-69 RF and Ethernet Utilization: Tabular

Column	Description
IP Address	The IP address of the access point or bridge.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10 .
Number of Associations	The number of client associations.
Ethernet Utilization (%)	The amount of Ethernet utilization.
RF Interface	The radio interface name.
RF Utilization (%)	The amount of radio frequency utilization.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying Top N Busiest Clients

This report lists the top number of busiest clients in terms of average bit rate as perceived by the access point for the selected period of time. The minimum and maximum bit rates for the clients are also displayed.

Wireless client polling frequency is set to 51 minutes by default. If 0 (zero) values are displayed in the report or if you want to increase the accuracy of the report, increase the polling frequency. To change the default setting, select **Devices > Discover > Inventory > Polling**.



Caution

Increasing the polling frequency could have an effect on performance.

Procedure

- Step 1** Select **Reports > Trends**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).

- Step 3** From the Report Name list, select **Top N Busiest Clients**.
- Step 4** From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.
- Step 5** From the Frequency list, select the frequency with which you want the performance data aggregated. For example, if you choose hourly, the information displayed will be one hour's aggregation of data.
- Step 6** In the N Value text box, enter the top number of clients you want to view. The following table is displayed:

Table 10-70 **Top N Busiest Clients**

Column	Description
Client Name	The name of the client.
Client IP Address	The IP address of the client.
Client MAC Address	The MAC address of the client.
Bit Rate (Avg) (in kbps)	The average bit rate for the client.
Bit Rate (Min) (in kbps)	The minimum bit rate for the client.
Bit Rate (Max) (in kbps)	The maximum bit rate for the client.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying Top N Client MIC Error Rate

Wireless client polling frequency is set to 51 minutes by default. To increase the accuracy of this report, increase the polling frequency. To change the default setting, select **Devices > Discover > Inventory > Polling**.



Caution

Increasing the polling frequency could have an effect on performance.

This report lists the top number of clients in terms of Message Integrity Check (MIC) rate as perceived by the access point for the selected period of time.

Procedure

- Step 1** Select **Reports > Trends**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **Top N Client MIC Error Rate**.
- Step 4** From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.

Step 5 From the Frequency list, select the frequency with which you want the performance data aggregated. For example, if you choose hourly, the information displayed will be one hour's aggregation of data.

Step 6 In the N Value text box, enter the top number of clients you want to view.

The following table is displayed:



Note Values such as MIC Error Rate might display empty because, when queried, access points sometimes return null values for the cDot11Client counters.

Table 10-71 **Top N Client MIC Error Rate**

Column	Description
Client Name	The name of the client.
Client IP Address	The IP address of the client.
Client MAC Address	The MAC address of the client.
MIC Error Rate (Avg) (per second)	The average value of the rate of Message Integrity Check (MIC) errors recorded for the client.
MIC Error Rate (Min) (per second)	The minimum value of the rate of Message Integrity Check (MIC) errors recorded for the client.
MIC Error Rate (Max) (per second)	The maximum value of the rate of Message Integrity Check (MIC) errors recorded for the client.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Server Response Time Graph

This graph plots the response time of the server over the period of time specified.



Note For PEAP servers, inventory must run twice before a graph is displayed.

Procedure

- Step 1** Select **Reports > Trends**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **Server Response Time Graph**.
- Step 4** From the Start Date list, select the start date for the graph, and from the For a period of list, select the number of days.

- Step 5** From the Frequency list, select the frequency with which you want the performance data aggregated. For example, if you choose hourly, the information displayed will be one hour's aggregation of data.

The following graph displays:

Table 10-72 *Server Response Time Graph*

Column	Description
Server Response Time	The x-axis displays the time intervals. The y-axis displays the response time in milliseconds.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying a Client Roaming Statistics Report

Procedure

- Step 1** Select **Reports > Trends**. The window refreshes with a device selector in the left pane.
- Step 2** Search for a device or select the device for which you want a report from the device selector in the left pane. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** From the Report Name list, select **Client Roaming Statistics**.
- Step 4** From the Start Date list, select the start date and from the For a period of list, select the number of days.
- Step 5** From the Frequency list, select the frequency with which you want the performance data aggregated. For example, if you choose hourly, the information displayed will be one hour's aggregation of data.

The following report displays:

Table 10-73 *Client Roaming Statistics*

Column	Description
IP Address	The IP address of the WLSM.
As Of	The time the WLSE polled information from the device. For more information, see Understanding WLSE Time Displays, page 1-10
Roams per five seconds	The number of roams in a five second period.
Roams per minute	The number of roams in a five second period.
Roams per five minutes	The number of roams in a five second period.

Related Topics

[Using the Basic Report Features, page 10-1](#)

Displaying Real-Time Reports

The real-time reports allow you to view a snapshot of activity which is a useful tool for troubleshooting problems.

Using this option, you can view the following types of real-time reports:

- AP Memory Utilization
- AP CPU Utilization
- AP Packet Statistics
- AP Packet Errors
- AP Radio Utilization
- Associated Clients Statistics
- WLSM Roaming Statistics

Procedure

-
- Step 1** Select **Reports > Real-time**. The window refreshes with a device selector in the left pane.
- Step 2** From the list, select the method you want to use to search for devices.
- Step 3** Enter the specific search criteria, or use an asterisk (*) as a wild card to denote numbers and letters.
- Step 4** Select the folder for which you want a report from the device selector in the left pane.



Note You cannot select an entire group; only up to 10 devices at a time.

The devices in the folder are displayed in the Available Devices list .

- Step 5** Select the devices for which you want to see a real time report and click **>>**.
- Step 6** Click **Next**. The list of reports is displayed.
- Step 7** Select the reports you want to view for the selected devices. (See [Viewing the Real-Time Reports, page 10-97](#).)
-

Viewing the Real-Time Reports

Procedure

-
- Step 1** Select the frequency with which you want the device or devices polled from the **Poll every n minutes** list.
- Step 2** Select the report or reports which you want to view.
- Step 3** Click **Apply** to begin polling.

Step 4 To view a report, click on the report name. The following reports are available:

- AP Memory Utilization—See [AP Memory Utilization](#), page 10-98
- AP CPU Utilization—See [AP CPU Utilization](#), page 10-99
- AP Packet Statistics—See [AP Packet Statistics](#), page 10-99
- AP Packet Errors—See [AP Packet Errors](#), page 10-100
- AP Radio Utilization—See [AP Radio Utilization](#), page 10-101
- Associated Clients Statistics—See [Associated Clients Statistics](#), page 10-101
- WLSM Roaming Statistics—See [WLSM Roaming Statistics](#), page 10-102

AP Memory Utilization

Table 10-74 *AP Memory Utilization*

Column	Description
Timestamp	The time the device's state last changed. For more information, see Understanding WLSE Time Displays , page 1-10.
Device	The name of the device.
Memory Pool Name	The name of the memory pool.
Memory Free	The amount of free memory available.
Memory Used	The amount of memory used.
%Utilization	The total percentage of memory used.
Graph	Click the graph icon to see a graph of the data. For information on the graphs, see Viewing RealTime Graphs , page 10-103

- To refresh the screen immediately, click **Now**.



Note If you turn off the auto refresh, and do not interact with the report at all, polling will be disabled.

- To turn on auto refresh, click **Auto**.
- To turn off the auto refresh, click **Off**.
- To close the report, click **Close**.

AP CPU Utilization

T

Table 10-75 AP CPU Utilization

Column	Description
Timestamp	The time the device's state last changed. For more information, see Understanding WLSE Time Displays, page 1-10 .
Device	The name of the device.
CPU 5sec	Traffic rate for CPU utilization displayed at 5 seconds.
CPU 1 min	Traffic rate for CPU utilization displayed at 1 minute.
CPU 5 min	Traffic rate for CPU utilization displayed at 5 minutes.
Graph	Click the graph icon to see a graph of the data. For information on the graphs, see Viewing RealTime Graphs, page 10-103

- To refresh the screen immediately, click **Now**.
- To turn off the auto-refresh, click **Off**.



Note If you turn off the auto refresh, and do not interact with the report at all, polling will be disabled.

- To turn on auto refresh, click **Auto**.
- To close the report, click **Close**.

AP Packet Statistics

This report includes information for the the following:

- Radio Interfaces
- Ethernet Interfaces

Table 10-76 AP Packet Statistics

Column	Description
Timestamp	The time the device's state last changed. For more information, see Understanding WLSE Time Displays, page 1-10 .
Device	The name of the device.
IfDecr	Identifies the interface.
Transmit (packets)	The number of packets transmitted.
Receive (packets)	The number of packets received.
Transmit (bytes)	The number of bytes transmitted.
Receive (bytes)	The number of bytes received.

Table 10-76 *AP Packet Statistics (continued)*

Column	Description
Retries	The total number of retries.
Graph	Click the graph icon to see a graph of the data. For information on the graphs, see Viewing RealTime Graphs, page 10-103

- To refresh the screen immediately, click **Now**.
- To turn off the auto-refresh, click **Off**.



Note If you turn off the auto refresh, and do not interact with the report at all, polling will be disabled.

- To turn on auto refresh, click **Auto**.
- To close the report, click **Close**.

AP Packet Errors

This report includes information about packet errors for access points. The table displays the following:

Table 10-77 *AP Packet Errors*

Column	Description
Timestamp	The time the device's state last changed. For more information, see Understanding WLSE Time Displays, page 1-10 .
Device	The name of the device.
IfDecr	Identifies the interface.
% Packet Errors	The total percentage of packet errors.
Graph	Click the graph icon to see a graph of the data. For information on the graphs, see Viewing RealTime Graphs, page 10-103

- To refresh the screen immediately, click **Now**.
- To turn off the auto-refresh, click **Off**.



Note If you turn off the auto refresh, and do not interact with the report at all, polling will be disabled.

- To turn on auto refresh, click **Auto**.
- To close the report, click **Close**.

AP Radio Utilization

This report includes information about the radio utilization and total number of clients for access points. The table displays the following:

Table 10-78 *AP Radio Utilization and Total Number of Clients*

Column	Description
Timestamp	The time the device's state last changed. For more information, see Understanding WLSE Time Displays, page 1-10 .
Device	The name of the device.
RF Interface	Identifies the interface.
Number of Clients Connected	The current number of clients connected to the access point.
% RF Utilization	The percentage of radio frequency utilization.
Graph	Click the graph icon to see a graph of the data. For information on the graphs, see Viewing RealTime Graphs, page 10-103

- To refresh the screen immediately, click **Now**.



Note If you turn off the auto refresh, and do not interact with the report at all, polling will be disabled.

- To turn on auto refresh, click **Auto**.
- To turn off the auto-refresh, click **Off**.
- To close the report, click **Close**.

Associated Clients Statistics

This report includes information for the following:

Table 10-79 *Associated Client Statistics*

Column	Description
Timestamp	The time the device's state last changed. For more information, see Understanding WLSE Time Displays, page 1-10 .
Device	The name of the device.
Client Name	The name of the associated client.
Client IP	The IP address of the client.
Client MAC	The MAC address of the client.
Tx (packets)	The number of packets transmitted.
Tx (octets)	The number of octets transmitted.

Table 10-79 *Associated Client Statistics (continued)*

Column	Description
Rx (packets)	The number packets received.
Rx (Octets)	The number of octets received.
Signal Strength (dBm)	A tally of the received signal power.
Signal Quality (%)	The current percentage of radio signal quality.
Packet Errors	The total number of packet errors.
Graph	Click the graph icon to see a graph of the data. For information on the graphs, see Viewing RealTime Graphs, page 10-103

- To refresh the screen immediately, click **Now**.
- To turn off the auto-refresh, click **Off**.



Note If you turn off the auto refresh, and do not interact with the report at all, polling will be disabled.

- To turn on auto refresh, click **Auto**.
- To close the report, click **Close**.

WLSM Roaming Statistics

This report includes information for the following:

Table 10-80 *WLSM Roaming Statistics*

Column	Description
Timestamp	The time the device's state last changed. For more information, see Understanding WLSE Time Displays, page 1-10 .
Device	The name of the device.
Roams 1 min	The number of roams in a one-minute period.
Roams 5 min	The number of roams in a five-minute period
Graph	Click the graph icon to see a graph of the data. For information on the graphs, see Viewing RealTime Graphs, page 10-103

- To refresh the screen immediately, click **Now**.
- To turn off the auto-refresh, click **Off**.



Note If you turn off the auto refresh, and do not interact with the report at all, polling will be disabled.

- To turn on auto refresh, click **Auto**.
- To close the report, click **Close**.

Viewing RealTime Graphs

Using this feature, you can display the data in the table graphically. You can do the following:

- To refresh the screen immediately, click **Refresh Now**.
- To turn on auto refresh, click **Auto Refresh-On**.
- To perform operations on the graph, right mouse click, then select one of the available options.

**Note**

You cannot print or save graphs.

Displaying Intrusion Detection System Reports

To view Intrusion Detection System information (such as data concerning rogue and friendly APs, interference, unregistered clients, or ad-hoc networks), select **IDS > Reports** (see [Using the IDS Reports Subtab, page 14-5](#)).



Configuring Your WLAN Radio Environment

The following topics provide information about the WLSE radio environment:

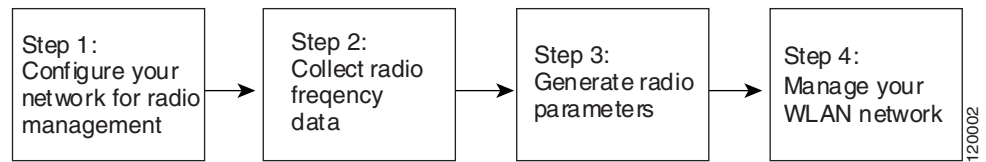
- [WLSE Radio Management, page 11-1](#)
- [Enabling and Disabling Radio Management Features, page 11-4](#)
- [Configuring Your Network for Radio Management, page 11-5](#)
- [Understanding Radio Management, page 11-7](#)
- [Understanding Frequency and Transmit Power Planning, page 11-14](#)
- [Collecting Radio Location Data, page 11-14](#)

WLSE Radio Management

The WLSE simplifies the deployment, expansion, and day-to-day management of your WLAN radio environment. Using radio management, intrusion detection, and site management features, you can:

- Automatically configure network-wide radio parameters during initial deployment and network expansion.
- Detect all neighboring APs and produce path loss data used for rogue location estimations, radio parameter generation, and coverage display data, generate additional data to help provide optimal coverage for the radio parameter generator, and provide configurations for APs based on measurement data collected from client walkabouts and AP radio scans.
- Continuously monitor the radio environment, adjust APs to cover potential areas of lost coverage, alert the WLAN administrator to radio network changes, and feed frame monitoring information to a third-party server for further analysis.
- Detect and report network intrusions, such as rogue APs, interference, ad-hoc networks, excessive management frame transmissions, unregistered clients, and authentication and protection attacks.
- Access a graphical view of the access points (APs) on each floor of your building(s) and view the relative location of unknown or rogue APs.

To set up and manage your WLAN radio environment, use the features provided by the Radio Manager, Sites, and the Intrusion Detection System:

Figure 11-1 Radio Management Setup Overview**Step 1: Configure your network for radio management**

All the device information shown under the Radio Manager, Sites, and Intrusion Detection Services tabs is polled from the managed devices in your network. The WLSE polls and receives aggregated data from WDS devices and provides intelligent processing of this data. The WLSE can manage multiple subnets, so it can receive radio frequency data from many WDS devices.

The WLSE must register with each WDS in each managed AP subnet to receive radio frequency data. If the WLSE is not registered, *none of the Radio Manager, Sites, or Intrusion Detection System functions will work.*

In addition, if Radio Management has been disabled, none of the Radio Manager functions will work. You must enable Radio Management to access the Radio Manager features (see [Enabling and Disabling Radio Management Features, page 11-4](#)).

For more information about preparing your network to manage radio devices, see:

- [What is WDS and Why Do I Need It?, page 11-8](#)
- [Configuring Your Network for Radio Management, page 11-5](#)
- [Verifying Radio Management Capability, page 13-27](#)
- The *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine*. For information about locating this document, see [Finding WLSE Documentation on Cisco.com, page 1-15](#).

Step 2: Collect radio location measurements.

After the access points have been configured for radio management, you can use selections under the Radio Manager and Sites tabs to gather radio location measurements. The WLSE uses these measurements to characterize the radio environment and determine the channels and power limits for each 802.11 Basic Service Set (BSS).

To collect this data, you can either:

- Run a wizard that walks you through the data collection process (see [Using the Location Manager Assisted Site Survey Wizard, page 13-17](#)).
- Run the data collection processes separately:
 - a. Run AP Radio Scan—see [Using AP Radio Scans to Collect RM Data, page 13-43](#)
 - b. Run Client Walkabout—see [Using Client Walkabouts to Collect RM Data, page 13-54](#)
 - c. Start Radio Monitoring—see [Using Radio Monitoring to Collect RM Data, page 12-1](#)

For more information about collecting and managing radio location measurements, see:

- [Collecting Radio Location Data, page 11-14](#)
- [Managing RM Data, page 13-81](#)

Step 3: Generate optimal radio parameters values for the APs.

You can use the selections under the Radio Manager or Sites tabs to recommend optimal radio transmit power, channel selection, and beacon interval (optional) for each AP, then apply these configuration settings.

To generate these parameters, you can either:

- Run a wizard that walks you through the parameter generation process
- Run the RM Assisted Configuration procedure

For more information about generating AP radio parameters, see [Generating Radio Parameters, page 13-66](#).

Step 4: Manage your WLAN network.

After you have configured your network for radio management, collected the radio location data, and generated the radio parameters, you are ready to manage your WLAN environment. You can:

- Use the Radio Manager to evaluate AP radio performance, adjust neighboring AP interfaces to cover potential areas of lost coverage, or use dedicated APs as sensors to feed information to a third-party server for further analysis (see [Managing Your WLAN Radio Environment, page 12-1](#)).
- Use a graphical view of the APs on each floor of your building(s) to display the predicted coverage of each AP (see [Managing Your WLAN Radio Environment by Sites, page 13-1](#)).
- Detect network intrusions such as rogue APs, ad-hoc networks, non-802.11 interference, and so on (see [Using the Intrusion Detection System, page 14-1](#)).

Related Topics

- [Configuring Your Network for Radio Management, page 11-5](#)
- [Enabling and Disabling Radio Management Features, page 11-4](#)
- [Understanding Radio Management, page 11-7](#)

Enabling and Disabling Radio Management Features

WLSE Radio Management includes three major groups of features: the Intrusion Detection System (IDS), the Radio Manager (Radio Mgr), and the Site planning features (Sites, including Location Manager). By default, these features are automatically enabled. However, customers that have large, distributed, or staged deployments of wireless solutions might only require the fault, performance, and configuration management features of WLSE and will want to disable Radio Management.

The following topics provided more information about disabling Radio Management:

- [Using the CLI Command, page 11-4](#)
- [Disabled Radio Management Related Faults, page 11-4](#)

Using the CLI Command

The following CLI command will enable or disable Radio Management and restart the WLSE:

```
radiomanager enable | disable
```

Enabling or disabling Radio Management causes the WLSE to reload. For more information about this command, see [Command Line Interface \(CLI\) Commands, radiomanager, page A-35](#).

Disabled Radio Management Related Faults

When Radio Management is disabled, no new Radio Management related faults are generated, and any Radio Management related faults that existed before the command was executed must be cleared manually. After the faults are manually cleared, they are not regenerated even if the fault condition still exists.

When Radio Management is disabled, the following faults are no longer generated:

- Ad-hoc detection (all)
- Auto re-site survey (all)
- General IDS settings (see **IDS > Manage IDS Settings**):
 - Unregistered Client
 - Excessive Frame Management
 - EAPOL Settings
- Inconsistent state fault
- Interference (all)
- Management frame protection (all)
- Non-IDS settings (see **Faults > Manage Fault Settings**):
 - Access Point/Bridge Policies > Registration Error
 - Radio 802.11x Policies > Dynamic Frequency Selection (DFS)
 - WDS > Authentication Failures
 - WDS > WLSE-WDS Link Status
- Rogue detection (all)

- Self healing (all)

Configuring Your Network for Radio Management

Before you can use the Radio Management features provided by WLSE, you must configure your network. If your network is not properly configured, *none of the Radio Manager, Sites, or Intrusion Detection System functions will work.*

If you are configuring APs or WLSM devices as WDS devices, you can use the Deployment Wizard (see [Using the Deployment Wizard, page 2-1](#)). The Deployment Wizard replaces many of the manual configuration procedures that are normally required to configure infrastructure access points and WDS devices and to configure the WLSE to discover and manage those devices.

Although you can use the Deployment Wizard to set up most APs, you must use the following manual procedure to configure an external ACS server for AP-WDS-WLSE authentication.

Procedure

-
- Step 1** Be sure that all APs are managed (discovered, inventoried, and managed—see [Device Discovery and Management, page 4-1](#)).
- Step 2** Configure one or more WDS devices (for more information about WDS, see [What is WDS and Why Do I Need It?, page 11-8](#)):
- AP-WDS: You can configure one or more APs in each AP subnet to run WDS. When multiple WDSs exist in the same subnet, one WDS becomes the active WDS and the other WDSs become backups. For more information about configuring AP-WDS devices, see the “Radio Management Setup—IOS Devices” chapter in *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.13*. For information about locating this document, see [Finding WLSE Documentation on Cisco.com, page 1-15](#).
 - WLSM-WDS: You can configure a Wireless LAN Services Module ([WLSM](#)) device to run WDS. A WLSM device is a module for the Cisco Catalyst 6500 Series switch that provides WDS to the wireless network. For information about configuring WLSM-WDS devices, see the WLSM device documentation.
- Step 3** Configure your devices for radio management.
- For information about radio management configuration procedures, see the “Radio Management Setup—IOS Devices” chapter in *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.13*.
- To verify that you have correctly configured the network for radio management, use the **Verify RM Capability** option under the Sites tab (see [Verifying Radio Management Capability, page 13-27](#)).
- Step 4** Enable LEAP authentication.



Note

All APs must authenticate with a WDS using LEAP. This requirement is separate from the client’s authentication scheme—clients can use a non-LEAP security scheme, but the AP and WLSE must use LEAP to authenticate to the WDS.

**Note**

A WDS can connect to Cisco's ACS v3.2 as the LEAP Authentication server. You can use the AP/WLSM's LEAP Local Authentication Server feature if the customer is not using LEAP for any purpose other than to fulfill the requirement on the WLSE/WDS/AP.

**Note**

Do not set a session timeout on the ACS server that is less than 600 seconds. A session timeout of less than 600 seconds can disrupt Radio Manager operations.

For more information about enabling LEAP authentication, see the *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.13*. For information about locating this document, see [Finding WLSE Documentation on Cisco.com, page 1-15](#).

Step 5 Configure the WLCCP credentials (see [Enter WLCCP Credentials for Wireless Domain Services, page 4-13](#)).

Step 6 Verify that the active WDS appears under the device tree:

- a. Select **Reports > Device Center**.
- b. Open the **Wireless Domain Services** folder.
- c. Open the **Active WDS** folder.
- d. Select the device.
- e. Select **WDS Summary Report**.
- f. Verify that the **WLSE to WDS Authentication Status** column contains the string "KeysSetUpWithWDS" or "Authenticated".

You can also verify this setting by running the "show wlccp wnm status" command on the active WDS in enable mode. A typical output would look like this:

```
NMS-AP1200-1#show wlccp wnm status
WNM IP Address: 172.16.0.0 Status: SECURITY KEYS SETUP
```

where:

- 172.16.0.0 = IP address of WLSE
- Status = SECURITY KEYS SETUP. This indicates that the active WDS is properly authenticated with WLSE.

Step 7 Verify that the APs are managed and registered with WDS:

- a. Select **Reports > Device Center**.
- b. Open the **Wireless Domain Services** folder.
- c. Open the **Active WDS** folder.
- d. Select the device.
- e. Select **WDS Registered APs**. A list of all the APs that are registered with this WDS is displayed.

You can also verify this setting by running the "show wlccp wds ap" CLI command on the active WDS in enable mode.

Step 8 Configure the ACS server to support fast roaming and simultaneous logins.

For information about configuring the ACS server to support roaming and simultaneous logins, see the ACS server documentation. For other information about configuring the ACS server, see the “Setting Up an ACS Server” chapter in *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.13*. For information about locating these documents, see [Finding WLSE Documentation on Cisco.com, page 1-15](#).

Step 9 Configure the AAA server to allow multiple jobs.

For information about configuring the AAA server to multiple logins, see the AAA server documentation. For other information about configuring the AAA server, see the “Setting Up an ACS Server” chapter in *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.13*. These documents are also located on Cisco.com.

Step 10 Now you are ready to collect radio location data (see [Collecting Radio Location Data, page 11-14](#)).

Related Topics

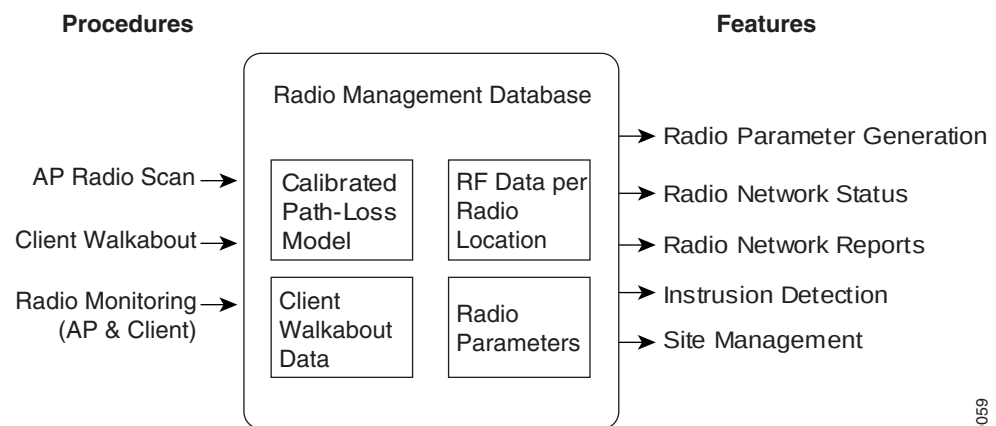
- [Enabling and Disabling Radio Management Features, page 11-4](#)
- [Understanding Radio Management, page 11-7](#)

Understanding Radio Management

The radio management environment provided by WLSE consists of:

- *Procedures* that gather data about the radio environment.
- The radio frequency *database*, which contains radio data and parameters.
- *Features* that use the information in the database.

Figure 11-2 WLSE Radio Management Environment



130059

The following topics describe how the WLSE implements radio management:

- [What is WDS and Why Do I Need It?, page 11-8](#)
- [Understanding Radio Performance—Coverage and Capacity, page 11-10](#)
- [Collecting Radio Location Data, page 11-14](#)

What is WDS and Why Do I Need It?

The critical software component in the network is a set of IOS features called the Wireless Domain Services (WDS). The following types of devices can supply the WDS:

- An access point configured for WDS
Each WDS access point supports one AP subnet. You can add additional WDS access points for redundancy. The priorities you set on the WDS access points determine which one is the active and which ones are backups.
- A Wireless LAN Services Module (WLSM)
Each WLSM supports multiple AP subnets, as long as all of the subnets are served by the switch on which the WLSM is installed.

The following topics describe these device types:

- [Understanding WDS Access Points, page 11-8](#)
- [Understanding WLSM WDS Devices, page 11-9](#)

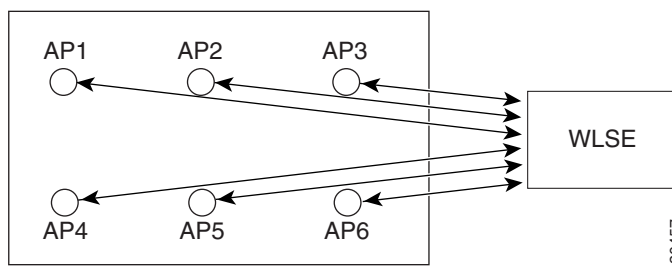
Understanding WDS Access Points

The WDS provides control path technologies that must be active on an AP in each AP subnet; a backup WDS can also be defined in each AP subnet. The WDS provides:

- Fast, secure layer-2 wireless client roaming—The WDS acts as an 802.1x authenticator for wireless clients within the layer-2 network.
- Radio Management (RM) data aggregation—The WLSE provides intelligent processing of aggregated data collected by the WDS access points from other wireless clients in the network. The WLSE can manage multiple subnets, so it can receive radio data from many APs running WDS.

There is no RM data aggregation without a WDS. Without a WDS, the communication between the access points and WLSE looks like this:

Figure 11-3 Basic Network Management Communications



Using this approach, the WLSE can communicate with the APs using only these two methods:

- Primary: SNMP
- Secondary: CLI over telnet or SSH

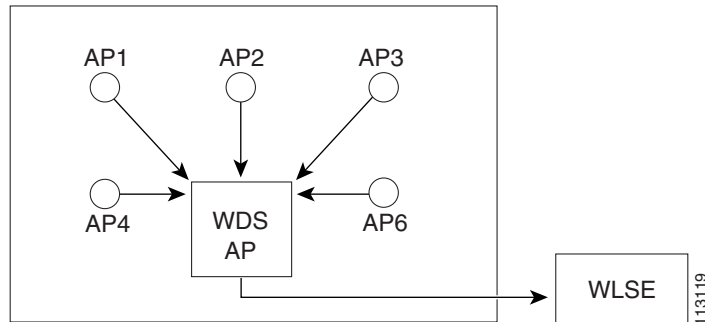


Caution

The WLSE must register with the WDS in each managed AP subnet to receive Radio Manager data. If the WLSE is not registered, *none of the Radio Manager functions will work.*

After you configure the network for Radio Management tasks (see [Configuring Your Network for Radio Management, page 11-5](#)), the WLSE communicates all Radio Management activities with one or more WDS APs instead of all APs in the network. Each WDS AP collects data from other wireless clients in the network and sends this aggregated data to the WLSE.

Figure 11-4 Additional Radio Management Communications



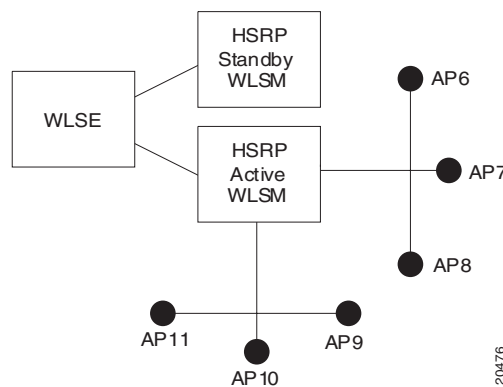
Understanding WLSM WDS Devices

A Wireless LAN Services Module (WLSM) device is a module for the Cisco Catalyst 6500 Series switch that provides WDS to the wireless network. Each WLSM supports multiple AP subnets, as long as all of the subnets are served by the switch on which the WLSM is installed.

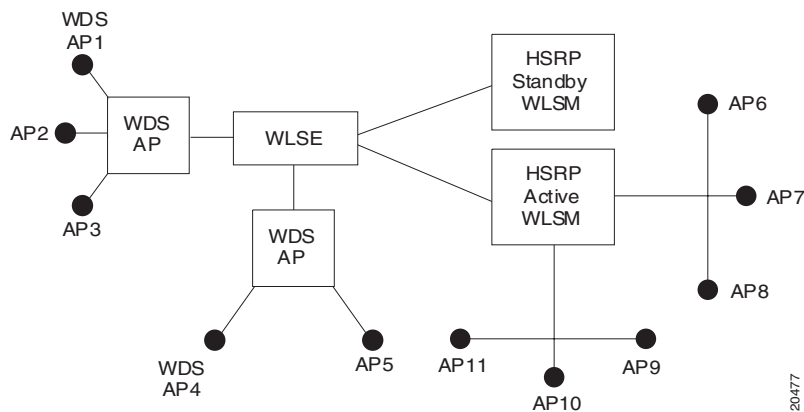
You can add a second WLSM to serve as a standby. The WLSE authenticates with both the HSRP active and HSRP standby WLSM devices (WLSM uses HSRP to handle redundancies). In the reports, both WLSM devices (HSRP active and HSRP standby) will appear as active WDSs.

If the HSRP active WLSM goes down, the HSRP standby WLSM will communicate with the AP subnets (see [Figure 11-5](#)).

Figure 11-5 WLSE-WLSM Communications



[Figure 11-6](#) illustrates a network that uses both AP and WLSM WDS devices to manage the access points in the network. In this example, additional access points have been identified as backup AP-WDS devices (AP1 and AP4), and an additional HSRP-based WLSM-WDS device has been added to as a standby for the active WLSM-WDS.

Figure 11-6 Sample Network Using AP-WDS and WLSM-WDS Devices

Understanding Radio Performance—Coverage and Capacity

The Radio Manager:

- Quantifies the performance within a region

Each region is defined by the rough degree of contention and packet collisions experienced by clients in the region due to traffic outside of the BSS.

The inter-BSS contention and collision translates into performance degradation, which the Radio Manager estimates for all potential clients within the region. Contention and collisions from managed APs *and* rogue and friendly APs are used in the performance evaluation.



Note

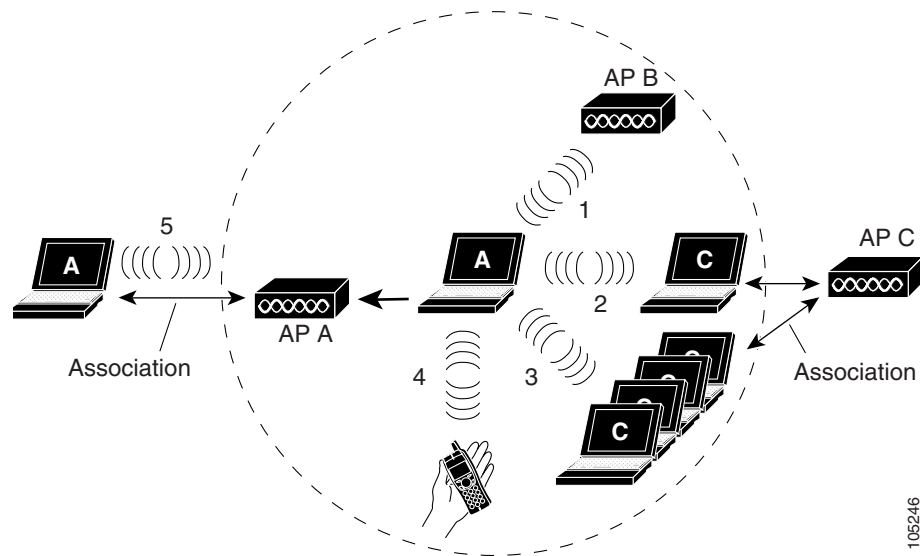
All relevant APs are used in the performance evaluation regardless of building or floor placement.

- Takes the region sizes into account to assure coverage over the region

The types and sizes of performance regions determine the expected maximum, minimum, and average performance of a particular domain.

AP/Client Relationships

The Radio Manager acquires knowledge of the WLAN radio environment from measurements obtained from Cisco APs and Cisco clients. [Figure 11-7](#) illustrates the relationships between three APs and their clients.

Figure 11-7 *AP/Client Relationships*

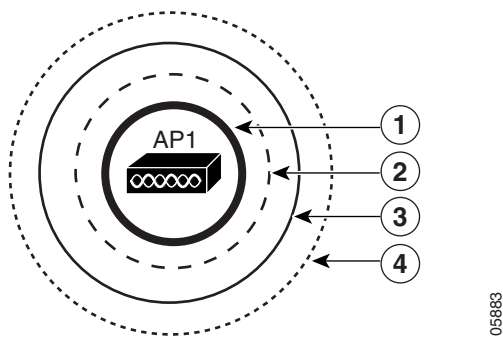
In this example, the measuring client and one other client are associated with AP A, but neither client detects the other AP's signal. AP B is close enough to be detected by the measuring client, and AP C is out of range, but the measuring client does detect some of AP C's associated clients. [Table 11-1](#) describes these relationships in more detail.

Table 11-1 *AP/Client Relationships*

Item	Description
1	The measuring client identifies access point B as a source of 802.11 contention.
2	The measuring client detects contention from a client in another BSS and identifies access point C as the BSS access point.
3	The measuring client reports significant contention due to clients in another BSS. Access point C is identified as the BSS access point.
4	The measuring client indicates intermittent non-802.11 interference and describes the statistics of its received strength.
5	The measuring client identifies another client in its BSS that appears to be hidden from it.

Radio Performance Regions

Radio performance regions within a BSS depend on the placement and transmit power of other co-channel APs. The transmit power of a BSS defines a set of RF reception rings around its AP (see [Figure 11-8](#)).

Figure 11-8 RF Reception Rings

1	Planned BSS coverage	3	Uplink may be decodable
2	Downlink RF influence	4	Uplink RF influence

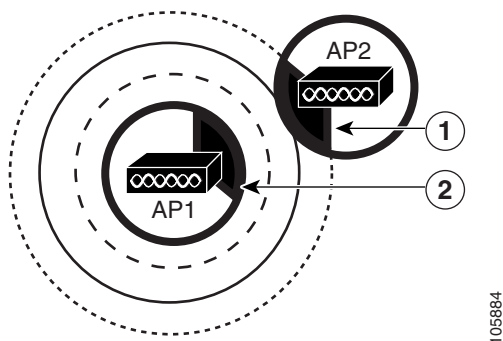
Two rings correspond to the downlink:

- The **planned BSS coverage ring** (1) corresponds to the area in which clients can reliably receive the downlink signal.
- The **downlink RF influence ring** (2) corresponds to the area in which reception is difficult, but the downlink signal may still contend or collide with a downlink from another AP on the same channel.

Two similar rings correspond with areas of reception and the RF influence emanating from a client positioned at the edge of the BSS coverage ring. The significant ring, the **uplink RF influence ring** (4), corresponds to the signal that originates from a client sending packets up to its AP.

Uplink Contention Regions

In [Figure 11-9](#), AP1 and AP2 share the same channel. AP2 is examined as the BSS of interest, while AP1 is the cochannel neighbor. The highlighted performance region corresponds with an area in which BSS2 clients must contend with traffic from BSS1. The source of contention is shown as a set of clients in BSS1 near the edge of their planned coverage ring. This is known as uplink contention because it delays uplink traffic from clients to their AP.

Figure 11-9 Sample Performance Region

1	BSS2 performance region: AP2 clients that experience contention from AP1's clients
2	Source of contention: AP1 clients that cause the contention.

If AP2 has neighbors sharing the same channel on all sides, then similar uplink contention regions are defined in the direction of each neighboring AP. If any of these neighbors is closer than the one shown in [Figure 11-9](#) or uses a higher power limit, then the uplink contention region is larger than shown in the figure. If clients of the neighboring BSSs are close enough to be detected by AP2, then AP2 experiences downlink contention due to the clients' traffic.

The BSS may also contain regions in which a client receives traffic that has collided with packets from another station. This occurs when the intended source and interfering source do not detect each other. This happens when:

- Stations in the same BSS are hidden from each other.
This situation can be remedied by blocking out time for an access point using RTS/CTS (request-to-send, clear-to-send) commands.
- A client in a neighboring BSS is within range of the client of interest but is not detected by the latter client's AP.
This situation is an inter-BSS interference problem that could exist in any dense WLAN and *cannot* be remedied with RTS/CTS. One goal of the Radio Manager is to minimize this occurrence with good radio configurations.

Understanding Multiple BSSIDs

The Base Service Set Identifier (BSSID) is typically the MAC address of the radio. WLSE also supports multiple BSSIDs (MBSSID) on a single radio (AP). MBSSIDs address several issues:

- Passive client scanning support for multiple SSIDs
- Multiple unencrypted multicast streams
- Segregation of unencrypted and encrypted broadcast streams
- Encrypted multicast streams to not cause decrypt errors at the client
- Support for existing clients (no changes allowed on the client)

To a *client*, an MBSSID AP appears to be several distinct co-located APs. An MBSSID AP transmits a beacon for each BSSID/SSID, which makes all of the SSIDs visible for passive scanning. The distinct VLAN multicast streams are easily separated using the BSSID, which allows multiple unencrypted multicast streams and eliminates the decryption errors that occur with encryption separation.

To the *WLSE*, the MBSSID AP appears to be one AP. Each radio that is configured with MBSSID will appear as one radio with multiple VLANs, and each distinct MAC address associated with the VLAN is considered a synonym of the real radio's MAC address.

Support for multiple BSSIDs does not imply full virtual AP capability and functionality. For example:

- All BSSIDs are synchronized to the same clock.
- All BSSIDs have the same transmit power.
- All BSSIDs use the same set of transmit data rates.
- The MAC address allocation is dynamically assigned by the radio.

Understanding Frequency and Transmit Power Planning

The Radio Parameter Generation algorithm in WLSE gives you a near-optimal frequency and power plan for managed APs. However at first look, the WLSE-recommended plan might be dramatically different from what you expect. If you have an understanding of 2G cellular technology, particularly GSM, it's important to know that the intuitive heuristics developed from 2G cellular telephony are misleading for WLANs.

In traditional 2G deployments, you design your power plan by making sure adjacent and nearby cells are on differing channels.

In 802.11 WLAN, the closest distance between two co-channel APs is less important than the total number of interfering APs in the entire coverage area.

There are significant differences in 2G and 802.11 WLANs:

- In 2G cellular telephony, devices in each cell transmit without regard to who is transmitting in other cells. Communication is reliable as long as the desired power is sufficiently above the total interference power from all other devices on the same channel. A frequency plan with adjacent co-channel APs is fatally poor.
- WLANs have much smaller cells than 2G systems and can achieve much higher per-user data rates. Instead of transmitting without regard to transmissions in other cells, 802.11 WLAN devices determine if the shared wireless medium is quiet and then transmit only when it is so. WLANs must minimize the number of interfering devices that can detect each other, *not* the total interference power.
- In 2G technology, the total interference *power* must be kept small by keeping co-channel devices far away from each other.
- In 802.11 WLAN systems, the total number of interfering *devices*, especially co-channel AP devices, must be kept small. In WLANs, a frequency plan that allows a few adjacent co-channel APs in exchange for making more co-channel APs completely undetectable is a better plan. *The closest distance between two co-channel APs is less important than the total number of interfering APs.*
- WLAN deployments cover multiple floors; in 2G cellular telephony, you cover the ground. In WLANs, you might be covering floors in 3 dimensions so you must take into consideration the signals from other floors and other buildings.

Collecting Radio Location Data

Radio location measurements characterize the radio environment and provide the information other Radio Manager features require to determine the channels and power limits for each Basic Service Set (BSS). To gather these measurements:

1. **Perform an AP Radio Scan.** The AP Radio Scan procedure (see , page 11-15) detects all neighboring APs and produces path loss data used for rogue location estimations, radio parameter generation data, and coverage display data.

**Note**

If you do not run AP Radio Scan, the Coverage Display under the Sites tab will be computed using the default pass loss model. Because no path loss measurement data has been collected, the coverage views could be distorted.

2. **Perform a Client Walkabout** (optional, but recommended—see [Using Client Walkabouts to Collect RM Data, page 13-54](#)). The additional data generated by a client walkabout helps provide optimal coverage for the radio parameter generator.

If you do not perform a client walkabout, you *must* enter a floor plan that includes the distances between APs (see [Adding Floors to Location Manager, page 13-9](#)).

3. **Enable Radio Monitoring.** Radio Monitoring (see [Using Radio Monitoring to Collect RM Data, page 12-1](#)) periodically gathers RF statistics, identifies specific signal sources, and is your primary means of detecting rogue access points.

**Note**

If you never enable Radio Monitoring or run AP Radio Scan, no unknown radios (rogue or friendly) will be detected. If you run AP Radio Scan but do not enable Radio Monitoring, some unknown radios will be detected, but not as many as would be detected if Radio Monitoring was running. Self healing also relies on the data generated by Radio Monitoring and AP Radio Scan.

You can also use the Assisted Site Survey wizard, which is part of Sites, to walk you through the process of determining the optimal radio transmit power and channel selection. This wizard interface steps you through AP radio scan, client walkabout, and radio parameter generation (see [Using the Location Manager Assisted Site Survey Wizard, page 13-17](#)).

Related Topics

- [Configuring Your Network for Radio Management, page 11-5](#)
- [Viewing Current Path Loss Results, page 10-17](#)
- [Viewing Historical Path Loss Results, page 10-19](#)
- [Viewing Current Channel Load Results, page 10-19](#)
- [Viewing Historical Channel Load Results, page 10-21](#)
- [Managing RM Data, page 13-81](#)
- [Understanding Radio Management, page 11-7](#)



Managing Your WLAN Radio Environment

Use the functions under the Radio Manager tab to simplify the deployment, expansion, and day-to-day management of your WLAN radio environment. Using the Radio Manager functions, you can:

- Radio Monitoring—helps you continuously monitor the radio environment. See [Using Radio Monitoring to Collect RM Data, page 12-1](#).
- Self Healing—evaluates current AP radio performance on a per-floor basis against baselined performance data. See [Healing Your Network, page 12-11](#).
- Auto Re-Site Survey—adjusts APs to cover potential areas of lost coverage. See [Evaluating AP Radio Performance, page 12-6](#).
- Frame Monitoring—lets you feed Frame Monitoring information to a third-party server for further analysis. See [Using Frame Monitoring, page 12-19](#).

Getting Started with Radio Manager

Before you can use the features provided by the Radio Manager:

- Radio Management must be enabled.

If Radio Management has been disabled, *none of the Radio Manager features will be displayed* (see [Enabling and Disabling Radio Management Features, page 11-4](#)).

- You must set up your network to manage your radio environment.

If your network is not properly configured, *none of the Radio Manager features will work*. To configure your network, see [Configuring Your WLAN Radio Environment, page 11-1](#).

Using Radio Monitoring to Collect RM Data

Radio location measurements characterize the radio environment and provide the information other Radio Manager features require to determine the channels and power limits for each Basic Service Set (BSS).

To gather these measurements, Radio Monitoring must be enabled. Radio Monitoring periodically gathers radio frequency statistics, identifies specific signal sources, and *is your primary means of detecting rogue access points*.

The following topics explain how and where to use Radio Monitoring:

- [Understanding Radio Monitoring, page 12-2](#)

- [Guidelines for Running Radio Monitoring, page 12-3](#)
- [Starting Radio Monitoring, page 12-4](#)

You can also use the Assisted Site Survey wizard to walk you through the process of determining optimal radio transmit power and channel selection. This wizard interface helps you through AP radio scan, client walkabout, and radio parameter generation.

Related Topics

- [Understanding Radio Management, page 11-7](#)

Understanding Radio Monitoring

Radio Monitoring:

- Is enabled by default.



Note

If you disable Radio Monitoring and do not run AP Radio Scan, no unknown radios (rogue or friendly) will be detected. If you run AP Radio Scan but disable Radio Monitoring, some unknown radios will be detected, but not as many as would be detected if Radio Monitoring was running.

- Runs on the specified Cisco IOS APs and its associated CCXV2-compliant clients.
- Continuously monitors the WLAN radio environment.
- Measures the path loss or RSSI between APs and between regular APs and their clients.
- Monitors client registration data for scanning-only APs.
- Discovers any new APs that are transmitting beacons.
- Generates alerts when new APs appear or interference occurs.

How It Works

During normal operation, the Radio Manager requests measurements from Cisco APs and clients to monitor the WLAN radio frequency environment. These measurements occur less frequently than during a client walkabout (see [Using Client Walkabouts to Collect RM Data, page 13-54](#)), typically one or more minutes apart.

Radio Monitoring allows you to select which channels are monitored; both APs and clients can measure serving channels (the channel on which the AP is transmitting) and non-serving channels (the channels on which the AP is *not* transmitting). You make this choice when you enable Radio Monitoring (see [Starting Radio Monitoring, page 12-4](#)).

Radio Monitoring only monitors managed devices that appear in its Selected Devices list. When Radio Monitoring is enabled, all devices in this list are monitored. There are two ways to monitor newly added APs:

- By default, any newly managed device is added to the Selected Devices list, regardless of the Radio Monitoring enable status.
- As long as the **Add Newly Managed AP to Selected AP List** check box is selected, *future* newly-managed APs will be automatically added to Radio Monitoring's Selected Devices list. This check box only affects devices that are managed *after this setting has been saved*.

**Note**

Radio Monitoring will be turned on for newly-managed devices only if Radio Monitoring has been enabled (see [Starting Radio Monitoring, page 12-4](#)).

Data Produced

Radio Monitoring periodically gathers radio frequency statistics and identifies specific signal sources. The channel measurements it collects are used for many features, such as radio configuration, rogue AP discovery, interference detection, network self-healing, auto re-site surveys, and certain Radio Manager reports.

**Note**

Radio Monitoring is enabled by default. *If you disable Radio Monitoring, you will not have access to these features.*

Related Topics

- [Guidelines for Running Radio Monitoring, page 12-3](#)
- [Healing Your Network, page 12-11](#)

Guidelines for Running Radio Monitoring

Prerequisites

Before running Radio Monitoring, you must:

1. Configure your network for radio management (see [Getting Started with Radio Manager, page 12-1](#)).

**Note**

If Radio Management has been disabled, *none of the Radio Manager features will be displayed* (see [Enabling and Disabling Radio Management Features, page 11-4](#)).

2. Define the location elements (buildings and floors) and place the APs on the floor images. This step is optional, but will help you get the best results from the Location Manager displays. For more information, see:
 - [Entering Building Information, page 13-4](#)
 - [Adding Floors to Location Manager, page 13-9](#)
 - [Adding Devices to Floors, page 13-14](#)

Tips

- Leave Radio Monitoring continuously running on your network so new APs are discovered promptly, the necessary faults are generated, and your reports are accurate and current.
- You can add an AP to the Radio Monitoring list and also include it in an AP Radio Scan or Client Walkabout; the measurement requests for these two features supersede the Radio Monitoring requests. When the other, shorter term procedures end, the APs return to normal radio monitoring mode.
- Radio Monitoring produces the data for these reports:
 - The Path Loss Between Managed APs report contains the calculated path loss data (see [Viewing Current Path Loss Results, page 10-17](#)).

- The Channel Loading report lets you see how busy the environment is before you deploy new sets of access points (see [Viewing Current Channel Load Results, page 10-19](#)).
- To detect rogue APs, you should enable both [serving channel](#) (the channel on which the AP is transmitting) and [non-serving channel](#) scanning (the channels on which the AP is *not* transmitting). If only serving channel scanning is enabled, then only the APs configured on the same channel as the rogue will actually report the rogue. By monitoring non-serving channels as well, Radio Manager can detect rogue APs that might not have been discovered had it monitored only the channel on which the AP is transmitting.
- By default, newly managed devices are automatically added to Radio Monitoring's Selected Devices list (see [Starting Radio Monitoring, page 12-4](#)). To manually add new devices to this list, select **Radio Mgr > Radio Monitoring > Select Options** and *deselect* the **Add Newly Managed AP to Selected AP List** check box. While that check box is *not* checked, newly managed devices are *not* automatically added to the Selected Devices list and you will have to manually select each AP using **Radio Mgr > Radio Monitoring > Select AP**.



Note Radio Monitoring will be turned on for newly-managed devices only if Radio Monitoring has been enabled (see [Starting Radio Monitoring, page 12-4](#)).

Related Topics

- [Understanding Radio Monitoring, page 12-2](#)
- [Detecting Rogue APs, page 14-12](#)

Starting Radio Monitoring



Note Your login determines whether you can use this procedure.

Before You Begin

Satisfy the Radio Monitoring prerequisites (see [Guidelines for Running Radio Monitoring, page 12-3](#)).

Procedure

- Step 1** Select **Radio Mgr > Radio Monitoring**. The Radio Monitoring Options window appears.
- Step 2** Complete the following:

Field	Description
Enable/Disable	Click Enable to re-enable Radio Monitoring. Note Radio Monitoring is your primary means of detecting rogue APs and is therefore enabled by default. <i>If you disable Radio Monitoring</i> , you will not have access to many features, including rogue AP detection, self-healing networks, auto re-site surveys, and certain Radio Manager reports.

Field	Description
Serving Channel Monitoring	Select one or both check boxes to collect measurements on the channel the devices are configured to: • APs to perform monitoring measurements on the Cisco IOS APs on the serving channel (the channel on which the AP is transmitting). • Clients to perform monitoring measurements on CCXV2-compliant clients on the serving channel.
Non-Serving Channel Monitoring	Select one or both check boxes to measure other channels in the band: • APs to perform monitoring measurements on the Cisco IOS APs on the non-serving channels (the channels on which the AP is <i>not</i> transmitting). • Clients to perform monitoring measurements on CCXV2-compliant clients on the non-serving channels. Note By monitoring non-serving channels as well as serving channels, Radio Manager can detect rogue APs that might not have been discovered had it monitored only the channel on which the AP is transmitting.
Add Newly Managed AP to Selected AP List	Select to add future newly-managed APs to the Selected Devices list in Step 3. Note If you deselect this check box, newly managed devices will <i>not</i> be automatically added to the Selected Devices list. You will have to <i>manually</i> move newly managed devices from the Available Devices list to the Selected Devices list. Note This check box affects devices that are managed <i>only after this setting has been saved</i>. Note Even if this check box is selected and the devices are appearing in the Selected Devices list, Radio Monitoring is enabled for those devices <i>only if the Enable check box has also been previously selected and saved</i>.
Enable History Data Collection	Select to collect and store history data, which is received every 90 seconds. Note If you do not enable this option, when you select Reports > Radio Manager > Path Loss Historical Report or Reports > Radio Manager > Channel Loading Historical Report, you get a message saying historical data collection has been disabled. You need to select this option before choosing one of these reports.

Step 3 From the menu in the left pane, click **Select AP**. All managed devices are listed in the Device selector in the middle pane.

Step 4 Select the devices you want to monitor (see [Using the Device Selector, page 1-12](#)).



Note If the **Add Newly Managed AP to Selected AP List** check box (see [Step 2](#)) is *not* checked, newly managed devices are *not* automatically added to the Selected Devices list.

- Step 5** From the menu in the left pane, click **Filter By PHY** to select the type of 802.11 radio that you want to monitor.



Note Only radios of the selected types are monitored. If a selected AP has no interfaces of the desired radio types, this is noted in the job run log.

- Step 6** To save your settings, click **Finish** from the menu in the left pane. The Finish dialog box appears.

- Step 7** Click **Save** to save your Radio Monitoring options.

Related Topics

- [Viewing Current Path Loss Results, page 10-17](#)
- [Viewing Current Channel Load Results, page 10-19](#)
- [Displaying Radio Manager Reports, page 12-25](#)
- [Understanding Radio Monitoring, page 12-2](#)

Evaluating AP Radio Performance

The following sections will help you understand how to use the Radio Manager Auto Re-Site Survey feature to evaluate AP radio performance:

- [Understanding Auto Re-Site Survey, page 12-6](#)
- [Guidelines for Running Auto Re-Site Surveys, page 12-7](#)
- [Establishing Baseline Data, page 12-8](#)
- [Monitoring AP Radio Performance, page 12-10](#)

Understanding Auto Re-Site Survey

Auto Re-Site Survey extends the Radio Manager Assisted Site Survey Wizard functionality. It periodically evaluates the current AP radio performance on a per-floor basis against baselined performance data that you specify (see [Guidelines for Running Auto Re-Site Surveys, page 12-7](#)) and alerts the user when the performance falls below a preset threshold.

How It Works

The Auto Re-Site Survey option uses data collected from previous RM Assisted Configuration jobs to compare the current performance of the selected APs against the performance data collected the last time radio parameter generation was generated for the specified APs and applied to the specific floor. If the APs' radio performance has decreased by 20% (a user-configurable setting), a fault is generated and you are asked if you want to generate new radio parameters. The new radio parameters are compared against the existing data, and if the newly generated radio parameter yield better results, you can apply the new radio parameters to the selected APs.

Data Produced

Auto Re-Site Survey generates a fault if the radio performance of the specified floor decreases by the specified percentage. It also allows you to generate new radio parameters and apply those parameters to the APs of the specified floor. (See [Establishing Baseline Data, page 12-8](#).)

Guidelines for Running Auto Re-Site Surveys

Prerequisites

Before you run Auto Re-Site Survey, you must:

1. Configure your network for radio management (see [Getting Started with Radio Manager, page 12-1](#)).



Note If Radio Management has been disabled, *none of the Radio Manager features will be displayed* (see [Enabling and Disabling Radio Management Features, page 11-4](#)).

2. Define the location elements (buildings and floors) and place the APs on the floor images. This step is optional, but will help you get the best results from the Location Manager displays. For more information, see:
 - [Entering Building Information, page 13-4](#)
 - [Adding Floors to Location Manager, page 13-9](#)
 - [Adding Devices to Floors, page 13-14](#)
3. Perform an AP Radio Scan on all APs on the specified floor (see [Using AP Radio Scans to Collect RM Data, page 13-43](#)).
4. Be sure that Radio Monitoring is enabled on all APs on the specified floor. Radio Monitoring is enabled by default; if it has been disabled, you must re-enable it (see [Using Radio Monitoring to Collect RM Data, page 12-1](#)).

Tips

- You cannot modify the “total throughput” and “coverage details” values after the WLSE has produced the survey results of an Automated Re-site Survey; these values are computed based upon current Radio Management data values.

You can, however, set a percentage value before you save the Auto Re-Site Survey settings. The percentage you set for a floor or building will be monitored with respect to the base for throughput and coverage. For example, if you set the percentage to 15%, WLSE issues a fault whenever the throughput or coverage values have more than a 15% change in the value (up or down) you previously set.

If you would like to change those values, perhaps to increase performance, use RM Assisted Configuration and Client Walkabout to fine-tune the network configuration.

Related Topics

- [Understanding Auto Re-Site Survey, page 12-6](#)

Establishing Baseline Data

The Auto Re-Site Survey feature compares the current performance of the selected APs against baseline performance data for a floor. You can also use Auto Re-Site Survey to establish this baseline data.



Note You should establish a set of baseline data only after you have determined that your network is stable and the parameter settings are optimal.

Typical Scenarios and FAQs

- I want to save the current performance data as the base data for future comparisons.



Note Your login determines whether you can use this option.

Before You Begin

Satisfy the Auto Re-Site Survey prerequisites (see [Guidelines for Running Auto Re-Site Surveys, page 12-7](#)).

Procedure

- Step 1** Select **Radio Mgr > Auto Re-Site Survey**. The Review Current screen displays the building, floor, and frequency band of the APs on the specified floor that are already enabled for Auto Re-Site Survey.
- Step 2** From the menu in the left pane, click **Select Floor**, then select a building from the Floors Selector list. The floors for the selected building appear in the Available Floors list.
- Step 3** Click on a floor, and click the right arrows (>>) to add it to the Selected Floors list.
- Step 4** From the menu in the left pane, click **Set Base Values**. The default is to calculate the performance of all floors. You can select individual floors from the Selected Floors pull-down menu and set its baseline data.
- Step 5** To set the baseline values for *all floors*, click **Compute and Apply**. The current performance data for each floor (specified in Step 3) is calculated and becomes the baseline performance data for future comparisons.
- Step 6** To set the baseline values *for individual floors*:
 - a. Select a floor from the Selected Floors dropdown list. The current values for that floor are displayed.
 - b. For one or both radio types, select:
 - **Re-evaluate** to evaluate the current performance of the selected floor.
 - **Current > Base** to make the current data the base for future comparisons.

Now that you have selected your Auto Re-Site Survey options, you need to save your settings.

Step 7 Click **Finish**. The Finish screen displays the current fault settings:

Field	Description
Enable	Select to enable Auto Re-Site Survey. Note On floors for which Auto ReSite Survey is enabled, both Serving and Non-Serving Channel Radio Monitoring must be enabled for all APs (see Using Radio Monitoring to Collect RM Data, page 12-1).
Settings	From the dropdown lists, select the severity level and percentage values. The severity level will be assigned to the fault when the radio performance of the AP decreases by the specified percentage.

Step 8 Click **Save** to save your settings.

Step 9 To view the log generated by the Auto Re-Site Survey process:

- a. Click **Review Current** from the menu in the left pane.
- b. Click **ARSS Run Log** (located below the list of buildings, floors, and frequencies). The ARSS Run Log table appears in a separate browser window. This table contains the following information for each run:

Field	Description
Select Run	Select this button to see the details for that run. The details for the selected job run appear below the list of runs for that job.
Start Time	The time the job started.
End Time	The time the job ended.

- c. The Auto Re-Site Survey run log for the selected run appears below this table. To view the details for a different run, select another run from the table and click **ARSS Run Log**.
- d. To be certain that you are looking at the latest information, click the **Refresh** button to refresh the job list.

Step 10 Every hour, the collected baseline data is compared against the current performance. If there is a 20% (default value) degradation in performance, a fault is generated.

In the Faults Detail Conditions table for an Auto Re-Site Survey fault, the presence of an icon (a note pad with glasses) between the Description and Timestamp columns in the Fault Detail Conditions table indicates that there is additional building and floor information for this fault. Select the icon to view these details (see [Monitoring AP Radio Performance, page 12-10](#)).

Related Topics

- [Guidelines for Running Auto Re-Site Surveys, page 12-7](#)
- [Device Fault Details, page 3-7](#)
- [Displaying Radio Manager Reports, page 12-25](#)

Monitoring AP Radio Performance

Use **Faults > Display Faults > Fault Details** to view the fault that is generated when any AP radio performance degradations are detected.

Typical Scenarios and FAQs

- I want to monitor the performance of an AP radio.
- I have just been notified of a decrease in the radio performance of an AP and I want to view the total throughput and coverage details.
- I have just been notified of a decrease in the radio performance of an AP and I have determined it is no longer a problem. I want to clear the fault.



Note

Your login determines whether you can use this option.

Before You Begin

Establish baseline performance data for each floor (see [Establishing Baseline Data, page 12-8](#)).

Procedure

- Step 1** Select **Faults > Display Faults**. The Faults Summary screen appears.
- Step 2** Select the filtering criteria to display any faults related to AP radio performance degradation.
- Step 3** To display more information about a fault, click the Description or Timestamp fields in the Fault Summary table for that fault.

The Fault Details screen displays details about the device, its current fault conditions, and a fault history (see [Viewing Fault Details, page 3-7](#)).

- Step 4** The presence of an icon (a note pad with glasses) between the Description and Timestamp columns in the Fault Detail Conditions table indicates that there is additional information about an AP radio performance degradation fault.

If you select this icon, a new window displays the following information:

Table 12-1 **Auto Re-Site Survey Fault Details**

Column	Description
Faults Details (first row)	See Device Fault Details, page 3-7
Building	All buildings that have performance degradations. Note Performance degradations are defined as a 20% difference between the base and current performance values.
Floor	All floors that have performance degradations.
Auto Re-Site Survey Details	A note pad with glasses icon. Click this icon to display the Auto Re-Site Survey Details window.

The Auto Re-Site Survey Details window displays the following information for the selected floor:

Table 12-2 **Auto Re-Site Survey Details Window**

Column	Description
Faults Details (first row)	See Device Fault Details, page 3-7
PHY Type	The type of 802.11 radio (11a or 11b/11g).
Timestamp	Indicates the time, based on the client browser, that the performance readings were collected for that band on that floor.
Dataset	CURRENT or BASELINE. The BASELINE dataset contains the initial readings for a floor; the CURRENT dataset contains the current values. A fault is issued when there is a 20% difference between the current and baseline values.
Throughput	Data transfer rate.
Coverage Details	A list of the coverage details by power step.
RM Assisted Configuration	Click RM Assisted Configuration to run the RM Assisted Configuration feature.

Step 5 To clear a radio performance fault, see [Clearing Summary Table Faults, page 3-6](#).

Healing Your Network

When the Radio Manager detects the loss or recovery of an AP radio, it can attempt to compensate for that change by adjusting the power levels of the neighboring APs. The following topics describe how and where to use the Radio Manager Self Healing feature:

- [Understanding Self Healing, page 12-11](#)
- [Guidelines for Healing Your Network, page 12-14](#)
- [Running Self Healing, page 12-15](#)
- [Managing Self Healing Faults, page 12-17](#)

Understanding Self Healing

How It Works

Self Healing runs on the WLSE and uses SNMP to adjust neighboring APs in response to the loss or recovery of a radio. Self Healing performs two functions:

- Monitoring:

Self Healing monitoring uses the path loss data collected from AP Radio Scan and Radio Monitoring and WDS registration information to determine a set of radio links for monitoring purposes. It uses this data to periodically check for any new radios or the loss of a radio.

The loss of a radio can be due to:

- Radio transmission failure—Every hour Self Healing polls the beacon information obtained using WLCCP via the WDS(s), and triggers an event when a radio has failed to transmit for 30 minutes or more.
- WDS deregistration—Self Healing immediately triggers an event when an AP powers down (if the radio was not administratively shut down) or loses connectivity to the WDS.
- Radar avoidance— When radar is detected on the current channel and the radio is in a DFS domain, Self Healing immediately triggers an event and changes the channel on that radio.



Note If an asynchronous event (radar avoidance or WDS deregistration) occurs between the hourly monitoring runs, the output of the event is added to the end of the log of the last polled run.

- Compensation:

Using the information previously gathered from AP Radio Scans and Radio Monitoring, Self Healing adjusts the transmit power levels of neighboring APs (which might or might not be on the same floor as the failed AP) to cover the potential areas of lost coverage, then generates a self healing fault.



Note Self Healing modifies *the power setting only*, not the channel frequency or beacon interval, of the neighboring APs.

Self healing faults have three states:

- Detection—Self Healing has determined that the network requires healing.
- Compensation determination—Self Healing is running Assisted Configuration (RPG—the radio parameter generation process).
- Reason—The status of the Self Healing run:
 - Error: Compensation calculation did not complete due to unrecoverable errors.
 - Incomplete: Compensation finished with errors.
 - Timeout: Compensation did not complete due to time-out (30 minutes).
 - CompensatedDown: Appeared Up/Down: Compensated for by up or down radio(s).
 - CompensatedUp: Appeared Up/Down: Compensated for by up or down radio(s).

Self healing is *not triggered* under the following conditions:

- When you are adjusting your network and you administratively shut down an AP's radio. Because this is an administrator-controlled operation, WLSE does not perform self healing on the network. In this case, when the device is re-enabled, the APs will still retain its original settings.
- When you are adjusting the power settings or channel settings.
- If an AP has an enabled hot-standby AP. In the event of a failure and the hot-standby takes over, Self Healing will monitor the hot-standby AP.
- If the AP radio avoids radar by selecting a channel that is not in a DFS domain (see [Compensating for Radar](#), below).

WLSE assumes you are using it for your initial setup and site planning, and therefore Self Healing is merely a rerun of the initial calculations minus the downed radio. When WLSE finds that a failed radio is back up, it reruns the calculations, this time including the radio.

If you use WLSE initially, the calculations will yield the same or equivalent results. If you set your power settings manually, then after the radio is detected as down and then back up, the results of the calculations could differ from your manual settings.

For example, assume you have a network with four APs {A,B,C,D}.

- **When WLSE is used for initial setup:**

You use Assisted Site Survey to generate your power settings and apply the following power settings (respectively):

{5,10,20,5}

AP C goes down and Self Healing adjusts the power settings:

{5,20,down,20}

AP C comes back up and Self Healing adjusts the power settings:

{10,5,20,5}

In the final state, this is an equivalent coverage—perhaps not the exact settings, but equivalent.

- **When you set the power manually and do not use WLSE to calculate the initial coverage:**

You manually set the power setting to:

{10,10,10,10}

AP C goes down and Self Healing adjusts the power settings:

{5,20,down,20}

AP C comes back up and Self Healing adjusts the power settings:

{10,5,20,5}

Self Healing uses the WLSE recommended settings when the AP comes back up, not the manual settings. WLSE is not designed to save check point configurations as part of the management.

**Note**

All Self Healing power settings are temporary, so any reload of the APs will revert to the last saved configuration on the AP itself.

Specifying Backup WDSs For Self Healing

The WDS provides WLSE with the data it needs to determine if a radio is up. If all the WDS devices configured for each AP on a floor are down (non-operational), Self Healing might try to heal those APs due to the missing data. Therefore, every AP on a floor configured with Self Healing should be registered with WDSs that have at least one standby.

**Note**

A fault is triggered when Radio Monitoring is not enabled for a radio, when the WDS is not registered, or when the WDS has lost connectivity to the WLSE.

If you have self healing enabled, it is *highly recommended* that you specify one or more backup WDS devices:

- Any AP or WDS router can be used as a backup WDS.
- You can have more than one backup, and your backups can have backups.
- You can configure HRSP on a second WLSM, which will then function as a standby WDS for your primary WLSM-WDS device.

Compensating for Radar

An AP radio that is in a [DFS](#) (Dynamic Frequency Selection) domain will change channels when radar is detected on the current channel.

- If the AP radio changes from the current radar detected channel to another DFS channel, the radio must wait one minute before operating on the new channel (if the channel is clear of radar).

During a simulation, if the channel change occurs immediately (that is, there is no one minute delay), self healing is not triggered. This is expected behavior because there is no interruption.

- If the AP changes channels from a DFS channel that is detecting radar to a channel that is not in the DFS regulatory domain (a non-DFS channel), the one minute delay does not occur and the AP radio will change channels immediately.

This type of change does not cause any loss in coverage and therefore does not warrant self healing, but may leave the floor in a sub optimal state. In this case, Auto Resite Survey is designed to monitor the performance of a floor and should be used to detect any path loss.

Data Produced

When Self Healing detects a network failure, a series of faults are generated. (See [Managing Self Healing Faults](#), page 12-17.)

Related Topics

- [What is WDS and Why Do I Need It?](#), page 11-8

Guidelines for Healing Your Network

Prerequisites

Before you run Self Healing, you must:

1. Configure your network for radio management (see [Getting Started with Radio Manager](#), page 12-1).



Note

If Radio Management has been disabled, *none of the Radio Manager features will be displayed* (see [Enabling and Disabling Radio Management Features](#), page 11-4).



Note

Before you enable self healing, you must specify one or more backup AP-WDSs or a single standby WLSM-WDS (see [What is WDS and Why Do I Need It?](#), page 11-8).

2. Define the location elements (buildings and floors) and place the APs on the floor images. For more information, see:
 - [Entering Building Information](#), page 13-4
 - [Adding Floors to Location Manager](#), page 13-9
 - [Adding Devices to Floors](#), page 13-14
3. Perform an AP Radio Scan on all APs on the specified floor (see [Using AP Radio Scans to Collect RM Data](#), page 13-43).
4. Enable Radio Monitoring on *all APs* (for both serving and non-serving channels) on the specified floor. Radio Monitoring is enabled by default; if it has been disabled, you must re-enable it (see [Using Radio Monitoring to Collect RM Data](#), page 12-1).

5. Ensure that the WLSE has properly authenticated and has connectivity to the WDSs for all APs on the floor to be monitored. To verify this, you can run the RM Capability Verifier in the Location Manager (see [Verifying Radio Management Capability, page 13-27](#)).

Tips

- To enable Self Healing monitoring:
 1. Select the buildings and floors for which self healing will be enabled and assign the self healing settings (see [Running Self Healing, page 12-15](#)).
 2. View the faults that are generated when self healing is activated (see [Managing Self Healing Faults, page 12-17](#)).



Note

Self Healing faults are *always enabled*. When you set up Self Healing for a floor, you will always receive fault notifications when a network disruption occurs.



Note

The fault RF Port AdminStatus is enabled by default and must remain enabled with a default polling time of 5 minutes (see [Setting RF Port AdminStatus Threshold, page 3-35](#)). Self healing ignores any radio set as administratively down, but this can only be detected if fault polling is enabled.

3. After the self healing process is complete, locate the failed interfaces and the AP interfaces that were modified to replace them (see [Running Self Healing, page 12-15](#)).
- Self Healing modifies the power setting only, not the channel frequency or beacon interval, of the neighboring APs. Because Self Healing can change APs on different floors from the failed AP but must do so without changing the channel frequency, the network might be operating in a sub-optimal manner. To resolve this problem, enable Auto Re-Site Survey (see [Evaluating AP Radio Performance, page 12-6](#)) and/or Self-Healing on the surrounding floors.
 - If an AP has a hot-standby enabled, it is *not* monitored by Self Healing. In the event of a failure and the hot-standby takes over, Self Healing will monitor the hot-standby AP.
 - If you have self healing enabled, you must specify one or more backup WDS devices.

Related Topics

- [Understanding Self Healing, page 12-11](#)

Running Self Healing

Typical Scenarios and FAQs

- How do I specify which floors will run self healing?
- I want to set the severity of a self healing notification.
- How do I specify whether the changes to neighboring APs are to be applied automatically or manually?
- I want to view the current self healing faults for a [P1...P5] setting.

- How can I monitor the progress of a self healing job?

**Note**

Your login determines whether you can use this option.

Before You Begin

Satisfy the Self Healing prerequisites (see [Guidelines for Healing Your Network, page 12-14](#)).

Procedure

- Step 1** Select **Radio Mgr > Self Healing**. The Review Current form appears displaying the floors currently selected for Self Healing.
- Step 2** From the menu in the left pane, click **Select Floors** and select a building from the Buildings list. The floors for the selected building appear in the Available Floors list.
- Step 3** Select a floor and click the right arrows (>>) to add it to the Selected Floors list.
- Now that you have selected your self healing options, you need to save your settings.
- Step 4** From the menu in the left pane, click **Finish**.
- Step 5** Select the severity level to assign to the fault when a self healing fault is triggered.
- Step 6** You can choose to automatically apply changes to neighboring APs:
- When automatic self healing is enabled, neighboring APs are adjusted to accommodate the loss of coverage.
 - When automatic self healing is disabled, the changes to neighboring APs must be applied from the Faults Display Details page for each fault occurrence.
- Step 7** Click **Save**. A new window displays the buildings and floors on which Self Healing is enabled. Close this window to view the **Review Current** screen.
- Step 8** To view the log generated by the self healing process, select the run and click **Self Healing Run Log** (located below the list of buildings and floors).

The Self Healing Run Log table appears in a separate browser window. This table contains the following information for each run:

Field	Description
Select Run	Click this button to see the details for that run. The details for the selected job run appear below the list of runs for that job.
Start Time	The time the job started.
End Time	The time the job ended.

The Self Healing run log for the selected run appears below this table. To view the details for a different run, select another run from the table and click **Self Healing Run Log**.

Self Healing creates a log file for each run. To be certain you are looking at the latest information, click the **Refresh** button to refresh the job list.

**Note**

If an asynchronous event (radar avoidance or WDS deregistration) occurs between the hourly monitoring runs, the output of the event is added to the end of the log of the last polled run.

- Step 9** To view more details about the fault that is generated while Self Healing is in progress, see [Managing Self Healing Faults, page 12-17](#).
- Step 10** Because Self Healing can choose an AP on a different floor from the failed AP to cover any holes in coverage, you should enable Auto Re-Site Survey to monitor performance of your APs (see [Evaluating AP Radio Performance, page 12-6](#)).
-

Related Topic

- [Understanding Self Healing, page 12-11](#)
- [Managing Self Healing Faults, page 12-17](#)

Managing Self Healing Faults

To manage the self healing faults in your network, use **Faults > Display Faults**. Or, to see only those faults pertaining to Self Healing, select **Radio Mgr > Self Healing**.

Typical Scenarios and FAQs

- Why was self healing initiated?
- I have just been notified that self healing has been initiated. How do I track its progress?
- I have just been notified that self healing has been initiated. How do I display a list of the failed interfaces and the neighboring AP interfaces that were modified to replace them?
- How do I review the history of self healing actions in my network?
- The self healing process on my network is complete. How can I view the new power settings? How do I clear the faults associated with this process?

**Note**

Your login determines whether you can use this option.

Before You Begin

- Satisfy the prerequisites for running self healing (see [Guidelines for Healing Your Network, page 12-14](#)).
- Select the buildings and floors for which self healing will be enabled and assign the self healing settings (see [Running Self Healing, page 12-15](#)).

Procedure

-
- Step 1** To display the Self Healing faults, you can:
- Display the general Fault Summary screen:
 - Select **Faults > Display Faults**. The Faults Summary screen appears.
 - Select the filtering criteria to display any self healing faults.
 - Display only active Self Healing faults:
 - Select **Radio Mgr > Self Healing**. The Review Current screen appears.
 - Select **View Active Faults**. The active Self Healing faults are displayed in a new window.
- Step 2** To display the Fault Details window, select the Description or Timestamp field for a fault.

- Step 3** To view the results of Self Healing compensation calculations, click the icon (a note pad with glasses) between the Description and Timestamp columns in the Fault Detail Conditions table. A new window displays the following information:

Table 12-3 Self Healing Compensation Results

Column	Description
Faults Details (first row)	See Device Fault Details, page 3-7
Failed Interface	MAC address of the failed radio.
Modified Interface/ Message	The IP address, MAC address, and radio interface type of the AP that has been modified to compensate for the failed radio.
Old OFDM(11g) Power	Previous OFDM (Orthogonal Frequency Division Multiplexing) setting on the modified AP (11g radios only).
New OFDM(11g) Power	New OFDM setting on the modified AP (11g radios only).
Old CCK/Tx Power	Previous setting on the modified AP. Contains: - For 11b and 11g radios: CCK (Complementary Code Keying) value - For 11a radios: Tx value
New CCK/Tx Power	New setting on the modified AP. Contains: - For 11b and 11g radios: CCK (Complementary Code Keying) value - For 11a radios: Tx value



Note

If an asynchronous event (radar avoidance or WDS deregistration) occurs between the monitoring runs, the output of the event is added to the end of the log of the last polled run.

- Step 4** When automatic self healing is disabled, the changes to neighboring APs must be applied from this page for each fault occurrence. To apply the new settings, click **Apply Changes Now**.
- Step 5** To see the changes immediately and graphically in Location Manager, run an inventory for the affected APs. This will show the new coverage details for the adjusted APs as well as the previous coverage for the downed AP (see [Managing Your WLAN Radio Environment by Sites, page 13-1](#)).
- Step 6** To determine why Self Healing was run, check the fault history log (see [Running Self Healing, page 12-15](#)).
- Step 7** To clear a self healing fault, see [Clearing Summary Table Faults, page 3-6](#).

Related Topics

- [Understanding Self Healing, page 12-11](#)
- [Displaying Radio Manager Reports, page 12-25](#)

Using Frame Monitoring

Frame Monitoring allows you to perform network troubleshooting and intrusion detection and send this information to a third-party server for further analysis. The following sections will help you understand how to use Frame Monitoring:

- [Understanding Frame Monitoring, page 12-19](#)
- [Guidelines for Using Frame Monitoring, page 12-19](#)
- [Configuring Frame Monitoring, page 12-20](#)
- [Displaying Frame Monitoring APs, page 12-23](#)
- [Disabling Frame Monitoring on Selected APs, page 12-24](#)

Understanding Frame Monitoring

How It Works

You can use the WLSE Frame Monitoring feature:

- To configure Frame Monitoring. Upon receiving a request to enable Frame Monitoring, an AP in scanning-only mode will:
 - a. Abort all its current operations and schedule Frame Monitoring jobs as directed by the given parameters.
 - b. Start Frame Monitoring on the channel that it was programmed to use on its radios and send the frames to the external UDP end point. If the default parameters were used (the configuration was done using the CLI or WLSE user interface), the AP will continuously monitor the channels it was currently scanning.
- To review Frame Monitoring results. The Review Current screen displays information about the APs that are performing Frame Monitoring tasks (see [Displaying Frame Monitoring APs, page 12-23](#)).

Guidelines for Using Frame Monitoring

Prerequisites

To use Frame Monitoring, you must:

1. Set up a third-party server to analyze the data collected by Frame Monitoring.
2. Configure your network for radio management (see [Getting Started with Radio Manager, page 12-1](#)).

**Note**

If Radio Management has been disabled, *none of the Radio Manager features will be displayed* (see [Enabling and Disabling Radio Management Features, page 11-4](#)).

3. Verify that the access points you have selected to perform Frame Monitoring are scanning-only APs (select **Reports > Device Center > Scanning AP**). If the APs are not in this list, re-run the inventory process.

**Note**

Only scanning-only APs can perform Frame Monitoring.

4. Enable monitor mode on selected APs (see [Configuring Frame Monitoring, page 12-20](#)).

Tips

- To remove APs that are already configured to run Frame Monitoring, see [Disabling Frame Monitoring on Selected APs, page 12-24](#).
- When an AP that is running in monitor mode receives a message to disable monitor mode, it aborts its Frame Monitoring tasks and resumes its previous scanning job.
- The scan duration time is set to 100ms and cannot be changed using the WLSE user interface.
- For maximum flexibility, use the XML APIs to configure Frame Monitoring. The WLSE user interface can always be used to check the status of Frame Monitoring.



Note If you are using a third-party system to configure Frame Monitoring via the XML APIs, *do not* use the WLSE interface to perform any configuration tasks.

- Only access points in scanning-only mode can be configured to monitor mode.
- After monitor mode has been enabled on an access point, that access point is considered to be a dedicated frame monitor until you explicitly disable monitor mode.
- If monitor mode is enabled on an AP that is running Radio Monitoring, Radio Monitoring is automatically disabled.



Note Any AP you select will perform Frame Monitoring indefinitely until you explicitly disable monitor mode on that AP.

- Although on dual-mode APs you can use the CLI to enable monitor mode on just one interface, this approach is *not officially supported* because the stress on the AP will result in dropped client associations.

Configuring Frame Monitoring

You can use the WLSE user interface to enable and disable Frame Monitoring operations and to assign Frame Monitoring configuration settings.

**Note**

Using the WLSE user interface, the Frame Monitoring scanning pattern is fixed and cannot be changed. For maximum flexibility, consider using the XML APIs to configure Frame Monitoring instead, and using the WLSE interface for ongoing monitoring tasks.

**Caution**

If you are using a third-party system to configure Frame Monitoring via the XML APIs, *do not* use the WLSE interface to perform any configuration tasks.

Typical Scenarios and FAQs

- How do I set up selected access points to run Frame Monitoring?

**Note**

Your login determines whether you can use this option.

Before You Begin

Satisfy the Frame Monitoring prerequisites (see [Guidelines for Using Frame Monitoring, page 12-19](#)).

Procedure

- Step 1** Select **Radio Mgr > Frame Monitoring**. The Frame Monitoring screen appears.
- Step 2** The Review Current screen displays the APs that are currently performing Frame Monitoring tasks (see [Displaying Frame Monitoring APs, page 12-23](#)).
- Step 3** To assign the Frame Monitoring settings, select **Configuration** from the menu in the left pane.
- Step 4** Complete the following:

Field	Description
Enable/Disable	Click to enable or disable Frame Monitoring: • Enable: Select this option to enable monitor mode and enter the Frame Monitoring configuration settings. • Disable: Select this option to <i>cancel</i> Frame Monitoring. – For scanning only APs, selecting Disable will cancel monitor mode operations on the selected APs. – For normal APs, selecting Disable will remove the selected APs from the Review Current screen only if the AP was a scanning-only AP and was previously performing Frame Monitoring operations. Note Verify the values in the other fields to make sure you are disabling monitor mode for the correct end point.
End Point IP Address	The IP address of the external third party end point to which the frames are to be sent. Note This field is restricted to numeric IPV4 addresses. Note The WLSE does not perform any validation on this IP address. You are responsible for ensuring that this field contains the correct end point IP address.
End Point Port Number	The UDP port number of the external third party end point to which the frames are to be sent. Default = 1024.
Frame Truncation	Frame truncation length (in bytes). Default = 128 bytes.

- Step 5** Choose **Select Scanning AP** from the menu in the left pane.
- Step 6** Select the scanning-only APs on which you want to enable or disable monitor mode (see [Using the Device Selector, page 1-12](#)).
- For *scanning only* APs, selecting Disable will cancel Frame Monitoring operations on the selected APs.

- For *normal* APs, selecting **Disable** will remove the selected APs from the Review Current screen only if the AP was a scanning-only AP and was previously performing Frame Monitoring operations.

Step 7 Choose **Select Radio Type** from the menu in the left pane.

Step 8 Select the types of 802.11 radios that will run Frame Monitoring (default = all radio types).

**Note**

Only radios of the selected types will perform Frame Monitoring. If a selected AP has no interfaces of the desired radio types, this is noted in the Job Run Log.

**Note**

All radio interfaces on an access point must be in scanning-only mode. The WLSE cannot enable monitor mode on an AP that has an interface that is not in scanning-only mode (see [Guidelines for Using Frame Monitoring, page 12-19](#)).

Step 9 To save your settings, select **Finish** from the menu in the left pane. The Finish dialog appears.

Step 10 Click **Save** to save the Frame Monitoring configuration settings.

**Note**

If a warning message appears saying that WLSE server is ahead of or behind your local time, see [Understanding Time Discrepancy Problems in Job Scheduling, page 1-11](#).

There are three possible results:

- An error message is displayed if there is no configuration (IP address and port number), no selected AP, or the selected AP is not a scanning-only AP. No further action can be taken until the problem is resolved.
- A warning message is displayed if monitor mode is disabled or no truncation value has been entered. Upon confirmation, the save process will continue.
- A summary displays the settings that have been saved. You can refresh the Review Current page to see the saved settings.

Related Topics

- [Displaying Frame Monitoring APs, page 12-23](#)
- [Disabling Frame Monitoring on Selected APs, page 12-24](#)
- [Guidelines for Using Frame Monitoring, page 12-19](#)

Displaying Frame Monitoring APs

You can use **Radio Mgr > Frame Monitoring** to display the scanning-only APs that are performing frame monitoring.

Typical Scenarios and FAQs

- How do I view the access points that are running Frame Monitoring?

**Note**

Your login determines whether you can use this option.

Before You Begin

Satisfy the Frame Monitoring prerequisites (see [Guidelines for Using Frame Monitoring, page 12-19](#)).

Procedure

- Step 1** Select **Radio Mgr > Frame Monitoring**. The Review Current screen displays the following information about the APs that are currently performing Frame Monitoring tasks:

Column	Description
AP Name	The IP address of the access point that is currently performing Frame Monitoring tasks.
Channel	The channel that is being monitored. The channels that are used depend on the radio type: • 11b/11g radios use channels 1 through 14. • 11a radios use channels 36, 40, 44, 48, 52, 60, 64, 149, 153, 157, and 161. Note Not all channels will be used for all regulatory domains.
PHY	The physical interface type (11a, 11b, or 11g) that is currently performing Frame Monitoring tasks.
End Point IP Address	The IP address of the external third party end point to which the frames are currently being sent.
End Point Port Number	The port number of the external third party end point to which the frames are currently being sent.

Column	Description
Frame Truncation	The number of bytes you want to see: • Default = 128 bytes • Minimum = 24 bytes of MAC header • Maximum = MTU on the radio
Status	The Frame Monitoring configuration setting status. Possible values: • pending—The initial status when the configuration setting is being saved in the database. • running—The WLSE is sending the configuration to the WDS. • success—The WDS has received the configuration and set up the scanning AP.

Related Topics

- [Configuring Frame Monitoring, page 12-20](#)
- [Disabling Frame Monitoring on Selected APs, page 12-24](#)
- [Guidelines for Using Frame Monitoring, page 12-19](#)

Disabling Frame Monitoring on Selected APs

You can use **Radio Mgr > Frame Monitoring** to remove APs from the list of APs that are configured to run Frame Monitoring.

Typical Scenarios and FAQs

- How do I disable Frame Monitoring on an access point?



Note

Your login determines whether you can use this option.

Before You Begin

- Satisfy the Frame Monitoring prerequisites (see [Guidelines for Using Frame Monitoring, page 12-19](#)).
- There must be at least one AP running Frame Monitoring.

Procedure

- Step 1** Select **Radio Mgr > Frame Monitoring**. The Review Current screen displays the APs that are currently performing Frame Monitoring tasks.
- Step 2** Select **Configuration** from the menu, then click **Disable** (you want to *disable* Frame Monitoring on selected APs).
- Step 3** Choose **Select Scanning AP** from the menu, then add the APs you want to remove to the Selected Devices list.

Step 4 Choose **Select Radio Type** and select the radio type (or select both 11a and 11b/11g if you are not sure).

Step 5 Select **Finish** to save the setting.

The Frame Monitoring operation on the selected APs will be canceled and they will be removed from the Currently Monitoring list.

Related Topics

- [Guidelines for Using Frame Monitoring, page 12-19](#)
- [Configuring Frame Monitoring, page 12-20](#)
- [Displaying Frame Monitoring APs, page 12-23](#)

Displaying Radio Manager Reports



Note

If Radio Management has been disabled, the **Reports > Radio Manager** subtab will *not* be displayed. To reenable Radio Management, see [Enabling and Disabling Radio Management Features, page 11-4](#).

The Radio Manager reports allow you to view radio management information. You can view, export, and email the following report types:

- Configured Radio Parameters Report
- Path Loss Between Managed APs Report
- Path Loss Historical Report
- Channel Loading Report
- Channel Loading Historical Report
- Radar Detection Report
- Radar Detection Historical Report

For more information about these reports, see [Displaying Radio Manager Reports, page 10-15](#).



Managing Your WLAN Radio Environment by Sites

Use the functions under the Sites tab to manage your WLAN network based on the physical location of your devices and your wireless environments.



Note

Before you can use the functions under the Sites tab, you must configure your network for radio management (see [Getting Started with Sites, page 13-2](#)).

- Location Manager—gives you a graphical view of the access points (APs) on each floor of your buildings, lets you view the relative location of unknown or rogue APs, and includes the Assisted Site Survey wizard. See [Using Location Manager, page 13-2](#).
- AP Radio Scan—detects all neighbor's APs and produces path loss data used for rogue location estimations, radio parameter generation, and coverage display data. See [Using AP Radio Scans to Collect RM Data, page 13-43](#).
- Client Walkabout—helps provide optimal coverage for the radio parameter generator by generating additional data. See [Using Client Walkabouts to Collect RM Data, page 13-54](#).
- Assisted Configuration—provides configurations for your APs based on measurement data collected from client walkabouts and AP radio scans. See [Generating Radio Parameters, page 13-66](#).
- Manage Data—allows you to delete previously collected radio location measurements, including links and path loss data. See [Managing RM Data, page 13-81](#).

Getting Started with Sites

Before you can use the functions provided by the Sites tab:

- Radio Management must be enabled.

If Radio Management has been disabled, *none of the Sites subtabs will be displayed* (see [Enabling and Disabling Radio Management Features, page 11-4](#)).

- You must set up your network to manage your radio environment.

If your network is not properly configured, *none of the Sites functions will work*. To configure your network, see [Configuring Your WLAN Radio Environment, page 11-1](#).

Using Location Manager

The Location Manager gives you a graphical view of the access points (APs) on each floor of your buildings, lets you view the relative location of unknown or rogue APs, and use the Assisted Site Survey wizard to determine optimal radio transmit power, channel selection, and beacon interval.

Before using Location Manager, you must enter information about site, building, and floor environments (see [Setting Up Location Manager, page 13-3](#))

The Location Manager supports up to 1,500 buildings per location with a maximum of 100 floors per building and a maximum of 100 APs per floor.

You can launch Location Manager in two ways:

- By clicking the Sites tab, then clicking **Location Manager**, and then **Launch**.
- By selecting **Faults > Display Faults** and clicking the link in the Address, Description, or Timestamp fields in the Fault Summary Table for an unknown access point. A new window displays the Rogue Access Point Details report. From the Rogue Access Point Details report, click on **Location Manager** to launch Location Manager.

Prerequisites for Using Location Manager

Before using Location Manager, you must have completed the following:

- Installed Java Runtime version 1.5. (Location Manager might work with Java Runtime versions 1.4.2_04 or higher, but if Location Manager does not launch correctly, it is recommended that you install Java Runtime version 1.5.) When you click on Location Manager, the Location Manager screen displays the version of Java Runtime version you have installed and displays a link to install the correct version if necessary.
- Discovered, inventoried, and managed all devices. See [Device Discovery and Management, page 4-1](#).
- Authenticated the devices with WDS. IOS Access Points or Wireless LAN Services Modules (WLSM) must be configured for Wireless Domain Service (WDS) and for LEAP authentication. For information on the minimum requirements for device setup, see the document *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine* on Cisco.com.

The following sections explain how to use Location Manager:

- [Setting Up Location Manager, page 13-3](#)
- [Using Location Manager Functions, page 13-16](#)

- [Understanding the Location Manager Window, page 13-36](#)

Setting Up Location Manager

To use all the features of Location Manager, you must enter information about your sites and buildings. When you launch Location Manager for the first time, use the Building Tool to enter campus/site, building, and floor information.

**Note**

The sites, buildings, and floors that you add appear alphabetically in the Location Manager navigation tree as well as the Physical Location folder under **Devices > Group Management**. You can modify the contents of the Physical Location folder using Location Manager only.

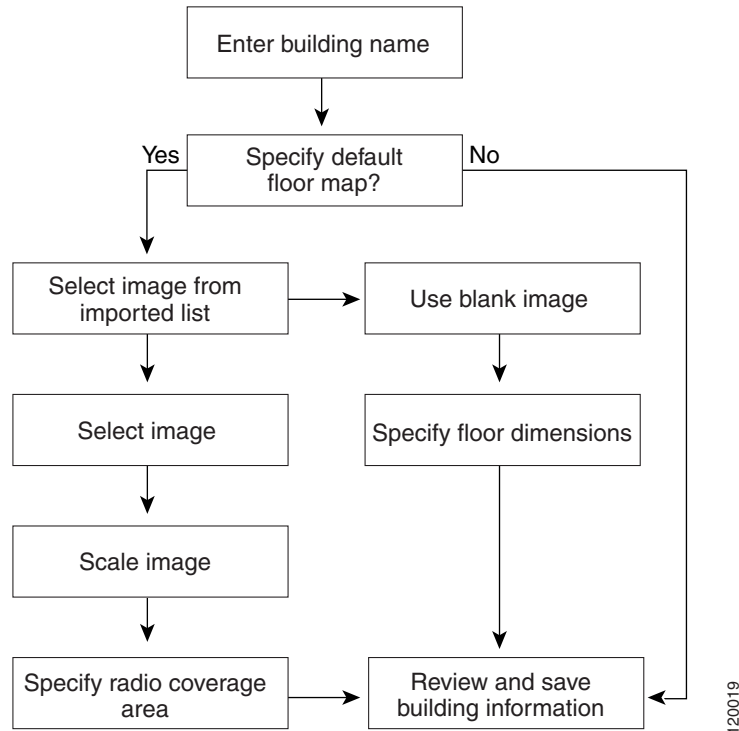
Procedure

- Step 1** If you have previously launched Location Manager and want to add site information, select **Edit > Add Site** or right-click on **All Locations** and select **Add Site**. The Site Tool appears.
- Step 2** Enter the name of the site and select the system settings:
- Check **Default to System Settings** to create a site with the default values. By default, the Service Type is *Data*. [Table 13-1](#) lists the default settings for the Service Type *Voice*.
 - Uncheck **Default to System Settings** to change the default values and enter the system settings for your site.

Table 13-1 *Default Values for Voice Service Type*

Device Type	Default RSSI Value	Default Voice Rate
802.11a	-72dBm	6 Mbps
802.11 b/g	-67 bBm	11 Mbps

- Step 3** If you unchecked **Default to System Settings**, select a Service Type from the pulldown menu and enter the values for your site.
- Step 4** If you select the Service Type *Voice* and do not use the default system settings, you must specify the following settings:
- RSSI value
The RSSI value can be any value from -78 dBm to -55 dBm. The value you select becomes the default value when you select **Voice Tx/Rx Coverage by Data Rate** from the View Mode pulldown menu in Location Manager.
 - Voice rates
- Step 5** Click **OK**.
- If this is the first time you've launched Location Manager, the Building Tool appears and walks you through the process shown in [Figure 13-1](#).

Figure 13-1 Building Tool Steps for Adding Building Information

Entering Building Information

Procedure

- Step 1** If you have previously created a site, you can right click on the site name and select **Add Building**. When you launch Location Manager for the first time, a form appears in which you can enter building and floor information as shown in the following steps.
- Step 2** Enter information in the Building Name, Contact (optional), and Address (optional) fields. The following table shows the character limits for each field on the Create Building Information form:

Field	Maximum Character Length
Building Name	64 characters
Contact	64 characters
Address	256 characters

- Step 3** Check **Default to Site Settings** to create a building with the same values as the site to which the building belongs. Uncheck **Default to System Settings** to change the values.
- Step 4** If you unchecked **Default to System Settings**, select a Service Type from the pulldown menu and enter the values for your building. By default, the Service Type is *Data*. [Table 13-1](#) lists the default settings for the Service Type *Voice*.

- Step 5** If you select the Service Type *Voice*, and do not use the default system settings, you must specify the following settings:
- RSSI value
- The RSSI value can be any value from -78 dBm to -55 dBm. The value you select becomes the default value when you select **Voice Tx/Rx Coverage by Data Rate** from the View Mode pulldown menu in Location Manager.
- Voice Rates
- [Table 13-1](#) lists the default settings for the Service Type *Voice*.
- Step 6** Click **Next**. The Default Floor Map form appears. See [Choosing a Default Floor Map, page 13-5](#).
-

Choosing a Default Floor Map

After you enter a building name, you need to decide if you want to use a default floor map that you can use for all floors in the building.

Procedure

- Step 1** Select a floor map setting:
- Click **Specify Default Floor Map** to specify a default map that all floors in the building can use. If the floors in the building have a similar floor plan, you can use the same floor map for all floors in the building which can save you time when entering floor information.
 - Click **No Default Floor Map** if you do not want to use a default map for all floors in the building.
- Step 2** Click **Next**.
- If you clicked **Specify Default Floor Map**, the Select Image Map Type form appears. See [Entering Default Floor Map Information, page 13-5](#).
- If you clicked **No Default Floor Map**, you need to review and save the information you entered. See [Saving Building Information, page 13-8](#).
-

Entering Default Floor Map Information

If you chose to specify a default floor map for all floors in the building, you need to enter information about the floor map image file.

Procedure

- Step 1** Select one of the following options:
- Click **Select an Imported Image** to chose an image (.gif, .jpg, .jpeg, or .png) that already exists.
 - Click **Use Blank Image** to chose a blank image that represents the floor area.
- Step 2** Click **Next**.
- If you specified **Select an Imported Image**, the Building Tool displays an image list. See [Selecting the Image Map, page 13-6](#).

If you specified **Use Blank Image**, enter the floor dimensions. See [Entering Floor Dimensions, page 13-6](#).

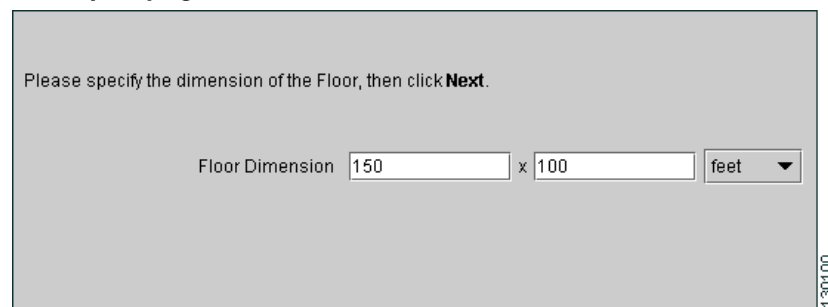
Entering Floor Dimensions

If you selected the blank image, the Building Tool displays a form to enter the floor dimensions.

Procedure

- Step 1** Enter a value in each Floor Dimension field. [Figure 13-2](#) illustrates how the values you enter correspond to the resulting floor image.

Figure 13-2 Specifying Floor Dimensions



- Step 2** From the pulldown menu, select feet or meters.

- Step 3** Click **Next**.

Now you need to review and save the building information you entered. See [Saving Building Information, page 13-8](#).

Selecting the Image Map

When you use the Building Tool and chose to select an image from an image list, the Building Tool displays a list of image files on the server.



Note The larger an image resolution is, the longer it takes to upload to the server and the more memory it uses. Therefore, we recommended that your image be less than 300KB and less than 1,000x1,000 pixels.

Procedure

- Step 1** The Select Image Map form lists the image files on the server. If your image file appears in the Select Image File window, skip to Step 4.
- Step 2** To add a new image file, click **Add to List**. The Upload File Selection window appears.
- Step 3** Browse to the location of your image file. Click on your image file, then click **Select**.
- If your file is a recommended size, your file is uploaded and added to the Select Image Map list. Go to Step 5.

If your image file contains more than the 1,000x1,000 pixels, a message appears stating that your image file appears to be larger than the recommended size and asks you if you want to abort importing.

- Click **Yes** to abort importing and select a new image. See Step 2.
- Click **No** to continue the import. A message appears asking if you would like Location Manager to resize your image. See Step 4.

Step 4 Chose whether to use the built-in image optimizer:

- Click **Yes** to have the image resized. A preview of the resized image is displayed. After viewing the preview of the resized image, click **OK**. A new image is created with the name `filename_sm.png`. Your original image file is not modified.
- Click **No** if you don't want to use the image optimizer. The import is canceled. You must use another program to reduce the size of your image before importing it.



Note If your image filename has any spaces, the spaces are replaced with underscores (_). For example, if your image filename is *my floor image.jpg*, it will become *my_floor_image.jpg* in Location Manager.

Step 5 Click on the image file, then click **Next**.

You now need to specify the scale of the image you selected. See [Specifying the Scale of the Image Map, page 13-7](#).

Specifying the Scale of the Image Map

The Building Tool displays the image file and asks you to enter information about the scale of the image.

Procedure

Step 1 Click and drag the red squares of the red scaler tool so that the line corresponds to an area in your building for which you know the exact distance in feet or meters.

Step 2 Enter the distance that corresponds to the scaler in the field provided.



Note The more accurate your measurement is, the more accurate Location Manager can determine the location of any interferers.

Step 3 Click **Next**.

You now need to specify the radio coverage area. See [Specifying Radio Coverage Area, page 13-7](#).

Specifying Radio Coverage Area

After you specify the scale of the floor map image, you need to enter information about what areas in the floor map image are included in the radio coverage area.

Procedure

- Step 1** Using the Coloring Tool to add areas or the Eraser Tool to remove areas, specify the area of the floor in which you want to optimize the radio configurations. During the Radio Parameter Generation calculation, Location Manager tries to optimize the radio settings within the area that is shaded.

There are several tools to help you shade the desired area:

- The first two icons let you add and remove areas by grid sections. Click on each section you want to add or remove.
- The second two icons let you add and remove larger sections. Hold down and drag your mouse to select areas you want to add or remove.

The colored icons let you change the color used in the image map.

- Step 2** Click **Next**.

You now need to review and save the information you entered. See [Saving Building Information, page 13-8](#).

Saving Building Information

The Review and Save form displays the information you entered in the Building Tool.

Procedure

- Step 1** If all the information displayed in the form is correct, click **Save**.
- Step 2** If you need to modify any information you previously entered, click **Previous** to return to the form you need to change.

After you click **Save**, you can use the Building Tool to create a new floor for the building you just created. See [Choosing the Next Step, page 13-8](#). By default, the new building is listed under Campus Site. All sites and buildings are listed alphabetically in the Location Manager window.

Related Topics

- [Choosing the Next Step, page 13-8](#)
- [Renaming Campus Sites, page 13-9](#)
- [Adding Floors to Location Manager, page 13-9](#)

Choosing the Next Step

After you save the building information, you can:

- Click **Close** to exit the Building Tool.
- Click **Add New Floor** to enter information about the floors in the building. See [Adding Floors to Location Manager, page 13-9](#).
- Click **Modify Existing Floor** to change a floor that was previously added. This option appears only if you have already added a floor to the building.

The buildings you added appear alphabetically under Campus Sites in the Location Manager navigation tree as well as the Physical Location folder under **Devices > Group Management**. You can modify the contents of the Physical Location folder using Location Manager only.

Related Topics

- [Adding Floors to Location Manager, page 13-9](#)

Renaming Campus Sites

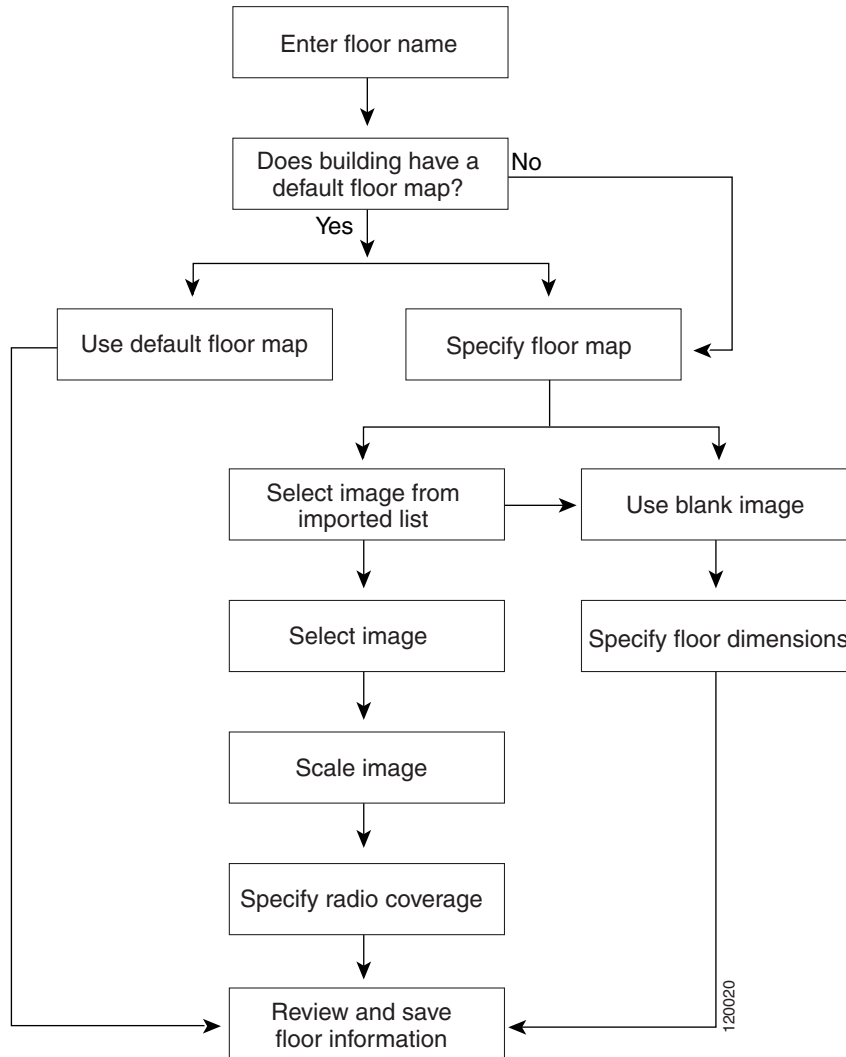
By default, when you create a new building, it is listed alphabetically under Campus Site. You can rename the Campus Site folder to any 64-character name you wish.

Procedure

-
Step 1	Right click on Campus Site, then click Edit Site .
Step 2	Enter the new name of the campus or site, then click OK . The new name appears in the Location Manager navigation tree.
-

Adding Floors to Location Manager

After you have added building information to Location Manager, you can add information about each of the floors. The Building Tool helps you enter floor information and walks you through the process shown in [Figure 13-3](#).

Figure 13-3 Building Tool Steps for Adding Floor Information**Note**

By default, floors are listed in alphabetical order. To change the order of the floors in a building, see [Reordering Floors, page 13-15](#)

Entering Floor Information**Procedure**

- Step 1** Right-click on a building and select **Add Floor**, or click on a building and select **Edit > Add Floor**. The Building Tool appears and displays the name of the building you selected in the Building Name field.
- Step 2** Enter a name in the Floor Name field. You can specify up to 64 characters in the Floor Name field.
- Step 3** Click **Next**.

You now need to enter floor map information. See [Entering Floor Map Information, page 13-11](#).

Entering Floor Map Information

The Building Tool displays information about whether the building you selected has a default floor previously assigned to it.

Procedure

Step 1 Select a floor map setting. If you previously specified a default floor map for the building, chose one of these options:

- Click **Use the Default Floor Map** to use the default map that was previously applied to the building.
- Click **Customize New Floor Map** to select a floor map, other than the default floor map assigned to the building, for this floor.

If you did not previously specify a default floor map for the building, chose one of these options described in [Selecting an Image Map Type, page 13-11](#).

Step 2 Click **Next**.

If you selected to use the default floor map, the Building Tool displays information about the default floor map you selected. Review the data and save it if correct. See [Saving Floor Information, page 13-14](#).

If you specified to use a new floor map, you need to enter information about the floor map image. See [Selecting an Image Map Type, page 13-11](#).

Selecting an Image Map Type

If you chose to use a new floor map, the Building Tool asks you to chose the type of image.

Procedure

Step 1 Select the type of floor map:

- Click **Select an Imported Image** to chose an image that already exists.
- Click **Use Blank Image** to chose a blank image that represents the floor area.

Step 2 Click **Next**.

If you specified **Select an Imported Image**, the Building Tool displays an image list. See [Selecting the Image Map, page 13-12](#).

If you specified **Use Blank Image**, you need to enter the floor dimensions. See [Entering Floor Dimensions, page 13-11](#)

Entering Floor Dimensions

If you selected blank image, the Building Tool displays a form to enter the floor dimensions.

Procedure

Step 1 Enter a value in each Floor Dimension field. [Figure 13-2](#) illustrates how the values you enter correspond to the resulting floor image.

Figure 13-4 Specifying Floor Dimensions

Step 2 From the pulldown menu, select whether the value is feet or meters.

Step 3 Click **Next**.

Now you need to review and save the floor information you entered. See [Saving Floor Information, page 13-14](#).

Selecting the Image Map

When you chose to select an image from an imported image list, the Building Tool displays a list of images on the server.



Note The larger an image resolution is, the longer it takes to upload to the server and the more memory it uses. Therefore, we recommended that your image be less than 300KB and less than 1,000x1,000 pixels.

Procedure

Step 1 The Select Image Map form lists the image files on the server. If your image file appears in the Select Image File window, skip to Step 4.

Step 2 To add a new image file, click **Add to List**. The Upload File Selection window appears.

Step 3 Browse to the location of your image file. Click on your image file, then click **Select**.

If your file is a recommended size, your file is uploaded and added to the Select Image Map list. Go to Step 5.

If your image file contains more than the 1,000x1,000 pixels, a message appears stating that your image file appears to be larger than the recommended size and asks you if you want to abort importing.

- Click **Yes** to abort importing and select a new image. See Step 2.
- Click **No** to continue the import. A message appears asking if you would like Location Manager to resize your image. See Step 4.

Step 4 Chose whether to use the built-in image optimizer:

- Click **Yes** to have the image resized. A preview of the resized image is displayed. After viewing the preview of the resized image, click **OK**. A new image is created with the name `filename_sm.png`. Your original image file is not modified.
- Click **No** if you don't want to use the image optimizer. The import is canceled. You must use another program to reduce the size of your image before importing it.

**Note**

If your image filename has any spaces, the spaces are replaced with underscores (_). For example, if your image filename is *my floor image.jpg*, it will become *my_floor_image.jpg* in Location Manager.

Step 5 Click on the image file, then click **Next**.

You now need to specify the scale of the image you selected. See [Specifying the Scale of the Image Map, page 13-13](#).

Specifying the Scale of the Image Map

The Building Tool displays the image file and asks you to enter information about the scale of the image.

Procedure

Step 1 Click and drag the red squares of the red scaler tool so that the line corresponds to an area in your building for which you know the exact distance in feet or meters.

Step 2 Enter the distance that corresponds to the scaler in the field provided.

**Note**

The more accurate your measurement is, the more accurate Location Manager can determine the location of any interferers.

Step 3 Click **Next**.

You now need to specify the radio coverage area. See [Specifying the Radio Coverage Area, page 13-13](#).

Specifying the Radio Coverage Area

After you specify the scale of the floor map image, you need to enter information about which areas in the floor map image are included in the radio coverage area.

Procedure

Step 1 Using the Coloring Tool to add areas or the Eraser Tool to remove areas, specify the area of the floor in which you want to optimize the radio configurations. During the Radio Parameter Generation calculation, Location Manager tries to optimize the radio settings within the area that is shaded.

There are several tools to help you shade the desired area:

- The first two icons let you add and remove areas by grid sections. Click on each section you want to add or remove.
- The second two icons let you add and remove larger sections. Hold down and drag your mouse to select areas you want to add or remove.

The colored icons let you change the color used in the image map.

Step 2 Click **Next**.

You now need to save and review the floor information you entered. See [Saving Floor Information, page 13-14](#).

Saving Floor Information

The Review and Save form displays the information you entered in the Building Tool.

Procedure

- Step 1** If all the information displayed in the form is correct, click **Save**.
- Step 2** If you need to modify any information previously entered, click **Previous** to return to the information you need to change.

After you click **Save**, you can use the Building Tool to add another new floor to the building. See [Choosing the Next Step, page 13-14](#).

Choosing the Next Step

After you have saved the floor information, you can:

- Click **Add New Floor** to add another new floor to the building. See [Adding Floors to Location Manager, page 13-9](#).
- Click **Modify Existing Floor** to change a floor that was previously added. This option appears only if you have already added a floor to the building.

Related Topics

- [Adding Devices to Floors, page 13-14](#)

Adding Devices to Floors

After you add a new campus site, building, and new floor(s), you can place the devices on the floor map for each floor.



Note

You must discover, inventory, and manage all devices before adding them to Location Manager. See [Device Discovery and Management, page 4-1](#).

Procedure

- Step 1** In the Location Manager navigation tree, click a floor name on which you want to add devices.
- Step 2** From the View Mode pulldown menu, select **Edit Location**.
- Step 3** To add devices to the floor map, from the list of devices in the Unspecified Location list, click and hold on a device name and drag it to its approximate location on the image of the floor map.

**Caution**

Place the devices on the floor map as close as possible to their exact location on the floor. Do not place the devices arbitrarily on the floor image.

If you move the devices on the floor map, all corresponding radio data (radio monitoring, radio scan, and client walkabout data) is deleted. If after moving the devices you do not perform a new radio scan and client walkabout (optional), the default radio measurement data is used for the internal calculation for radio coverage, assisted configuration, and estimation of rogue location.

After you drag and drop a device to a different floor in Location Manager, the server is updated. However, it could take a little while (usually less than 1 minute) before the **Devices > Group Management** data is updated. You need to refresh or reload the **Devices > Group Management** page to get the latest data.

The closer the device on the map matches its location on the floor, the more accurate coverage displays will be and the more accurate Location Manager will be when giving information about unknown radios and interferers.

After you place an AP on the floor map, the RM Capability Verifier is automatically started. The RM Capability Verifier checks the AP for connectivity, registration with WDS, and capabilities that are listed under the Test Description Field and displays the results. See [Verifying Radio Management Capability, page 13-27](#).

You can disable the RM Capability Verifier when you add APs to the floor by deselecting that setting in **Edit > Preferences**. See [Setting Location Manager User Preferences, page 13-16](#).

Step 4 Move your mouse over an AP icon and a pop-up window appears showing the name, IP address, Ethernet MAC address, and the status of the AP's infrastructure mode:

- If Infrastructure Mode is *No*, the AP is not registered with WDS.
- If Infrastructure Mode is *Yes*, the AP is registered with WDS. The parent WDS address is displayed along with additional information about the AP.

For more information about WDS, see [What is WDS and Why Do I Need It?, page 11-8](#).

Related Topics

- [Reordering Floors, page 13-15](#)
- [Understanding Location Manager Device Icons, page 13-40](#)
- [Selecting a Location Manager View Mode, page 13-29](#)
- [Verifying Radio Management Capability, page 13-27](#)

Reordering Floors

By default, the sites and buildings you add are listed in alphabetical order in the Location Manager navigation tree. Floors are listed in the order in which they were created. You can change the order in which the floors are listed.

Procedure

Step 1 Right click on the floor whose order you want to modify.

- Step 2** Select **Move Up** or **Move Down** from the pop-up menu to change its order in the list.
-

Setting Location Manager User Preferences

You can set your preferences for how Location Manager displays information.

Procedure

- Step 1** Select **Edit > Preferences**. The User Preferences form opens. You can
- Select **Remember current location for next time** to have Location Manager automatically display the last-viewed floor or building when you launch Location Manager.
 - Select **Display coverage for operational radio interfaces only** to display coverage for APs that are functional. If this box is selected (default), the coverage for radios that are determined to be down are not displayed.
 - Select **Run Radio Manager Verifier the first time APs are placed** to run the Radio Management verification automatically when you place an AP on the floor map. See [Verifying Radio Management Capability, page 13-27](#).
 - Specify how you want Location Manager to respond when you click on a floor:
 - Open View in Current Window—Displays floor map in the current window.
 - Open View in New Window—Opens a new window in which the floor map is displayed.
 - Specify which View Mode you want Location Manager to open with when you click on a floor. You can select any of the View Modes. See [Using Location Manager Functions, page 13-16](#).



Note You can override which View Mode to open with by right-clicking on a floor name and selecting a different option.

- Step 2** Click **OK** to apply the changes and return to Location Manager.
-

Using Location Manager Functions

Location Manager provides several tools and functions to help you manage your WLAN radio environment. This section contains:

- [Using the Location Manager Assisted Site Survey Wizard, page 13-17](#)
- [Displaying Information About Rogue Access Points, page 13-22](#)
- [Displaying the Location of Unknown or Rogue Radios, page 13-22](#)
- [Verifying Radio Management Capability, page 13-27](#)
- [Locating Devices in Location Manager, page 13-27](#)
- [Editing Antenna Placement, page 13-28](#)
- [Selecting a Location Manager View Mode, page 13-29](#)
- [Viewing Interference Reports, page 13-34](#)

- [Obtaining Server Information, page 13-34](#)
- [Using the Location Manager Window Tools, page 13-34](#)

Using the Location Manager Assisted Site Survey Wizard

The Assisted Site Survey walks you through the process of determining the optimal radio transmit power and channel selection to optimize throughput and coverage for a given area. It helps you select APs, run an AP radio scan job, perform a client walkabout, and generate radio parameters for the selected APs.

The Assisted Site Survey takes you through the following steps:

1. **AP Selection**—See [Selecting the APs, page 13-17](#).
2. **AP Radio Scan**—See [Performing AP Radio Scan, page 13-17](#).
3. **Client Walkabout**—See [Performing a Client Walkabout, page 13-19](#).
4. **Radio Parameter Generation**—See [Generating Radio Parameters, page 13-19](#).



Note

Because the more devices included in an Assisted Site Survey Wizard session the more time is required for completion, it is recommended that you run a separate Assisted Site Survey Wizard session for each building or for each floor.

Selecting the APs

Procedure

- Step 1** From the Location Manager window, select **Wizard > Assisted Site Survey**. The Assisted Site Survey Wizard appears.
- Step 2** Select the APs you want to participate in the site survey:
 - To select all APs in a building, click on the building name, then click **Add**.
 - To select all APs on a floor, click on the floor name, then click **Add**.
 - To select individual APs, click on the AP name, then click **Add**.
- Step 3** To remove an AP that you previously selected, click on the AP name, then click **Remove**.
- Step 4** Click **Next** to go to the next step, **Filter By PHY**.
- Step 5** Select the type of 802.11 radio that will participate in the assisted site survey.



Note

Only radios of the selected types take part in the assisted site survey. If a selected AP has no interfaces of the desired radio types, this is noted in the job run log.

- Step 6** Click **Next** to go to the next step (see [Performing AP Radio Scan, page 13-17](#)).

Performing AP Radio Scan

After you selected the APs to participate in the assisted site survey, the wizard checks to see if there is any existing radio scan data for the APs you selected. If there is no previous scan data, the wizard asks you to run a new radio scan setup. In addition, the following information is displayed in the table:

Field	Description
Name	Name of the AP
IP Address	IP address of the AP
Radio Type	The type of radio
Radio MAC	The MAC address of the radio
Last Scan Time	Time the most recent radio scan job started. If this field indicates <i>None</i> , you need to run a new radio scan.

Procedure

Step 1 Select one of the following options:

- Start new radio scan setup—The wizard starts a new radio scan job. Select this option if there is no previous radio scan date for the selected APs.
- Use previous radio scan data—The wizard uses the data collected from the most recent radio scan job. Use this option if all APs have a time stamp in the “Last Scan Time” field.



Note A running scan job temporarily degrades wireless LAN service, which might affect client associations. To minimize any disruption, run scan jobs during off-hours.

Step 2 If you select to start a new radio scan setup, you need to specify the AP’s maximum transmit power setting for the radio scan procedure. The default is 100mW. See [Understanding AP Radio Scans, page 13-44](#).

Step 3 To start the new radio scan, click **Start**. You’ll see informational messages appear in the text box and when the scan is complete, the form will display the following information:

Field	Description
Name	Name of the AP
IP Address	IP address of the AP
Radio Type	The type of radio
Radio MAC	The MAC address of the radio
Last Scan Time	Time the most recent radio scan job started

Step 4 Click **Next** to go to the next step (see [Performing a Client Walkabout, page 13-19](#)).

Related Topics

- [Understanding AP Radio Scans, page 13-44](#)
- [Using AP Radio Scans to Collect RM Data, page 13-43](#)

Performing a Client Walkabout

Performing a client walkabout is an optional procedure in the Assisted Site Survey Wizard. If the APs you selected have data from a previous Client Walkabout session, this information is displayed in the wizard. For more information, see [Understanding Client Walkabouts, page 13-54](#).

Procedure

-
- Step 1** Select one of the following options:
- Start Client Walkabout Setup—The wizard walks you through the steps of setting up a client walkabout. See [Guidelines for Running a Client Walkabout, page 13-55](#).
 - Skip Client Walkabout—If the location data is accurate, you can skip the client walkabout and go directly to [Generating Radio Parameters, page 13-19](#).
- Step 2** If you select to start client walkabout Setup, you need to enter at least one client MAC address, and up to five IP addresses. These addresses will move around during the walkabout.
- Step 3** Select the AP power setting. You might choose to enter a lower power setting when, for example, the default power level might affect a neighboring network.
- Step 4** Click **Start** to start the client walkabout. When the client walkabout is complete, click **Stop** and the following information is displayed:

Field	Description
Name	Name of the AP
IP Address	IP address of the AP
Radio Type	The type of radio
Radio MAC	The MAC address of the radio
Total WA Data	Accumulated data from previous walkabouts
New WA Data	Data from the current walkabout session

While you are running a client walkabout session, the data in the Total WA Data and New WA Data fields should increase. If these fields remain at zero, make sure you have set up the walkabout session correctly (see [Guidelines for Running a Client Walkabout, page 13-55](#)).

- Step 5** Click **Next** to go to the next step (see [Generating Radio Parameters, page 13-19](#)).
-

Related Topics

- [Understanding Client Walkabouts, page 13-54](#)
- [Guidelines for Running a Client Walkabout, page 13-55](#)

Generating Radio Parameters

You need to set channel constraints and transmit power constraints for the APs you selected. The wizard can help you configure your APs by using measurement data collected from a client walkabout and AP radio scanning. The wizard recommends optimal radio transmit power, channel selection, and beacon interval (optional), and then applies these configuration settings to the APs, if desired. For more information, see [Creating a New Assisted Configuration Task, page 13-75](#).

**Tip**

To get optimal channel settings, run the radio parameter generation on a per building basis. That is, include all APs in one building in a single radio parameter generation job.

**Note**

When you generate parameters from the Assisted Site Survey Wizard, you cannot edit or run that parameter generation job from the Sites tab (**Sites > Assisted Configuration**).

Procedure

-
- Step 1** Click on one of the Constraints options:
- All APs—Applies the constraints to all APs you selected to participate in the site survey
 - Individual AP—Allows you to specify constraints for individual APs.
- Step 2** Select the Channel Sets. Use ctrl-click to select more than one channel set. The radio parameter generation feature will give you a suggested channel within the channels you select. Click **Presets** to choose from a pre-selected set of channels.
- Step 3** If you click **Presets**, the Select Channel Sets window appears. Click on a channel set, then click **Select**. The channels you selected appear in the Channel Sets field.
- Step 4** Enter a value in the Minimum and Maximum Transmit Power fields. You might choose to enter a lower power setting when, for example, the default power level might affect a neighboring network. You must enter a numerical value greater than zero and less than 100.
- Step 5** Select whether to enable black hole mitigation. If you select this option, the wizard recommends a beacon interval, which is slightly altered from what the AP is configured to, for the APs. If you do not select the Black Hole Mitigation option, the wizard will not recommend a beacon interval.
- Step 6** Select **Ignore Rogues and Friendly APs** to have the parameter generation algorithm ignore all rogue and friendly APs and consider interference from managed APs only.
- Step 7** Select **Ignore Client Walkabout Location Data** to have the parameter generation algorithm ignore any data collected during client walkabout. You might want to use this option if your client walkabout data is not up to date or is no longer relevant. The calculation generation completes faster by selecting this option, but the result might be as accurate.
- Step 8** Select the service type **Voice** or **Data**. If you select Voice, you must select an RSSI value from the pulldown menu and also select the appropriate voice data rate check boxes.
- Step 9** Click **Start** to start the configuration parameter calculation. A status bar appears indicating the progress of the parameter generation. When the radio parameter generation is complete, a message appears at the bottom of the screen.
- Step 10** Click **Log** to view the progress and run log of the parameter calculation. The bottom of the log window shows statistics and a summary of the parameter calculation.
- Step 11** To stop the parameter calculation, click **Stop**.
- Step 12** Click **Next** to view the calculation results and apply the configuration to the APs. The wizard displays the calculation results. These results show the following information:

Field	Description
Name	Name of the AP
Transmit Power	Recommended transmit power for this AP. If the radio type is 11g, the CCK power and OFDM power are also displayed.
Channel	Recommended channel for the AP
Beacon Interval	Recommended beacon interval for the AP. If you did not select the Enable Black Hole Mitigation option, this column displays the value to which the AP is currently configured (see Assigning Constraints and Goals , page 13-77).
Estimated Max Throughput	The estimated maximum megabytes per second that the AP can process. The maximum throughput is an estimated value that is calculated from either: • Data collected from all client walkabouts. • Predicted walkabout data if no walkabouts were performed. Using the walkabout data and the potential RF configuration parameters, an analysis is performed to predict the degree of transmit collisions and contention that may result in the coverage area for each AP, given a predefined ratio of AP-to-client and client-to-AP traffic. The collision and contention values are then applied to the theoretical throughput maximum to come up with the real predicted throughput.

Step 13 Select **Write NVRAM on Success** to have the new configuration changes copied from the AP's running configuration to its startup configuration.

Step 14 After reviewing the calculation results, click **Preview** to preview the changes in the Location Manager window or click **Apply Configuration** to apply the configuration changes to the APs.



Note The configuration on your devices will not change unless you click **Apply Configuration**.

The Apply Status column in the table indicates if the configuration was successfully applied.

Related Topics

- [Creating a New Assisted Configuration Task](#), page 13-75

Displaying Information About Rogue Access Points

When Radio Monitoring detects a rogue AP, a new fault is generated. (See [Understanding Rogue AP Detection, page 14-12](#) for more information.) When you select the link in the Address, Description, or Timestamp fields in the Fault Summary Table for an unknown access point, the Rogue Access Point Details window displays information about the rogue AP such as details about the unknown access point, beacon and location information, switch port tracing, reporting access points, and fault history. You access the faults window from WLSE, not from within Location Manager.

You can also view this information, except for switch port tracing, from the Location Manager Unknown Radio List (see [Understanding the Location Manager Window, page 13-36](#)).

Procedure

-
- Step 1** From WLSE, select **Faults > Display Faults**. The Fault window appears.
- Step 2** Click the link in the Description or Timestamp fields in the Fault Summary Table for an unknown access point.
- A new window displays the Rogue Access Point Details report. For information about this report, see [Managing Rogue APs, page 14-24](#)
- For more information about faults, see [Displaying Fault Information, page 3-1](#).
-

Related Topics

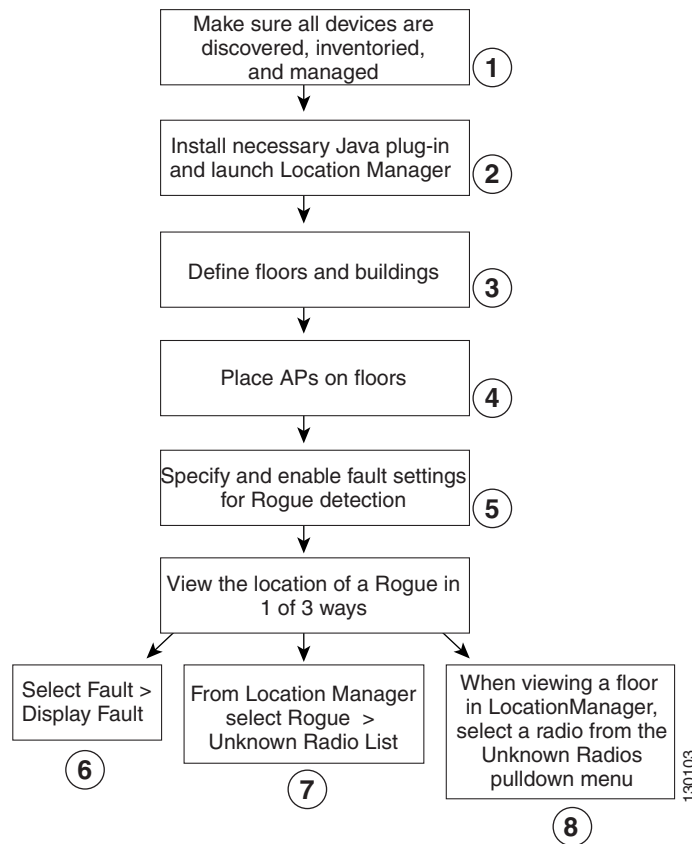
- [Understanding Rogue AP Detection, page 14-12](#)
- [Understanding the Location Manager Window, page 13-36](#)

Displaying the Location of Unknown or Rogue Radios

Location Manager helps you see the approximate location of unknown (rogue or friendly) radios in your network by using the received signal strength from all detecting APs to locate the unknown radio relative to the detecting APs.

Location Manager can also estimate the distance between the detecting AP and the unknown radio.

Before you can detect Rogue radios and view their coverage areas, you need to perform the following steps:

Figure 13-5 Recommended Setup To Detect Rogue Radios

Number	Description
1	See Device Discovery and Management , page 4-1.
2	See Prerequisites for Using Location Manager , page 13-2.
3	See Setting Up Location Manager , page 13-3.
4	See Understanding Location Manager Device Icons , page 13-40.
5	See Setting the Rogue AP Detection Policy , page 14-16.
6	See Understanding Rogue AP Detection , page 14-12.
7	See Understanding the Location Manager Window , page 13-36.
8	See Figure 13-7Location Manager Window , page 13-37.

**Note**

Radio Monitoring is enabled by default. See [Using Radio Monitoring to Collect RM Data](#), page 12-1).

**Note**

Although running AP Radio Scan is not required for Rogue AP detection, it is required to see the AP's coverage display. See [Using AP Radio Scans to Collect RM Data](#), page 13-43.

Procedure

- Step 1** In the Location Manager window, click on the Unknown Radio List icon or select **Rogue > Unknown Radio List**. The Unknown Radio List window opens displaying a list of all unknown radios interfaces.



Note If you click on a floor, the Unknown Radios pulldown menu lists the unknown radios on the floor that you are currently viewing. You can click on a unknown radio from this pulldown menu. Unknown Radios on a different floor from the floor you are currently viewing do not appear on the pulldown menu.

You can click on any column in the Unknown Radio List form to sort the information by that column. By default, the information is sorted by BSSID.

- Step 2** From the Unknown Radio Type pulldown menu, select which devices you want to view:
- Rogue APs—Infrastructure APs that have not been identified as Friendly. By default, all unknown radios are classified as Rogue until you change them to Friendly.
 - Rogue AdHoc Devices—Rogue AdHoc APs that have not been identified as Friendly.
 - All Friendly Devices—APs that you know exists, for example, a neighboring network's AP, but that you are not going to modify in any way.

The window refreshes to display the devices of the unknown radio type you selected.

- Step 3** Click on a row in the table or click **Select All** to select all devices of the unknown radio type you selected. When you click on a single row, the Unknown Radio List window refreshes with data specific to that device as shown in [Table 13-2](#).



Note If you select more than one row, the information fields are blank and you can change the status of the devices or delete the devices only. All other buttons are disabled.

Table 13-2 Unknown Radio List Information Fields

Field	Description
BSSID	Basic Service Set (BSS) Identifier.
SSID	Service Set Identifier used by client devices to associate with an access point. If you have unprintable characters in the SSID, they are displayed as hexadecimal values. Also, if you have double quotes (") or backslashes (\) in your SSID, they are preceded by a backslash (\) . The length field (for example, "[12]") appears at the end of the string. If your Cisco AP is configured to not allow its SSID to be broadcast, a string of zeros appears in the SSID field.
Rogue Status	The state of the device.
Vendor	The name of the vendor that manufactured this AP.
Detection Timestamp	The date and time the unknown radio was detected

Table 13-2 Unknown Radio List Information Fields

Field	Description
PHY Type	The physical interface type (11a, 11b, or 11g) of the radio interface.
Beacon Interval	The beacon interval on which the rogue AP is transmitting.
Beacon Channel	The channel on which the rogue AP is transmitting.
Data Rates	The data rates supported by this interface (in Mbps).

The **Switch Port Detection** field shows information about the switch port and who reported it as show in [Table 13-3](#).

**Note**

CatOS is not supported for switch port tracing.

Table 13-3 Unknown Radio List Switch Port Detection Fields

Field	Description
Switch IP Address	The IP address of the switch to which the rogue AP is connected. If the switch IP address is <i>Unknown</i> , the IP address of the switch that the unknown radio is connected to could not be determined. ¹
Switch Port	The port of the switch to which the rogue AP is connected.
Traced MAC Address	The MAC address of the rogue AP.
Timestamp	The time, based on the client browser, the rogue AP switch port was detected (see Understanding WLSE Time Displays , page 1-10).

1. To find the switch port to which the rogue AP is connected, the Switch Port Location feature uses the rogue AP's BSSID that it hears over the air to make a heuristic guess of the rogue's Ethernet MAC address. This might not be possible, however, if its Ethernet MAC address and BSSID do not follow the one-off rule, where the MAC address is the same or one-off of the BSSID. For more information, see [Understanding Switch Port Tracing and Suppression](#), page 14-30.

The **Reported By** field shows the device(s) that detected the unknown radio:

- If the **APs** checkbox is selected, the Reported By field displays the APs that detected the selected unknown radio. The Reported By list contains the sysname of the reporting AP, the IP address of the reporting AP, and the reporting AP's RSSI value.
- If the **Clients** checkbox is selected, the Reported By list contains the sysname of the reporting AP and the IP address of the AP that the detecting client is associated to, not the IP address of the client itself. The RSSI value is shown as *not available*.

If the device you selected does not have a building name listed in the Building field, the **Location Estimation** field indicates the estimated location as unknown.

- Step 4** Click **Change to Friendly** (if you selected Rogue from the Unknown Radio Type pulldown) to change the status of the selected unknown radio from Rogue to Friendly.

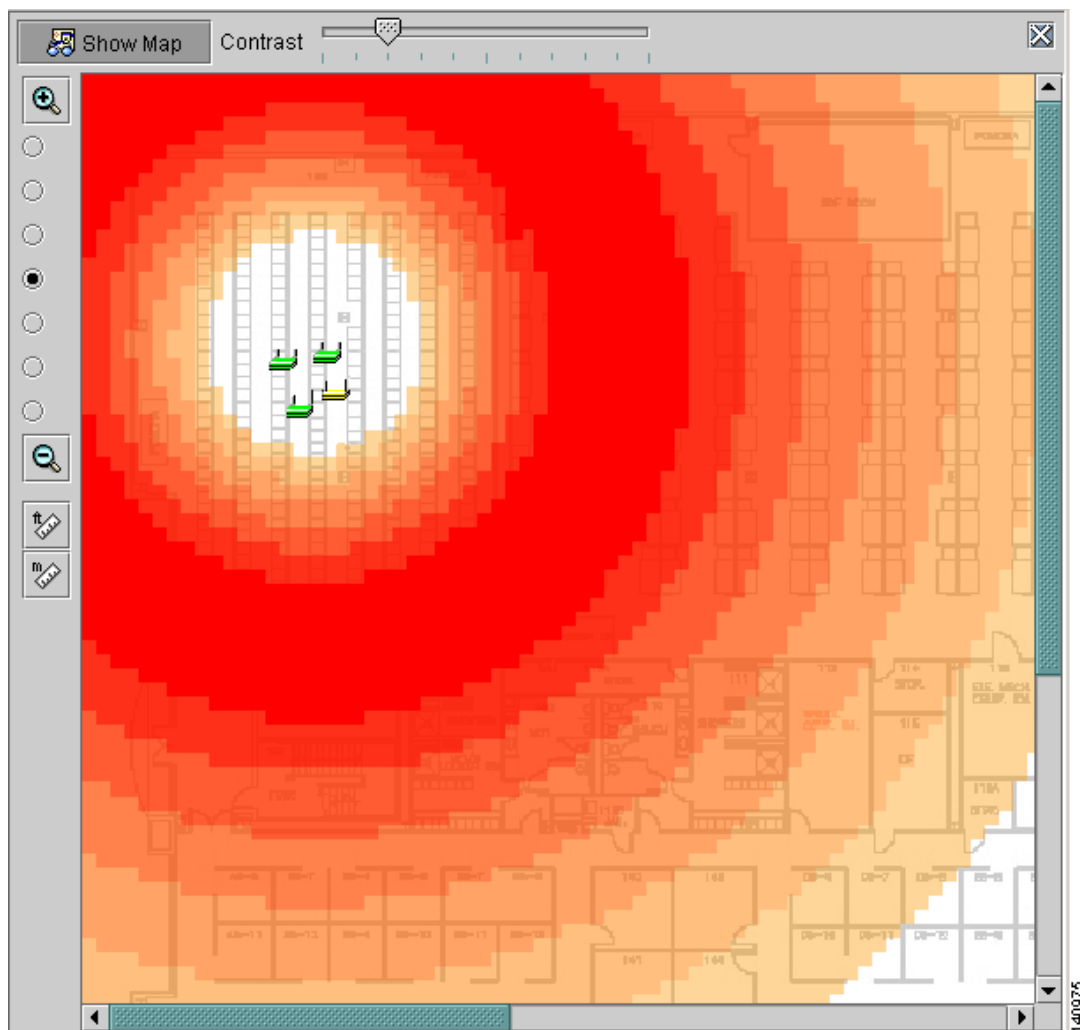
If you selected Friendly from the Unknown Radio Type pulldown, you can click **Change to Rogue** to change the status of the selected unknown radio from Friendly to Rogue.

- Step 5** Click **Display Location** to view the approximate location of the unknown radio on the floor map. The possible location of the unknown radio shaded is in color where the darkest shade indicates the most probable location, as show in [Figure 13-6](#).



Note If the Estimated Location indicates “Unknown,” the Display Location button is greyed out. The location might be unknown because you didn’t specify the location of the reporting APs on the floor map before the APs detected the unknown radio. In this case, after specifying the location of the reporting APs on the Location Manager floor map, run Radio Monitoring again to get the estimated location (see [Using Radio Monitoring to Collect RM Data](#), page 12-1).

Figure 13-6 Viewing the Possible Location of Unknown Radios



Because Location Manager does not know the transmit power of the unknown radio, you might need to change the display options by selecting a value for the Transmit Power Assumption. The default transmit power is 50mW and 100mW. If you select all transmit powers, the floor map displays all possible areas that the selected unknown radio might be located.

**Tip**

If the Unknown Radio List dialog box is covering the Location Manager window, you might need to close the dialog box to see the unknown radio displayed on the building map in Location Manager.

- Step 6** To delete a rogue AP when you have determined that it no longer exists, you can remove it by clicking **Delete**.

Related Topics

- [Setting the Rogue AP Detection Policy, page 14-16](#)
- [Displaying Information About Rogue Access Points, page 13-22](#)

Verifying Radio Management Capability

You can verify that your APs, the WDS, and the WLSE are configured correctly for Radio Management, which might help troubleshoot any problems you encounter. The first time you place an AP on the floor map, the Radio Management verification runs automatically. You can suppress this feature by setting your preference in the User Preferences. See [Selecting a Location Manager View Mode, page 13-29](#).

Procedure

- Step 1** Right-click on the device whose Radio Management capability you want to verify and select **Verify RM Capability**. The RM Capability Verifier window opens. The Devices column lists all devices on which you have run the RM Capability Verifier.
- The RM Capability Verifier checks the AP for connectivity, registration with WDS, and capabilities that are listed under the Test Description Field.
- Step 2** Check the Test Status column. OK indicates the test passed. Failed indicates a problem.
- Step 3** If a test fails, click on the failed test, and the Suggested Action field displays information about how to fix the problem.
- Step 4** To re-run the RM Capability Verifier, click **Re-run**.

Locating Devices in Location Manager

You can search for devices in the Location Manager window.

Procedure

- Step 1** From the Location Manager window, select **Tools > Find AP**. The Find AP window appears.
- Step 2** From the pulldown menu, select whether to search by device name, IP Address, or MAC Address.
- Step 3** Select either Containing or Exactly Matching.
- Step 4** Enter the text string to search for in the text field.
- Step 5** Click **Search**. The Find AP form displays the device or devices that match your search criteria.

- Step 6** Click on the name of the device you want to locate, then click **Locate AP** at the bottom of the form. The AP you selected appears in the center of the floor map.

You can right-click on any AP and select **Device Details**. A new browser opens displaying the AP Summary Report for the AP you selected.

Editing Antenna Placement

If you have a directional antenna or an external antenna, you can modify the antenna placement in Location Manager to specify the direction the antenna is pointing in, to specify the height of the antenna, and to specify any cable loss. Changing the antenna placement affects radio parameter calculation, rogue location estimation, and coverage display. After you change the antenna placement, you need to schedule an AP radio scan and schedule a new radio parameter generation job.



Note

You must be in Edit Location View Mode to modify the antenna placement. See [Edit Location View Mode](#), page 13-30

Procedure

- Step 1** Right-click on the device whose antenna you want to modify and select **Edit Antenna > radio type**. Select **2.4 GHz** for .11b and .11g radios; select **5 GHz** for .11a radios.
- If you are not in Edit Location View Mode, a message appears asking if you want to change to Edit Location View Mode. Click **Yes**.
- Step 2** In the Antenna Placement form, select an option from the Antenna Type pulldown menu, which contains the list of supported antennas. If you are unsure what type of antenna you are using, leave the default antenna. The description of the antenna you specified is displayed.



Note

If the antenna used by the AP is not listed on the Antenna Type pulldown menu, select *Unspecified 2.4 GHz* for .11b/g radios or *Unspecified 5GHz* for .11a radios. The Unspecified antenna is treated as 2.2 dBi omni antenna.



Note

If the antenna used by the AP1200 series access point for 5 GHz operation is an *internal omni* antenna, select either KODIAK-OMNI or OSPREY-OMNI. If the antenna used by the AP1200 series access point for 5 GHz operation is an *internal directional* antenna, select either KODIAK-DIRECTIONAL or OSPREY-DIRECTIONAL.

- Step 3** If your AP has an omni antenna, skip this step. (You will not be allowed to enter any values.) Enter values in the Azimuth (direction) and Downtilt (from horizon) fields:
- The Azimuth (direction) is the angle where the directional antenna points to on the horizontal plane. The angle ranges from 0 to 359 degrees clockwise. You can either enter a numerical value or drag the arrow to the direction you specify. The red arrow indicates the direction in which the antenna points.

- The Downtilt (from horizon) is where the directional antenna points down away from the horizontal plane. The angle ranges from -90 to 90 degrees. Enter a positive degree if the angle is pointing down; enter a negative degree if the angle is pointing up. You can either enter a numerical value or drag the arrow to the direction you specify.

Click the right arrow under the photo of the antenna to see direction references.

Step 4 Enter the height of antenna from the floor in the **Height (from floor bottom)** field and select whether the value is in feet or meters. Make sure you enter the height for the antenna, not the height for the AP, which might be different.

Step 5 If your AP has an internal antenna, an antenna integrated with an AP or an AP's radio card, skip this step. For an external antenna, enter the additional attenuation (or loss) in dB in the **Additional Cable Loss** field. The default value is 0 dB.

If you use the original cable that came with the antenna, you must keep the default value of 0 dB, unless there is a non-zero cable loss specified in the antenna's specifications. If you use a cable extension to the antenna, you must enter a positive value in dB. To estimate the value you need to enter if you use any cable extension, consult the cable manufacturer. The manufacturer typically provides the cable loss in meters or in feet; you can multiply this value by the length of the cable and round it to the nearest number. If you are not sure of the value you need to enter, leave the default value (0 dB) unchanged.

Step 6 Click **OK** to apply the changes and return to the Location Manager window. Click **Apply** to apply the changes and leave the Antenna Placement form open.



Note

After you change the antenna placement, you need to schedule an AP radio scan, schedule a client walkabout (optional), and schedule a new radio parameter generation job.

Selecting a Location Manager View Mode

The Location Manager View Mode pulldown menu appears in the pane beneath the navigation tree and allows you to quickly change what information is displayed in the image map.

When you click on a floor in the Location Manager navigation tree, the View Mode menu contains these options:

- Summary (If you click on a site or building name instead of a floor name, Summary is the only option available in the View Mode menu. See [Summary View Mode, page 13-30](#).)
- Edit Location (see [Edit Location View Mode, page 13-30](#))
- Tx/Rx Coverage by Data Rate (see [Tx/Rx Coverage by Data Rate View Mode, page 13-30](#))
- Voice Tx/Rx Coverage by Data Rate (see [Voice Tx/Rx Coverage by Data Rate View Mode, page 13-31](#))
- Tx/Rx Coverage by Signal Strength with Overlaps (see [Tx/Rx Coverage by Signal Strength With Overlaps View Mode, page 13-32](#))
- Tx/Rx Coverage by Signal Strength without Overlaps (see [Tx Coverage by Signal Strength Without Overlaps View Mode, page 13-33](#))
- Unknown Radio Location Estimation (see [Unknown Radio Location Estimation View Mode, page 13-33](#))

Summary View Mode

If you select **Summary** from the View Mode pulldown menu, Location Manager displays summary information which includes:

- Managed Access Points—Number of managed APs
- Major Alarms—P1 and P2 alarms (see [Displaying Fault Information, page 3-1](#))
- Minor Alarms—P3, P4, and P5 alarms (see [Displaying Fault Information, page 3-1](#))
- Radio Manager feature status. This information appears only if you click on a floor name in the Location Manager navigation tree.

**Note**

If you click on a site or building name instead of a floor name in the Location Manager navigation tree, **Summary** is the only option available in the View Mode menu. See [Summary View Mode, page 13-30](#).)

Edit Location View Mode

When you select **Edit Location** from the View Mode pulldown menu, the image map does not change; however, you can now move the devices to a different location on the floor map. You can also edit antenna placement in the **Edit Location** View Mode (see [Editing Antenna Placement, page 13-28](#)).

**Note**

Edit Location is available when you click on a floor name in the Location Manager navigation tree. If you click on a building name, the **Edit Location** option is greyed out.

Procedure

- Step 1** In the View Mode pulldown menu, select **Edit Location**.
- Step 2** Click on the device you want to move.
- Step 3** You can either drag the device to a new location on the map, or you can select **Edit > Cut** from the menu or by right-clicking on the device.
- Step 4** If you select **Edit > Cut**, click on the new location for the device (or to move it to a different floor but at the same location, click on different floor), then select **Edit > Paste** from the menu or by right-clicking on the device.

The device appears in the new location on the image map.

Tx/Rx Coverage by Data Rate View Mode

When you select **Tx/Rx Coverage by Data Rate** from the View Mode pulldown menu, the image map refreshes the display the coverage area of the devices you selected.

**Note**

Tx/Rx Coverage by Data Rate is available when you click on a floor name in the Location Manager navigation tree. If you click on a building name, the **Tx/Rx Coverage by Data Rate** option is greyed out.

Procedure

-
- Step 1** From the View Mode pulldown menu, select **Tx/Rx Coverage by Data Rate**.
- Step 2** From the Coverage Display pulldown menu, select the radio interface whose coverage you want to display in the image map.
- Step 3** Select which range to display:
- **Transmission Range**—shows the coverage area of each data rate specified at any given place on the floor map. You can see which area is covered at which data rate.
 - **Reception Range**— shows that the AP can detect a radio source with the specified mW at the different data rates. The colors in the floor map correspond to the data rates.
- If you select Reception Range, you need to chose a value from the mW pulldown menu. If you pick a larger value, for example 5mW, the colored regions become larger because the reception range has been increased.
- Step 4** Click **Show Received Signal Strength for Selected AP** to view how strong a signal is for a particular area. The darker the color, the stronger the signal strength. Due to attenuation, the received signal strength for an AP is lower than the transmit power that is set on the AP.
- Step 5** Click on the data rates (in Mbps) you want to display. The color next to each data rate indicates the corresponding color that is displayed on the floor map. You can also click on one of the Quick Selection Choices, which automatically selects the signals that correspond to the specified radios.
-

Voice Tx/Rx Coverage by Data Rate View Mode

When you select **Voice Tx/Rx Coverage by Data Rate** from the View Mode pulldown menu, the image map displays the voice coverage area by data rate.

Procedure

-
- Step 1** From the Coverage Display pulldown menu, select the data rate whose coverage you want to display in the image map.
- Step 2** Select which range to display:
- **Transmission Range**—shows the coverage area of each data rate specified at any given place on the floor map. You can see which area is covered at which data rate.
 - **Reception Range for Radio Source**— displays the areas in which the AP can detect a radio source with the specified mW.
- If you select Reception Range, you need to chose a value from the mW pulldown menu. If you pick a larger value, for example 5mW, the colored region become larger because the reception range has been increased.
- Step 3** Click **Show Received Signal Strength for Selected AP**, then click on an AP to view a grid of RSSI values overlaid on the current coverage display. The predicted RSSI value is displayed for each point on the map.
- Step 4** Select an RSSI value from the Select RSSI pulldown menu. By default, the RSSI values are as follows:
- -75dBm for 802.11 a radios
 - -67dBm for 802.11 b and g radios

You can select any value from -78 dBm to -55 dBm. If you entered an RSSI value when you created the site or building, the value you entered is the default.

- Step 5** In the Voice Rate Selection for Display field, click on the data rates (in Mbps) you want to display. The color next to each data rate indicates the corresponding color that is displayed on the floor map. You can also click on one of the Quick Selection Choices, which automatically selects the signals that correspond to the specified radios.

Tx/Rx Coverage by Signal Strength With Overlaps View Mode

When you select **Tx/Rx Coverage by Signal Strength With Overlaps** from the View Mode pulldown menu, the image map displays the coverage area by signal strength of the devices you selected. You can use this option to see if you have a hole, which appears as a white spot, in your coverage on the specified floor.



Note

Tx/Rx Coverage by Signal Strength With Overlaps is available when you click on a floor name in the Location Manager navigation tree. If you click on a building name, the **Tx/Rx Coverage by Signal Strength With Overlaps** option is greyed out.

Procedure

- Step 1** From the View Mode pulldown menu, select **Tx/Rx Coverage by Signal Strength with Overlaps**.
- Step 2** From the Coverage Display pulldown menu, select the radio interface whose coverage you want to display in the image map.
- Step 3** Select which range to display:
- **Transmission Range**—shows how far the transmit signal can reach given the cutoff value you specify in the Display Cutoff pulldown menu. The colors displayed on the floor map correspond to the different channels. The darker the color, the stronger the signal strength.
 - **Reception Range**— displays (in yellow) the areas in which the AP can detect a radio source with the specified mW.
- If you select Reception Range, you need to chose a value from the mW pulldown menu. If you pick a larger value, for example 5mW, the colored region become larger because the reception range has been increased.
- Step 4** Click **Show Received Signal Strength for Selected AP**, then click on an AP to view a grid of RSSI values overlaid on the current coverage display. The predicted RSSI value is displayed for each point on the map.



Note

For 802.11g radios, the estimated Received Signal Strength is based on the configured **CCK** (Complementary Code Keying) transmit power only and is not affected by the **OFDM** (Orthogonal Frequency Division Multiplexing) power setting.

- Step 5** From the Display Cutoff pulldown menu, select a value for which you want to display each AP's signal strength. For example, if you select 80% (-55dBm), the floor map displays the area in which the AP signal strength is at least 80% (-55dBm).

Tx Coverage by Signal Strength Without Overlaps View Mode

When you select Tx/Rx Coverage by Signal Strength Without Overlaps from the View Mode pulldown menu, the image map refreshes the display the transmit coverage by signal strength of the devices you selected. You can use this option to see if you have a hole, which appears as a white spot, in your coverage on the specified floor.



Note

Tx Coverage by Signal Strength Without Overlaps is available when you click on a floor name in the Location Manager navigation tree. If you click on a building name, the **Tx Coverage by Signal Strength Without Overlaps** option is greyed out.

Procedure

- Step 1** From the View Mode pulldown menu, select **Tx Coverage by Signal Strength with Overlaps**.
- Step 2** From the Coverage Display pulldown menu, select the radio interface whose coverage you want to display in the image map.

The floor map shows which AP's signal strength is the strongest at any given location on the floor. The color used in the floor map corresponds to the AP's channel.
- Step 3** Move your mouse to any area on the floor map, and a line is drawn to the AP whose signal is the strongest in that location. The AP's received signal strength is also displayed automatically.



Note

For 802.11g radios, the estimated Received Signal Strength is based on the configured **CCK** (Complementary Code Keying) transmit power only and is not affected by the **OFDM** (Orthogonal Frequency Division Multiplexing) power setting.

Unknown Radio Location Estimation View Mode

When you select **Unknown Radio Location Estimation** from the View Mode pulldown menu, you can select different display options for the unknown radios to change the information that is displayed on the floor map. Changing display options can help you find the unknown radio by increasing the area in which you're likely to find the unknown radio



Note

Unknown Radio Location Estimation is available when you click on a floor name in the Location Manager navigation tree. If you click on a building name, the **Unknown Radio Location Estimation** option is greyed out.

Procedure

- Step 1** Select Unknown Radio Location Estimation from the View Mode pulldown menu.
- Step 2** From the Unknown Radios pulldown menu, select an unknown radio. The pulldown menu contains MAC addresses of the unknown radio interfaces on the specific floor you are viewing. If you want to see all unknown radios, regardless of their location, select **Rogue > Unknown Radio List**. (See [Understanding the Location Manager Window](#), page 13-36.)

The colors displayed on the floor map correspond to the probability of the unknown radio being in that area; the darkest shade indicates the most probable location, as shown in [Figure 13-6](#).

- Step 3** You can click on different transmit power options to see different areas on the floor map in which the unknown radio might be located by selecting a value for the Transmit Power Assumption. The default transmit power is 50mW and 100mW. If you select all transmit powers, the floor map displays all possible areas that the selected unknown radio might be located.
- Step 4** Click **Use Exclusion Algorithm**. By default, the Exclusion Algorithm is selected so that, in its calculations, Location Manager includes the APs in the general area that did not detect the unknown radio. If you deselect the Exclusion Algorithm option, only the APs that detected the unknown radio are used in the location calculation.
-

Viewing Interference Reports

You can quickly run an interference report from Location Manager.

Procedure

- Step 1** Right-click on a device on which you want to detect interference, then select **Interference Report**. The WLSE Fault Details window opens. See [Viewing Fault Details, page 3-7](#).
-

Obtaining Server Information

From Location Manager, you can:

- Verify Server Status

To verify the status of your server, select **Server > Status**. The Server Status window appears displaying the IP address of the server and the time the server was started. The Server status form also displays the following information:

- UserID—Username of the person who launched Location Manager
- Client Address—Address of the client machine that launched Location Manager
- Login Time—Time that the user launched Location Manager

- View Server Messages

To view server messages after you configure your floor plan with APs, select **Server > Message**. The Message Server Message Log window appears displaying messages about your server. This information might be helpful when troubleshooting issues, for example, if the AP display coverage isn't correct.

Using the Location Manager Window Tools

Location Manager provides the following tools:

- [Exporting a Floor Image, page 13-35](#)
- [Printing a Floor Image, page 13-35](#)
- [Using Location Manager Measuring Tool, page 13-35](#)

- [Using Location Manager Contrast Sliding Tool, page 13-36](#)
- [Zooming In and Out, page 13-36](#)

Exporting a Floor Image

You can save a floor image view that you can use for troubleshooting or debugging purposes.

Procedure

-
Step 1	From the Location Manager window, select Tools > Export View Image . The Save Image As form appears.
Step 2	Navigate to the location in which you want to save the image, enter a name in the File Name field, then click Save . The exported image file is saved with a <i>.png</i> extension.
-

Printing a Floor Image

You can print a floor image view that you can use for troubleshooting or debugging purposes. To print an image, from the Location Manager window, select **Tools > Print View Image**.

Using Location Manager Measuring Tool

The Location Manager Distance Measure Tools allow you to measure the distance (in either feet or meters) between APs and perform other measure functions.



Note

The Distance Measure Tool icons appear only when you have added floor information to your buildings. (See [Adding Floors to Location Manager, page 13-9](#).)

Procedure

-
Step 1	In the Location Manager window, click on either Distance Measure Tool icon. The icon with ft indicates feet, and the icon with m indicates meters. The icon you selected is shaded grey, and the bottom of the Location Manager displays the following message: Distance Measure Tool: On
Step 2	Click and drag your mouse anywhere on the floor map to start your measurement from.
Step 3	Drag your mouse to the desired location. You'll see the measurement display as you're dragging the mouse.
Step 4	To end the measurement, lift your finger from the mouse.



Note

If the Distance Measure Tool is enabled, the Edit Location tool is disabled automatically.

Using Location Manager Contrast Sliding Tool

You can modify the background contrast in the image of your floor map by using the Location Manager Contrast sliding tool.

- To make the background image lighter, move the sliding bar to the left.
- To make the background image darker, move the sliding bar to the right.

Zooming In and Out

When using Location Manager, you might need to zoom in and out to see APs displayed on the floor map. You can zoom in and out by selecting a radio button to the left of your floor image. There are 7 radio buttons that correspond to the following zoom levels:

- 32 pixels per foot
- 16 pixels per foot
- 8 pixels per foot
- 4 pixels per foot
- 3 pixels per foot
- 2 pixels per foot
- 1 pixel per foot

To return to the normal view, select the fourth radio button (4 pixels per foot) in the list.

Understanding the Location Manager Window

The following sections explain the parts of the Location Manager window and what information is displayed in each part.

- [All Locations or Building View, page 13-36](#)
- [Floor View, page 13-38](#)

All Locations or Building View

When you launch Location Manager for the first time and select **All Locations** or a campus site name in the navigation tree, the Location Manager window looks similar to [Figure 13-7](#). See [Table 13-4](#) for an explanation of the numbered fields.

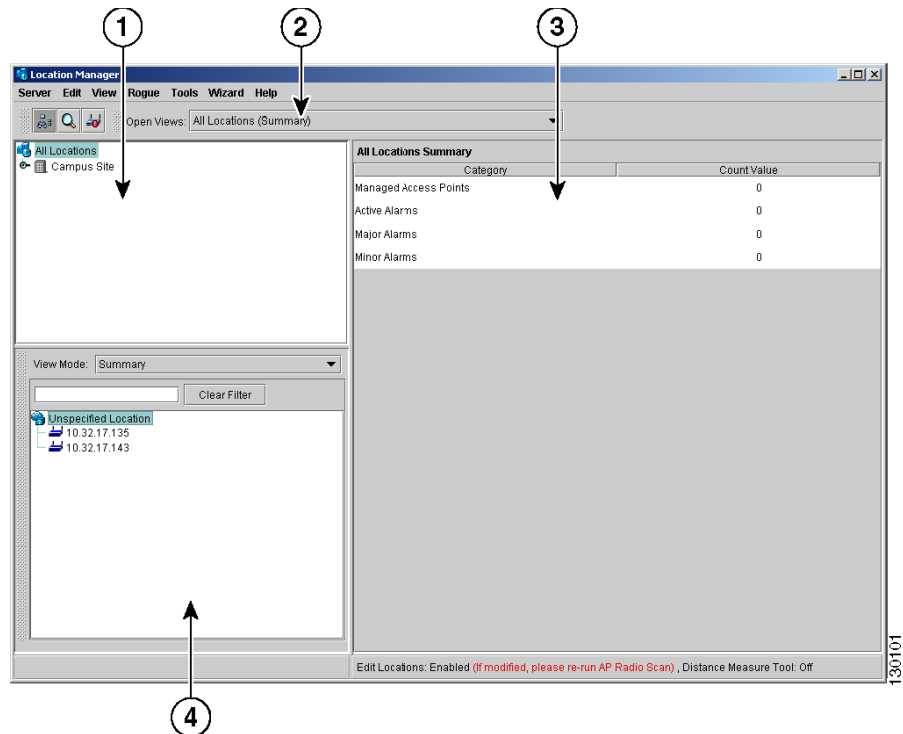
Figure 13-7 Location Manager Window

Table 13-4 describes the Location Manager fields that are numbered above.

Table 13-4 Location Manager Window Descriptions

Number	Description
1	By default, the Location Manager navigation tree displays All Locations as the top folder. If you have previously launched Location Manager, the All Locations folder contains the sites, buildings, and floors that have been added. • If you click on All Locations or a campus site name, the summary appears in field 3. See All Locations and Building Summary, page 13-38. • If you click on a building, the Building Summary and the Radio Manager Feature Status appear in field 3. • If you double-click on a building name or expand a building folder, you see the floors that have been added to that building. • If you click on a floor name, the floor map is displayed in field 3. See Floor View, page 13-38 for more information. You can modify what information is displayed when you click on a floor name by setting user preferences (see Setting Location Manager User Preferences, page 13-16). • If you double-click on a device name, the device is centered in the floor map in field 3.
2	The Open Views pulldown menu lists the sites, building, and floors that you have previously viewed. See Using Location Manager Functions, page 13-16.

Table 13-4 Location Manager Window Descriptions (continued)

Number	Description
3	The All Locations Summary displays information about all the sites, buildings and floors that have been previously added to Location Manager. (See All Locations and Building Summary , page 13-38.)
4	The View Mode pane contains the View Mode pulldown menu (see Using Location Manager Functions , page 13-16) and lists discovered, inventoried, and managed devices not assigned to a building or floor (see Device Discovery and Management , page 4-1).

When you click on a floor name in the navigation tree, the Location Manager window changes. See [Floor View](#), page 13-38.

Related Topics

- [Setting Location Manager User Preferences](#), page 13-16

All Locations and Building Summary

When you first launch Location Manager, the default view is All Locations. The window on the right displays the All Locations Summary which contains the following information:

- Managed Access Points—Number of managed APs
- Major Alarms—P1 and P2 alarms (see [Displaying Fault Information](#), page 3-1)
- Minor Alarms—P3, P4, and P5 alarms (see [Displaying Fault Information](#), page 3-1)

When you expand the All Locations folder, you see a list of the sites and corresponding buildings and floors that have been entered in to Location Manager.

The Building Summary, which appears when you click on a building name, displays the same information as the All Locations Summary, but the information is specific to the building you selected.

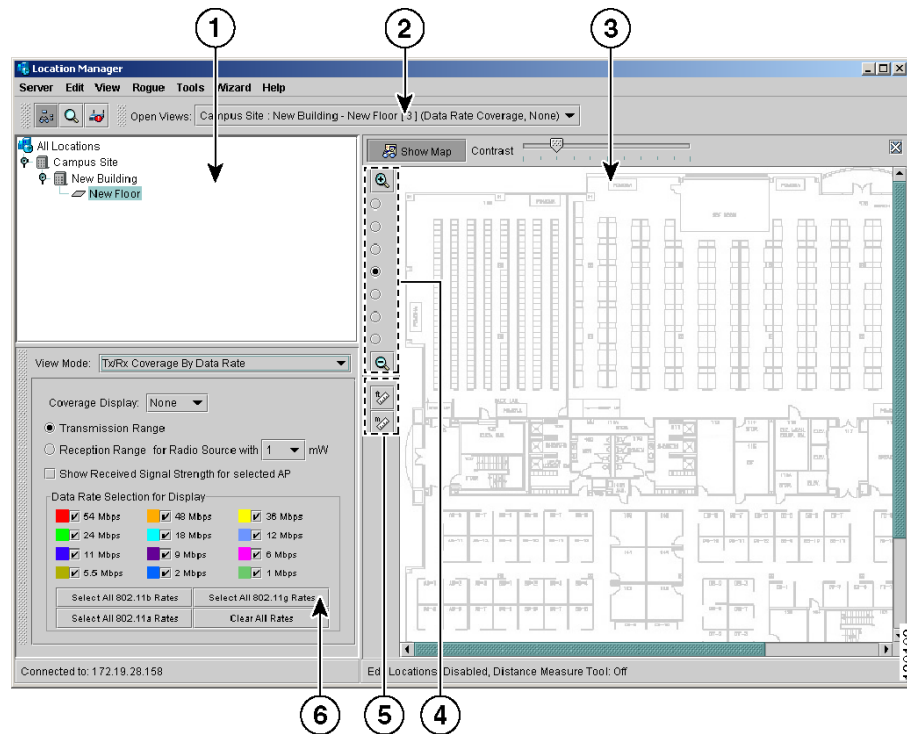
When you click on a floor, the All Locations Summary is replaced with the corresponding floor map image. See [Floor View](#), page 13-38 for more information.

Using the Open Views Menu

The Open Views pulldown menu at the top of the Location Manager window provides quick access to any views you recently viewed. When you click on a building or floor in the All Locations list, the name of the building or floor is added to the Open Views pulldown menu. When you select an option from the Open Views menu, Location Manager displays your selection with the same view mode and same coverage display setting you specified when you last viewed it.

Floor View

When you click on a floor name in the Location Manager navigation tree, the window changes to display additional options and menus. [Figure 13-8](#) illustrates the floor view. See [Table 13-5](#) for an explanation of the numbered fields.

Figure 13-8 Location Manager Floor View**Table 13-5** Floor View Window Descriptions

Number	Description
1	The Location Manager navigation tree. If you click on a floor name, the floor map is displayed in field 3. If you double-click on a device name, the device is centered in the floor map in field 3.
2	The Open Views pulldown menu lists the buildings and floors that you have previously viewed. See Using Location Manager Functions , page 13-16.
3	This field displays the floor image map of the floor you selected in the navigation tree.
4	Zoom options for the floor image map. See Zooming In and Out , page 13-36.
5	Measuring tool. See Using Location Manager Contrast Sliding Tool , page 13-36.
6	The View Mode pulldown menu contains viewing options that modify the information that is displayed on the floor image map. For more information on selecting a view mode and the resulting coverage display, see Using Location Manager Functions , page 13-16.

Understanding Location Manager Coverage Display

Location Manager displays the predicted coverage of the APs that you place on a floor map. The coverage prediction is based on the current AP settings as well as the floor dimensions you entered, the location in which you placed the APs on the floor map, the AP-to-AP measurements taken during AP Radio Scan, and the direction and coverage of the AP's antenna. The most important factors affecting AP-to-AP measurement data are signal attenuation in the air (known as path loss) and multi-path reflection in the building.

Coverage display does not take in to account any environmental effects; therefore, the predicted coverage area might not be exactly the same as the real coverage area, especially around the boundary of the building and areas outside the building. The coverage display reflects the transmit power level of the AP; the higher the power level is set on the AP, the larger the area that AP will cover, and thus, a larger coverage area is displayed on the floor map.

Coverage display is two-dimensional and per floor. Coverage display does not show the coverage of an AP on a different floor, even though an AP might have a very strong signal that covers a different floor.

**Note**

Client Walkabout does not modify the Location Manager coverage display. Client Walkabout is used for the generation of parameters during the Assisted Site Survey and does not have an effect on the coverage display.

Related Topics

- [Understanding the Location Manager Window, page 13-36](#)

Understanding Location Manager Device Icons

After you have placed the devices on the floor map, the devices are represented by icons as shown in [Table 13-6](#). The color of the icons correspond to the devices' fault status:

- Red indicates the device has major (P1 or P2) faults.
- Yellow indicates the device has minor (P3, P4, or P5) faults.
- Green indicates the device has no faults.

The color of the buildings and icons in the location tree also correspond to their fault status.

For more information about faults, see [Displaying Fault Information, page 3-1](#).

Table 13-6 *Device Icons Used in Location Manager*

Icon	Meaning
	AP with no faults
	Interference reporting AP with minor faults
	Scanning-only AP with major faults

Based on the options you select in the **View** menu, the information that is displayed with the device icons might be different (see [Modifying Information Displayed with Device Icons](#), page 13-41).

You can right-click on any AP and select **Device Details**. A new browser opens displaying the AP Summary Report for the AP you selected.

You can your mouse over an AP icon and a pop-up window appears showing the name, IP address, Ethernet MAC address, and the status of the AP's infrastructure mode:

- If Infrastructure Mode is *No*, the AP is not registered with WDS.
- If Infrastructure Mode is *Yes*, the AP is registered with WDS. The parent WDS address is displayed along with additional information about the AP.

For more information about WDS, see [What is WDS and Why Do I Need It?](#), page 11-8.

Related Topics

- [Modifying Information Displayed with Device Icons](#), page 13-41
- [Displaying Information About Rogue Access Points](#), page 13-22

Modifying Information Displayed with Device Icons

From the **View** menu, you can select which information to display with the device icons on the Location Manager floor map. [Table 13-7](#) explains what information is displayed with each View option.



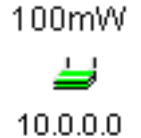
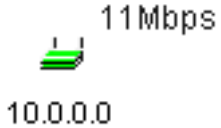
Note

Labels are displayed for each radio. If an AP has both an .11a and .11g radio, information about both radios is displayed.

Table 13-7 Location Manager View Menu Options

Location Manager Menu Sequence	Option Selected	Information Displayed on the Floor Map	Example
View > AP Label	Name	Device name (as specified in Devices > Discover > Discover > Advanced Options , NameFormat. See Selecting the Device Name Format , page 4-41.)	 ap-1.cisco.com
	IP Address	Device IP address	 10.0.0.0
	Ethernet MAC Address	Device Ethernet MAC address	 000c8515xxxx

Table 13-7 Location Manager View Menu Options (continued)

Location Manager Menu Sequence	Option Selected	Information Displayed on the Floor Map	Example
View > Radio Channel	n/a	Radio channel of each radio interface (channel 9 in the example). The color corresponds to the channel color.	 Note Scanning-only APs have an “S” in place of the radio channel.
View > Transmit Power	n/a	Transmit power (in mW) of each radio interface (100 mW in the example)	 Note Scanning-only APs display “N/A.”
View > Data Rate	n/a	Data rate (in Mbps) of each radio interface (11 Mbps in the example).	 Note Scanning-only APs display “N/A.”

Moving Devices on Location Manager Image Map

If you already placed a device on your Location Manager image map and need to change its location, you can move it to a new location by following these steps.



Note

You must be in Edit Location View Mode to change the location of a device. See [Edit Location View Mode](#), page 13-30

Procedure

- Step 1** In the View Mode pulldown menu, select **Edit Location** or select **Edit > Enable Edit Location**.
- Step 2** Click on the device you want to move.
- Step 3** You can either drag the device to a new location on the map, or you can select **Edit > Cut** from the menu or by right-clicking on the device.

Step 4 If you select **Edit > Cut**, click on the new location for the device (or to move it to a different floor but at the same location, click on different floor), then select **Edit > Paste** from the menu or by right-clicking on the device.

The device appears in the new location on the image map.

**Note**

After you drag and drop a device to a different floor in Location Manager, the server is updated. However, it could take a little while (usually less than 1 minute) before the **Devices > Group Management** data is updated. You need to refresh or reload the **Devices > Group Management** page to get the latest data.

Related Topics

- [Understanding Location Manager Device Icons, page 13-40](#)

Using AP Radio Scans to Collect RM Data

AP Radio Scan produces path loss data that is used for rogue location estimations, radio parameter generation data, self healing monitoring, and coverage display data. These topics provide procedures for collecting AP Radio Scan data:

- [Understanding AP Radio Scans, page 13-44](#)
- [Guidelines for Running AP Radio Scans, page 13-45](#)
- [Viewing AP Radio Scan Jobs, page 13-46](#)
- [Managing AP Radio Scan Jobs, page 13-48](#)
- [Creating a New AP Radio Scan Job, page 13-50](#)
- [Viewing AP Radio Scan Job Run Logs, page 13-53](#)

Related Topics

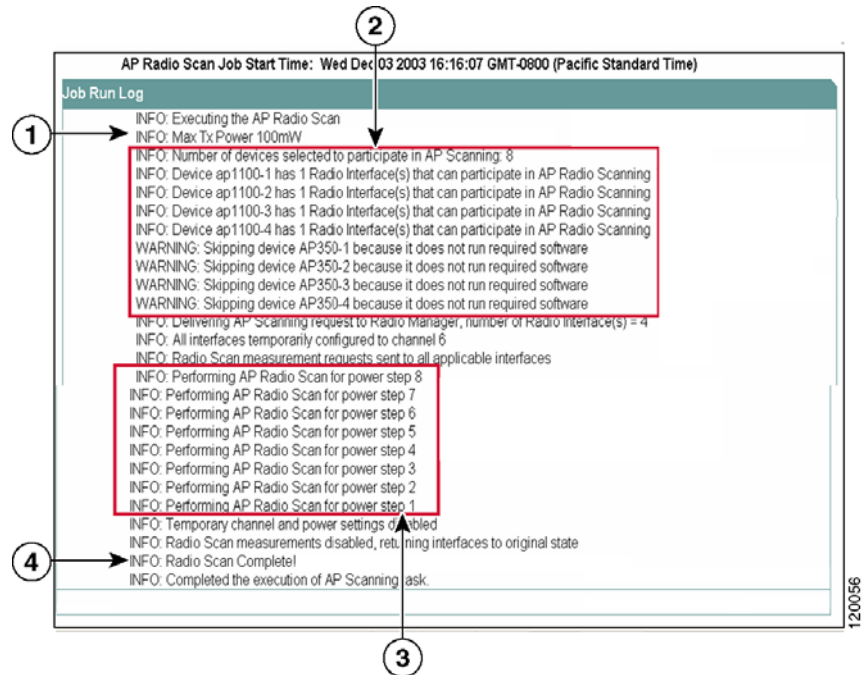
- [Understanding Radio Management, page 11-7](#)
- [Collecting Radio Location Data, page 11-14](#)

Understanding AP Radio Scans

Each AP broadcasts beacons and simultaneously listens for neighboring beacons. AP Radio Scan uses the resulting AP-to-AP measurements to establish the path loss model for the WLAN. You should run AP Radio Scan during initial setup, then periodically to capture any changes (for example, when APs are added, deleted, or moved).

How It Works

During the scanning process, AP Radio Scan performs the following tasks:



1	Sets the selected APs to transmit beacons on the same channel at maximum transmit power. The maximum power threshold is user configurable. During a scan, AP frequencies, data rates, and power levels are temporarily changed. Then, for each AP, the channel is fixed and the procedure steps through the power levels up to the specified maximum transmit power level. Note The radio scan uses temporary configuration parameters so the AP can revert back to its normally configured parameters if the AP is reset or loses connection with the WLSE during the procedure.
2	Measures the signal strength and calculates the path loss of each AP.
3	Repeats this step, with the APs transmitting at successively lower power levels until the lowest setting is reached, to determine the power step calibration of each AP.
4	Saves this information in the database as AP radio locations, sets all APs back to their original power and channel settings, and notifies the user when the scan is complete.

Data Produced

The result of AP Radio Scan is a snapshot of the radio frequency interference at each AP and a set of signal strength measurements indicating the level at which each AP receives each neighbor AP. When the neighbor AP is controlled by WLSE, the Radio Manager uses that AP's current transmit level to compute the path loss between the two APs, which it saves to characterize the radio frequency environment. When the neighbor AP is not under WLSE control, the Radio Manager saves the received signal strength.

These results are used in Assisted Configuration, Location Manager, Radio Manager Reports, and Faults to:

- Determine how an AP is positioned relative to other APs
- Determine the amount of path loss due to obstructions (such as walls) between APs
- Compute rogue location estimations, radio parameter generation data, and coverage display data

Guidelines for Running AP Radio Scans

Prerequisites

Before running an AP Radio Scan job, you must:

1. Configure your network for radio management (see [Getting Started with Sites, page 13-2](#)).



Note Be sure that the community string you are using provides write access. To run AP Radio Scan, you *must* have SNMP write access. Most other WLSE functions only require read access.

2. Define the location elements (buildings and floors) and place the APs on the floor images (optional, but recommended—see [Setting Up Location Manager, page 13-3](#), [Adding Floors to Location Manager, page 13-9](#), and [Adding Devices to Floors, page 13-14](#)). This will help you get the best results from Location Manager displays.



Note If you deploy only a single AP, WLSE cannot gain any knowledge about the building's radio environment. In this case, WLSE applies a default indoor path loss model and displays the coverage using this model. Without any measurements, WLSE assumes the transmission characteristics are the same in all directions, so the coverage display appears as circular.

Tips

- If you do not run AP Radio Scan, the Coverage Display in the Location Manager will be computed using the default pass loss model. Because no path loss measurement data has been collected, the coverage views could be distorted.
- You should run an AP radio scan during initial setup, then periodically during brief maintenance periods when the WLAN is not in use to capture any changes made to the APs (for example, when APs are added, deleted, or moved).
- A running scan job temporarily degrades wireless LAN service, which might affect client associations. To minimize any disruption, schedule scan jobs to run during off-hours (for example, 2:00AM).

**Note**

AP Radio Scan jobs affect an access point's performance. With all APs configured to the same channel and maximum power, there is some degradation in throughput. In addition, while the APs step through their various power settings, there might be some loss of coverage. This only lasts for the length of the AP scan (3 to 4 minutes).

- When you run a new AP radio scan, the previously-collected radio location information for the selected APs is deleted automatically.
- Instead of using AP Radio Scan, you can use the Assisted Site Survey wizard, which is part of Location Manager, to walk you through the process of determining the optimal radio transmit power and channel selection. This wizard interface steps you through AP radio scan, client walkabout, and radio parameter generation (see [Using the Location Manager Assisted Site Survey Wizard, page 13-17](#)).

Related Topics

- [Understanding AP Radio Scans, page 13-44](#)

Viewing AP Radio Scan Jobs

Use the default AP Radio Scan screen to view radio scan jobs.

**Note**

Your login determines whether you can use this procedure.

Before You Begin

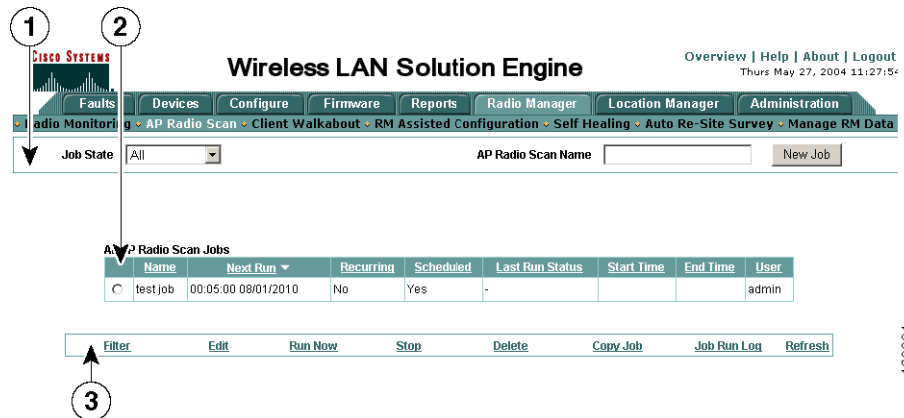
Before you can view the list of AP Radio scan jobs, you must:

- Satisfy the AP Radio Scan prerequisites (see [Guidelines for Running AP Radio Scans, page 13-45](#)).
- Create at least one job (see [Creating a New AP Radio Scan Job, page 13-50](#)).

Procedure

- Step 1** Select **Sites > AP Radio Scan**. The AP Radio Scan screen appears.

Figure 13-9 Sample AP Radio Scan Screen



1	Job state selection list
2	List of jobs
3	Job management buttons

Step 2 From the Job State list, select the type of job you want to view:

- **Scheduled**—Lists all AP radio scan jobs that have been scheduled
- **Unscheduled**—Lists all AP radio scan jobs that have not been scheduled
- **Running**—Lists all AP radio scan jobs that are currently running
- **All**—Lists all AP radio scan jobs

The screen refreshes to show you details about the specified jobs. The information displayed depends on the selected job state:

Table 13-8 Job Details—Scheduled and Unscheduled

Field	Description
Job Name	The job name.
Recurring	Indicates if the job is run periodically (Yes or No).
Next Schedule	For scheduled jobs, this indicates when the job will run. For completed jobs, this is the time the job ran.
Owner	The user who last edited the job.

Table 13-9 Job Details—Running

Field	Description
Job Name	The job name.
Recurring	Indicates if the job is run periodically (Yes or No).
Job Start Time	The time the job started.
Percent Complete	The percent of the job that has completed running.

Table 13-9 *Job Details—Running*

Field	Description
Next Schedule	The job is not a recurring job.
Owner	The user who last edited the job.

Table 13-10 *Job Details—All*

Field	Description
Job Name	The job name.
Recurring	Indicates if the job is run periodically (Yes or No).
Job State	The state of the job. Note A job in the DidNotStart state must be rescheduled.
Next Schedule	For scheduled jobs, this indicates when the job will run. For completed jobs, this is when the job ran.
Last Run Status	The status of the job the last time it was run.
Owner	The user who last edited the job.

- Step 3** From this window, you can use the job management buttons (see [Figure 13-9](#)) to manage your AP radio scan jobs (see [Managing AP Radio Scan Jobs](#), page 13-48).

Related Topics

- [Using AP Radio Scans to Collect RM Data](#), page 13-43
- [Sorting Table Data](#), page 1-13

Managing AP Radio Scan Jobs

The buttons below the table of AP radio scan jobs (see [Viewing AP Radio Scan Jobs](#), page 13-46) allow you to manage these jobs.

**Note**

Your login determines whether you can use these procedures.

Before You Begin

Before you can manage an AP Radio scan job, you must:

- Satisfy the AP Radio Scan prerequisites (see [Guidelines for Running AP Radio Scans](#), page 13-45).
- Create at least one job (see [Creating a New AP Radio Scan Job](#), page 13-50).

Procedure

- Step 1** Select **Sites > AP Radio Scan**. The AP Radio Scan screen appears (see [Figure 13-9 on page 13-47](#)).

- Step 2** From the Job State list, select the type of job you want to manage. The screen refreshes to show the corresponding jobs.



Note AP radio scan jobs created using the Assisted Site Survey Wizard cannot be edited or run using the **Sites > AP Radio Scan** tab. To manage these jobs, see [Using the Location Manager Assisted Site Survey Wizard, page 13-17](#).

- Step 3** Click the radio button for the job you want to manage, then click one of the buttons that appear after the list of jobs:

- **Filter**—This button displays a limited set of AP radio scan jobs, making it easier to search for a particular job by name. The filter remains in effect until the page is refreshed.



Note You can use % as a wildcard: for example, entering %name% displays all the jobs that contain the word “name.”

- **Edit**—Use this button to edit jobs from the displayed list of previously-created jobs.



Note If you have deleted the image that was associated with the job you are editing, the job will show that no image has been selected.

- **Run Now**—Use this button to run the currently selected job immediately. This option clears all other schedule settings.
- **Stop**—Use this button to stop a running AP Radio Scan job.
- **Delete**—Use this button to delete jobs from the displayed list of jobs. Jobs that are scheduled, unscheduled, completed, or did not start can be deleted. Jobs that are running cannot be deleted.
- **Copy Job**—Use this button to create a new job using the data (maximum transmit power and selected APs) from a previously-created job.



Note This procedure does *not* copy the schedule data.

- **Job Run Log**—Use this button to view the run log for a selected job (see [Viewing AP Radio Scan Job Run Logs, page 13-53](#)).
- **Refresh**—To be certain that you are looking at the latest information, click the **Refresh** button to refresh the job list after you have made changes to one or more AP radio scan jobs.

Related Topics

- [Using AP Radio Scans to Collect RM Data, page 13-43](#)
- [Sorting Table Data, page 1-13](#)

Creating a New AP Radio Scan Job

**Note**

Your login determines whether you can use this procedure.

Before You Begin

Before you can create a new AP radio scan job, you must satisfy the AP Radio Scan prerequisites (see [Guidelines for Running AP Radio Scans, page 13-45](#)).

Procedure

Step 1 Select **Sites > AP Radio Scan**. The AP Radio Scan job creation screen appears.

Step 2 Enter a name for the job and click **New Job**. For guidelines on job names, see [Appendix B, “Naming Guidelines.”](#)

The window refreshes with the Job Creation menu in the left pane and the Job Name dialog box in the right pane.

**Note**

Clicking on any subtab before you have saved your entries in the Job Creation window will reset the window and you will lose all the information you entered.

Step 3 Select the following numbered choices in the left pane to create and run the AP radio scan jobs:

**Note**

These steps, except Schedule Job, must be completed, but do not have to be done in order. You can omit scheduling the job and edit the job later to provide a schedule.

1. **Job Name**—See [Name the Job and Select the Maximum Transmit Power, page 13-51](#).
2. **Select AP**—See [Select the APs, page 13-51](#).
3. **Filter By PHY**—See [Select Radio Types, page 13-51](#).
4. **Schedule Job**—See [Schedule the Job, page 13-52](#).
5. **Finish**—See [Finish the Job, page 13-52](#).

Name the Job and Select the Maximum Transmit Power

Procedure

Step 1 From the menu in the left pane, click **Job Name**.

Step 2 Enter the following information:

Field	Description
Job Name	Enter a unique name for the job. For guidelines on naming jobs, see Appendix B, “Naming Guidelines.”
Description	Enter a description of the job. For guidelines on entering descriptions, see Appendix B, “Naming Guidelines.”
Maximum Transmit Power	You can choose to enter a lower power setting when, for example, the default power level might affect a neighboring network.

Step 3 Go to the next step, [Select the APs](#).

Select the APs

Procedure

Step 1 From the menu in the left pane, click **Select AP**. All managed devices are listed in the Device selector in the middle pane.

Step 2 Select the devices you want to include in the job (see [Using the Device Selector, page 1-12](#)).

Step 3 Go to the next step, [Select Radio Types](#).

Select Radio Types

Procedure

Step 1 From the menu in the left pane, click **Filter By PHY**.

Step 2 Select the type of 802.11 radio that will perform the AP radio scan. By default, both options (11a and 11b/11g) are selected.



Note Only radios of the selected types will take part in the scan. If a selected AP has no interfaces of the desired radio types, this is noted in the job run log.

Step 3 Go to the next step, [Schedule the Job](#).

Schedule the Job

When scheduling an AP radio scan job, you can:

- Create multiple scan jobs, but only one job can be run at a time.
- Select **Run Now** to start the job immediately, or you can schedule the job for a future date and time.
- Save a job without scheduling it, then edit the job later to add the scheduling information.



Note A running scan job temporarily degrades wireless LAN service, which might affect client associations. To minimize any disruption, schedule scan jobs to run during off-hours.

Procedure

Step 1 From the menu in the left pane, click **Schedule Job**.

Step 2 Enter the following information:

Field	Description
Run Now	Click to run the job. The job will run after you click Save (see Finish the Job , page 13-52). Note This option ignores all of the other scheduling options (Start Date, Start Time, and Repeat).
Start Date	From the lists, select the month, day, and year you want your job to run.
Start Time	From the list, select the hour and minutes of the day you want your job to run.
Repeat	
Enable	Check to run the job repeatedly.
Every	Indicate how often you want the job to repeat by entering a numerical value, then selecting an interval of time: Hours, Days, Weeks, or Months. Note Selecting this option runs the job periodically, starting with the date and time that you entered in the Start Date and Start Time lists.

Step 3 Go to the next step, [Finish the Job](#).

Finish the Job

Procedure

Step 1 From the menu in the left pane, click **Finish** to save your settings. The Finish dialog appears.

- Step 2** Click **Save** to save the AP Radio Scan jobs settings. The job will be added to the list of scheduled jobs or run immediately, depending on whether you scheduled the job for a later time or chose Run Now in the scheduling screen.



Note If a warning message appears saying that WLSE server is ahead of or behind your local time, see [Understanding Time Discrepancy Problems in Job Scheduling, page 1-11](#)

The screen refreshes and the AP Radio Scan Job Save Summary window displays the following information:

Field	Description
Name	Name of the job.
Description	Job description, if any.
Maximum Power	The maximum power setting selected for the job.
Selected APs	Names of the devices selected for the job.
Schedule	Scheduled date and time for the job, or <i>No Schedule</i> if the job has not been scheduled. You do not have to complete the scheduling information—you can save a job without scheduling it, then edit the job later to add the schedule.

At the scheduled time, the AP Radio Scan job will begin scanning for neighboring APs. The job stops automatically after all the required APs respond with the appropriate radio measurements.

- Step 3** To view the progress of a running job, select **Sites > AP Radio Scan > Job Run Log** (see [Viewing AP Radio Scan Job Run Logs, page 13-53](#)).
- Step 4** To stop the job manually, see [Managing AP Radio Scan Jobs, page 13-48](#).
- Step 5** After the AP Radio Scan has completed successfully, you should:
- Run a client walkabout (optional, but recommended)—see [Using Client Walkabouts to Collect RM Data, page 13-54](#).
 - Configure your APs—see [Using Assisted Configuration, page 13-71](#).

Viewing AP Radio Scan Job Run Logs

Use the Job Run Log button to view the run log for a selected job. The job run log displays information about running and completed AP Radio Scan jobs.

Procedure

- Step 1** Select **Sites > AP Radio Scan > Job Run Log**.

The Job Runs table appears in a separate browser window. This table contains the following information for each run:

Field	Description
Select Run	Select this button to see the details for that run. The details for the selected job run appear below the list of runs for that job.
Job Start Time	The time the job started.
Job End Time	The time the job ended.
Job Status	The status of the job.
Percent Complete	The percent of the job that completed.

The job run log appears below this table.

- Step 2** To view the details for a different job run, select another run from the Job Runs table and click **Job Run Log**.

Related Topics

- [Managing AP Radio Scan Jobs, page 13-48](#)

Using Client Walkabouts to Collect RM Data

Client Walkabout allows you create, view, and manage client walkabout jobs. Client walkabout measurements can help determine AP coverage, and are used to provide optimal coverage for the radio parameter generator. These topics describe the procedures for managing Client Walkabout jobs:

- [Understanding Client Walkabouts, page 13-54](#)
- [Guidelines for Running a Client Walkabout, page 13-55](#)
- [Viewing Client Walkabout Jobs, page 13-57](#)
- [Managing Client Walkabout Jobs, page 13-59](#)
- [Creating a New Client Walkabout, page 13-61](#)
- [Running the Walkabout, page 13-64](#)

Related Topics

- [Understanding Radio Management, page 11-7](#)
- [Collecting Radio Location Data, page 11-14](#)

Understanding Client Walkabouts



Note

Client Walkabout is currently supported only when using Cisco cards or non-Cisco client adapters that are compliant with Cisco Compatible Extensions version 2 (CCXV2). For the client adapters that support this feature, see the *Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine, 2.13*, on Cisco.com.

After running AP Radio Scan, you can run a client walkabout. A client walkabout is an optional step that reports all detected APs and provides optimal coverage for the radio parameter generator (see [Generating Radio Parameters](#), page 13-66).



Note Running a client walkabout does *not* modify the Location Manager coverage display. Client walkabout data is used only by the radio parameter generator and the Assisted Site Survey Wizard (see [Using the Location Manager Assisted Site Survey Wizard](#), page 13-17).



Note If no client walkabout data is available, default walkabout data is synthesized based on radio scan and radio monitoring data.

How It Works

During a client walkabout, you walk the client (typically a laptop) around the desired coverage area. During the walkabout, you can use up to five clients, each identified by its 802.11 MAC address, to cover different areas. Walk these client stations around the area of WLAN or a portion of the WLAN where you want proper coverage. During the walkabout:

- The APs are set to the same channel.
- The transmit power in the APs is increased so that the power required to cover the edges of the WLAN can be determined.

As you walk the coverage area, the serving AP changes as the client moves from one BSS to another. As long as the client remains inside the coverage area, the serving AP continually commands it to measure and report the signal strength and background radio frequency energy it receives from neighboring APs. All measurements are passed to the Radio Manager, which incorporates them into its RF environment database. This database provides the information that is used to compute the next radio configuration.

Data Produced

Although these measurements are not accompanied by location information, sets of measurements correspond to specific locations in the WLAN coverage area. The Radio Manager uses these measurements to create measurement objects, each containing path losses to the strongest controlled APs and received signal strength from uncontrolled sources at a specific location. These results are used in Assisted Configuration, Location Manager, and Radio Manager reports.

Guidelines for Running a Client Walkabout

Prerequisites

Before you can run a client walkabout job, you must:

1. Configure your network for radio management (see [Getting Started with Sites](#), page 13-2).
2. Configure the walkabout client to associate with the APs selected for the walkabout.

General

- If you do not perform a client walkabout, you *must* enter a floor plan that includes the distances between APs (see [Adding Floors to Location Manager](#), page 13-9).

- Instead of using Client Walkabout, you can use the Assisted Site Survey wizard, which is part of Location Manager, to walk you through the process of determining the optimal radio transmit power and channel selection. This wizard interface steps you through AP radio scan, client walkabout, and radio parameter generation (see [Using the Location Manager Assisted Site Survey Wizard, page 13-17](#)).

Configuring Your Access Points

- When you set up your APs, *do not* enable the option in the ACU (Aironet Client Utility) that periodically scans for a better AP if the threshold is below a specified value. *This feature conflicts with Radio Manager procedures.*
- Although there is no limit to the number of APs that may participate in a walkabout and no performance impact when you include a large number of APs, the total number of *data points* collected during a walkabout job does affect the processing time of Assisted Configuration:
 - The more data points, the longer it takes to calculate the parameters.
 - Too few data points might skip locations between APs, which could result in a recommended transmit power that is higher than expected.

Performing the Walkabout

To set the coverage area, walk the client around the area. Use these guidelines as you walk:

- Only one walkabout job can be active at any time.
- Walk at a slow, measured pace. The client takes measurements every 10 seconds, so if you walk too quickly, you will not collect enough data points.
- Walk a grid pattern that covers the entire area.
- Walk the edges of the network.
- Emphasize areas where you want coverage, such as conference rooms and other enclosed areas.
- When you have finished collecting the data, *stop the walkabout*. The client will continue taking measurements if you do not explicitly stop the process.
- Client walkabout data collection is cumulative, so you can stop and start as often as necessary.
- For a network that contains both 11a and 11b/g radios (for example, when you are using a AP1200 dual mode AP), both types of radios must participate in a Client Walkabout operation to generate location data. Data collected using the 11b clients during a Client Walkabout *cannot be used* for 11a network planning. You can mix the two types of clients together in the same Client Walkabout procedure, but you must collect the Client Walkabout data using both types of clients.
- To delete the current client walkabout data, use the Manage Data tab (see [Managing RM Data, page 13-81](#)).

To minimize the time it takes to calculate the radio parameters, try to use these guidelines when performing the walkabout:

- Walk around the proximity of each AP for which you want coverage for approximately 2 minutes. At a rate of capturing one walkabout location every 10 seconds, this will yield about 12 walkabout locations over a 2-minute period. For a floor that contains 10 APs, this translates to a 20-minute walkabout that covers the perimeter of the floor as well as the areas between different APs.
- If you use the Location Manager's RM Assisted Wizard (see [Using the Location Manager Assisted Site Survey Wizard, page 13-17](#)), you can also see the walkabout results in a table that includes each AP and the number of walkabout locations that can hear that AP. If a location can hear multiple APs,

it will be counted multiple times, once per AP. Therefore, the sum of the total location numbers across all selected APs may be (and almost always is) larger than the total number of actual walkabout locations.

- You can run Assisted Configuration either on a per-building or per-floor basis. You will usually get better channel combinations if you run Assisted Configuration for an entire building.
- A longer walkabout will generate more location data. Although collecting more location samples can improve the parameter generation results, it will also increase the number of computations. For a floor consisting of the 10 APs described above, a WLSE takes 10 to 12 minutes or less to complete the parameter generation process—*without* other jobs, such as inventory, configuration, discovery, or other Radio Manager tasks running simultaneously.

Related Topics

- [Understanding Client Walkabouts, page 13-54](#)
- [Running the Walkabout, page 13-64](#)

Viewing Client Walkabout Jobs

Use the default Client Walkabout screen to view client walkabout jobs.



Note

Your login determines whether you can use this procedure.

Before You Begin

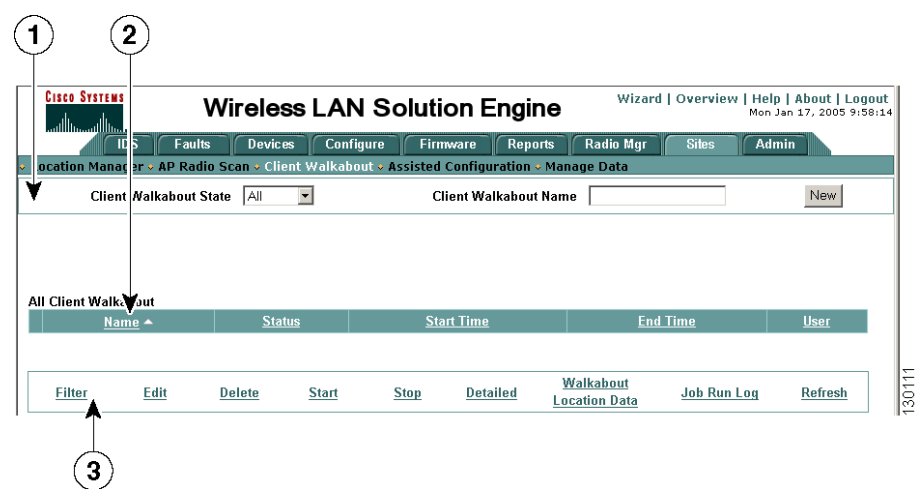
Before you can view the list of client walkabout jobs, you must:

- Satisfy the Client Walkabout prerequisites (see [Guidelines for Running a Client Walkabout, page 13-55](#)).
- Create at least one client walkabout job (see [Creating a New Client Walkabout, page 13-61](#)).

Procedure

-
- Step 1** Select **Sites > Client Walkabout**. The Client Walkabout screen appears.

Figure 13-10 Sample Client Walkabout Screen



1	Client walkabout state selection list
2	List of walkabouts
3	Walkabout management buttons

Step 2 From the Client Walkabout State list, select the type of walkabout you want to view (Running or All). The window refreshes and the walkabouts are displayed.

Field	Description
Name	The client walkabout name.
Status	The status of the walkabout.
Last Run Started	The time the last run of this client walkabout was started.
Last Run Stopped	The time the last run of this client walkabout was stopped.
Owner	The user who last edited the job.

Step 3 From this window, you can use the walkabout management buttons (see [Figure 13-10](#)) to manage your client walkabout jobs (see [Managing Client Walkabout Jobs](#)).

Related Topics

- Guidelines for Running a Client Walkabout, page 13-55
- Sorting Table Data, page 1-13

Managing Client Walkabout Jobs

The buttons below the table of client walkabout jobs (see [Viewing Client Walkabout Jobs, page 13-57](#)) allow you to manage these jobs.


Note

Your login determines whether you can use these procedures.

Before You Begin

Before you can manage client walkabout jobs, you must:

- Satisfy the Client Walkabout prerequisites (see [Guidelines for Running a Client Walkabout, page 13-55](#)).
- Create at least one client walkabout job (see [Creating a New Client Walkabout, page 13-61](#)).

Procedure

- Step 1** Select **Sites > Client Walkabout**. The Client Walkabout screen appears (see [Figure 13-10 on page 13-58](#)).
- Step 2** From the Client Walkabout State list, select the type of walkabout you want to manage (Running or All). The screen refreshes to show the corresponding jobs.


Note

Client walkabout jobs created using the Assisted Site Survey Wizard cannot be edited or run using the **Sites > Client Walkabout** tab. To manage these jobs, see [Using the Location Manager Assisted Site Survey Wizard, page 13-17](#).

- Step 3** Click the radio button for the job you want to manage, then click one of the buttons that appear after the list of client walkabouts:
- **Filter**—This button displays a limited set of client walkabouts, making it easier to search for a particular walkabout by name. The filter remains in effect until the page is refreshed.


Note

You can use % as a wildcard: for example, entering %name% displays all the walkabouts that contain the word “name.”

- **Edit**—Allows you to edit previously-created walkabouts.
- **Delete**—Deletes the selected walkabout from the displayed list of previously-created walkabouts. Walkabouts that are running cannot be deleted.
- **Start**—Starts the selected client walkabout.
- **Stop**—Stops the walkabout that is currently running.
- **Detailed**—Allows you to view the details of the selected client walkabout.

The Client Walkabout Details window shows the following information for each job:

Field	Description
Name	Name of the walkabout.
Description	Walkabout description, if any.

Field	Description
Power Mode	AP power setting selected for the walkabout.
Max. Power	The value of the AP power setting. This field is populated only if you entered a value in Use No More Than __ mW (see Enter Walkabout Options, page 13-63).
Selected APs	Names of the AP devices selected for the walkabout.
Client MAC Address	The list of client MAC addresses to be used during the walkabout.
Status	The status of the walkabout.
Last Run Started	The time the last run of this client walkabout was started.
Last Run Stopped	The time the last run of this client walkabout was stopped.

- **Walkabout Location Data**—Allows you to view the AP locations collected during a client walkabout job.

**Note**

AP location information is available only for the *most recently completed* walkabout. If a new walkabout job is in progress, this information is not available for the latest completed walkabout.

The Client Walkabout Details window shows the following information:

Field	Description
AP Name	The name of the access point
IP Address	The IP address for that access point.
Number of Location Data	The number of location data points collected for that access point.

- **Job Run Log**—Use this button to view the run log for a selected walkabout (see [Viewing Client Walkabout Run Logs, page 13-65](#)).
- **Refresh**—Allows you to refresh the list of walkabouts to make sure you are looking at the latest information.

Related Topics

- [Understanding Client Walkabouts, page 13-54](#)

Creating a New Client Walkabout

**Note**

Your login determines whether you can use this procedure.

Before You Begin

Before you can run a client walkabout, you must satisfy the Client Walkabout prerequisites (see [Guidelines for Running a Client Walkabout, page 13-55](#)).

Procedure

Step 1 Select **Sites > Client Walkabout**.

Step 2 Click **New**.

The window refreshes with the Client Walkabout menu in the left pane and the Client Walkabout Name dialog box in the right pane.

**Note**

Clicking on any subtab before you have saved your entries in the Job Creation window will reset the window and you will lose all the information you entered.

Step 3 Select the following numbered choices in the left pane to create a client walkabout:

**Note**

All these steps must be completed, but do not have to be done in order.

1. **Name**—See [Name the Walkabout, page 13-61](#).

2. **Select AP**—See [Select the APs, page 13-62](#).

3. **Filter By PHY**—See [Select Radio Types, page 13-62](#)

4. **Enter Client MAC**—See [Enter Client MAC Addresses, page 13-63](#)

5. **Options**—See [Enter Walkabout Options, page 13-63](#)

6. **Finish**—See [Finish Creating the Walkabout, page 13-63](#)

Step 4 Run the client walkabout (see [Running the Walkabout, page 13-64](#)).

Name the Walkabout

Procedure

Step 1 From the menu in the left pane, click **Name**.

Step 2 Enter the following data:

Field	Description
Job Name	Enter a unique name for the walkabout. To make each job easy to identify, consider including the floor number or a similar identifier in the job name. For additional naming convention guidelines, see Appendix B, “Naming Guidelines.”
Description	Enter a description of the walkabout. For guidelines on entering descriptions, see Appendix B, “Naming Guidelines.”

Step 3 Go to the next step, [Select the APs](#).

Select the APs

Procedure

Step 1 From the menu in the left pane, click **Select AP**. All managed devices are listed in the Device selector in the middle pane.

Step 2 Select the APs you want to include in the job (see [Using the Device Selector, page 1-12](#)).



Note In each walkabout job, include only the APs on that floor (see [Guidelines for Running a Client Walkabout](#)).

Step 3 Go to the next step, [Select Radio Types](#).

Select Radio Types

Procedure

Step 1 From the menu in the left pane, click **Filter By PHY**.

Step 2 Select the type of 802.11 radio that will perform the client walkabout. By default, both options (11a and 11b/11g) are selected.



Note Only radios of the selected types will take part in the walkabout. If a selected AP has no interfaces of the desired radio types, this is noted in the Job Run Log.

Step 3 Go to the next step, [Enter Client MAC Addresses](#).

Enter Client MAC Addresses

Procedure

-
- Step 1** From the menu in the left pane, click **Enter Client MAC**.
- Step 2** Enter the 802.11 MAC addresses for up to five clients, or select up to five MAC addresses from the Most Recent pulldown list. These are the clients that will move around during the walkabout.



Note Entering a MAC address that consists of more than 12 characters will generate an error message.

- Step 3** Go to the next task, [Enter Walkabout Options](#).
-

Enter Walkabout Options

During a walkabout, the transmit power in the APs is increased so that the power required to cover the edges of the WLAN can be determined. Use this option to reset the maximum transmit power level used by the APs.

Procedure

-
- Step 1** From the menu in the left pane, click **Options**.
- Step 2** Select the AP power setting.
- You can choose to enter a lower power setting when, for example, the default power level might affect a neighboring network.
- Step 3** Go to the next task, [Finish Creating the Walkabout](#).
-

Finish Creating the Walkabout

Before selecting this option, you must name the walkabout, select the devices, enter the client MAC addresses, and choose the AP power setting option.

Procedure

-
- Step 1** From the menu in the left pane, click **Finish** to save your settings. The Finish dialog appears.
- Step 2** Click **Save** to add the walkabout to the list of client walkabout jobs.



Note If a warning message appears saying that WLSE server is ahead of or behind your local time, see [Understanding Time Discrepancy Problems in Job Scheduling, page 1-11](#).

The screen refreshes and the Client Walkabout Summary window shows the following information:

Field	Description
Name	Name of the walkabout.
Description	Walkabout description, if any.
Power Mode	AP power setting selected for the walkabout.
Maximum Power	The value of the AP power setting. This field is populated only if you entered a value in Use No More Than __ mW (see Enter Walkabout Options, page 13-63).
Devices	Names of the AP devices selected for the walkabout.
Client MAC Address	The list of client MAC addresses to be used during the walkabout.

Step 3 Run the walkabout (see [Running the Walkabout, page 13-64](#)).

Running the Walkabout

When you start a client walkabout, the walkabout job starts immediately and continues until you stop the procedure. Only one client walkabout job can be active at any time.



Note

The Client Walkabout feature temporarily degrades wireless LAN service, which might affect client associations. You should run a walkabout job during off-hours to minimize any disruptions to the network.

Before You Begin

Before you can run a client walkabout, you must create a client walkabout job (see [Creating a New Client Walkabout, page 13-61](#)).

Procedure

Step 1 Take the client (typically a laptop) to the area where the walkabout will be run.

Step 2 Select **Sites > Client Walkabout**. A list of the current Client Walkabout jobs appears.



Note

Client walkabout jobs created using the Assisted Site Survey Wizard cannot be run using the **Sites > Client Walkabout** tab. To manage these jobs, see [Using the Location Manager Assisted Site Survey Wizard, page 13-17](#).

Step 3 Select the name of the client walkabout job that you want to run from the list.

Step 4 Click **Start**.

Step 5 To set the coverage area, walk the client (the laptop) around the area (see [Guidelines for Running a Client Walkabout, page 13-55](#)).

- Step 6** When you have finished collecting the data, *stop the walkabout*. Select the walkabout job name from the list and click **Stop**.



Note The client will continue taking measurements if you do not explicitly stop the process.

- Step 7** To view the results of the walkabout:
- Click **Detailed** to view walkabout details (see [Managing Client Walkabout Jobs, page 13-59](#).)
 - Click **Walkabout Details** to view the AP locations collected during a walkabout (see [Managing Client Walkabout Jobs, page 13-59](#)).
 - Use the Location Manager to view the results of the walkabout job (see [Managing Your WLAN Radio Environment by Sites, page 13-1](#)).
- Step 8** After the client walkabout has completed successfully, you are ready to generate the radio parameters and configure your APs (see [Using Assisted Configuration, page 13-71](#)).

Viewing Client Walkabout Run Logs

Use the Job Run Log button to view the run log for a selected job. The job run log displays information about running and completed AP Radio Scan jobs.

Before You Begin

Before you can view a client walkabout run log, you must create and run a client walkabout job (see [Creating a New Client Walkabout, page 13-61](#) and [Running the Walkabout, page 13-64](#)).

Procedure

- Step 1** Select **Sites > Client Walkabout**. The list of Client Walkabout jobs appears.
- Step 2** Select a job from the list and click **Job Run Log**.
- The Job Runs table appears in a separate browser window. This table contains the following information for each run:

Field	Description
Select Run	Select this button to see the details for that run. The details for the selected job run appear below the list of runs for that job.
Job Start Time	The time the job started.
Job End Time	The time the job ended.
Job Status	The status of the job.
Percent Complete	The percent of the job that completed.

The job run log appears below this table.

- Step 3** To view the details for a different job run, select another run from the Job Runs table and click **Job Run Log**.
-

Generating Radio Parameters

You can use selections under the Sites tab to recommend optimal radio transmit power, channel selection, and beacon interval (optional) for each AP, then apply these configuration settings. There are two ways to generate radio parameters and configure your APs:

- **Use Assisted Configuration**
Use this option after you have collected data from a AP radio scanning and a client walkabout.
- **Use the Assisted Site Survey Wizard**
Use this option, which is part of Location Manager, when you want to use a wizard interface to step through AP radio scan, client walkabout, and radio parameter generation (see [Using the Location Manager Assisted Site Survey Wizard](#), page 13-17).

The following topics describe how to use Assisted Configuration to generate radio parameters and configure your APs:

- [Understanding Radio Parameter Generation](#), page 13-66
- [Using Assisted Configuration](#), page 13-71

Related Topics

- [Creating a New Assisted Configuration Task](#), page 13-75
- [Understanding Radio Management](#), page 11-7

Understanding Radio Parameter Generation

The Assisted Configuration function can generate optimal radio parameters for a given selection of APs. The radio parameters include:

- AP operating channel
- AP Tx power level and client power level
- AP beacon interval

Assisted Configuration calculates the optimal radio transmit power, channel selection, and beacon interval (optional), and then applies these configuration settings to the APs, if desired.



Note

If you use Assisted Configuration to change the AP power and channel, the WLSE database will reflect the change within several seconds (using an on-demand inventory on those changed APs to update the data). However, if you change the AP's configuration directly using the AP's interface, WLSE will not know about the change until it performs the next scheduled inventory (the default is 12-hour intervals).

How It Works

Assisted Configuration uses data collected from client walkabouts and AP radio scans to calculate the optimal settings for the APs. The radio parameter generation process (RPG)—and the amount of time this process takes—depends on the following factors:

- The number of managed radios involved.
- The number of allowed channels and power steps involved. The more available radio channels and power steps, the more solutions there are to evaluate and the longer RPG will take to finish.
- The number of radio links each managed radio can hear as its neighbor. This includes other managed neighboring APs but can also include non-managed APs (such as friendly neighbor APs, rogue APs, and non-802.11 interference). The more radio links it has to other devices, the longer it takes RPG to process all of these constraints.

**Note**

Assisted Configuration chooses power and channel settings that will balance the radio transmissions across the entire radio space, not just the managed APs. If surrounding unknown APs are more heavily skewed towards one channel, that channel will likely be minimized within the managed APs. In this case, when viewing the channel plan for managed APs, it may appear that all channels have not been evenly spread across the managed APs. This behavior can be overridden by selecting the option to ignore unknown radios from the constraints selection page. In this case the RPG algorithm will make its channel selections based only on managed APs.

- The number of walkabout points (actual or generated). If a walkabout is performed, RPG examines only the locations collected during the walkabout sessions. If no walkabout is performed, walkabout locations are automatically generated. The number of generated walkabout locations is dependent on the floor size. RPG ensures that each walkabout (actual or generated) point has adequate coverage and throughput.
- The areas of coverage. The larger the areas to be covered, the more data points RPG will check. (This directly impacts the generated walkabout points.)
- The selected radio bands. RPG runs 11a (5GHz) and 11b/11g (2.4GHz) bands separately. If you choose both bands, RPG will separate them internally.
- The number of simultaneous jobs. RPG uses a significant amount of the WLSE CPU, so simultaneous jobs will greatly impact the completion time of the RPG process.

Data Produced

Assisted Configuration recommends optimal radio transmit power, channel selection, and beacon interval (optional) for the managed APs.

Related Topics

- [Analyzing and Comparing Radio Parameter Generation Results, page 13-67](#)
- [Using Assisted Configuration, page 13-71](#)
- [Creating a New Assisted Configuration Task, page 13-75](#)
- [Using the Location Manager Assisted Site Survey Wizard, page 13-17](#)

Analyzing and Comparing Radio Parameter Generation Results

You can analyze and compare the results generated by the WLSE Radio Parameter Generation algorithm against your current radio plan by using WLSE tests.

The goal of the WLSE radio parameter generation algorithm is to recommend a radio plan whose performance is at least 90% of the best-case plan. Due to limited CPU resources, we do not aim for the best radio plan because the time it takes to find the absolute best solution grows exponentially as the number of APs increases.

**Note**

The following tests can be performed on WLSE 2.11 or later. It is not recommended that you run this test on an earlier version of WLSE.

[Table 11](#) shows the four tests you need to run. By running these four tests, you will have the necessary data to compare the WLSE-recommended radio parameters against your current radio plan.

Table 11 *Test Cases for Evaluating Radio Parameter Generation Results*

Test Name	Client Walkabout Data Included?	Method of Configuration Radio Plan Configuration
Case_Manual	No	Manually
Case_Auto	No	Automatically by WLSE
Case_CWA_Manual	Yes	Manually
Case_CWA_Auto	Yes	Automatically by WLSE

Each test case gives you a combined score, also called a combined metric, which is a mathematical quantity that takes both data capacity (or data throughput) and radio coverage into consideration. A higher combined score represents a better radio plan.

If you use a non-Cisco site survey tool, that tool most likely collects location data similar to (or more detailed than) a client walkabout. To accurately compare the data, we recommend you perform all four tests listed in [Table 11](#).

Prerequisites for Running Test Cases

Before performing any of the tests you must:

1. Configure your network for radio management (see [Getting Started with Sites, page 13-2](#)).

**Note**

Be sure that the community string you are using provides write access. To run AP Radio Scan, you *must* have SNMP write access. Most other WLSE functions only require read access.

2. Define the location elements (buildings and floors) and place the APs on the floor images (optional, but recommended—see [Setting Up Location Manager, page 13-3](#), [Adding Floors to Location Manager, page 13-9](#), and [Adding Devices to Floors, page 13-14](#)). If necessary, edit the antenna information also.
3. Run AP Radio Scan (see [Guidelines for Running AP Radio Scans, page 13-45](#)).
4. Perform a Client Walkabout in hard-to-read areas or potential black hole areas (see [Guidelines for Running a Client Walkabout, page 13-55](#)). You can skip this if you are running the Case_Manual and Case_Auto tests only.
5. Navigate to **Sites > Assisted Configuration**.

Running the Case_Manual Test

The Case_Manual test evaluates the manually configured radio plan without client walkabout data.

-
- Step 1** Select **Sites > Assisted Configuration**, create a new job called *Case_Manual*, then select **New**.
The job creation menu appears. You can enter a description for the job.
- Step 2** Select devices to include in the new job.
- Step 3** Select the Radio Type in the Filter by PHY Type screen.
- Step 4** Complete the Constraints and Goals screen as follows:
- Click **Override Default Values** to override the voice or data profiles that you entered in Location Manager (see [Entering Building Information, page 13-4](#)).
 - Select the Service Type **Data**.
 - Select **Apply Constraints to Individual APs** and select an AP from the list.
 - For channel set, select **Custom** and enter the channel number for the AP.
 - For Minimum and Maximum Transmit Power, enter the same power level for which the AP is currently operating.
 - Deselect **Enable Black Hole Mitigation**.
 - Deselect **Ignore Rogue APs and Friendly APs when calculating Radio Parameters**.
 - Select **Ignore Walkabout Location Data when calculating Radio Parameters**.
- Step 5** Click **Calculate Parameters**, then click **Calculate**.
After successfully completing the RGP calculations, WLSE automatically displays the RPG results. The results list the channel and power setting for each AP, and the estimated data throughput. The channel and power setting should be the same as those you entered.
- Step 6** Select **Sites > Assisted Configuration**, select the *Case_Manual* job, then click **Run Log**. The RM Assisted Configuration Run Log window opens. Check the combined score in RPG Result and write down the value for the combined score for future reference.
-

Running the Case_Auto Test

The Case_Auto test allows WLSE to configure a radio plan without any client walkabout.

-
- Step 1** Select **Sites > Assisted Configuration**, create a new job called *Case_Auto*, then select **New**.
- Step 2** Select devices to include in the new job.
- Step 3** Select Radio Type in the Filter by PHY Type screen.
- Step 4** Complete the Constraints and Goals screen as follows:
- Click **Override Default Values** to override the voice or data profiles that you entered in Location Manager (see [Entering Building Information, page 13-4](#)).
 - Select the Service Type **Data**.
 - Deselect **Ignore Rogue APs and Friendly APs when calculating Radio Parameters**.
 - Select **Ignore Walkabout Location Data**.
 - Deselect **Enable Black Hole Mitigation**.
 - Keep the default values for all other fields.
- Step 5** Click **Calculate Parameters**, then click **Calculate**.

After successfully completing the RGP calculations, WLSE automatically displays the RPG results. The results list the channel and power setting for each AP, and the estimated data throughput.

- Step 6** Select **Sites > Assisted Configuration**, select the *Case_Auto* job, then click **Run Log**. The RM Assisted Configuration Run Log window opens. Check the combined score in RPG Result and write down the value for the combined score for future reference.
-

Running the Case_CWA_Manual Test

The Case_CWA_Manual test evaluates the manually configured radio plan with client walkabout.

- Step 1** Select **Sites > Assisted Configuration**, create a new job called *Case_CWA_Manual*, then select **New**.
- Step 2** Select devices to include in the new job.
- Step 3** Select Radio Type in the Filter by PHY Type screen.
- Step 4** Complete the Constraints and Goals screen as follows:
- Click **Override Default Values** to override the voice or data profiles that you entered in Location Manager (see [Entering Building Information, page 13-4](#)).
 - Select the Service Type **Data**.
 - Select **Apply Constraints to Individual APs** and select an AP from the list.
 - For channel set, select **Custom** and enter the channel number for the AP.
 - For Minimum and Maximum Transmit Power, enter the same power level for which the AP is currently operating.
 - Deselect **Ignore Rogue APs and Friendly APs when calculating Radio Parameters**.
 - Do *not* select **Ignore Walkabout Location Data**. You want to include walkabout data in the calculation.
 - Deselect **Enable Black Hole Mitigation**.
 - Click **Calculate Parameters**, then click **Calculate**.

After successfully completing the RGP calculations, WLSE automatically displays the RPG results. The results list the channel and power setting for each AP, and the estimated data throughput.

- Step 5** Select **Sites > Assisted Configuration**, select the *Case_CWA_Auto* job, then click **Run Log**. The RM Assisted Configuration Run Log window opens. Check the combined score in RPG Result and write down the value for the combined score for future reference.
-

Running the Case_CWA_Auto Test

The Case_CWA_Auto test evaluates the manually configured radio plan with client walkabout.

- Step 1** Select **Sites > Assisted Configuration**, create a new job called *Case_CWA_Auto*, then select **New**.
- Step 2** Select devices to include in the new job.
- Step 3** Select Radio Type in the Filter by PHY Type screen.
- Step 4** Complete the Constraints and Goals screen as follows:

- Click **Override Default Values** to override the voice or data profiles that you entered in Location Manager (see [Entering Building Information, page 13-4](#)).
- Select the Service Type **Data**.
- Deselect **Ignore Rogue APs and Friendly APs when Calculating Radio Parameters**.
- Do *not* select **Ignore Walkabout Location Data**.
- Deselect **Enable Black Hole Mitigation**.
- Keep the default values for all other fields.

Step 5 Click **Calculate Parameters**, then click **Calculate**.

After successfully completing the RGP calculations, WLSE automatically displays the RPG results. The results list the channel and power setting for each AP, and the estimated data throughput.

Step 6 Select **Sites > Assisted Configuration**, select the Case_CWA_Auto job, then click **Run Log**. The RM Assisted Configuration Run Log window opens. Check the combined score in RPG Result and write down the value for the combined score for future reference.

Comparing Test Results

You can now evaluate and compare the performance of the different radio plans based on the combined score, as shown in [Table 12](#).

Table 12 *Sample Radio Parameter Generation Test Results*

Test Name	Client Walkabout Data Included?	Method of Configuring the Radio Plan	Combined Score
Case_Manual	No	Manually	1.29789
Case_Auto	No	Automatically by WLSE	2.74457
Case_CWA_Manual	Yes	Manually	1.26660
Case_CWA_Auto	Yes	Automatically by WLSE	2.67253

[Table 12](#) shows that the WLSE recommendation is better than the manually configured radio plan because the combined score of the recommended radio plan is higher than that of the manually configured plan.

If you run the tests with the radio plan (channel and power) based on a third-party site planning/survey tool, you can compare its radio performance (combined score) against the RPG recommendation.

Using Assisted Configuration

Use Assisted Configuration to configure your APs. This feature uses the measurement data collected from client walkabouts and AP radio scans. The following topics describe how to run Assisted Configuration:

- [Guidelines for Running Assisted Configuration, page 13-72](#)

- [Viewing Assisted Configuration Tasks, page 13-73](#)
- [Managing Assisted Configuration Tasks, page 13-74](#)
- [Creating a New Assisted Configuration Task, page 13-75](#)

Guidelines for Running Assisted Configuration

Prerequisites

Before you run Assisted Configuration, you must:

1. Run AP Radio Scan on the devices you select for an Assisted Configuration job (see [Guidelines for Running AP Radio Scans, page 13-45](#)).

**Note**

If you delete RM measurement data, you must re-run AP Radio Scan on those devices before running an Assisted Configuration job.

If you have not run (or re-run) AP Radio Scan on the selected devices before running Assisted Configuration, Assisted Configuration will assume no radio links exist for these devices and use the default RM measurement data. In that case, *the recommended radio settings generated by Assisted Configuration will not be optimum.*

2. Perform a Client Walkabout (optional but recommended) or add the device information in Location Manager (see [Guidelines for Running a Client Walkabout, page 13-55](#) and [Managing Your WLAN Radio Environment by Sites, page 13-1](#)).

Tips

- To get optimal channel settings, run Assisted Configuration on a *per building* basis. That is, include all APs in one building in a single Assisted Configuration task.
- Assisted Configuration runs on a per-floor basis (2-D perspective).
- Instead of using Assisted Configuration, you can use the Assisted Site Survey Wizard (part of Location Manager) to use a wizard interface to step through AP radio scan, client walkabout, and radio parameter generation (see [Using the Location Manager Assisted Site Survey Wizard, page 13-17](#)).
- Use the WLSE to make any configuration changes. If you must make a manual change to the AP, run another inventory job to update the WLSE database.
- You can push the parameters recommended by Assisted Configuration to the APs.

**Caution**

If you use the AP's interface to make a change to the AP and an AP radio scan is run before WLSE's next inventory, WLSE will remember the *old setting*, set the new channel for the AP radio scan, then *restore the old setting*. This overwrites the changes done manually on the AP.

Related Topics

- [Understanding Radio Parameter Generation, page 13-66](#)
- [Analyzing and Comparing Radio Parameter Generation Results, page 13-67](#)

Viewing Assisted Configuration Tasks



Note

Your login determines whether you can use this option.

Before You Begin

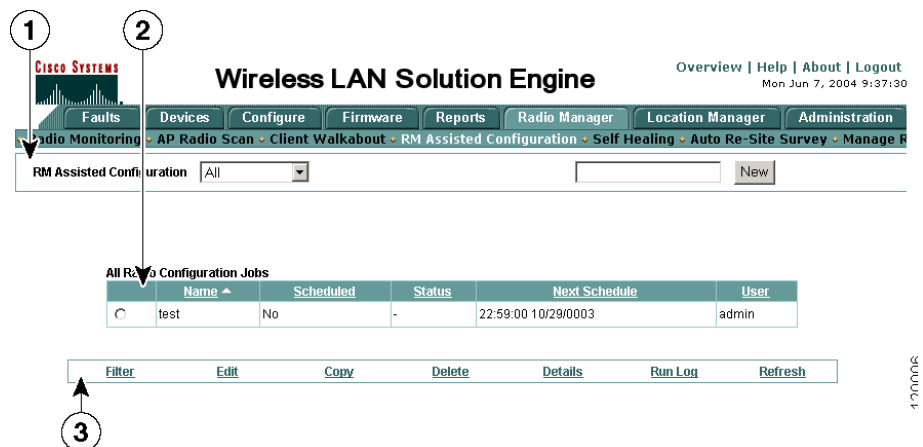
Before you can view the assisted configuration tasks, you must:

- Satisfy the Assisted Configuration prerequisites (see [Guidelines for Running Assisted Configuration](#), page 13-72).
- Create at least one assisted configuration task (see [Creating a New Assisted Configuration Task](#), page 13-75).

Procedure

Step 1 Select **Sites > Assisted Configuration**. The Assisted Configuration screen appears.

Figure 13-11 Sample Assisted Configuration Screen



1	Radio configuration job selection list
2	List of radio configuration jobs
3	Job management buttons

Step 2 From the pulldown menu, select the type of configuration tasks you want to view:

- **All**—Lists all configuration tasks
- **Planning**—Lists configuration tasks whose constraints are still being calculated by the Assisted Configuration engine.



Note

A configuration job stays in the Planning state if something disrupts the network, for example, a server crashes or is restarted.

- **Unscheduled**—Lists all configuration tasks that have not been scheduled

- **Scheduled**—Lists all configuration tasks that have been scheduled
- **Completed**—Lists all completed configuration tasks

The screen refreshes to show you details about the specified configuration tasks. By clicking on the corresponding column heading, you can sort the configuration tasks by name, status, next schedule, or owner.

- Step 3** From this window, you can manage existing assisted configuration tasks (see [Managing Assisted Configuration Tasks, page 13-74](#)).

Managing Assisted Configuration Tasks

The buttons below the list of existing assisted configuration tasks (see [Viewing Assisted Configuration Tasks, page 13-73](#)) allow you to manage these tasks.



Note

Your login determines whether you can use these options.

Before You Begin

Before you can manage the assisted configuration tasks, you must:

- Satisfy the prerequisites for running Assisted Configuration (see [Guidelines for Running Assisted Configuration, page 13-72](#)).
- Create at least one Assisted Configuration task (see [Creating a New Assisted Configuration Task, page 13-75](#)).

Procedure

- Step 1** Select **Sites > Assisted Configuration**. The Assisted Configuration screen appears (see [Figure 13-11 on page 13-73](#)).
- Step 2** From the Assisted Configuration pulldown menu, select the configuration tasks you want to edit. The screen refreshes to show the corresponding tasks.



Note

Parameter generation jobs created using the Assisted Site Survey Wizard cannot be edited or run using the **Sites > Assisted Configuration** tab. To manage these jobs, see [Using the Location Manager Assisted Site Survey Wizard, page 13-17](#).

- Step 3** Click on the radio button next to the task you want to manage, then click one of the buttons that appear after the lists of tasks:
- **Filter**—This button displays a limited set of radio configuration jobs, making it easier to search for a particular job by name. The filter remains in effect until the page is refreshed.



Note

You can use % as a wildcard: for example, entering %name% displays all the walkabouts that contain the word “name.”

- **Edit**—Allows you to edit assisted configuration tasks that were previously created.

- **Copy**—Allows you to create a new assisted configuration task that is similar to a previously created configuration task, you can make a copy of an existing configuration task and then make modifications to the copied task.
- **Delete**—Allows you to delete assisted configuration tasks that were previously created.
- **Details**—Allows you to view details of selected configuration tasks.
- **Run Log**—Use this button to view the run log for a selected configuration job.
- **Refresh**—Refreshes the list of configuration tasks to make sure you are looking at the latest information. You might also need to refresh the configuration tasks if you have a configuration in the Planning state.

Creating a New Assisted Configuration Task

You can use Assisted Configuration to configure the power level, channel settings, and beacon interval of an AP or a group of APs. Using AP Scan and Client Walkabout data, Assisted Configuration generates optimal values for the radio parameters of a given group of APs.



Note

Your login determines whether you can use this option.

Before You Begin

Before you can create a new assisted configuration task, you must satisfy the Assisted Configuration prerequisites (see [Guidelines for Running Assisted Configuration, page 13-72](#)).

Procedure

Step 1 Select **Sites > Assisted Configuration**. The assisted configuration information appears.



Note

Clicking on any subtab (for example, Radio Monitoring or Client Walkabout) before you have saved your entries in the Jobs window will cause the window to reset and you will lose all the information you entered.

Step 2 Enter a task name in the blank field and click **New**. The screen refreshes with the Job Name dialog box in the right pane, and the Task Creation job in the left pane.

Step 3 Select the following numbered choices in the left pane to create a new assisted configuration task:

1. **Name**—See [Naming the Configuration Task, page 13-76](#).
2. **Select Devices**—See [Selecting Devices, page 13-76](#).
3. **Filter by PHY**—[Filtering by Radio Type, page 13-77](#).
4. **Constraints/Goals**—See [Assigning Constraints and Goals, page 13-77](#).
5. **Calculate Parameters**—See [Calculating Parameters, page 13-79](#).
6. **Results**—See [Viewing the Calculated Results, page 13-80](#).
7. **Schedule**—See [Scheduling the Configuration Job, page 13-81](#).

8. **Finish**— See [Finishing the Task, page 13-81](#).

Naming the Configuration Task

Procedure

Step 1 From the menu in the left pane, click **Name**.
The screen refreshes so you can enter information about the new task. You will see the name you entered in the Task Name field.

Step 2 Enter the following information:

Field	Description
Task Name	Enter a unique name for the job. For guidelines on naming jobs, see Appendix B, “Naming Guidelines.”
Description	Enter a description of the job. For guidelines on entering descriptions, see Appendix B, “Naming Guidelines.”

Step 3 Go to the next step, [Selecting Devices](#).

Selecting Devices

Procedure

Step 1 From the menu in the left pane, click **Select Devices**. All managed devices are listed in the Device selector in the middle pane.

Step 2 Select the devices you want to include in the job (see [Using the Device Selector, page 1-12](#)).



Note AP Radio Scan must already have been run on any devices you select.



Note If you have deleted RM measurement data, you must re-run AP Radio Scan on those devices.

Step 3 Go to the next step, [Filtering by Radio Type](#).

Filtering by Radio Type

Procedure

-
- Step 1** From the menu in the left pane, click **Filter By PHY**.
- Step 2** Select the type of 802.11 radio that you want to include in the assisted configuration task.



Note Only radios of the selected types are included in the assisted configuration task. If a selected AP has no interfaces of the desired radio types, this is noted in the job run log.

- Step 3** Go to the next step, [Assigning Constraints and Goals](#).
-

Assigning Constraints and Goals

Procedure

-
- Step 1** Click **Override Defaults** to override the voice or data profiles that you entered in Location Manager (see [Entering Building Information, page 13-4](#)).
- Step 2** Select the Service Type—**Voice** or **Data**.
- Step 3** Select how to apply the constraints:
- **Apply Constraints to All APs**—Applies constraints to all APs that you selected
 - **Apply Constraints to Individual APs** —Allows you to select with APs to apply the constraints to. A list box appears in which you can select the APs on which to apply the constraints.
- Step 4** Select the channel set option:
- **Recommended**—Use the channels Assisted Configuration recommends in the Recommended field.
 - **Custom**—Select the channels from the Custom selection box. You can Ctrl-click to select more than one channel from the selection box.



Note Some channels are not approved for use in specific regulatory domains. [Table 13-13](#) lists the regulatory domains and their valid, approved channel sets.

Table 13-13 Regulatory Domains and Their Approved Channel Sets¹

Radio Type	Regulatory Domain	Approved Channel Set
802.11b/g	FCC (United States)	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
	DOC (Canada)	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
	ETSI	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13
	Spain	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13
	France	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13
	Belgium	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13
	MKK (Japan)	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 (b only)
	Singapore	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13
	Taiwan	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
	Israel	5, 6, 7, 8
	Australia	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
	China	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13
	Korea	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13
802.11a	FCC (United States)	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161
	DOC (Canada)	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161
	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
	Spain	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
	France	36, 40, 44, 48, 52, 56, 60, 64
	Belgium	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
	MKK (Japan)	34, 38, 42, 46
	Singapore	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161
	Taiwan	56, 60, 64, 149, 153, 157, 161
	Israel	36, 40, 44, 48, 52, 56, 60, 64
	Australia	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161
	China	149, 153, 157, 161
	Korea	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 149, 153, 157, 161

1. Not all radios support all approved channel sets listed.

Step 5 If you selected the service type Voice, select a value from the Minimum Required Voice RSSI pulldown list and select the appropriate Voice Data Rates.

Step 6 Enter values for the minimum and maximum transmit powers. You might choose to enter a lower power setting when, for example, the default power level might affect a neighboring network. You must enter a numeric value greater than zero and less than 100.

**Note**

The recommendation is to give WLSE the full range of power settings (that is, 1mW to 100mW) when it generates radio parameters. The minimum and maximum fields are included to handle any special cases that WLSE could not know about. For example, you could have an agreement with a neighboring office that you will not configure an AP higher than 50mW. Or you may have special knowledge about the environment where it is known that an AP should not be configured at less than 5mW. It is these types of cases where the minimum and maximum fields should be changed from something other than the default.

Step 7 Select whether to enable black hole mitigation. If you select this option, Assisted Configuration recommends a beacon interval (which is slightly altered from what the AP is configured to) for the APs. If you do not select the Black Hole Mitigation option, Assisted Configuration displays the beacon interval to which the AP is currently configured.

Step 8 If you want to restrict the data that is used when calculating radio parameters, select one or both of these options:

- Ignore Rogue APs and Friendly APs when calculating Radio Parameters. You might want to use this option if you have an excessive number of radios in your network, for example, 2-3 rogue or friendly radios per available channel.
- Ignore Walkabout Location Data when calculating Radio Parameters. You might want to use this option if your client walkabout data is not up-to-date or is no longer relevant. The calculation generation completes faster by selecting this option, but the result might not be as accurate as when collected data is used in the calculation.

Step 9 Go to the next step, [Calculating Parameters, page 13-79](#).

Calculating Parameters

Procedure

Step 1 From the menu in the left pane, click **Calculate Parameters**. The Calculate Parameters screen appears.

Step 2 Click **Calculate**.

As Assisted Configuration calculates the parameters, a progress bar indicates the progress it is making in its calculations.

**Note**

Depending on the number of APs selected for the job and how much data was collected during Client Walkabout, the calculating parameters step could take a while to complete.

Step 3 To stop the parameter calculation, click **Stop Calculations**.

Step 4 Go to the next step, [Viewing the Calculated Results](#).

Viewing the Calculated Results

Procedure

Step 1 From the menu in the left pane, click **Results**.

After Assisted Configuration calculates the parameters for the assisted configuration job, it displays the calculation results. These results provide the following information:

Field	Description
Name	Name of the AP
Transmit Power	Recommended transmit power for this AP. If the radio type is 11g, the CCK power and OFDM power are also displayed.
Channel	Recommended channel for the AP
Beacon Interval	Recommended beacon interval for the AP. If you did not select the Enable Black Hole Mitigation option, this column displays the value to which the AP is currently configured (see Assigning Constraints and Goals , page 13-77).
Estimated Max Throughput	The estimated maximum megabytes per second that the AP can process. The maximum throughput is an estimated value that is calculated from either: • Data collected from all client walkabouts. • Predicted walkabout data if no walkabouts were performed. Using the walkabout data and the potential RF configuration parameters, an analysis is performed to predict the degree of transmit collisions and contention that may result in the coverage area for each AP, given a predefined ratio of AP-to-client and client-to-AP traffic. The collision and contention values are then applied to the theoretical throughput maximum to come up with the real predicted throughput.

Step 2 To review these results in the Location Manager, click **Preview**.

Step 3 Go to the next step, [Scheduling the Configuration Job](#).

Scheduling the Configuration Job

Procedure

-
Step 1	From the menu in the left pane, click Schedule . The Schedule Assisted Configuration Job screen appears.
Step 2	To start the assisted configuration task immediately, click Run Now .
Step 3	To run the assisted configuration task at a later time, under Run Later, select a Month, Day, Year to run the configuration task. You must also specify the start time by selecting the hour and minute to start the job.
Step 4	Click Write NVRAM on Success to save the configuration to the startup configuration
Step 5	Click Write to Device Specific Settings to save the parameters to the device specific settings. See Managing Device Specific Configurations, page 8-47 .
Step 6	Go to the next step, Finishing the Task .
-

Finishing the Task

Procedure

-
Step 1	From the menu in the left pane, click Finish .



Note	If a warning message appears saying that WLSE server is ahead of or behind your local time, see Understanding Time Discrepancy Problems in Job Scheduling, page 1-11 .
-

The Done form appears indicating that the job has completed or has been scheduled (if you scheduled it to run later).

Related Topics

- [Viewing the Radio Configuration Parameters, page 10-16](#)
- [Analyzing and Comparing Radio Parameter Generation Results, page 13-67](#)

Managing RM Data

You can use Manage Data to delete previously-collected radio location measurements, including links and path loss data.

Use this feature only under these circumstances:

- When new APs have been added.
- After any major reconfiguration of a floor (changes in the physical environment).
- If you notice any inconsistencies in reports.

When you run a new AP radio scan, the radio location information for the selected APs is automatically deleted.

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **Sites > Manage Data**.

Step 2 Choose the radio location measurements to be deleted:

- **Delete Radio Measurements**—Deletes the AP radio locations collected during AP radio scans and radio monitoring.

**Note**

When you choose this option, *all features that rely on AP radio scans are affected*. After deleting the radio measurement data, for example, you must re-run AP Radio Scan on the selected devices before you can use Assisted Configuration, self healing, rogue AP detection, or the Location Manager coverage displays.

- **Delete Walkabout Measurements**—Deletes the client radio locations collected during client walkabouts.

**Note**

When you choose this option, *all data collected during the client walkabouts is removed*.

Step 3 From the menu in the left pane, click **Select Devices**. All managed devices are listed in the Device selector in the middle pane.

Step 4 Select the devices (see [Using the Device Selector, page 1-12](#)). Only measurements for the selected devices will be deleted.

Step 5 From the menu in the left pane, click **Filter By PHY**.

Step 6 Select the 802.11 radio types. Only measurements for radios of the selected types will be deleted.

Step 7 From the menu in the left pane, click **Finish**. The data for the selected devices and radio types is deleted immediately.

Related Topics

- [Using AP Radio Scans to Collect RM Data, page 13-43](#)
- [Using Client Walkabouts to Collect RM Data, page 13-54](#)
- [Using Radio Monitoring to Collect RM Data, page 12-1](#)



Using the Intrusion Detection System

Use the WLSE Intrusion Detection System (IDS) tab to display intrusion detection information for devices in your network, manage IDS settings, and set up IDS notifications. Using the WLSE Intrusion Detection System features, you can:

- Detect unknown access points. See [Detecting Rogue APs, page 14-12](#).
- Detect and suppress the switch ports of rogue APs. See [Detecting Switch Port Locations and Suppressing Ports, page 14-30](#).
- Detect ad-hoc networks. See [Detecting Ad-Hoc Networks, page 14-37](#).
- Detect non-802.11 interference. See [Detecting Interference, page 14-43](#).
- Detect excessive management frame transmissions. See [Detecting Excessive Management Frame Transmissions, page 14-47](#).
- Implement management frame protection. See [Detecting Management Frame Protection Faults, page 14-52](#).
- Detecting unregistered clients. See [Detecting Unregistered Clients, page 14-58](#).
- Detect authentication and protection attacks. See [Detecting Authentication and Protection Attacks, page 14-63](#).

Getting Started with IDS

Before you can use the features provided by the Intrusion Detection System, you should configure your network to manage your radio environment.



Note

If you choose to disable radio management, only one Intrusion Detection System subtab, **Manage Remaining IDS Settings**, is displayed (see [Using the Manage Remaining IDS Settings Subtab, page 14-11](#)). For information about the faults that will not be generated when Radio Management is disabled, see [Disabled Radio Management Related Faults, page 11-4](#).

Related Topics

- [Using the Manage Remaining IDS Settings Subtab, page 14-11](#)
- [Configuring Your WLAN Radio Environment, page 11-1](#)
- [Enabling and Disabling Radio Management Features, page 11-4](#)

- [Understanding the IDS Subtabs, page 14-2](#)

Understanding the IDS Subtabs

The following sections describe the IDS subtabs:

- [Using the Summary Subtab, page 14-2](#)
- [Using the Faults Subtab, page 14-4](#)
- [Using the IDS Reports Subtab, page 14-5](#)
- [Using the Manage IDS Settings Subtab, page 14-6](#)
- [Using the Manage Rogues Subtab, page 14-11](#)
- [Using the Manage Network-Wide IDS Settings Subtab, page 14-11](#)
- [Using the Notification Settings Subtab, page 14-12](#)

Using the Summary Subtab

The Intrusion Detection System Summary allows you to view a summary of all intrusions that have been detected.

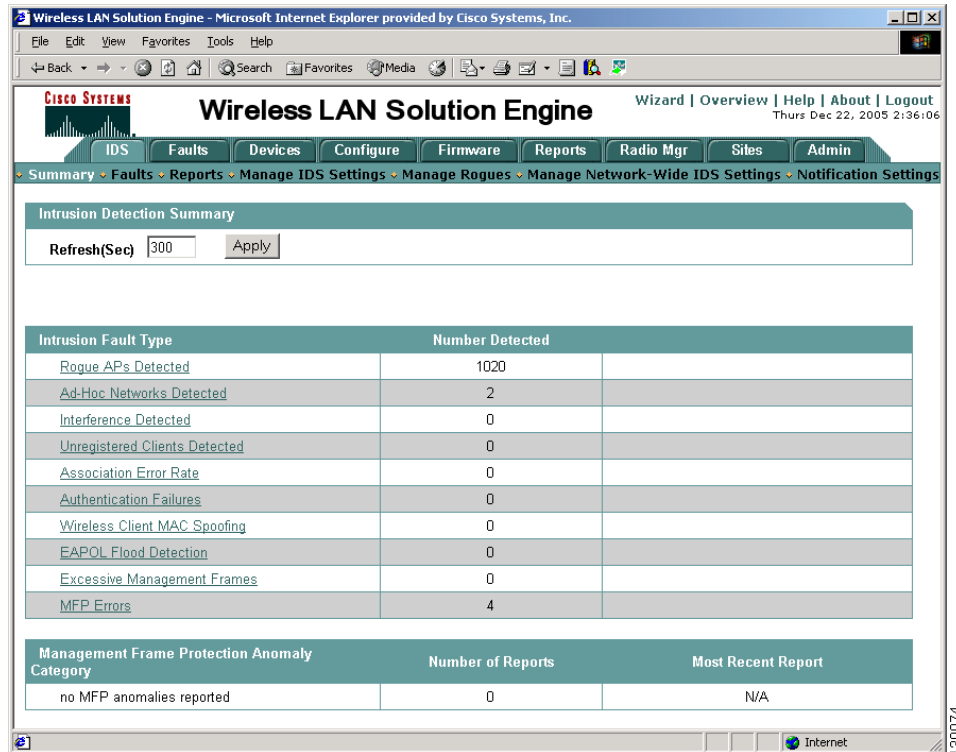
**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **IDS > Summary**. The Intrusion Detection Summary window appears.

Figure 14-1 Sample IDS Summary Screen



Step 2 The Intrusion Fault Type table summarizes the number of occurrences of each of the IDS fault types. You can use this table to acknowledge, unacknowledge, or clear selected faults or to view the details of a selected fault.

To display the faults of a particular type, select one of the following fault types from the Intrusion Fault Type table:

- Rogue APs Detected
- Ad-Hoc Networks Detected
- Interference Detected
- Unregistered Clients Detected
- Association Error Rate
- Authentication Failures
- Wireless Client MAC Spoofing
- EAPOL Flood Detection
- Excessive Management Frames
- MFP Errors

The Faults Summary table appears, displaying only the data for that type of fault. For information about the contents of this table, see [Display Faults Table, Table 3-2 on page 3-5](#).

**Note**

For an explanation of the faults, in the online help click **Troubleshooting**, or on Cisco.com see the Fault Description Table in the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.13*.

- Step 3** The Management Frame Protection Anomaly Category panel summarizes the number of MFP reports that are reporting different MFP errors.

Related Topics

- [Clearing Summary Table Faults, page 3-6](#)
- [Displaying Rogue AP Faults, page 14-19](#)
- [Displaying Ad-Hoc Network Faults, page 14-39](#)
- [Displaying Interference Faults, page 14-46](#)
- [Displaying EMF Detection Faults, page 14-49](#)
- [Displaying Management Frame Protection Faults, page 14-54](#)
- [Displaying Unregistered Client Faults, page 14-60](#)
- [Displaying Authentication and Protection Attack Faults, page 14-79](#)

Using the Faults Subtab

The **IDS > Faults** option displays only the IDS (Intrusion Detection System) faults. To display all fault information, select **Faults > Display Faults**.

**Note**

For an explanation of the faults, in the online help click **Troubleshooting**, or on Cisco.com see the Fault Description Table in the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.13*.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Faults**. The Fault Summary table appears. This table displays device fault information for all intrusion detection faults.

You can use this table to acknowledge, unacknowledge, clear selected faults, or view fault details (see [Displaying Faults, page 3-4](#)).

- Step 2** Use the Filter Faults bar to display the faults you want to view (see [Displaying Faults, page 3-4](#)).

**Note**

If no data is displayed in the table, there are no faults for your filtering selection to report.

- Step 3** Click the Description or Timestamp fields for a fault. A new window containing the details for that fault appears. The contents of the window depends on the fault type.

Step 4 To clear a fault, see [Clearing Summary Table Faults, page 3-6](#).

Related Topics

[Clearing Summary Table Faults, page 3-6](#)

Using the IDS Reports Subtab

The Intrusion Detection Reports subtab displays Intrusion Detection information about the devices in your network.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Reports**. The Rogue AP report is displayed.
- Step 2** To view other IDS reports, select the report type from the **Report Name** dropdown list.

The following IDS reports are available:

- Rogue AP Report—see [Viewing Rogue AP Reports, page 14-26](#)
 - Friendly AP Report—see [Viewing Friendly AP Reports, page 14-28](#)
 - EMF Detection Report—see [Viewing EMF Detection Reports, page 14-50](#)
 - Unregistered Client Report—see [Viewing Unregistered Client Reports, page 14-61](#)
 - Ad-Hoc Network Report—see [Viewing Ad-Hoc Network Reports, page 14-41](#)
 - MFP Capabilities Report—see [Viewing MFP Capabilities Reports, page 14-55](#)
 - MFP Events Report—see [Viewing MFP Events Reports, page 14-56](#)
-

Related Topics

- [Using the Basic Report Features, page 10-1](#)
- [Detecting Rogue APs, page 14-12](#)
- [Detecting Ad-Hoc Networks, page 14-37](#)
- [Detecting Excessive Management Frame Transmissions, page 14-47](#)
- [Detecting Management Frame Protection Faults, page 14-52](#)
- [Detecting Unregistered Clients, page 14-58](#)

Using the Manage IDS Settings Subtab

Every device managed by the WLSE has an IDS fault profile (also called a fault setting) assigned to it. IDS fault profiles include threshold values and security policies. You can create an IDS fault profile, customize it, and then assign it to a single device or a group of devices.



Note If you have not assigned a specific profile to a device, it uses the system IDS Default profile. The IDS Default profile can be edited, but cannot be deleted and you cannot change its name.

The **IDS > Manage IDS Settings** tab allows you to:

Task	For More Information, See:
Create a new IDS profile	Creating IDS Fault Profiles, page 14-6
Copy an existing profile to create a new profile	Copying an IDS Fault Profile, page 14-7
Rename an existing profile	Renaming an IDS Fault Profile, page 14-7
Edit an existing profile	Editing an IDS Fault Profile, page 14-8
Delete a profile	Deleting an IDS Fault Profile, page 14-8
View the IDS fault profile summary	Viewing the IDS Fault Profile Summary, page 14-9
Assign an IDS fault profile to one or more devices	Assigning Devices to an IDS Fault Profile, page 14-9

Related Topics

- [Managing Fault Settings, page 3-10](#)
- [Using the Manage Remaining IDS Settings Subtab, page 14-11](#)

Creating IDS Fault Profiles

Use this option to create an IDS fault profile. After you create a new IDS fault profile, you can customize it and then assign it to one or more devices.



Note Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings dialog box appears.
- Step 2** Enter a unique name in the **Name** text box (see [Naming Guidelines, page B-1](#)).
- Step 3** Click **Create New**. The new name appears in the Existing IDS Fault Profiles list.



Note All the settings in the new profile are assigned default values.

- Step 4** Select the name, then click **Edit**. The Editing Profile window appears (see [Editing an IDS Fault Profile, page 14-8](#)).
-

Related Topics

- [Editing an IDS Fault Profile, page 14-8](#)
- [Assigning Devices to an IDS Fault Profile, page 14-9](#)
- [Using the Manage IDS Settings Subtab, page 14-6](#)

Copying an IDS Fault Profile

Use this option to copy an existing IDS fault profile to use as a base for a new profile.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings dialog box appears.
- Step 2** Select the profile you want to copy from the Existing IDS Fault Profiles box.
- Step 3** Click **Create Copy**. A dialog box appears asking you to enter a name for the copy.
- Step 4** Enter a unique name (see [Naming Guidelines, page B-1](#)).
- Step 5** Click **OK**. The new name appears in the Existing IDS Fault Profiles list.
- Step 6** Select the name, then click **Edit**. The Editing Profile window appears (see [Editing an IDS Fault Profile, page 14-8](#)).
-

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Renaming an IDS Fault Profile

Use this option to rename an IDS fault profile.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings dialog box appears.
- Step 2** Select the profile you want to rename from the Existing IDS Fault Profiles box.



Note

You can edit the IDS Default profile, but you cannot delete it or change its name.

- Step 3** Click **Rename**. A dialog box appears asking you to enter a new name.
- Step 4** Enter a unique name (see [Naming Guidelines, page B-1](#)).
- Step 5** Click **OK**. The new name appears in the Existing IDS Fault Profiles list.
-

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Editing an IDS Fault Profile

Use this option to edit an IDS fault profile (including the IDS Default profile).



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings dialog box appears.
- Step 2** Select the profile you want to edit from the Existing IDS Fault Profiles box.
- Step 3** Click **Edit**. The Editing Setting window appears.
- Step 4** Select the policies and thresholds in the left pane that you want to assign to the profile (see [Setting Policies and Thresholds, page 3-14](#)).
-

Related Topics

- [Renaming an IDS Fault Profile, page 14-7](#)
- [Creating IDS Fault Profiles, page 14-6](#)
- [Using the Manage IDS Settings Subtab, page 14-6](#)

Deleting an IDS Fault Profile

Use this option to delete an IDS fault profile.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings dialog box appears.
- Step 2** Select the profile you want to delete from the Existing IDS Fault Profiles box.



Note

You can edit the IDS Default profile, but you cannot delete it or change its name.

- Step 3** Click **Delete**. A window appears asking if you want to delete the profile.

**Note**

Any devices that were assigned the deleted profile will be automatically assigned the IDS Default profile.

Step 4 Click **OK** to delete the profile.

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Viewing the IDS Fault Profile Summary

Use this option to view a summary of the current settings for a particular IDS fault profile.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings dialog box appears.
- Step 2** Select the profile you want to view from the Existing IDS Fault Profiles box.
- Step 3** Click **View Summary**. A window displays the current fault settings and the devices to which this IDS fault profile is assigned.
- Step 4** Click **OK** to close the window.

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Assigning Devices to an IDS Fault Profile

Use this option to assign a single device or a group of devices to a fault profile. Devices can be assigned to only one profile at a time.

If you have not assigned a device to a specific profile, it uses the IDS Default profile.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** To access the windows that allow you to assign devices to a profile:
- From the IDS Fault Settings window, select **IDS > Manage IDS Settings**, select an existing IDS fault profile, then select:
 - **Assign Devices** (located in the top right of the screen under the subtabs).
 - **Assign Devices to <profilename>** (located to the left of the Reset button).

- From any IDS Editing Setting window, select the **Assign Devices** link located at the top right of the window.

The window refreshes with a device selector in the left pane.

- Step 2** To search for devices, use the dialog box in the left pane above the device selector. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** If you know which device or device group you want, use the device selector to select the devices. They are added to the list of Available Devices.
- Step 4** From the list of Available Devices, select the device you want to assign to the profile and click >>. The devices are moved to the Selected Devices list.
- Step 5** Click **Continue**. A confirmation dialog box appears for the device assignment.
- Step 6** Click **OK** to accept the device assignment or **Cancel** to cancel the device assignment.
-

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Setting IDS Policies and Thresholds

Use the IDS settings to activate or deactivate a set of predefined policies for access points and radio interfaces and to set polling and [exception](#) threshold values collected from the devices you are monitoring. The policies and threshold values you set in this window will determine how the faults are displayed in the **IDS > Faults** subtab.

You can set pre-defined policies for general and radio interface-specific settings:

- General IDS settings are applicable to the access point or bridge. They are set on the access point or bridge and are reported on the faults page. For each profile, you can set the following general IDS settings:
 - Unregistered Client—See [Enabling Unregistered Client Detection, page 14-59](#)
 - Excessive Management Frame Detection—See [Setting the Excessive Management Frame Detection Policy, page 14-48](#)
 - Authentication and Protection Attack Detection—See [Enabling Authentication and Protection Attack Detection, page 14-65](#)
- Radio interface-specific settings (see [Setting the Association Error Rate Policy, page 14-73](#)) are applicable only to the radio interface type (11a, 11b, or 11g) on which they are set. They are set on the radio interface and are reported by interface type on the faults page.



Note

Policies (settings) are disabled by default unless otherwise noted.

Using the Manage Remaining IDS Settings Subtab

When Radio Management is disabled, the **IDS > Manage IDS Settings** subtab is replaced with the subtab **Manage Remaining IDS Settings**. This subtab allows you to create policies and thresholds for the IDS monitoring features that can still be used when Radio Management is disabled.

Although they still appear, the following general IDS fault settings are *not* active when Radio Management is disabled:

- Unregistered Client
- Excessive Frame Management
- EAPOL Settings

Other Radio Management related faults (including rogue detection, ad-hoc detection, interference, self healing, and other non-IDS faults) are also either inactive or not displayed when Radio Management is disabled. For more information, see [Enabling and Disabling Radio Management Features, page 11-4](#).

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Using the Manage Rogues Subtab

See [Managing Rogue APs, page 14-24](#).

Using the Manage Network-Wide IDS Settings Subtab



Note

The Rogue, Ad-Hoc, and Interference network-wide settings were moved here from Faults > Manage Network-Wide Settings in the previous release.

You can use the **IDS > Manage Network-Wide IDS Settings** option to set the following network-wide IDS policies:

- Rogue AP Detection—See [Setting the Rogue AP Detection Policy, page 14-16](#)
- Automatic Rogue AP Detection and Suppression—See [Setting the Automatic Rogue AP Suppression Policy, page 14-32](#)
- Automatic Friendly AP to Rogue AP Reclassification—See [Setting the Friendly AP to Rogue AP Reclassification Policy, page 14-18](#)
- Ad-Hoc Network Detection—See [Setting the Ad-Hoc Network Detection Policy, page 14-38](#)
- Interference Detection—See [Setting the Interference Detection Policy, page 14-45](#)
- Management Frame Protection—See [Setting the Management Frame Protection Policy, page 14-53](#)

Using the Notification Settings Subtab

When a fault is detected, the WLSE can send automated notifications in the form of SNMP traps, syslog messages, and email alerts. You can specify multiple recipients for each notification type, and choose to deliver the message using either a plain text or XML format.

To create fault notification targets for IDS traps, syslog messages, and emails, select either of these options:

- **IDS > Notification Settings**
- **Faults > Notification Settings**

For more information about this dialog, see [Notification Settings, page 3-56](#).

Detecting Rogue APs

The following sections will help you understand how and where to use the rogue AP detection feature:

- [Understanding Rogue AP Detection, page 14-12](#)
- [Guidelines for Detecting Rogue APs, page 14-14](#)
- [Setting the Rogue AP Detection Policy, page 14-16](#)
- [Displaying Rogue AP Faults, page 14-19](#)
- [Managing Rogue APs, page 14-24](#)
- [Viewing Rogue AP Reports, page 14-26](#)
- [Viewing Friendly AP Reports, page 14-28](#)

Understanding Rogue AP Detection

Radio Monitoring continuously monitors your WLAN radio environment to discover the presence of any new APs that are transmitting beacons. Any newly discovered AP that is not currently managed by WLSE generates a new rogue AP fault. You can view rogue AP faults using any of these options: **IDS > Summary > Rogue APs Detected**, **IDS > Faults**, **IDS > Reports**, or **IDS > Manage Rogues**.

The Radio Monitoring feature uses the radio measurement capabilities on Cisco IOS APs and Cisco client adaptors and CCX V2 clients to discover any new 802.11 APs that are transmitting beacons. Both clients and APs periodically scan for other 802.11 beacon frames on all channels. Reports of detected beacons are returned to the Radio Manager, which validates these beacons against a list of APs known to be authorized to provide wireless access.

**Note**

For the access points that support this feature, see the *Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine, 2.13*, on Cisco.com.

A newly discovered AP that cannot be identified as a known authorized AP generates an administrator alert. You can categorize this new AP as one of the following AP types:

Type	Description
Managed AP	An AP that is authorized to provide wireless access to the LAN and requires management services provided by the WLSE. Note Only managed APs can participate in Radio Manager operations (see Configuring Your Network for Radio Management, page 11-5).
Unmanaged AP	An AP that is authorized to provide wireless access to the LAN but does <i>not</i> require any management services from the WLSE. The WLSE categorizes unmanaged devices into two groups: • Rogue—An AP that may or may not be connected to the LAN, is detected by client's or AP's 802.11 radios within the managed WLAN, and has not been identified as Friendly. By default, all unmanaged radios are classified as Rogue until you change them to Friendly. When WLSE detects a rogue device, it sends alerts to the administrators and starts extra processing (such as switch port tracking). • Friendly—An AP that is not connected to the LAN, but is known to be detectable by client's or AP's 802.11 radios within the managed WLAN. A Friendly AP is an AP that you know exists, for example, a neighboring network's AP or a neighboring company's AP. All friendly devices begin on the WLSE as rogue devices and are explicitly categorized as friendly by the WLSE administrator.

How Rogue AP Detection Works

Rogue AP detection is based on the detection of an unknown radio broadcasting over the air. When Radio Monitoring detects a rogue AP, a new rogue AP fault is generated. When you select the link in the Description or Timestamp fields in the Fault Summary Table for an unknown access point, the Rogue Access Point Details window displays information about the rogue AP (see [Managing Rogue APs, page 14-24](#)).

Some networks might experience large numbers of rogues due to the nature of their neighboring networks or a one-time storm. When the number of unknown (rogue infra-structure or ad-hoc) radios is high (greater than 5000), your network might experience performance degradation. This can occur when your network is in a crowded airspace, you have products such as printers that have wireless functions that create and/or rotate ad-hoc network IDs, that are attacked by the FakeAP program, or that have APs sending corrupt beacon reports.



Note For an explanation of the fault that is generated when this occurs, in the online help click **Troubleshooting**, or on Cisco.com see the Fault Description Table in the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.13*.

How Friendly AP to Rogue AP Reclassification Works

For each unmanaged AP that has been classified as friendly, the WLSE periodically compares the present set of observers of that AP to its previous set of observers. If the relative power levels received by the observers changes, or the ratio of power levels between observers substantially changes, the friendly AP will be considered to have been relocated and will be reclassified as a rogue.

**Note**

To be less sensitive to changes in friendly AP power levels, only those observer APs in common between the two sets are considered in this comparison. If only one (or zero) APs remain in common between the two observer sets, the AP is reclassified as rogue unless the reason for this change is that one or more observers have been removed from the network or the observer AP in question has been moved to a new location.

When the Friendly-to-Rogue policy evaluates a site, any device that has not been seen in “too long a time” is reclassified as rogue. This time period starts when WLSE *last observed* the device, not after the administrator has set it to Friendly. To keep an unmanaged device as Friendly, set the maximum unobserved time to a value larger than the amount of time the device is *expected* to not be observed (see [Setting the Friendly AP to Rogue AP Reclassification Policy, page 14-18](#)). For example, if a friendly AP is turned off after business hours, the maximum unobserved time should be at least 14 hours (or more for weekends) or the WLSE will reclassify it as rogue.

Upon reclassification, the WLSE default actions for a newly-discovered rogue AP are performed, including (but not limited to) switchport-tracing within the managed network to ensure that the AP is not connected to that network.

Related Topics

- [Guidelines for Detecting Rogue APs, page 14-14](#)
- [Setting the Rogue AP Detection Policy, page 14-16](#)
- [Setting the Friendly AP to Rogue AP Reclassification Policy, page 14-18](#)
- [Displaying Information About Rogue Access Points, page 13-22](#)

Guidelines for Detecting Rogue APs

Prerequisites

Before you can detect rogue APs, you must:

1. Configure your network for radio management (see [Configuring Your Network for Radio Management, page 11-5](#)).

**Note**

If you choose to disable radio management, only one Intrusion Detection System subtab, **Manage Remaining IDS Settings**, is displayed (see [Using the Manage Remaining IDS Settings Subtab, page 14-11](#)). For information about the faults that will not be generated when Radio Management is disabled, see [Disabled Radio Management Related Faults, page 11-4](#).

**Note**

During initial network deployment, rogue detection must be turned off. Otherwise, between the time an AP is deployed and it is put into the managed state in WLSE, WLSE will attempt to locate the switch port of the newly deployed AP. This can generate many unnecessary faults.

2. Define the location elements (buildings and floors) and place the APs on the floor images. This step is optional, but will help you get the best results from the Location Manager displays. For more information, see:
 - [Entering Building Information, page 13-4](#)
 - [Adding Floors to Location Manager, page 13-9](#)
 - [Adding Devices to Floors, page 13-14](#)
3. Optional (but necessary to accurately locate rogue APs): Perform an AP Radio Scan on all APs on the specified floor (see [Using AP Radio Scans to Collect RM Data, page 13-43](#)).
4. Be sure Radio Monitoring is enabled on all APs (for both serving and non-serving channels) on the specified floor (see [Starting Radio Monitoring, page 12-4](#)).

**Note**

Radio Monitoring is enabled by default; if it has been disabled, you must re-enable it.

**Note**

If only serving channel scanning is enabled, then only the APs configured on the same channel as the rogue will actually report the rogue.

5. Set policies to enable rogue AP detection and assign a severity level to the fault that is generated when a rogue AP is detected (see [Setting the Rogue AP Detection Policy, page 14-16](#)).

Tips

- To detect rogue APs, Radio Monitoring *must* be running.
- Although you might be tempted to disable Radio Monitoring and detect rogue APs only during AP Radio Scans, *this approach is not recommended*. AP Radio Scan jobs can detect rogues, but only during the scan (approximately 3 to 4 minutes); any rogues that show up after the scan are not detected. In addition, because the scan is so short, it is possible that some rogues will not be detected because they do not respond with a Probe Request during the active scan. When Radio Monitoring is enabled, the rogue will eventually be detected by the beacon frame; it is statistically possible that a beacon will not be seen during an AP scan.

**Note**

If you disable Radio Monitoring and do not run AP Radio Scan, no unknown radios (rogue or friendly) will be detected. If you run AP Radio Scan but disable Radio Monitoring, some unknown radios will be detected, but not as many as would be detected if Radio Monitoring was running.

- An 11a-capable client that is associated with an 11g network *cannot* detect 11a rogues. No matter what the client is capable of supporting, it only searches for rogues that match the band of the AP. Therefore, when a client is associated to a 2.4Ghz AP (b or g), it only detects 2.4Ghz rogues (b or g). When it is associated to a 5Ghz (11a) AP, it only detects 5Ghz (11a) rogues.
- To detect all rogue APs in a network in which several hundred 11g APs have been deployed, you must also deploy 11a APs. Depending on the deployment, however, you might not have to deploy one 11a for each 11g radio. Using scanning-only APs, it is possible to completely cover the area for 11a rogue AP detection using fewer APs.
- A scanning-only AP that has a dual radio (both a and g) can detect all types of rogues (a, b, and g).
- If several rogue APs with similar MAC addresses appear in exactly the same location, there might be only one physical AP.

- If you disable the rogue AP fault detection, only the notification is removed; the rogue AP detection still occurs. The Location Manager still displays all the rogues in the system regardless of the fault detection setting.
- If you delete a rogue and the rogue still exists in the network, WLSE will detect it the next time AP Radio Scan or Radio Monitoring runs. Deleting the rogue will not mark it to be ignored; it is removed from the system as if it never occurred.



Note If the rogue is persistent in the network and not a problem, change the access point category type to Friendly. Then it will appear in the Friendly AP report and the Friendly list in Location Manager.

To handle large numbers of rogues:

- Use **IDS > Manage Network Wide Settings** to disable all rogue detection and processing from either infrastructure or ad-hoc rogues (or both).
- If your network is in a crowded airspace, examine the report **IDS > Manage Rogues**. This report shows you the RSSI value for the detected rogues. Sorting by RSSI might give you a limit of RSSI values that you could use in **IDS > Manage Network Wide Settings** as a threshold.
- Use **IDS > Manage Rogues** to delete the rogues that are no longer an issue (for example, from a temporary storm or isolated occurrence) to free up space in the WLSE.
- For an explanation of the fault, in the online help click **Troubleshooting**, or on Cisco.com see the Fault Description Table in the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.13*.

Related Topics

- [Understanding Rogue AP Detection, page 14-12](#)
- [Displaying Information About Rogue Access Points, page 13-22](#)
- [Viewing Rogue AP Reports, page 14-26](#)
- [Viewing Friendly AP Reports, page 14-28](#)

Setting the Rogue AP Detection Policy

Use **IDS > Manage Network-Wide IDS Settings** to enable rogue AP detection and to assign a severity level to the fault that is generated when a rogue AP is detected.

When a rogue AP is detected, a fault is generated and can be viewed under **IDS > Summary**, **IDS > Faults**, **IDS > Manage Rogues**, or **IDS > Reports**.



Note For information about setting the friendly AP to rogue AP reclassification policy, see [Setting the Friendly AP to Rogue AP Reclassification Policy, page 14-18](#).

Typical Scenarios and FAQs

- I want (or no longer want) to be notified when a rogue AP is detected.
- I want to specify the severity of rogue AP detection notifications.
- I want to view the current rogue AP detection faults associated with the current [P1...P5] setting.

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage Network-Wide IDS Settings**.

Step 2 Select **Rogue AP Detection**.

Step 3 Complete the following:

Field	Description
Enable	Click Enable to start rogue AP fault detection. This policy is enabled by default. Note If you disable rogue AP fault detection, only the fault notification is removed; the rogue AP detection still occurs. The Location Manager displays all the rogues in the system regardless of the fault detection setting.
Priority	From the dropdown list, select the severity level to assign the fault when a rogue access point is detected.
RSSI	Enter the minimum RSSI value. This is the received signal strength indicator of the reporting AP, and is used to estimate the location of the rogue AP relative to the reporting AP. Note This threshold is applied only when the rogue AP is <i>first detected</i> . Over time, this value may fall below the minimum value.
Enable Switch Port Tracing for Rogue	Click Enable to start rogue AP switch port tracing. This policy is enabled by default. Note For information about rogue AP switch port suppression, see Detecting Switch Port Locations and Suppressing Ports, page 14-30 .

Step 4 Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

Step 5 To see the faults associated with this setting, you can:

- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
- Select **IDS > Summary > Rogue APs Detected**.

Related Topics

- [Detecting Rogue APs, page 14-12](#)
- [Setting the Automatic Rogue AP Suppression Policy, page 14-32](#)
- [Managing Rogue APs, page 14-24](#)
- [Viewing Rogue AP Reports, page 14-26](#)
- [Guidelines for Detecting Rogue APs, page 14-14](#)

- [Understanding Rogue AP Detection, page 14-12](#)

Setting the Friendly AP to Rogue AP Reclassification Policy

Use **IDS > Manage Network-Wide IDS Settings** to enable friendly AP to rogue AP reclassification and to assign threshold levels to determine when a friendly AP should be reclassified.

Typical Scenarios and FAQs

- I want (or no longer want) to enable automatic friendly AP to rogue AP reclassification.
- I want to specify how long a friendly AP may be undetected before it is reclassified as a rogue.
- I want to specify the maximum difference in RSSI values that will be allowed before a friendly AP is reclassified.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage Network-Wide IDS Settings**.

Step 2 Select **Rogue AP Detection**.

The friendly AP to rogue AP reclassification settings appear *below* the rogue AP settings and the switch port suppression settings.

Step 3 Complete the following:

Field	Description
Enable	Click Enable to start automatic friendly AP to rogue AP reclassification. This policy is <i>not</i> enabled by default.
Unobserved time	The time a friendly AP can be unobserved before it is reclassified as a rogue, specified using days, hours, and minutes dropdown lists. Increments of 5 minutes can be specified. To keep an unmanaged device as Friendly, set the maximum unobserved time to a value larger than the amount of time the device is <i>expected</i> to not be observed (see How Friendly AP to Rogue AP Reclassification Works, page 14-13).
RSSI difference	Enter the maximum difference between the original and currently-observed RSSI (received signal strength indicator) values from one observer to the next that is allowed before the friendly AP is reclassified as a rogue.

Step 4 Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

Related Topics

- [Detecting Rogue APs, page 14-12](#)

- [Understanding Rogue AP Detection, page 14-12](#)

Displaying Rogue AP Faults

You can view rogue AP faults using options under **IDS > Summary**, **IDS > Faults**, **IDS > Reports**, or **IDS > Manage Rogues**.

**Note**

You can also display a graphical view of the estimated location of rogue radios using the Location Manager (see [Displaying Information About Rogue Access Points, page 13-22](#)).

Typical Scenarios and FAQs

- How do I view a list of APs that have reported the rogue AP and the location of the AP?
- How do I find the switch port to which the rogue AP is connected?
- I have just been notified of a rogue AP and I have determined it is a friendly AP. How do I delete the AP and clear the fault?
- I have just been notified of a rogue AP. Which APs are reporting the rogue AP?
- I have just been notified of a rogue AP. Where is its physical location in my network?
- How do I change the category type of a rogue AP to friendly?
- How do I delete a rogue AP from the database?

**Note**

Your login determines whether you can use this option.

Before You Begin

Satisfy the prerequisites for detecting rogue APs (see [Guidelines for Detecting Rogue APs, page 14-14](#)).

Procedure

- Step 1** Select **IDS > Summary**. The Intrusion Detection Summary window appears.
- Step 2** Select **Rogue APs Detected**. The Faults for Rogue APs Detected window appears.
- Step 3** Select the Description or Timestamp fields for the fault. The Unknown AP Details window displays information about the selected fault.

Figure 14-2 Sample Unknown AP Detail Window

WLSE Unknown AP Detail - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Rogue Access Point Details

BSSID	State	Vendor	
0012d9c8c103	Rogue Access Point	unknown	Change to Friendly Delete

Beacon Information

SSID	Beacon Interval	Channel	PHY	Data Rates
[7] "leapmhc"	100	36	802.11a	Basic: 6.0Mbps, 9.0Mbps, Basic: 12.0Mbps, 18.0Mbps, Basic: 24.0Mbps, 36.0Mbps, 48.0Mbps, 54.0Mbps

Location Estimation

Location	Timestamp	
Estimated location SJC/Second	Wed Jan 12 23:23:11 GMT+00:00 2005	View in Location Manager

Switch Port Tracing

Switch IP	Switch Port	Traced MAC Address	Timestamp	
unknown			-	Re-Trace

Reporting APs

Reporting AP IP Address	Reporting AP BSSID	RSSI	Reporting AP Location
12.10.80.21	000dbc9332b3	-91	SJC/Second

Associated Clients

Client MAC Address

Fault History

State	Severity	Description	Change	Timestamp	By
Active	P1	Device state is rogue access point	Device state is rogue access point	16:45:06 01/11/2005	



Note For rogue AP faults, the Unknown AP Details window contains this information:

Rogue Access Point Details

This table contains information about the rogue AP. It also allow you to:

- Change the classification of an access point from Rogue to Friendly.
- Delete the rogue AP from the database.

Table 14-1 Rogue Access Point Details Table

Column	Description
BSSID	Basic Service Set (BSS) identifier.
State	The state of the device.
Vendor	The name of the vendor that manufactured this AP.

Table 14-1 *Rogue Access Point Details Table (continued)*

Column	Description
Change To Friendly AP	To add this AP to the list of recognized APs, click Change To Friendly AP. Then refresh your browser window to view the updated fault display. Note It may be a few seconds before the classification is changed. Note When a rogue AP is changed to Friendly, the fault will be cleared and will subsequently be displayed as a Friendly AP.
Delete	To delete this unknown AP, click Delete. Then refresh your browser window to view the updated fault display. Note It may be a few seconds before the rogue AP is deleted.

Beacon Information

This table contains information about the beacon on which the rogue AP is transmitting.

Table 14-2 *Beacon Information Table*

Column	Description
SSID	Service set identifier used by client devices to associate with an access point. Note When an AP is configured to not broadcast its SSID, this field will either be blank or contain hex zeros. (When a Cisco AP is configured to not broadcast its SSID, that AP sends null characters (hex zeros) in place of the SSID in the beacon.)
Beacon Interval	The amount of time between beacons in kilo microseconds (one kilo microsecond equals 1,024 microseconds).
Channel	The channel on which the rogue AP is transmitting.
PHY	The physical interface type (11a, 11b, or 11g) of the radio interface.
Data Rates	The data rates supported by this interface (in Mbps).

Location Estimation**Table 14-3** **Location Estimation Table**

Column	Description
Location	The estimated location (building and floor) of the rogue AP. The following messages indicate that a problem occurred when trying to identify the location: - Estimated location could not be determined. Reporting AP location was not specified. When the APs are not placed using the Location Manager, WLSE cannot determine the location of the rogue because it does not know the location of the reporting AP. Use the Location Manager to define the location elements (buildings and floors) and place the APs in the floors. - Location could not be determined. Device was reported by clients only. When a rogue access point is detected only by clients, the Location Manager cannot determine the location of the rogue because the client's own location can change rapidly.
Timestamp	The time, based on the client browser, the rogue was detected (see Understanding WLSE Time Displays, page 1-10).
View in Location Manager	Click View in Location Manager to display a graphical view of the approximate location of the rogue AP. For more information about how the Location Manager locates an unknown radio, see Displaying Information About Rogue Access Points, page 13-22.

Switch Port Tracing

See [Tracing Switch Ports and Monitoring Automatic Rogue AP Suppression, page 14-34](#).

Reporting APs

This table contains information about the APs that have detected the rogue AP.

Table 14-4 **Reporting APs Table**

Column	Description
Reporting AP IP Address	The IP address of the AP that has located the rogue AP.
Reporting AP BSSID	The basic service set (BSS) identifier that contains the AP that has located the rogue AP.
Current RSSI	Received signal strength indicator of the reporting AP. This value is used to estimate the location of the rogue AP relative to the reporting AP.
Reporting AP Location	The physical location of the AP that has located the rogue AP.

Associated Clients

This table contains information about the clients associated with the rogue AP.

Table 14-5 *Associated Clients Table*

Column	Description
Client MAC Address	The MAC address of each client radio (that WLSE knows of) that is associated with the rogue AP.

Fault History

This table contains a history of the faults raised against this rogue AP.

Table 14-6 *Fault History Table*

Column	Description
State	The state of the device. For a description of the states, see Understanding Fault States, page 3-2 .
Severity	The severity level to be assigned to the fault.
Description	A description of the fault. Note For an explanation of the faults, in the online help click Troubleshooting , or on Cisco.com see the Fault Description Table in the <i>FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.13</i> .
Change	A description of the state change.
Timestamp	The time, based on the client browser, that the state of the device last changed (see Understanding WLSE Time Displays, page 1-10).
By	Displays the username of the person who changed the fault state. Note If the fault state has not been cleared or acknowledged, nothing is displayed in this column.

Related Topics

- [Managing Rogue APs, page 14-24](#)
- [Viewing Rogue AP Reports, page 14-26](#)
- [Viewing Friendly AP Reports, page 14-28](#)
- [Detecting Switch Port Locations and Suppressing Ports, page 14-30](#)
- [Guidelines for Detecting Rogue APs, page 14-14](#)

Managing Rogue APs

You can use the **IDS > Manage Rogue** option to manage rogue and friendly AP faults.



Note Similar functionality is also available from the **IDS > Faults** and **Faults > Display Faults** subtabs.

Typical Scenarios and FAQs

- How do I change the category type of a rogue AP to friendly?
- How do I delete a rogue AP from the database?



Note Your login determines whether you can use this option.

Before You Begin

Satisfy the prerequisites for detecting rogue APs (see [Guidelines for Detecting Rogue APs, page 14-14](#)).

Procedure

- Step 1** Select **IDS > Manage Rogue**. The Rogue AP List appears.
- Step 2** From the **Select Unknown Station Type**, select the type of unknown stations you want to display (Infrastructure or Adhoc).
- Step 3** To display the rogue AP list, select **Rogue** from the **Select Status** bar (this is the default). This table contains the following information:

Table 14-7 *Rogue AP List*

Column	Description
BSSID	Basic Service Set (BSS) identifier.
SSID	The Service Set ID broadcast by the rogue access point. Note When an AP is configured to not broadcast its SSID, this field will either be blank or contain hex zeros. (When a Cisco AP is configured to not broadcast its SSID, that AP sends null characters (hex zeros) in place of the SSID in the beacon.) Note This column displays non-printable characters as \xNN, where NN is the hex value of each character, followed by the length of the SSID in bytes. For example, "\x00" [1] means that the SSID contains the hex value \x00 and is 1 byte long. In addition, any double quote marks or backslashes that are part of the SSID octets are displayed using a preceeding backslash (for example, \" or \\).
Vendor Name	The name of the vendor that manufactured this AP.
Reported By	The AP that is reporting the rogue AP.
RSSI	Received signal strength indicator of the reporting AP. This value is used to estimate the location of the rogue AP relative to the reporting AP.
Channel	The channel on which the rogue AP is transmitting.

Table 14-7 *Rogue AP List*

Column	Description
PHY	The physical interface type (11a, 11b, or 11g) of the radio interface.
Building	The estimated location (building) of the rogue AP.
Floor	The estimated location (floor) of the rogue AP.
Reporting Time	The time, based on the client browser, the rogue AP was reported by the AP (see Understanding WLSE Time Displays, page 1-10).

- Step 4** To add one or more rogue APs to the list of recognized (friendly) APs, select the corresponding checkboxes and click **Change to Friendly** from the Select AP Type bar.



Note It may be a few seconds before the classification is changed.



Note When the rogue AP is marked as friendly, the fault will be cleared and will subsequently be displayed as a Friendly AP.

- Step 5** To view the list of recognized APs, select **Friendly** from the **Select Status** bar. The Friendly AP List appears. This table contains one additional field:

Table 14-8 *Friendly AP List*

Column	Description
AP Name	A text entry box that contains the user-defined name for this AP. To create a new name for this friendly AP or change the existing name, enter the name in the text entry box and click Save Name(s) .

- Step 6** To change the AP type for one or more friendly APs to Rogue, select the corresponding checkboxes and click **Change to Rogue** from the Select AP Type bar.



Note It may be a few seconds before the classification is changed.

- Step 7** To delete one or more rogue or friendly APs, select the corresponding checkboxes and click **Delete**.



Note It may be a few seconds before the APs are deleted.

Related Topics

- [Viewing Rogue AP Reports, page 14-26](#)
- [Viewing Friendly AP Reports, page 14-28](#)
- [Guidelines for Detecting Rogue APs, page 14-14](#)

Viewing Rogue AP Reports

The **IDS > Reports > Rogue AP Report** option displays any rogue access points that are present in the wireless network. A rogue AP is an AP that may or may not be connected to the LAN, is detected by client's or AP's 802.11 radios within the managed WLAN, and has not been identified as Friendly. By default, all unmanaged radios are classified as Rogue until you change them to Friendly.

Typical Scenarios and FAQs

- I want to view the rogue APs that are present in my network.

**Note**

Your login determines whether you can use this option.

Before You Begin

Satisfy the prerequisites for detecting rogue APs (see [Guidelines for Detecting Rogue APs, page 14-14](#)).

Procedure

Step 1 Select **IDS > Reports**.

Step 2 Select **Rogue AP Report** from the Report Name list.

Step 3 To view all records, click **View** (located to the right of the Report Name, Start Date, and End Date dropdown lists).

**Note**

To see all records *after* a filtering selection has been entered, select another report, then return to this one and click **View**.

Step 4 To view the information for a longer time period (the default is one day), select **Start Date** and **End Date** values from the pulldown lists and click **View**.

Step 5 To narrow the search criteria:

- Select **Building Name** or **Floor Name** from the dropdown list.
- Enter any filtering criteria in the text box. You can use an asterisk (*) as a wild card to denote numbers and letters.
- Click **Search**.

The building or floor names are displayed below the Search field. The Rogue AP report, which appears to the right of this list, displays the information for the first entry in the list.

- Click any other entry in the list to display its corresponding report.

The Rogue AP report contains the following information:

Table 14-9 *Rogue AP Report*

Column	Description
BSSID	Basic Service Set (BSS) identifier of the rogue AP.
SSID	The Service Set ID broadcast by the rogue access point. Note When an AP is configured to not broadcast its SSID, this field will either be blank or contain hex zeros. (When a Cisco AP is configured to not broadcast its SSID, that AP sends null characters (hex zeros) in place of the SSID in the beacon.) Note This column displays non-printable characters as \xNN, where NN is the hex value of each character, followed by the length of the SSID in bytes. For example, "\x00" [1] means that the SSID contains the hex value \x00 and is 1 byte long. In addition, any double quote marks or backslashes that are part of the SSID octets are displayed using a preceding backslash (for example, \" or \\).
Vendor Name	The name of the vendor that manufactured this AP.
Reported By	The name of the AP that located the rogue AP.
RSSI	Received signal strength indicator of the reporting AP. This value is used to estimate the location of the rogue AP relative to the reporting AP.
Channel	The channel on which the rogue AP is transmitting
PHY	The physical interface type (11a, 11b, or 11g) of the radio interface.
Building	The estimated location (building) of the rogue AP.
Floor	The estimated location (floor) of the rogue AP.
Switch IP	The IP address of the switch to which the rogue access point is connected.
Switch Port	The port of the switch to which the rogue access point is connected.
Reporting Time	The time the rogue was reported by the AP (based on the client browser—see Understanding WLSE Time Displays, page 1-10).

- Step 6** To view the fault details for a selected AP, click the value in the BSSID column. The Rogue Access Point Details window displays this information (see [Table 14-1Rogue Access Point Details Table, page 14-20](#)).
- Step 7** Use the buttons to the right of the Report Name, Start Date, and End Date lists to export or email this report.

Related Topics

- [Managing Rogue APs, page 14-24](#)
- [Using the IDS Reports Subtab, page 14-5](#)
- [Viewing Friendly AP Reports, page 14-28](#)

Viewing Friendly AP Reports

The Friendly AP Report displays any friendly access points that are present in the wireless network. A Friendly AP is an AP that is not connected to the LAN, but is known to be detectable by client's or AP's 802.11 radios within the managed WLAN. A Friendly AP is an AP that you know exists, such as a neighboring network's AP or a neighboring company's AP.

Typical Scenarios and FAQs

- I want to view the APs that have been identified as friendly in my network.



Note

Your login determines whether you can use this option.

Before You Begin

- Satisfy the prerequisites for detecting rogue APs (see [Guidelines for Detecting Rogue APs, page 14-14](#)).
- Designate one or more unknown APs as Friendly (see [Managing Rogue APs, page 14-24](#)).

Procedure

Step 1 Select **IDS > Reports**.

Step 2 From the Report Name list, select **Friendly AP Report**.

Step 3 To view all records, click **View** (located to the right of the Report Name, Start Date, and End Date dropdown lists).



Note

To see all records *after* a filtering selection has been entered, select another report, then return to this one and click **View**.

Step 4 To view the information for a longer time period (the default is one day), select **Start Date** and **End Date** values from the pulldown lists and click **View**.

Step 5 To narrow the search criteria:

- a. Select **Building Name** or **Floor Name** from the dropdown list.
- b. Enter any filtering criteria in the text box. You can use an asterisk (*) as a wild card to denote numbers and letters.
- c. Click **Search**.

The building or floor names are displayed below the Search field. The Friendly AP report, which appears to the right of this list, displays the information for the first entry in the list.

- d. Click any other entry in the list to display its corresponding report.

The Friendly AP report displays the following information:

Table 14-10 **Friendly AP Report**

Column	Description
AP Name	The user-defined name of the friendly AP.
BSSID	Basic Service Set (BSS) identifier of the friendly AP.

Table 14-10 Friendly AP Report (continued)

Column	Description
SSID	The Service Set ID broadcast by the friendly access point. Note When an AP is configured to not broadcast its SSID, this field will either be blank or contain hex zeros. (When a Cisco AP is configured to not broadcast its SSID, that AP sends null characters (hex zeros) in place of the SSID in the beacon.) Note This column displays non-printable characters as \xNN, where NN is the hex value of each character, followed by the length of the SSID in bytes. For example, "\x00" [1] means that the SSID contains the hex value \x00 and is 1 byte long. In addition, any double quote marks or backslashes that are part of the SSID octets are displayed using a preceeding backslash (for example, \" or \\).
Vendor Name	The name of the vendor that manufactured this AP.
Reported By	The name of the AP that located the friendly AP.
RSSI	Received signal strength indicator of the reporting AP. This value is used to estimate the location of the friendly AP relative to the reporting AP.
Channel	The channel on which the friendly AP is transmitting
PHY	The physical interface type (11a, 11b, or 11g) of the radio interface.
Building	The estimated location (building) of the friendly AP.
Floor	The estimated location (floor) of the friendly AP.
Switch IP	The IP address of the switch to which the access point is connected.
Switch Port	The port of the switch to which the access point is connected.
Reporting Time	The time the friendly AP was reported (based on the client browser—see Understanding WLSE Time Displays, page 1-10).

- Step 6** To view the fault details for a selected AP, click the value in the BSSID column. The Friendly Access Point Details window displays this information (see [Table 14-1Rogue Access Point Details Table, page 14-20](#)).
- Step 7** Use the buttons to the right of the Report Name, Start Date, and End Date lists to export or email this report.

Related Topics

- [Using the IDS Reports Subtab, page 14-5](#)
- [Viewing Rogue AP Reports, page 14-26](#)
- [Guidelines for Detecting Rogue APs, page 14-14](#)
- [Understanding Rogue AP Detection, page 14-12](#)

Detecting Switch Port Locations and Suppressing Ports

When a rogue AP fault is generated, the Rogue Access Point Details window displays information about the switch port to which the rogue AP is connected. The following sections describe how and where to use the switch port location and suppression feature:

- [Understanding Switch Port Tracing and Suppression, page 14-30](#)
- [Guidelines for Detecting and Suppressing Switch Ports, page 14-31](#)
- [Setting the Automatic Rogue AP Suppression Policy, page 14-32](#)
- [Tracing Switch Ports and Monitoring Automatic Rogue AP Suppression, page 14-34](#)

Understanding Switch Port Tracing and Suppression

To find the switch port to which the rogue AP is connected (if it is connected), the Switch Port Location feature uses BSSIDs of the rogue APs that it hears over the air to make a heuristic guess of the rogue's Ethernet MAC address.

**Note**

Switch port tracing and suppression is a best-effort approach and is not 100% guaranteed to yield accurate results.

**Note**

Catalyst Operating System (CatOS) software is not supported for switch port tracing.

How It Works

The WLSE determines whether an AP is a rogue:

1. While Radio Monitoring is enabled, the APs report the BSSIDs of their neighboring APs.
2. WLSE compares the BSSIDs of the APs with those in the managed list. Any AP not in the managed list is considered to be rogue and a fault is reported.

After a rogue AP has been detected by WLSE:

1. The WLSE receives frame reports from the reporting and scanning APs. These reports contain the MAC addresses of any clients associated with the rogue AP.
2. WLSE tries to locate the MAC addresses of both the client and the rogue in the switches via a CAM table search (using the approach described in the following note) to determine which port is forwarding packets to the client via the rogue.

**Note**

While searching the CAM table, WLSE tries to locate the client MAC address, the radio MAC of the rogue, the (radio MAC + 1) of the rogue, and the (radio MAC - 1) of the rogue.

To start the CDP neighbor search, the "Seed IP Addresses" list is pre-populated with one of the following:

- The IP address of the directly connected switch (if available) of the reporting APs.
- The IP address of the reporting AP.

3. Switch port tracing starts with the rogue MAC address and resumes tracing when it receives a client MAC address. To search for the associated client's MAC address, WLSE includes managed switches in the same subnet as the switch that is directly connected with the reporting AP.

You can manually add and delete devices to this list. CDP traversal will use these devices as seed devices. This list of devices, called the "Suspected Device List", will change as the client addresses are reported by the reporting APs.



Note Restarting the Scan & Trace will start the algorithm from the beginning, including the CAM table search.

4. After a CAM search yields a port, an elimination algorithm is run to reduce false positives:
 - If a port is a Gig port, skip.
 - If a port is part of channeling ports, skip.
 - If a port is part of port grouping, skip.
 - If CDP neighbor of a port is a managed AP, skip.
 - If CDP neighbor of a port is a non-AP Cisco device, skip.



Note If a hub is connected to a switch port and the hub connects a managed AP and a rogue AP on its downlink, the port will not be suppressed.

5. If the switch port location is found and the switch port suppression feature has been enabled, the WLSE will attempt to shut down the switch port using SNMP.



Note A switch port is suppressed only if a single switch port is traced. When multiple STA addresses are reported and more than one switch port is traced, all switch ports are reported and switch port suppression is skipped. In rare cases, multiple switch ports might appear in the report, for example, when a client is moved in the time between a radio scan and a CAM search.

6. When the switch port location fault is cleared, the WLSE will send a notification to the reporting APs.

Data Produced

When a rogue AP fault is generated and if the rogue AP can be traced, the Rogue Access Point Details window displays information about the switch port to which the rogue AP is connected (see [Tracing Switch Ports and Monitoring Automatic Rogue AP Suppression, page 14-34](#)).

Guidelines for Detecting and Suppressing Switch Ports

Prerequisites

Before you can suppress the switch ports of rogue APs, you must:

1. Satisfy the rogue AP detection prerequisites (see [Guidelines for Detecting Rogue APs, page 14-14](#)).

**Note**

During initial network deployment, rogue detection must be turned off. Otherwise, between the time an AP is deployed and it is put into the managed state in WLSE, WLSE will attempt to locate the switch port of the newly deployed AP. This will generate many unnecessary faults.

2. Enable rogue AP switch port tracing (see [Setting the Rogue AP Detection Policy, page 14-16](#)).
3. Assign the network-wide settings for enabling automatic rogue access point suppression (see [Setting the Automatic Rogue AP Suppression Policy, page 14-32](#)).

Tips

- To find the switch port to which the rogue AP is connected, check the Switch Port Location information displayed in the Unknown AP Detail window (see [Table 14-11 on page 14-35](#)). If the rogue AP can be traced, this window displays information about the switch port to which the rogue AP is connected.
- If you suspect that a rogue AP was moved and connected to a different port (and automatic suppression has not been enabled), you can click **Re-Trace** on the Rogue Access Point Details window to locate the switch port again (see [Tracing Switch Ports and Monitoring Automatic Rogue AP Suppression, page 14-34](#)).

Related Topics

- [Understanding Switch Port Tracing and Suppression, page 14-30](#)

Setting the Automatic Rogue AP Suppression Policy

Use **IDS > Manage Network-Wide IDS Settings** to enable or disable automatic rogue access point suppression and to view currently suppressed ports.

Typical Scenarios and FAQs

- I want (or no longer want) to suppress the switch port and enable the automatic suppression of switch ports.
- I want to see a list of the currently suppressed switch ports.

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage Network-Wide IDS Settings**.

Step 2 Select **Rogue AP Detection**.

**Note**

The switch port suppression settings appear below the rogue AP settings.

Step 3 Complete the following:

Field	Description
Enable	Click Enable to enable automatic rogue AP suppression.
CDP Hop Count	The number of CDP hops made during the rogue discovery process. • When the hop count=1, only the seed device and any directly connected neighbor devices are discovered. • The seed devices are the APs that reported the rogue.
Skip Criterion:	
• Gigabit Ethernet Port	If a port is a Gig port, skip.
• Managed AP Port	If CDP neighbor of a port is a managed AP, skip.
• Port Channeling Port	If a port is part of channeling ports, skip.
• Port Grouping Port	If a port is part of port grouping, skip.
• Non-AP CDP Neighbor	If CDP neighbor of a port is a non-AP Cisco device, skip.



Note If a hub is connected to a switch port and the hub connects a managed AP and a rogue AP on its downlink, the port will not be suppressed.

Step 4 Click **Apply** to set the new entry.

Step 5 To view the currently suppressed switch ports, click **View current suppression**. The following information is displayed:

Field	Description
Switch IP	The IP address of the switch to which the rogue AP is connected.
Switch Port	The port to which the rogue AP is connected.
Suppressed AP	The MAC address of the rogue AP.
Timestamp	The time, based on the client browser, the rogue AP switch port was detected (see Understanding WLSE Time Displays, page 1-10).

Step 6 To turn on the port, select **Unshut Port**.

Step 7 Click your browser's **Back** button to return to the network-wide setting window.

Related Topics

- [Tracing Switch Ports and Monitoring Automatic Rogue AP Suppression, page 14-34](#)
- [Setting the Rogue AP Detection Policy, page 14-16](#)

Tracing Switch Ports and Monitoring Automatic Rogue AP Suppression

Use **IDS > Faults** to view information about the switch port to which a rogue AP is connected.

**Note**

Catalyst Operating System (CatOS) software is not supported for switch port tracing.

Typical Scenarios and FAQs

- I want to find the switch port to which a rogue AP is connected.
- I suspect that a rogue AP was moved and connected to a different port. How do I locate it again?

**Note**

Your login determines whether you can use this option.

Before You Begin

Satisfy the switch port detection and suppression prerequisites (see [Guidelines for Detecting and Suppressing Switch Ports, page 14-31](#)).

Procedure

-
- Step 1** Select **IDS > Faults**. The Faults Summary window appears.
- Step 2** Click the Description or Timestamp fields in the Fault Summary table for the device in question.
- In addition to the rogue AP information, the Unknown AP Details window also contains information about the switch to which the rogue AP is connected.

Figure 14-3 Sample Switch Port Tracing Details

1

WLSE Unknown AP Detail - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Help

Rogue Access Point Details

BSSID	State	Vendor	
000c305baf32	Rogue Access Point	Cisco	Change to Friendly Delete

Beacon Information

SSID	Beacon Interval	Channel	PHY	Data Rates
"tsunami"	100	64	802.11a	Basic: 6.0Mbps, 9.0Mbps, Basic: 12.0Mbps, 18.0Mbps, Basic: 24.0Mbps, 36.0Mbps, 48.0Mbps, 54.0Mbps

Location Estimation

Location	Timestamp	
Location could not be determined. Reporting AP location was not specified.	Wed Nov 03 20:56:51 GMT+00:00 2004	View in Location Manager

Switch Port Tracing

Switch IP	Switch Port	Traced MAC Address	Timestamp	
unknown			-	Re-Trace

Reporting APs

Reporting AP IP Address	Reporting AP BSSID	RSSI	Reporting AP Location
12.10.10.212	000e3870ba80	-66	
12.10.10.215	000c305baf34	-75	

Associated Clients

Client MAC Address

Fault History

State	Severity	Description	Change	Timestamp	By
Active	P1	Device state is rogue access point	Device state is rogue access point	12:56:51 11/03/2004	

The Switch Port Tracing table contains the following information about the switch to which the rogue AP is connected:

Table 14-11 Switch Port Tracing Table

Column	Description
Switch IP	The IP address of the switch to which the rogue AP is connected.
Switch Port	The port of the switch to which the rogue AP is connected.
Traced MAC Address	The MAC address of the rogue AP or the associated client.
Timestamp	The time, based on the client browser, the rogue AP switch port was detected (see Understanding WLSE Time Displays, page 1-10).
Re-Trace	Click Re-Trace to locate the switch port again. This is useful when you suspect that the rogue AP was moved and connected to a different port. The Re-Trace Switchport window allows you to enter additional seed devices. Using CDP discovery, the Switch Port Location feature uses these seed devices to find the neighboring switches, and then tries to locate the rogue or associated client Ethernet MAC on these switches by querying the MAC address table (see Understanding Switch Port Tracing and Suppression, page 14-30).

- Step 3** To locate a switch port (for example, when you suspect that the rogue AP was moved and connected to a different port):
- Click **Re-Trace**. The Re-Trace Switchport window appears.

Figure 14-4 Sample Re-Trace Switchport Window

- To add additional seed addresses, enter the IP addresses in the text window and click **Add**. Each new seed address will appear in the Seed IP Addresses list box.
- To delete an address, select the address in the list box and click **Delete**.
- To start the retrace, click **Trace**.

A log of the switch port tracing progress is displayed in a separate window. This log shows you the detailed state of the fault, including whether a switch port trace is in progress and which switches have already been searched.



Note Refreshing this window while tracing is in progress will *restart* the trace.

- The log will be updated when the switch port tracing process is complete. You can then print the log and close the window.

Related Topic

- [Understanding Switch Port Tracing and Suppression, page 14-30](#)
- [Managing Rogue APs, page 14-24](#)

Detecting Ad-Hoc Networks

The following sections will help you understand how and where to use the ad-hoc network detection feature:

- [Understanding Ad-Hoc Network Detection, page 14-37](#)
- [Guidelines for Detecting Ad-Hoc Networks, page 14-37](#)
- [Setting the Ad-Hoc Network Detection Policy, page 14-38](#)
- [Displaying Ad-Hoc Network Faults, page 14-39](#)
- [Viewing Ad-Hoc Network Reports, page 14-41](#)

Understanding Ad-Hoc Network Detection

When setting up a wireless local area network (WLAN), nodes are typically set up as access points to act as bridges to a wired network. The 802.11 standard also specifies an ad-hoc mode for client radio network interface cards (NIC). In this way clients can set up a local network in which participants communicate directly with each other (stations without access points). This is known as an independent basic service set network configuration (IBSS), also known as an ad-hoc network.

Computer manufacturers, specifically laptop manufacturers, are supplying radio NIC's as standard components. The likelihood of having ad-hoc networks created inside an infrastructure WLAN is expected to increase. Ad-hoc networks formed inside a LAN or an infrastructure WLAN are considered a security risk. A member of a wired or infrastructure WLAN that participates in an ad-hoc network could potentially provide unwilling and unwanted access to a wired network. Security conscious customers would like to identify when and where an ad-hoc network is created within their management domain.

When creating an ad-hoc network, the participants issue beacons that synchronize their communication. APs deployed in an infrastructure WLAN can detect these beacons, and therefore the WLSE can detect ad-hoc network creation using this beacon information.

**Note**

The WLSE does not classify IBSS beacons as interference data because it only identifies energy as interference when it cannot interpret the signal data. Because the IBSS beacons are 802.11 data, it *does* interpret these signals and handles them as rogue intrusions.

Guidelines for Detecting Ad-Hoc Networks

Prerequisites

Before you can detect ad-hoc networks, you must:

1. Configure your network for radio management (see [Configuring Your Network for Radio Management, page 11-5](#)).

**Note**

If you choose to disable radio management, only one Intrusion Detection System subtab, **Manage Remaining IDS Settings**, is displayed (see [Using the Manage Remaining IDS Settings Subtab, page 14-11](#)). For information about the faults that will not be generated when Radio Management is disabled, see [Disabled Radio Management Related Faults, page 11-4](#).

2. Be sure Radio Monitoring is enabled on all APs (for both serving and non-serving channels) on the specified floor (see [Starting Radio Monitoring, page 12-4](#)).



Note Radio Monitoring is enabled by default; if it has been disabled, you must re-enable it.

3. Set network-wide policies to enable ad-hoc network detection and assign a severity level to the fault that is generated when an ad-hoc network is detected. See [Setting the Ad-Hoc Network Detection Policy, page 14-38](#).

Tips

- If you disable the ad-hoc network fault notification, only the notification is removed; the ad-hoc network detection still occurs.

Related Topics

- [Understanding Ad-Hoc Network Detection, page 14-37](#)

Setting the Ad-Hoc Network Detection Policy

Use **IDS > Manage Network-Wide IDS Settings** to enable ad-hoc network detection and to assign a severity level to the fault that is generated when an ad-hoc network is detected. When an ad-hoc network is detected, a fault is generated and can be viewed under **IDS > Summary**, **IDS > Faults**, or **IDS > Reports**.

Typical Scenarios and FAQs

- I want (or no longer want) to be notified when an ad hoc network is detected.
- I want to specify the severity of an ad hoc network detection notification.
- I want to view the current ad-hoc network faults associated with the current [P1...P5] setting.



Note Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage Network-Wide IDS Settings**.

Step 2 Select **Ad-Hoc Network Detection**.

Step 3 Complete the following:

Field	Description
Enable	Click Enable to enable ad-hoc network detection. This policy is enabled by default. Note If you disable ad-hoc network detection, only the fault notification is removed; the ad-hoc network detection still occurs. The Location Manager displays all rogue stations (ad-hoc networks) in the system regardless of the fault detection setting.
Priority	From the dropdown list, select the severity level to assign the fault when an ad-hoc network is detected.

- Step 4** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.
- Step 5** To see the faults associated with this setting, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > Ad-Hoc Networks Detected**.
-

Related Topics

[Detecting Ad-Hoc Networks, page 14-37](#)

Displaying Ad-Hoc Network Faults

Use **IDS > Summary** to view the fault that is generated when an ad-hoc network is detected. This window allows you to:

- View a list of APs that have reported the ad-hoc network and, if available, the building and floor the AP is in.
- View a list of clients that are associated with the ad-hoc network (if available). The grouping is based upon the SSID used in the ad-hoc network.

Typical Scenarios and FAQs

- I have just been notified of an ad hoc network. What part of my network has detected this? Where is it physically in my network?
- I have just been notified of an ad hoc network. What other NICs are participating in this network?
- I have just been notified of an ad hoc network and I have determined it is no longer a problem. How do I clear the fault?



Note

Your login determines whether you can use this option.

Before You Begin

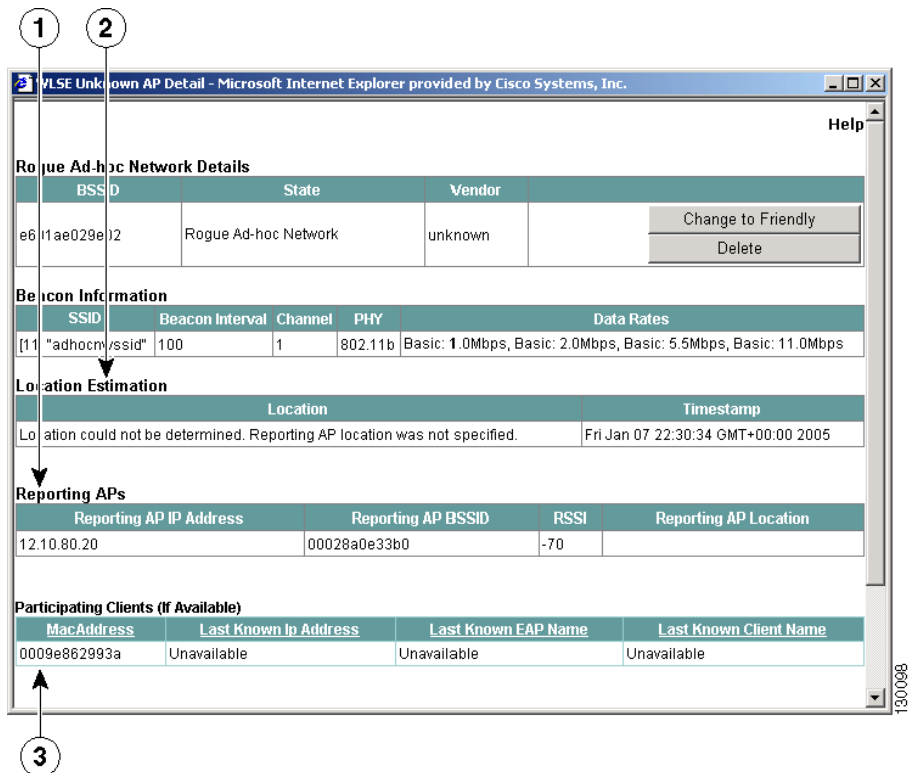
Satisfy the ad-hoc network detection prerequisites (see [Guidelines for Detecting Ad-Hoc Networks, page 14-37](#)).

Procedure

-
- Step 1** Select **IDS > Summary**. The Intrusion Detection Summary window appears.
- Step 2** Select **Ad-Hoc Networks Detected**. The Faults for Ad-Hoc Networks Detected window appears.
- Step 3** Select the Description or Timestamp fields for the fault. The Fault Details window displays the information about the fault for the selected device (see [Viewing Fault Details, page 3-7](#)).

Step 4 The Unknown AP Detail window for ad-hoc networks contains the following information:

Figure 14-5 Sample Unknown AP Detail Window For Ad-hoc Networks



1	A list of the APs that have reported the ad-hoc network and, if available, the approximate location (building and floor) of each reporting AP.
2	The approximate location of the ad-hoc participant.
3	A list of the other NICs that are participating in this network. This list is a “best effort” given the beacon information. The source MAC address in the beacon is used to identify each NIC. The ad-hoc network is identified based on the BSSID and the SSID combination used in the network.

Step 5 To clear a fault that is generated when an ad-hoc network is detected, see [Clearing Summary Table Faults](#), page 3-6.



Note Because only the *creation* of a network can be detected, this is the only means of clearing an ad-hoc network detection fault.

Related Topics

- [Understanding Ad-Hoc Network Detection](#), page 14-37
- [Setting the Rogue AP Detection Policy](#), page 14-16

- [Viewing Ad-Hoc Network Reports, page 14-41](#)
- [Using the Faults Subtab, page 14-4](#)

Viewing Ad-Hoc Network Reports

The Ad-hoc Networks report allows you to view a history of the APs within buildings and floors that have reported ad-hoc networks.



Note The NICs participating in an ad-hoc network will be a *best effort* given the beacon information.

Typical Scenarios and FAQs

- How can I see any ad-hoc networks and their participating clients?



Note

Your login determines whether you can use this option.

Before You Begin

Satisfy the ad-hoc network detection prerequisites (see [Guidelines for Detecting Ad-Hoc Networks, page 14-37](#)).

Procedure

- Step 1** Select **IDS > Reports**.
 - Step 2** From the Report Name list, select **Ad-hoc Network Report**.
 - Step 3** To view all records, click **View** (located to the right of the Report Name, Start Date, and End Date dropdown lists).
- 

Note To see all records *after* a filtering selection has been entered, select another report, then return to this one and click **View**.
- Step 4** To view the information for a longer time period (the default is one day), select **Start Date** and **End Date** values from the pulldown lists and click **View**.
 - Step 5** To narrow the search criteria:
 - a. Select **Participant MAC Address**, **Participant IP Address**, **Participant EAP User Name**, or **Network BSSID** from the dropdown list.
 - b. Enter any filtering criteria in the text box. You can use an asterisk (*) as a wild card to denote numbers and letters.
 - c. Click **Search**.

The data that satisfies the search criteria is displayed below the Search field. The Ad-Hoc Network report, which appears to the right of this list, displays the information for the first entry in the list.

 - d. Click any other entry in the list to display its corresponding report.

The Ad-Hoc Network report contains the following information:

Column	Description
Client MAC Address	The MAC address of each client radio (that WLSE knows of) that is participating in the network (there could be more). The source MAC address in the beacon is used to identify each NIC.
BSSID	Basic Service Set Identifier—The unique identifier for the ad-hoc network.
Last SSID	The last Service Set Identifier. The SSID is an identifier that client devices use to associate with the access point. Note When an AP is configured to not broadcast its SSID, this field will either be blank or contain hex zeros. (When a Cisco AP is configured to not broadcast its SSID, that AP sends null characters (hex zeros) in place of the SSID in the beacon.)
Last Known IP Address	Last known IP address of the client when it was associated with any AP managed by the WLSE. Note This information might not be available or it might not be current.
Last Known EAP Name	The RADIUS username of the client. (User names are not available for non-EAP authentications.) The RADIUS username is generally available in all EAP authentication cases, except for PEAP and EAP-TTLS. In these instances, the availability of the information is dependent on vendor support. Note This information might not be available or it might not be current.
Last Known Client Name	Last known client name. Note This information might not be available or it might not be current.
Last Association With	The last AP managed by WLSE with which the client was associated. Note This information might not be available or it might not be current.
PHY	The type of 802.11 radio the client is using (11a or 11b/11g).
Estimated Location	The estimated location of the client (uses the same location algorithm as rogue AP detection).
Reported By Client	Y = A client detected the network. N = An infrastructure AP detected the network.
First Seen	The time WLSE first heard one of the ad-hoc network beacons that was transported to WLSE via the WDS setup. For more information, see Understanding WLSE Time Displays, page 1-10 .

- Step 6** Use the buttons to the right of the Report Name, Start Date, and End Date lists to export or email this report.

Related Topics

- [Understanding Ad-Hoc Network Detection, page 14-37](#)
- [Using the Basic Report Features, page 10-1](#)

- [Using the IDS Reports Subtab, page 14-5](#)

Detecting Interference

Radio Monitoring continuously monitors your WLAN radio environment to discover the presence of any interference.

**Note**

Interference information is collected only from access points that are on the Radio Monitoring list and the clients associated with these APs.

The following sections will help you understand how and where to use the interference detection feature:

- [Understanding Interference Detection, page 14-43](#)
- [Guidelines for Detecting Interference, page 14-44](#)
- [Setting the Interference Detection Policy, page 14-45](#)
- [Displaying Interference Faults, page 14-46](#)

Understanding Interference Detection

This feature allows you to start interference detection and choose what level of signal strength and duration of signal is required to detect interference. Only APs in the Radio Monitoring list and clients associated with these APs can participate in interference detection.

**Note**

Radio Monitoring is enabled by default. *If you disable Radio Monitoring, you will not be able to detect non-802.11 interference.*

How It Works

The Radio Monitoring feature uses the radio measurement capabilities to discover any new interference. The WLSE defines interference as a non-802.11 signal. An interference fault, therefore, reports signals that cannot be decoded by the AP; that is, energy that cannot be decoded as a valid 802.11 signal.

The WLSE can tell if a signal is from an 802.11 device (such as another AP or client) or a non-802.11 device (such as a microwave oven or cordless phone) as long as the signal is strong enough to be demodulated. When APs are close enough to each other, the AP can tell that the signal is from another AP and will not generate an interference report. If the AP is not known to the WLSE, it flags it as an unknown radio and lets the user make the disposition decision.

If the signal is too weak to be demodulated, or the signal is garbled, or the signal is coming from a non-802.11 device, it presents itself as energy. The AP then reports the detection of such energy levels to the WLSE, which uses the appropriate interference fault profile parameter to decide whether to generate a fault.

If a signal can be decoded as 802.11, then it is a contending signal, not interference. While this neighboring 802.11 signal may interfere with the operation of the AP, it is not causing any radio interference. However, because the AP can actually decode the signal, the two APs will be contending for the channel. Neither one will be allowed to transmit at the same time because they are following the MAC rules. In other words, they never cause each other any radio interference. You can use the Location Manager to see the interaction of 802.11 signals and determine the amount of overlap between neighboring APs.

Data Produced

When Radio Monitoring detects interference, a new fault is generated. To view details about an interference fault:

1. Select **IDS > Summary > Interference Detected**.
2. Click the link in the Description or Timestamp fields to view the Fault Details window (see [Viewing Fault Details, page 3-7](#)).

Related Topics

- [Using Radio Monitoring to Collect RM Data, page 12-1](#)

Guidelines for Detecting Interference

Prerequisites

Before you can detect non-802.11 interference, you must:

1. Configure your network for radio management (see [Configuring Your Network for Radio Management, page 11-5](#)).

**Note**

If you choose to disable radio management, only one Intrusion Detection System subtab, **Manage Remaining IDS Settings**, is displayed (see [Using the Manage Remaining IDS Settings Subtab, page 14-11](#)). For information about the faults that will not be generated when Radio Management is disabled, see [Disabled Radio Management Related Faults, page 11-4](#).

2. Be sure Radio Monitoring is enabled on all APs (for both serving and non-serving channels) on the specified floor (see [Starting Radio Monitoring, page 12-4](#)).

**Note**

Radio Monitoring is enabled by default; if it has been disabled, you must re-enable it.

3. Set the threshold condition for interference detection (see [Setting the Interference Detection Policy, page 14-45](#)).
4. Define the location elements (buildings and floors) and place the APs on the floor images. This step is optional, but will help you get the best results from the Location Manager displays. For more information, see:
 - [Entering Building Information, page 13-4](#)
 - [Adding Floors to Location Manager, page 13-9](#)
 - [Adding Devices to Floors, page 13-14](#)

Tips

- To detect interference, Radio Monitoring must be running.
- When the signal from a friendly AP is strong enough to cause an interference fault but not strong enough to see the signal as a valid 802.11 signal, there is no way to exclude the transmission from this device. If WLSE can decode the signal as 802.11, then it will not classify it as interference; if it cannot decode the signal, it does not know it comes from a friendly device.

Therefore, if you see “Non-802.11 Interference Detected” fault messages from a friendly AP, you should raise the level at which interference is faulted (see [Setting the Interference Detection Policy, page 14-45](#)).

Related Topics

- [Understanding Interference Detection, page 14-43](#)

Setting the Interference Detection Policy

Use **IDS > Manage Network-Wide IDS Settings** to enable radio frequency interference detection and to assign a severity level to the fault that is generated when interference is detected. When interference is detected, a fault is generated and can be viewed under **IDS > Faults**.



Note

Applying new settings will clear all existing non-802.11 interference faults.

Typical Scenarios and FAQs

- I want (or no longer want) to be notified when the interference level for a radio type exceeds a certain level for a specified time.
- I want to choose what level of signal strength and duration of signal is required to detect interference.
- I want to choose at what level of signal strength and duration of signal an interference fault is automatically cleared.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage Network-Wide IDS Settings**.

Step 2 Select **Interference Detection**.

Step 3 Complete the following:

Field	Description
Interference Fault Severity	Select the severity level to associate with this setting. For more information about fault severity levels, see Displaying Faults, page 3-4 .
Enable 802.11b/g Interface Settings - and - Enable 802.11a Interface Settings	Select to enable the policy.

Field	Description
Degraded	Select the criteria that identifies an interference fault: • The minimum interference level (in dB) • The percentage of time the interference level exceeds the minimum interference level during each measurement interval • The time interval
Up	Select the time interval after which, if the interference level falls below the minimum interference level for a percentage of time, the interference fault for that device is cleared.

**Caution**

Applying new settings will clear all existing non-802.11 interference faults.

Step 4 Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

Step 5 To see the faults associated with this setting, you can:

- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
- Select **IDS > Summary > Interference Detected**.

Related Topics

- [Understanding Interference Detection, page 14-43](#)

Displaying Interference Faults

Use **IDS > Summary > Interference Detected** to view a summary of the devices that have detected non-802.11 interference. This window allows you to:

- View a list of APs that have reported the interference and, if available, the building and floor in which the AP is located.
- View a history of the interference faults for the selected device.
- Clear a fault that is generated when radio frequency interference is detected.

Typical Scenarios and FAQs

- How can I see a history of radio frequency interference in my network?
- I have just been notified of radio interference and I have determined it is no longer a problem. How do I clear the fault?

**Note**

Your login determines whether you can use this option.

Before You Begin

Satisfy the interference detection prerequisites (see [Guidelines for Detecting Interference, page 14-44](#)).

Procedure

-
Step 1	Select IDS > Summary . The Intrusion Detection Summary window appears.
Step 2	Select Interference Detected . The Faults for Interference Detected window appears.
Step 3	Select the Description or Timestamp fields for the fault. The Fault Details window displays the information about the fault for the selected device (see Viewing Fault Details, page 3-7).
Step 4	To clear an interference fault, see Clearing Summary Table Faults, page 3-6 .
-

Related Topics

[Understanding Interference Detection, page 14-43](#)

Detecting Excessive Management Frame Transmissions

Radio Monitoring continuously monitors your WLAN radio environment to discover the presence of any Excessive Management Frame (EMF) transmissions.



Note

EMF information is collected only from access points that are on the Radio Monitoring list and the clients associated with these APs.

The following sections will help you understand how and where to use the EMF detection feature:

- [Understanding Excessive Management Frame Detection, page 14-47](#)
- [Guidelines for Using Excessive Management Frame Detection, page 14-48](#)
- [Setting the Excessive Management Frame Detection Policy, page 14-48](#)
- [Displaying EMF Detection Faults, page 14-49](#)
- [Viewing EMF Detection Reports, page 14-50](#)

Understanding Excessive Management Frame Detection

APs must provide a means of determining that normal WLAN management and control frames have exceeded a default threshold. In a DOS attack, an attacker can broadcast so many management frames that the APs become overwhelmed while trying to process the frames and throughput is affected. As part of the WLSE IDS feature set, scanning-only APs can monitor radio frequency signals, detect excessive management frame transmission, and raise a fault when a user-defined threshold is crossed.

There are two types of EMF faults:

- **Per Station:** A station can be a laptop, an access point, a PDA, or any device. The station is identified by the radio MAC address, which is the BSSID.
- **Per Channel:** For channel faults, frames from all stations are aggregated, so it doesn't matter which station is generating the fault.

You can use Excessive Management Frame (EMF) detection to detect transmissions of the following frames:

- Association requests and responses

- Reassociation requests and responses
- Probe requests and responses
- Disassociation
- Authentication
- Deauthentication
- Action Frames

You can specify the duration and count of each type of management frame.

Guidelines for Using Excessive Management Frame Detection

Prerequisites

Before you can use Excessive Management Frame detection, you must:

1. Configure your network for radio management (see [Configuring Your Network for Radio Management, page 11-5](#)).



Note

If you choose to disable radio management, only one Intrusion Detection System subtab, **Manage Remaining IDS Settings**, is displayed (see [Using the Manage Remaining IDS Settings Subtab, page 14-11](#)). For information about the faults that will not be generated when Radio Management is disabled, see [Disabled Radio Management Related Faults, page 11-4](#).

2. Be sure Radio Monitoring is enabled (see [Starting Radio Monitoring, page 12-4](#)).



Note

Radio Monitoring is enabled by default; if it has been disabled, you must re-enable it.

3. Enable Excessive Management Frame detection mode on selected scanning-only APs (see [Configuring Frame Monitoring, page 12-20](#)).
4. Set the threshold condition for EMF detection (see [Setting the Excessive Management Frame Detection Policy, page 14-48](#)).

Related Topics

[Understanding Excessive Management Frame Detection, page 14-47](#)

Setting the Excessive Management Frame Detection Policy

Use **IDS > Manage IDS Settings** to enable EMF detection, assign thresholds, and assign a severity level to the fault that is generated when an EMF is exceeded. When an EMF threshold is exceeded, a fault is generated and can be viewed under **IDS > Faults** or **IDS > Summary**.

Typical Scenarios and FAQs

- I want to specify the severity and threshold levels for frame management request counts.

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.

Step 2 Select an existing IDS fault profile and click **Edit**.

Step 3 Select **Excessive Management Frame Detection**.

Step 4 Complete the following:

Field	Description
Severity	From the dropdown list, select the severity level to assign the fault.
Per Channel Settings and Per Station Settings	
Enabled	For each frame type, select to enable the policy.
Frame Count	The threshold for generating the EMF fault. If the number of frames seen during the observation time exceed the frame count, then that EMF fault is raised.
Observation Time	A sliding window of time over which the number of frames is monitored (that is, “if x frames have been seen in the last y ms, generate a fault”).

Step 5 Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

Step 6 To see the faults associated with this threshold, you can:

- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser’s **Back** button to return to the network-wide setting window.
- Select **IDS > Summary > Excessive Management Frames**.

Step 7 To assign this profile to a device or group of devices, click **Assign Devices** (see [Assigning Devices to an IDS Fault Profile, page 14-9](#)).

Related Topics

- [Using the Manage IDS Settings Subtab, page 14-6](#)
- [Detecting Excessive Management Frame Transmissions, page 14-47](#)

Displaying EMF Detection Faults

Use **IDS > Summary** to view a summary of the devices that have detected excessive management frame transmissions. This window allows you to:

- View a list of APs that have reported the EMF transmission and, if available, the building and floor in which the AP is located.
- View a history of the EMF transmission faults for the selected device.
- Clear a fault that is generated when an EMF transmission is detected.

**Note**

Your login determines whether you can use this option.

Before You Begin

Satisfy the prerequisites for detecting excessive management frame transmissions (see [Guidelines for Using Excessive Management Frame Detection, page 14-48](#)).

Procedure

-
- Step 1** Select **IDS > Summary**. The Intrusion Detection Summary window appears.
- Step 2** Select **Excessive Management Frames**. The Faults for Excessive Management Frames window appears.
- Step 3** Select the Description or Timestamp fields for the fault. The Fault Details window displays the information about the fault for the selected device (see [Viewing Fault Details, page 3-7](#)).
- Step 4** To clear an EMF fault, see [Clearing Summary Table Faults, page 3-6](#).
-

Related Topics

- [Viewing EMF Detection Reports, page 14-50](#)
- [Understanding Excessive Management Frame Detection, page 14-47](#)

Viewing EMF Detection Reports

The EMF Detection Report displays the collected Excessive Management Frame (EMF) statistics.

Typical Scenarios and FAQs

- How do I view the EMF statistics?

**Note**

Your login determines whether you can use this option.

Before You Begin

Satisfy the prerequisites for detecting excessive management frame transmissions (see [Guidelines for Using Excessive Management Frame Detection, page 14-48](#)).

Procedure

-
- Step 1** Select **IDS > Reports**.
- Step 2** From the Report Name list, select **EMF Detection Report**.
- Step 3** To view all records, click **View** (located to the right of the Report Name, Start Date, and End Date dropdown lists).

**Note**

To see all records *after* a filtering selection has been entered, select another report, then return to this one and click **View**.

Step 4 To view the information for a longer time period (the default is one day), select **Start Date** and **End Date** values from the pulldown lists and click **View**.

Step 5 To narrow the search criteria:

- a. Select **Reported From**, **Frame Type**, **Network BSSID**, or **Transmit Address** from the **Filter By** dropdown list.
- b. Enter any filtering criteria in the text box. You can use an asterisk (*) as a wild card to denote numbers and letters.
- c. Click **Search**.

The data that satisfies the search criteria is displayed below the Search field. The Excessive Management Frame report, which appears to the right of this list, displays the information for the first entry in the list.

- d. Click any other entry in the list to display its corresponding report.

The Excessive Management Frame report displays the following information:

Table 14-12 Excessive Management Frame Report

Column	Description
Reported From	The station that reported the attack.
BSSID	The radio interface of the reporting AP. Note This column is meaningful only for Station faults (see Understanding Excessive Management Frame Detection, page 14-47).
AP Name	For channel faults, the name of the scanning-only AP that detected excessive management frame transmissions.
Channel	The channel that is performing EMF detection.
Frame Type	The frame types that are being monitored: • Associated • ReAssociated • DisAssociated • Authenticated • DeAuthenticated • Probe • Action Frame
Observed Frame Count	The total number of frames detected during the observation interval.
Observation Time	The duration (200 to 5000 milliseconds) during which measurements were taken.
Threshold Frame Count	The number of frames that must be seen in the Observation Time period to generate a fault.

Table 14-12 Excessive Management Frame Report (continued)

Column	Description
Transmit Address	For Station faults, the address of the station that is sending the excessive management packets. For Channel faults, the transmit address is just one of the stations.
Detection Time	The time, based on the client browser, that the scanning-only AP detected excessive management frame transmissions (see Understanding WLSE Time Displays, page 1-10).

- Step 6** Use the buttons to the right of the Report Name, Start Date, and End Date lists to export or email this report.

Related Topics

- [Using the IDS Reports Subtab, page 14-5](#)

Detecting Management Frame Protection Faults

The following sections describe how to use the Management Frame Protection (MFP) feature:

- [Understanding Management Frame Protection, page 14-52](#)
- [Setting the Management Frame Protection Policy, page 14-53](#)
- [Displaying Management Frame Protection Faults, page 14-54](#)
- [Viewing MFP Capabilities Reports, page 14-55](#)
- [Viewing MFP Events Reports, page 14-56](#)

Understanding Management Frame Protection

Although the data frames passing through an 802.11 network are considered to have excellent authentication and privacy through the protocol enhancements of 802.11i, control and management frames are still extremely vulnerable in a strictly 802.11-standard network. Because control and management frames are unauthenticated, any rogue device can, for example, mimic an access point and tell 802.11 client devices that they are no longer associated to that AP.

Management Frame Protection (MFP) inserts secure authentication information into 802.11 management frames to prevent this type of attack. This feature allows network infrastructure devices (APs and their related servers) to be MFP generators and detectors, essentially cross-checking each other during network operations. The primary network-level management takes place at the Wireless Domain Server (WDS) level, and the managed APs provide both generation and detection capabilities. The WLSE functions as a reporting mechanism by logging alerts, sending email to administrators, and so on.

When MFP is enabled for a network, each MFP-capable detector AP queries the WDS when it first observes a management frame from a given generator AP. The WDS tells the detector whether the generator should be producing MFP frames, and, if so, what its AAA keys should be. If the WDS's expectation of the MFP state of the generator AP is violated, the detector AP sends the WDS an MFP report. As all generator APs' AAA keys are rotated, the WDS informs all detector APs ahead of time to avoid false alarms.

Anomalies are reported by a detector AP when the AP receives an 802.11 management frame with one of the following packet states:

MFP State	802.11 Packet States
Enabled	Invalid MIC
	Invalid NTP/Sequence Counter
	No MIC in packet
Disabled	MIC was found when none was expected

Guidelines for Using Management Frame Protection

Prerequisites

Before you can run Management Frame Protection (MFP), you must:

1. Configure your network for radio management (see [Configuring Your Network for Radio Management, page 11-5](#)).



Note

If you choose to disable radio management, only one Intrusion Detection System subtab, **Manage Remaining IDS Settings**, is displayed (see [Using the Manage Remaining IDS Settings Subtab, page 14-11](#)). For information about the faults that will not be generated when Radio Management is disabled, see [Disabled Radio Management Related Faults, page 11-4](#).

2. Enable the Management Frame Protection network-wide setting (see [Setting the Management Frame Protection Policy, page 14-53](#)).
3. Configure the APs and WDSs within your network to make use of a Simple Network Time Protocol (SNTP) server. Without time synchronization of the APs and WDSs to an SNTP server, the strength of MFP to protect the network is substantially weakened.

Setting the Management Frame Protection Policy

Use **IDS > Manage Network-Wide IDS Settings** to enable Management Frame Protection (MFP) and to assign a severity level to MFP faults.

Typical Scenarios and FAQs

- I want (or no longer want) to be notified when a Management Frame Protection fault is detected.
- I want to specify the severity of Management Frame Protection detection notifications.
- I want to view the current Management Frame Protection faults associated with the current [P1...P5] setting.

Before You Begin

Satisfy the Management Frame Protection prerequisites (see [Guidelines for Using Management Frame Protection, page 14-53](#)).

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage Network-Wide IDS Settings**.

Step 2 Select **Management Frame Protection**.

Step 3 Complete the following:

Field	Description
Enable	Click Enable to start Management Frame Protection fault detection. This policy is not enabled by default.
MFP Violation	Select the severity level to assign the fault when a Management Frame Protection fault is detected.
MFP Configuration Mismatch	Select the severity level to assign the fault when an AP's MFP configuration is not as expected.
MFP Time Sync Error	Select the severity level to assign the fault when an AP's MFP timebase is not synchronized.

Step 4 Click **Apply** to set the new entries.

Step 5 To view the MFP Violation faults associated with this profile, click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)) . Click your browser's **Back** button to return to the network-wide setting window. You can also use these options to display MFP faults:

- To view all other faults in addition to the MFP faults, select **IDS > Faults**.
- To view only the MFP Violation faults, select **IDS > Reports > MFP Events**.

Related Topics

[Understanding Management Frame Protection, page 14-52](#)

Displaying Management Frame Protection Faults

You can use **IDS > Summary > MFP Errors** to:

- View a list of APs that are *generating* MFP violations (*not* detecting them).
- View a history of the MFP faults for the selected device.
- Clear a fault that is generated when an MFP violation is detected.

**Note**

Your login determines whether you can use this option.

Before You Begin

Satisfy the prerequisites for detecting Management Frame Protection (MFP) violations (see [Guidelines for Using Management Frame Protection, page 14-53](#)).

Procedure

Step 1 Select **IDS > Summary**. The Intrusion Detection Summary window appears.

Step 2 Select **MFP Errors**. The Faults for MFP Errors window appears.

**Note**

The Management Frame Protection Anomaly Category panel, located below the **MFP Errors** link, summarizes the number of MFP reports that are reporting different MFP errors.

Step 3 Select the Description or Timestamp fields for the fault. The Fault Details window displays the information about the fault for the selected device (see [Viewing Fault Details, page 3-7](#)).

Step 4 To clear an MFP fault, see [Clearing Summary Table Faults, page 3-6](#).

Related Topics

- [Understanding Management Frame Protection, page 14-52](#)
- [Setting the Management Frame Protection Policy, page 14-53](#)

Viewing MFP Capabilities Reports

The MFP Capabilities Report displays the Management Frame Protection (MFP) capabilities of the WLSE's managed APs.

**Note**

Your login determines whether you can use this option.

Before You Begin

Satisfy the prerequisites for detecting Management Frame Protection (MFP) transmissions (see [Guidelines for Using Management Frame Protection, page 14-53](#)).

Procedure

Step 1 Select **IDS > Reports**.

Step 2 From the Report Name list, select **MFP Capabilities Report**.

Step 3 To view all records, click **View** (located to the right of the Report Name, Start Date, and End Date dropdown lists).

**Note**

To see all records *after* a filtering selection has been entered, select another report, then return to this one and click **View**.

Step 4 To view the information for a longer time period (the default is one day), select **Start Date** and **End Date** values from the pulldown lists and click **View**.

Step 5 To narrow the search criteria:

- a. Select **AP Name**, **BSSID**, **PHYType**, or **Software Version** from the **Filter By** dropdown list.
- b. Enter any filtering criteria in the text box. You can use an asterisk (*) as a wild card to denote numbers and letters.
- c. Click **Search**.

The data that satisfies the search criteria is displayed below the Search field. The Management Frame Protection Capabilities report, which appears to the right of this list, displays the information for the first entry in the list.

- d. Click any other entry in the list to display its corresponding report.

The Management Frame Protection Capabilities report displays the following information:

Table 14-13 Management Frame Protection Capabilities Report

Column	Description
AP Name	The name of the managed AP.
BSSID	The radio interface of the managed AP.
PHY	The physical interface type (11a, 11b, or 11g) of the managed AP's radio interface.
Software Version	The software version running on the device.
Generator Capability	The generator capability of the managed AP: None, Full, Non-Beacon/Non-Probe Response.
Detector Capability	The detector capability of the managed AP: None, Full.

Step 6 Use the buttons to the right of the Report Name, Start Date, and End Date lists to export or email this report.

Related Topics

- [Guidelines for Using Management Frame Protection, page 14-53](#)

Viewing MFP Events Reports

The MFP Events Report displays details about the Management Frame Protection (MFP) events reported by the WLSE's managed APs.

Multiple reports are combined together as a single MFP event when the reports are received:

- From the same Detector AP
- About the same Generator AP

- In the same Anomaly Category
- Less than two minutes apart from each other

This information is used to compute the First Event and Latest Event times (see [Table 14-14](#)).

**Note**

Your login determines whether you can use this option.

Before You Begin

Satisfy the prerequisites for detecting Management Frame Protection (MFP) transmissions (see [Guidelines for Using Management Frame Protection](#), page 14-53).

Procedure

Step 1 Select **IDS > Reports**.

Step 2 From the Report Name list, select **MFP Events Report**.

Step 3 To view all records, click **View** (located to the right of the Report Name, Start Date, and End Date dropdown lists).

**Note**

To see all records *after* a filtering selection has been entered, select another report, then return to this one and click **View**.

Step 4 To view the information for a longer time period (the default is one day), select **Start Date** and **End Date** values from the pulldown lists and click **View**.

Step 5 To narrow the search criteria:

- Select **Generator AP Name**, **Generator BSSID**, **Detector AP Name**, **Detector BSSID**, **Generator PHY Type**, or **Category of Anomaly** from the dropdown list.
- Enter any filtering criteria in the text box. You can use an asterisk (*) as a wild card to denote numbers and letters.
- Click **Search**.

The data that satisfies the search criteria is displayed below the Search field. The Management Frame Protection Events report, which appears to the right of this list, displays the information for the first entry in the list.

- Click any other entry in the list to display its corresponding report.

The Management Frame Protection Events report displays the following information:

Table 14-14 Management Frame Protection Events Report

Column	Description
Generator AP Name	The name of the generator AP.
Generator BSSID	The radio interface of the generator AP.
Detector AP Name	The name of the detector AP.
Detector BSSID	The radio interface of the detector AP.
Generator PHY	The physical interface type (11a, 11b, or 11g) of the generator AP's radio interface.

Table 14-14 Management Frame Protection Events Report (continued)

Column	Description
First Event	The time of the first report of this event during the time interval.
Latest Event	The time of the most recent report of this event during the time interval.
Category of Anomaly	The type of anomaly reported by the detector AP (see Understanding Management Frame Protection, page 14-52).
Number of Anomalies	The total number of anomalies of this event during the time interval.
Packet Types	The type of 802.11 packets in which the anomaly was observed.

- Step 6** Use the buttons to the right of the Report Name, Start Date, and End Date lists to export or email this report.

Related Topics

- [Guidelines for Using Management Frame Protection, page 14-53](#)

Detecting Unregistered Clients

The following sections describe how to use the Unregistered Client detection feature:

- [Understanding Unregistered Client Detection, page 14-58](#)
- [Guidelines for Using Unregistered Client Detection, page 14-59](#)
- [Enabling Unregistered Client Detection, page 14-59](#)
- [Displaying Unregistered Client Faults, page 14-60](#)
- [Viewing Unregistered Client Reports, page 14-61](#)

Understanding Unregistered Client Detection

Unregistered clients are clients that are:

- Unsuccessfully attempting to authenticate with the APs during the observation interval and the number of failed attempts crosses the threshold defined by the administrator.
- Sending probe requests.

When you enable the Unregistered Client feature, the WLSE will command all clients (CCX V2 or later with radio management capability) to perform the same radio measurements both on- and off-channels. The clients will then scan other channels in a similar manner to the APs that are performing Radio Monitoring.



Note Clients that participate in Radio Monitoring *do not* increase the coverage area of the network.

Guidelines for Using Unregistered Client Detection

Prerequisites

Before you can use detect unregistered clients, you must:

1. Configure your network for radio management (see [Configuring Your Network for Radio Management, page 11-5](#)).



Note

If you choose to disable radio management, only one Intrusion Detection System subtab, **Manage Remaining IDS Settings**, is displayed (see [Using the Manage Remaining IDS Settings Subtab, page 14-11](#)). For information about the faults that will not be generated when Radio Management is disabled, see [Disabled Radio Management Related Faults, page 11-4](#).

2. Configure access points that will be checking for unregistered clients to run in scanning-only mode.
3. Set the threshold condition for unregistered client detection (see [Enabling Unregistered Client Detection, page 14-59](#)).

Tips

- The Unregistered Client option is applicable only for an AP in *scanning* mode. When an AP is in scanning mode, it monitors the radio environment by looking for rogue APs and unassociated clients; it does not accept client associations.

Enabling Unregistered Client Detection

Use this option to enable unregistered client detection and set the threshold condition and fault priority level.



Note

Your login determines whether you can use this option.

Typical Scenarios and FAQs

- I want (or no longer want) to be notified when an unregistered client has been detected.
- I want to specify the severity of an unregistered client detection notification.

Before You Begin

Satisfy the unregistered client detection prerequisites (see [Guidelines for Using Unregistered Client Detection, page 14-59](#)).

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **Unregistered Client**.



Note

The Unregistered Client option is applicable only for an AP in *scanning* mode.

Step 4 Complete the following:

Field	Description
Enable	Click Enable to enable unregistered client detection. This setting is enabled by default.
Priority	From the dropdown list, select the severity level to assign the fault.
Client Registration Request Count	Enter the minimum value that, when exceeded during a period of 15 minutes, will generate a fault.

Step 5 To see the faults associated with this threshold, you can:

- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
- Select **IDS > Summary > Unregistered Clients Detected**.

Step 6 Click **Apply** to set the new entries.

Step 7 To assign this profile to a device or group of devices, click **Assign Devices** (see [Assigning Devices to an IDS Fault Profile, page 14-9](#)).

Related Topics

- [Using the Manage IDS Settings Subtab, page 14-6](#)
- [Viewing Unregistered Client Reports, page 14-61](#)

Displaying Unregistered Client Faults

Use **IDS > Summary > Unregistered Clients Detected** to view a summary of the unregistered clients.

Typical Scenarios and FAQs

- I have just been notified of an unregistered client. What part of my network has detected this?
- I have just been notified of an unregistered client and I have determined it is no longer a problem. How do I clear the fault?



Note

Your login determines whether you can use this option.

Before You Begin

Satisfy the unregistered client detection prerequisites (see [Guidelines for Using Unregistered Client Detection, page 14-59](#)).

Procedure

Step 1 Select **IDS > Summary**. The Intrusion Detection Summary window appears.

Step 2 Select **Unregistered Clients Detected**. The Faults for Unregistered Clients Detected window appears.

Step 3 To view information about a specific fault, select the Description or Timestamp fields for that fault. The Fault Details window displays the fault information (see [Viewing Fault Details, page 3-7](#)).

- Step 4** To clear an unregistered client fault, see [Clearing Summary Table Faults, page 3-6](#).

Related Topics

[Understanding Unregistered Client Detection, page 14-58](#)

Viewing Unregistered Client Reports

The Unregistered Client Report displays any unregistered clients that are present in the wireless network.

Typical Scenarios and FAQs

- I want to view the unregistered clients that are present in my network.



Note

Your login determines whether you can use this option.

Before You Begin

Satisfy the unregistered client detection prerequisites (see [Guidelines for Using Unregistered Client Detection, page 14-59](#)).



Note

This report is only available from APs in scanning-only mode.

Procedure

- Step 1** Select **IDS > Reports**.
- Step 2** From the Report Name list, select **Unregistered Client Report**.
- Step 3** To view all records, click **View** (located to the right of the Report Name, Start Date, and End Date dropdown lists).
-  **Note** To see all records *after* a filtering selection has been entered, select another report, then return to this one and click **View**.
- Step 4** To view the information for a longer time period (the default is one day), select **Start Date** and **End Date** values from the pulldown lists and click **View**.
- Step 5** To narrow the search criteria:
- Select **Scanning AP Name** or **Client MAC Address** from the dropdown list.
 - Enter any filtering criteria in the text box. You can use an asterisk (*) as a wild card to denote numbers and letters.
 - Click **Search**.
- The data that satisfies the search criteria is displayed below the Search field. The Unregistered Clients report, which appears to the right of this list, displays the information for the first entry in the list.
- Click any other entry in the list to display its corresponding report.

The Unregistered Clients report displays the following information:

Table 14-15 *Unregistered Clients Report*

Column	Description
Scanner AP	The IP address of the reporting AP.
Client MAC	The MAC address of the unregistered client.
Probe Request	The probe request from the unregistered client.
Association Request	The association request from the unregistered client.
Last Seen Time	Indicates the time, based on the client browser, that a scan was run and the unregistered client was detected.

- Step 6** Use the buttons to the right of the Report Name, Start Date, and End Date lists to export or email this report.
-

Related Topics

- [Using the IDS Reports Subtab, page 14-5](#)
- [Detecting Unregistered Clients, page 14-58](#)

Detecting Authentication and Protection Attacks

The following sections describe how to use the Authentication and Protection Attack detection features:

- [Understanding Authentication and Protection Attack Detection, page 14-63](#)
- [Guidelines for Using Authentication and Protection Detection, page 14-64](#)
- [Enabling Authentication and Protection Attack Detection, page 14-65](#)
- [Displaying Authentication and Protection Attack Faults, page 14-79](#)

Understanding Authentication and Protection Attack Detection

The WLSE provides several methods of authentication and protection attack detection:

- [MIC/Encryption Failures, page 14-63](#)
- [MAC Spoofing, page 14-63](#)
- [EAPOL Flooding, page 14-64](#)

MIC/Encryption Failures

After a client successfully authenticates with an AP, it can begin protecting data frames sent to and from the AP. Several failures that can be identified during this protection phase can broadly be categorized as decrypt errors, MIC failures or replay failures. In all cases, when the AP detects a given failure, it updates the appropriate MIB counter.

In addition, the Michael MIC employed in TKIP is known to be weak and requires some additional counter measures to ensure protection. The counter measure involves disabling the interface whenever the MIC has been deemed to be compromised. Each time a counter measure is enforced a MIB variable is incremented.

The WLSE periodically polls the MIB counters described above and compares against a pre-defined threshold to determine when a failure has occurred. When a failure takes place, the WLSE generates a fault.

MAC Spoofing

When a client roams from one AP to another, the switches connected to the AP must update the forwarding tables so that the client's layer 2 frames are properly forwarded to the new AP. However, it is possible for a client to authenticate with a new AP using another client's MAC address, causing the frames for the valid client to be sent to the spoofing client.

The WDS, however, is in a position to detect when a valid client has had its MAC address spoofed. The WDS maintains a mapping of user ID to client MAC address based on WLCCP registrations. When there is another authentication request from the same MAC address with a different user ID it is flagged as a MAC spoofing.

When the Wireless Client MAC Spoofing IDS fault is enabled on the WLSE, it polls the MIB `ciscoWdsIdsMacSpoofClient` at the configured polling interval. (The default polling interval is 5 minutes.)

The WLSE generates faults for all clients identified by the MIB `ciscoWdsIdsMacSpoofClient`. The MIB retains the history of all spoofed MAC addresses. An entry from the WDS MIB is cleared when:

- The WDS AP reaches the maximum number of events to hold for a reporting non-WDS AP. The maximum number is determined by the MIBS `ciscoWdsIdsMaxMacAddresses` and `ciscoWdsIdsMaxEntriesPerMac`.
- When the WDS is not configured. Because the AP maintains a history, the WLSE raises the MAC spoofing fault on the next polling cycle even after clearing the fault on the WLSE.

EAPOL Flooding

The vast majority of wireless LANs deployed today employ some form of 802.1X authentication. In these networks a client can only transmit data packets after it successfully authenticates with an AP. The 802.1X authentication that takes place between the client and the AP triggers a series of messages between the AP, the authenticator, and an authentication server using EAPOL (Extensive Authentication Protocol over LAN) messaging. The authentication server, typically a RADIUS server, can quickly become overwhelmed if there are too many authentication attempts. If not regulated, a single client can trigger enough authentication requests to launch a DoS attack on the rest of the network.

Currently Cisco APs provide rate limiting functionality that prevents these types of attacks. If any single user makes more than three 802.1X authentication attempts within 30 seconds the client is placed on a black list for a configurable period of time (default of 60 seconds). Once blacklisted, the client's subsequent 802.1X authentication attempts are rejected. For this existing rate limiting feature the detection threshold is not configurable.

This rate limiting functionality now provides general detection of the EAPOL flood attacks. An administrator-controlled number of 802.1X authentication attempts per unit of time can be entered via the CLI on an AP or via the WLSE GUI. The parameters apply to the entire radio interface. When the threshold is crossed, the AP indicates the event by recording a MIB variable indicating that the failure occurred and the MAC address of the client with the largest number of attempts.

The WLSE periodically polls these MIB variables to determine when an EAPOL flooding failure occurred. The WLSE generates a fault when it finds a record of this event.

Guidelines for Using Authentication and Protection Detection

Prerequisites

Before you can use detect the Authentication and Protection Attack detection features, you must:

1. Configure your network for radio management (see [Configuring Your Network for Radio Management](#), page 11-5).



Note

If you choose to disable radio management, only one Intrusion Detection System subtab, **Manage Remaining IDS Settings**, is displayed (see [Using the Manage Remaining IDS Settings Subtab](#), page 14-11). For information about the faults that will not be generated when Radio Management is disabled, see [Disabled Radio Management Related Faults](#), page 11-4.

2. Set the threshold condition for Authentication and Protection Attack detection features (see [Enabling Authentication and Protection Attack Detection](#), page 14-65).

Enabling Authentication and Protection Attack Detection

The following sections describe how to set the authentication and protection attack fault settings. When the thresholds are exceeded, faults are generated and can be viewed under **Faults > Display Faults** or **IDS > Faults**.

- MIC/encryption failure thresholds:
 - [Setting the TkipReplayClient Policy, page 14-65](#)
 - [Setting the TkipLocalMicFailureClient Policy, page 14-66](#)
 - [Setting the TkipRemoteMicFailureClient Policy, page 14-67](#)
 - [Setting the CcmpReplaysClient Policy, page 14-68](#)
 - [Setting the CcmpDecryptErrorsClient Policy, page 14-69](#)
- MAC spoofing threshold:
 - [Setting MAC Spoofing Policy, page 14-70](#)
- EAPOL flooding thresholds:
 - [Setting EAPOL Settings \(IOS\) Policy, page 14-71](#)
 - [Setting the EAPOL Detection \(IOS\) Policy, page 14-72](#)
- Radio interface thresholds:
 - [Setting the Association Error Rate Policy, page 14-73](#)
 - [Setting the TKIP Local MIC Failures Policy, page 14-74](#)
 - [Setting the TKIP Remote MIC Failures Policy, page 14-75](#)
 - [Setting the TKIP Counter Measure Invoked Policy, page 14-76](#)
 - [Setting the TKIP Replays Detected Policy, page 14-77](#)
 - [Setting the CCMP Replays Discarded Policy, page 14-78](#)

Setting the TkipReplayClient Policy

Use this policy to check **TKIP** replay errors. A fault is generated when the counter value increases from the last polled value. By default, polling is every 5 minutes. This setting can be applied to IOS devices only.

**Note**

This setting is applicable to the *access point*; it is not set per radio interface type and is not reported by interface type on the Faults page.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **TkipReplayClient[IOS]**.

Step 4 Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from the list.
Detect	Select the severity level to be assigned to the fault.

Step 5 Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

Step 6 To see the faults associated with this threshold, you can:

- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
- Select **IDS > Summary**, then select the fault type.

Step 7 To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

- [Using the Manage IDS Settings Subtab, page 14-6](#)
- [Understanding Authentication and Protection Attack Detection, page 14-63](#)

Setting the TkipLocalMicFailureClient Policy

Use this policy to check local **TKIP** MIC failure errors. A fault is generated when the counter value increases from the last polled value. By default, polling is every 5 minutes.



Note

This setting is applicable to the *access point*; it is not set per radio interface type and is not reported by interface type on the Faults page.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.

Step 2 Select an existing IDS fault profile and click **Edit**.

Step 3 Select **TkipLocalMicFailureClient**.

Step 4 Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from the list.
Detect	Select the severity level to be assigned to the fault.

Step 5 Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

Step 6 To see the faults associated with this threshold, you can:

- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
- Select **IDS > Summary**, then select the fault type.

Step 7 To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

- [Using the Manage IDS Settings Subtab, page 14-6](#)
- [Understanding Authentication and Protection Attack Detection, page 14-63](#)

Setting the TkipRemoteMicFailureClient Policy

Use this policy to check remote **TKIP** MIC failure errors. A fault is generated when the counter value increases from the last polled value. By default, polling is every 5 minutes.



Note

This setting is applicable to the *access point*; it is not set per radio interface type and is not reported by interface type on the Faults page.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.

Step 2 Select an existing IDS fault profile and click **Edit**.

Step 3 Select **TkipRemoteMicFailureClient**.

Step 4 Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from the list.
Detect	Select the severity level to be assigned to the fault.

Step 5 Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

Step 6 To see the faults associated with this threshold, you can:

- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
- Select **IDS > Summary**, then select the fault type.

Step 7 To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

- [Using the Manage IDS Settings Subtab, page 14-6](#)
- [Understanding Authentication and Protection Attack Detection, page 14-63](#)

Setting the CcmpReplaysClient Policy

Use this policy to check the number of unicast fragments received by the **CCMP** play mechanism on the interface. A fault will be generated when the counter value increases from the last polled counter value. By default, the polling is every 5 minutes.



Note

This setting is applicable to the *access point*; it is not set per radio interface type and is not reported by interface type on the Faults page.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.

Step 2 Select an existing IDS fault profile and click **Edit**.

Step 3 Select **CcmpReplaysClient**.

Step 4 Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from the list.
Detect	Select the severity level to be assigned to the fault.

Step 5 Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

Step 6 To see the faults associated with this threshold, you can:

- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
- Select **IDS > Summary**, then select the fault type.

Step 7 To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

- [Using the Manage IDS Settings Subtab, page 14-6](#)
- [Understanding Authentication and Protection Attack Detection, page 14-63](#)

Setting the CcmpDecryptErrorsClient Policy

Use this policy to check the number of decryption errors detected by the **CCMP** play mechanism on the interface. A fault will be generated when the counter value increases from the last polled counter value. By default, the polling is every 5 minutes.



Note

This setting is applicable to the *access point*; it is not set per radio interface type and is not reported by interface type on the Faults page.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.

Step 2 Select an existing IDS fault profile and click **Edit**.

Step 3 Select **CcmpDecryptErrorsClient**.

Step 4 Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from the list.
Detect	Select the severity level to be assigned to the fault.

Step 5 Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

Step 6 To see the faults associated with this threshold, you can:

- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
- Select **IDS > Summary**, then select the fault type.

Step 7 To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

- [Using the Manage IDS Settings Subtab, page 14-6](#)
- [Understanding Authentication and Protection Attack Detection, page 14-63](#)

Setting MAC Spoofing Policy

This policy counts the number of times a valid client has had its MAC address spoofed. A fault will be generated when the counter value increases from the last polled counter value. By default, the polling is every 5 minutes.



Note

This setting is applicable to the *access point*; it is not set per radio interface type and is not reported by interface type on the Faults page.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.

Step 2 Select an existing IDS fault profile and click **Edit**.

Step 3 Select **Wireless Client MAC Spoofing**.

Step 4 Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from the list.
Detect	Select the severity level to be assigned to the fault when Wireless Client MAC Spoofing is detected.

- Step 5** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.
- Step 6** To see the faults associated with this threshold, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > Wireless Client MAC Spoofing**.
- Step 7** To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Setting EAPOL Settings (IOS) Policy

This policy sets the threshold settings for **EAPOL** flood attacks. A fault will be generated when the counter value increases from the last polled counter value.



Note

This setting is applicable to the *access point*; it is not set per radio interface type and is not reported by interface type on the Faults page.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **EAPOL Settings**.
- Step 4** Complete the following:

Field	Description
Enable	Select to enable the policy.

Field	Description
EAP Attempts [1-512]	Number of allowed EAP attempts during a polling interval before a fault is raised.
Interval [1-60]	The polling interval (in seconds).

- Step 5** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.
- Step 6** To assign this profile to a device or group of devices, click **Assign Devices** from the IDS Fault Settings window (see [Assigning Devices to an IDS Fault Profile](#), page 14-9).
- Step 7** Go to [Setting the EAPOL Detection \(IOS\) Policy](#), page 14-72.

Related Topics

[Using the Manage IDS Settings Subtab](#), page 14-6

Setting the EAPOL Detection (IOS) Policy

Use this policy to count the number of [EAPOL](#) flood attacks that have been attempted on a valid client. A fault will be generated when the counter value increases from the last polled counter value. By default, the polling is every 10 minutes.



Note

This setting is applicable to the *access point*; it is not set per radio interface type and is not reported by interface type on the Faults page.



Note

Your login determines whether you can use this option.

Before You Begin

Set the EAPOL Settings (see [Setting EAPOL Settings \(IOS\) Policy](#), page 14-71).

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **EAPOL Detection**.
- Step 4** Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from the list.
Detect	Select the severity level to be assigned to the fault when an excessive number of EAPOL flooding faults are detected (see Setting EAPOL Settings (IOS) Policy , page 14-71).

- Step 5** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.
- Step 6** To see the faults associated with this threshold, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > EAPOL Flood Detection**.
- Step 7** To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Setting the Association Error Rate Policy

Use this policy to check the number of association errors detected on the interface. A fault is generated when the counter value increases from the last polled counter value. By default, polling is every 5 minutes.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **IDS-802.11x** (where x = a, b, or g).
- Step 4** Select **Association Error Rate**.
- Step 5** Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from each list.
Overloaded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Overloaded.
Degraded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Degraded.
OK	Select the number of consecutive polling cycles after which, when the error rate falls below the minimum per-minute error rate for the Degraded state, the status is OK.

- Step 6** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.
- Step 7** To see the faults associated with this threshold, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > Authentication Failures**.
- Step 8** To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Setting the TKIP Local MIC Failures Policy

Use this policy to check the number of **TKIP** local MIC failures detected on the interface. A fault is generated when the counter value increases from the last polled counter value. This setting can be applied to IOS devices only.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **IDS-802.11x** (where x = a, b, or g).
- Step 4** Select **TKIP Local MIC failures [IOS]**.
- Step 5** Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from each list.
Overloaded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Overloaded.
Degraded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Degraded.
OK	Select the number of consecutive polling cycles after which, when the error rate falls below the minimum per-minute error rate for the Degraded state, the status is OK.

- Step 6** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.
- Step 7** To see the faults associated with this threshold, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > Authentication Failures**.
- Step 8** To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Setting the TKIP Remote MIC Failures Policy

Use this policy to check the number of **TKIP** remote MIC failures detected on the interface. A fault is generated when the counter value increases from the last polled counter value. This setting can be applied to IOS devices only.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **IDS-802.11x** (where x = a, b, or g).
- Step 4** Select **TKIP Remote MIC failures [IOS]**.
- Step 5** Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from each list.
Overloaded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Overloaded.
Degraded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Degraded.
OK	Select the number of consecutive polling cycles after which, when the error rate falls below the minimum per-minute error rate for the Degraded state, the status is OK.

- Step 6** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.
- Step 7** To see the faults associated with this threshold, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > Authentication Failures**.
- Step 8** To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Setting the TKIP Counter Measure Invoked Policy

Use this policy to check the number of **TKIP** counter measures invoked on the interface. A fault is generated when the counter value increases from the last polled counter value. This setting can be applied to IOS devices only.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **IDS-802.11x** (where x = a, b, or g).
- Step 4** Select **TKIP Counter Measure Invoked [IOS]**.
- Step 5** Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from each list.
Overloaded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Overloaded.
Degraded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Degraded.
OK	Select the number of consecutive polling cycles after which, when the error rate falls below the minimum per-minute error rate for the Degraded state, the status is OK.

- Step 6** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.
- Step 7** To see the faults associated with this threshold, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > Authentication Failures**.
- Step 8** To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Setting the TKIP Replays Detected Policy

Use this policy to check [TKIP](#) replay errors. A fault is generated when the counter value increases from the last polled value. This setting can be applied to IOS devices only.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **IDS-802.11x** (where x = a, b, or g).
- Step 4** Select **TKIP Replays Detected [IOS]**.
- Step 5** Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from each list.
Overloaded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Overloaded.
Degraded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Degraded.
OK	Select the number of consecutive polling cycles after which, when the error rate falls below the minimum per-minute error rate for the Degraded state, the status is OK.

- Step 6** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

- Step 7** To see the faults associated with this threshold, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > Authentication Failures**.
- Step 8** To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Setting the CCMP Replays Discarded Policy

Use this policy to check the number of received unicast fragments discarded by the **CCMP** play mechanism on the interface. A fault will be generated when the counter value increases from the last polled counter value. This setting can be applied to IOS devices only.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **IDS-802.11x** (where x = a, b, or g).
- Step 4** Select **CCMP Replays Discarded [IOS]**.
- Step 5** Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from each list.
Overloaded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Overloaded.
Degraded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Degraded.
OK	Select the number of consecutive polling cycles after which, when the error rate falls below the minimum per-minute error rate for the Degraded state, the status is OK.

- Step 6** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

- Step 7** To see the faults associated with this threshold, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > Authentication Failures**.
- Step 8** To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Displaying Authentication and Protection Attack Faults

Use **IDS > Summary** to view a summary of the various authentication and protection attack faults.



Note

Your login determines whether you can use this option.

Before You Begin

Satisfy the authentication and protection detection prerequisites (see [Guidelines for Using Authentication and Protection Detection, page 14-64](#)).

Procedure

- Step 1** Select **IDS > Summary**. The Intrusion Detection Summary window appears.
- Step 2** Select one of the following fault types:
- **Association Error Rate**
 - **Authentication Failures**
 - **Wireless Client MAC Spoofing**
 - **EAPOL Flood Detection**
- The Fault Summary window for the selected fault type appears.
- Step 3** To view information about a specific fault, select the Description or Timestamp fields for that fault. The Fault Details window displays the fault information (see [Viewing Fault Details, page 3-7](#)).
- Step 4** To clear a fault, see [Clearing Summary Table Faults, page 3-6](#).

Related Topics

[Understanding Authentication and Protection Attack Detection, page 14-63](#)



Managing Your Voice Network

The WLSE allows you to display voice call information for devices in your network, manage voice settings and set up voice notifications. Using the WLSE VoWLAN features, you can:

Table 15-1 **Voice Features**

Feature	For More Information, See
Enable radio management for VoWLAN on your network and assign voice configuration settings	Enabling VoWLAN, page 15-6
Display and update voice-related faults.	Monitoring Your Voice Network, page 15-7
Display voice-related information for an AP, a floor, or the entire network.	Generating Voice Reports, page 15-8

Related Topics

- [Understanding Radio Management for VoWLAN, page 15-1](#)
- [Guidelines for Using Voice, page 15-5](#)

Understanding Radio Management for VoWLAN

The following topics explain some basic voice fundamentals and how WLSE has implemented these features:

- [Understanding Call Admission Control, page 15-1](#)
- [Understanding Roaming, page 15-3](#)
- [Understanding Voice Packet Latency, Jitter, and Loss, page 15-3](#)
- [Voice Capacity Planning, page 15-5](#)

Understanding Call Admission Control

A WLAN provides differentiated services for voice, best-effort data, and other traffic. For these differentiated services to provide sufficient quality of service (QoS) for voice packets, only a certain amount of voice bandwidth can be serviced or admitted. If the amount of voice traffic is increased

beyond this limit, the QoS of all calls will suffer. The Call Admission Control (CAC) function allocates this bandwidth to client devices on a first-come, first-served basis. However, it also maintains a small reserve so mobile phone clients can roam into a BSS, even if the BSS would otherwise be at full capacity.

One of the key aspects when considering the network capacity of a WLAN is that it is a *shared* medium, and therefore radio contention among various client devices is limited when compared to that of a wired LAN. This affects the overall throughput of packet processing and transportation, especially for the voice traffic, which requires timely delivery when other types of packets such as data are competing for the medium.

When transmitted over a WLAN IP network, the requirements of voice and data are very different:

	Voice	Data
Packet Flow	Steady/Consistent	Bursts
Packet Delay	Sensitive	Insensitive
Packet Loss	Sensitive	Insensitive
Bandwidth Contention	On demand (UDP)	As much as allowed (TCP)
Mobility	Delay sensitive	Delay insensitive

With the growing demand and broader deployment of voice application on WLAN, the issues of packet latency and packet loss become more important. The WLSE provides voice-related measurements on APs and clients that help isolate where the network bottleneck problems or impairments such as interference are introduced.

Radio management for VoWLAN on the WLSE consists of two components: radio coverage and radio diagnostics.

- **Radio coverage:**

- Ensures that there is sufficient signal strength everywhere the handset will be used.

To ensure good radio coverage, the coverage predictions made by WLSE must be based on site survey measurements—otherwise there is not sufficient confidence to reliably predict coverage.

- Ensures that there is sufficient overlap in radio coverage provided by adjacent APs so that a client roaming from one BSS to another has sufficient signal strength.

Radio management predicts call capacity on an AP basis to give the network administrator a prediction of overall network call capacity.

- Predicting the voice capacity of the network and individual APs.

- **Radio diagnostics** are used to troubleshoot problems (in particular, audio problems) encountered by handset users. Diagnostic information helps the network administrator decide whether the problem is in the WLAN or in the wired infrastructure. The WLSE:

- Receives and displays aggregated WLAN instrumentation metrics and traffic specification metrics.

The traffic stream metrics measurements are collected by the APs and their associated clients, aggregated by the WDS, and archived and displayed at the WLSE. The WLSE can also enable or disable traffic stream metrics collection on a global or AP basis.

- Provides network troubleshooting by reporting WLAN instrumentation networks on a network and AP basis.

WLAN instrumentation metrics help network administrators diagnose problems on the VoWLAN. In particular, this data provides an administrator with the ability to determine whether a problem (which is most likely reported by end users as poor audio quality) is caused by an impairment on the WLAN. There are only a few impairments caused by the WLAN that impact audio quality. By observing these metrics, a network administrator can determine whether they are within normal limits or out-of-range for WLAN operation, and which APs and their corresponding service areas are affected by interference.

Understanding Roaming

Roaming is the ability to move from one AP coverage area to another without interruption in service or loss in connectivity. There are two types of roaming:

- Layer 2 roaming occurs when a WLAN device (such as a Cisco 7920 phone) moves far enough that its radio associates with a different AP. During Layer 2 roaming, the original and the new AP offer coverage for the same IP subnet, so the device's IP address is still valid after the roam.
- Layer 3 roaming occurs when a client moves from an AP that covers one IP subnet to an AP that covers another IP subnet. At that point, the client no longer has an IP address and default gateway that are valid within the new IP subnet. Because the client's IP address and default gateway are no longer valid, its existing data sessions or voice calls fail because the remote client can no longer reach the local client.

To maintain robust audio quality during roaming, the radio design for the WLAN must provide for sufficient BSS overlap. When a handset approaches the edge of a BSS during a call, it must have sufficient coverage overlap to the adjacent cell so that radio coverage is maintained while the handset is making the decision to roam. If there is insufficient overlap, there will be an audio gap when the handset roams. Typically handsets will continually scan the APs in the neighbor list to stay associated with the best AP.

Roaming delay is the time it takes for roaming to complete, depending on the duration of:

- The scanning process—Determining which neighboring APs have sufficient received signal level (RSL) and capacity. Typically this is a continuous background process that does not impact roaming time. *Roaming time* is the time the last downstream voice packet is received on the old AP to the time the first downstream voice packet is received on the new AP. Roaming time is measured by the client and reported to the AP.
- The 802.1x authentication process.
- The 802.11 association process.

Understanding Voice Packet Latency, Jitter, and Loss

Voice packets (also known as media or RTP packets) are time sensitive. If they are delivered too late to a receiver's playout buffer, which briefly stores packets prior to the voice decoder converting the packet to audio, the buffer runs dry and must employ a packet loss concealment algorithm to mitigate the effect of the lost or delayed packet. If packets suffer too much jitter while traversing the network or WLAN, they will be of no use. If the packets are delayed too long while traversing the end-to-end network, the quality of the conversation will degrade.

All SWAN components measure and report traffic stream metrics; the APs and clients measure them, the APs collect the measurements and send them to WLSE through WDS, and the WLSE displays and archives them and raises faults if they exceed certain configurable thresholds. By studying packet latency, jitter, and loss, a network administrator can isolate the source of bad voice quality.

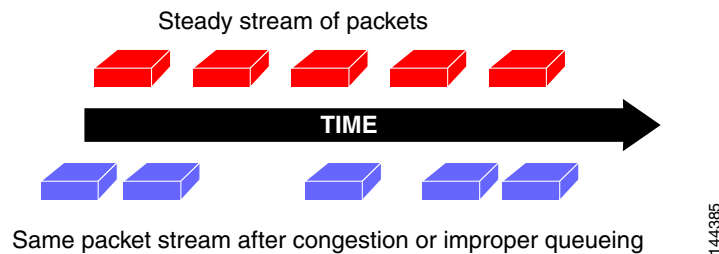
Packet Latency (Delay)

Packet latency is the time it takes for a packet (a unit of data, in this case voice data) to cross a network connection from sender to receiver. Packet delays on WLAN are usually caused by excessive data traffic volume traversing on APs and clients or by congested radio on the air. If end-to-end delay is too high, the two parties will have a tendency to double talk.

When packet delay is measured, the AP indicates whether the client is using **U-APSD** (unsolicited automatic power save delivery). Although the U-APSD feature provides a dramatic improvement in talk time for battery-powered handsets, the **jitter** performance can be quite different when compared to normal packet delivery.

Packet Jitter

Jitter is a variation in the latency of received packets. At the sending side, packets are sent, spaced evenly apart, in a continuous stream. Jitter results when a packet gets queued or delayed somewhere in the circuit, where there was no delay or queueing for other packets. Due to network congestion, improper queueing, or configuration errors, the delay between each packet can vary instead of remaining constant.



The **DSPs** inside the router can make up for some jitter, but can be overcome by excessive jitter. This results in poor voice quality.

Packet Loss

Packet loss, which is measured on the uplink and downlink, takes into account:

- Queue management. This may happen on either the uplink or the downlink, but might be more likely to happen on the downlink, where packets cannot be delivered to a specific client. In this case, the AP might discard packets to prevent its queues from overflowing.
- Maximum retry count. Maximum retry count is reached, for example, under congested conditions or due to foreign interference.
- Because VoWLAN is using the unlicensed spectrum, there is no way to prevent foreign interference, but fault notifications generated by WLSE will enable a network administrator to know when foreign interference is occurring.
- Packet age-out mechanism. To make sure it does not add significant delay for voice traffic, the AP drops a voice packet if it is already too old. It also drops the oldest voice packet in the queue when it detects voice traffic congestion.

If there is too much packet loss for voice packets, the audio **codecs** are unable to adequately conceal the packet loss, resulting in reduced audio quality.

- Radio Management (RM) events. The WLAN continuously employs an RM function to scan for rogue APs, perform self healing, and other related functions. APs must momentarily stop traffic on their serving channel to scan other channels to support these tasks.

Voice Capacity Planning

After sufficient radio coverage and BSS overlap have been set by the RPG, the network administrator needs to know the number of calls each AP is capable of handling. Voice capacity prediction is based on analyzing the amount of BSS overlap from co-channel APs in conjunction with the knowledge of the basic call capacity of the AP on a clear channel. To the extent that APs overlap, the voice capacity between these APs is shared. The degree of overlap is quite different between the 2.4-GHz and 5-GHz bands. AP coverage overlap can be caused by APs on the same floor or by APs on a different floor of the building. Overlap from APs on different floors is expected to be much greater in the 2.4-GHz band.

WLSE provides two ways to specify a usage limit for voice traffic:

- A global limit that applies to all APs; the network administrator can use this limit to ensure that a certain percentage of the WLAN is reserved for mission-critical data traffic.
- An AP-specific limit. The lower value of the two limits should be pushed to each AP during configuration. The AP-specific limit can be used to:
 - Fine tune the network during the planning phase.

Example 1: Some APs are in disadvantaged locations (prone to interference) and require a lower capacity limit to maintain good audio quality. For example, there might be a 2.4-GHz AP servicing a lunchroom that has a microwave oven, or a hospital with legacy frequency-hopping APs that limit call capacity.

Example 2: The radio frequency planning tool identifies that two APs have overlapping coverage and one of the APs primarily services a conference room while the other primarily services cubicles. In this situation, the network administrator may might to apply most of the channel's capacity to the AP servicing the conference room.

- Fine tune the network during troubleshooting. Some APs might have too high a delay or packet loss during operation. If the network administrator is unable to locate any problem interference or other bug, reducing the call limit could help solve the user complaint.

Guidelines for Using Voice

Prerequisites

Before you can use WLSE to manage voice traffic over your WLAN, you must:

1. Configure your network for radio management (see [Configuring Your Network for Radio Management, page 11-5](#)). If your network is not properly configured, *none of the Voice functions will work*.
2. Define the location elements (buildings and floors) and place the APs on the floor images. This step is optional, but will help you get the best results from the Location Manager displays. For more information, see:
 - [Entering Building Information, page 13-4](#)
 - [Adding Floors to Location Manager, page 13-9](#)
 - [Adding Devices to Floors, page 13-14](#)
3. Optional (but necessary to accurately locate rogue APs): Perform an AP Radio Scan on all APs on the specified floor (see [Using AP Radio Scans to Collect RM Data, page 13-43](#)).
4. Be sure Radio Monitoring is enabled on all APs (for both serving and non-serving channels) on the specified floor (see [Starting Radio Monitoring, page 12-4](#)).

**Note**

Radio Monitoring is enabled by default; if it has been disabled, you must re-enable it.

5. Set policies to enable voice management (see [Enabling VoWLAN, page 15-6](#)).

Tips

- Use the *roaming count* value to diagnose problems in a client roaming algorithm or the network design that cause the client to micro-roam between two APs (ping-pong quickly back and forth).
- When compared to normal packet delivery, the jitter performance might be quite different for clients using U-APSD (unsolicited automatic power save delivery).
- Before a voice handset can have reliable audio quality, there must be sufficient signal strength (RSSI or RSL) wherever a user will go in the enterprise. For network administrators to have confidence in the radio coverage, a site survey must be performed and the data imported into WLSE. Then, as the RPG (radio parameter generation) program adjusts the transmitter power levels and performs channel assignments, the coverage levels will be correct. It is important the antenna gain of the radio used for site survey be accounted for when the site survey data is imported as it is likely to be higher than that of the voice handset.
- Due to the interaction between the desired capacity and the required level of radio coverage, the network administrator must have some knowledge of the desired capacity when setting the coverage level requirements. For example, VoWLAN operation based on 24-Mbps results in greater capacity than 6-Mbps but reduced radio coverage. The trade-off between capacity and radio coverage is different in each deployment as well as between 2.4-GHz and 5-GHz bands.
- Radio coverage is *not* static. Enterprise users routinely change their environment by doing things such as adding walls or shelves. Radio coverage will need to be reevaluated after these occurrences and the affected area might need to be resurveyed.

Enabling VoWLAN

Use the procedures in this section to enable voice management on the WLSE.

**Note**

Your login determines whether you can use this option.

Before You Begin

Satisfy the prerequisites for running voice monitoring (see [Guidelines for Using Voice, page 15-5](#)).

Procedure

- Step 1** To enable CAC and Traffic Stream metrics in the APs and generate the default voice settings, select **Configure > Templates**, create a new template or edit an existing template, then select **Voice Express**. Enter the required information (see [Configuring Voice Express, page 5-14](#)), then push the new configuration to the devices.
- Step 2** Enable voice bandwidth faults.
To enable voice bandwidth faults on a device or group of devices, select **Faults > Manage Fault Settings**. Select the fault setting you want to edit from the Existing Fault settings table, click **Edit**, then select **Radio-802.11a Thresholds > Voice Bandwidth**. For more information about this feature, see [Setting Voice Bandwidth Threshold, page 3-41](#).

Step 3 Enable QoS status faults.

To enable voice quality of service (QoS) status faults on a device or group of devices, select **Faults > Manage Fault Settings**. Select the fault setting you want to edit from the Existing Fault settings table, click **Edit**, then select **Radio-802.11a Thresholds > Voice QoS Status**. For more information about this feature, see [Setting Voice QoS Status Threshold](#), page 3-42.

Step 4 Assign voice QoS settings.

To configure the voice QoS settings, select **Faults > Voice QoS Settings**. You can assign the following Voice QoS settings:

- Downstream Delay with U-ASPD not used
- Downstream Delay with U-ASPD used
- Upstream Delay
- Downstream Packet Loss Rate
- Upstream Packet Loss Rate
- Roaming Time

For more information about this feature, see [Assigning Voice QoS Fault Settings](#), page 3-54.

Step 5 Define voice fault notification targets.

When a fault is detected, the WLSE can send automated notifications in the form of SNMP traps, syslog messages, and email alerts. You can specify multiple recipients for each notification type, and choose to deliver the message using either a plain text or XML format.

To create fault notification targets for Voice traps, syslog messages, and emails, select **Faults > Notification Settings**. For more information about this feature, see [Notification Settings](#), page 3-56.

Related Topics

[Monitoring Your Voice Network](#), page 15-7

Monitoring Your Voice Network

Select **Faults > Voice Summary** to display all voice fault information. Voice faults will not appear in this table until the fault has been enabled. For more information about this feature, see [Viewing the Status of the VoWLAN](#), page 3-53.

Generating Voice Reports

The **Reports > Voice** option displays voice call information about the devices in your network. This information can be shown for an AP, a single floor, or the entire network. You can view, export, and email the reports. Using this option, you can view the following types of current reports:

- Group Reports:
 - [AP Group Call Summary: Current, page 10-24](#)
 - [AP Group Metrics Summary: Current, page 10-25](#)
- Access Point Reports:
 - [AP Detail: Current, page 10-27](#)
 - [AP Detail: Last Hour, page 10-29](#)
 - [Voice Queuing Delay, page 10-30](#)
 - [Voice Packet Loss, page 10-31](#)
 - [Voice Roaming, page 10-33](#)
 - [Bandwidth In Use, page 10-34](#)
 - [Voice Streams In Progress, page 10-35](#)
 - [Rejected Voice Streams, page 10-36](#)
- Wireless Clients:
 - [Voice Client Detail: Last Hour, page 10-43](#)

For more information about these reports, see [Displaying Voice Reports, page 10-24](#) and [Displaying Wireless Client Reports, page 10-37](#).



Managing the WLSE System

This chapter contains the following major sections:

- [Ports and Protocols, page 16-1](#)
- [Overview of the Admin Tab, page 16-2](#)
- [Managing the Appliance, page 16-2](#)
- [Managing Firmware Version Support, page 16-49](#)
- [Managing GUI Users, page 16-49](#)
- [Modifying Your Profile, page 16-55](#)
- [Creating Links, page 16-57](#)



Note

Some of the Admin subtabs may not be visible to some users; what you see under the Admin tab depends on the roles assigned to your login.



Note

WLSE 2.13 does not support MS NT Domain authentication.

Ports and Protocols

For information by the ports hosted by and used by the WLSE and the protocols used for network management functions, see [Appendix C, “Ports and Protocols.”](#)

Overview of the Admin Tab

Table 16-1 describes the subtabs and options that are displayed under the Admin tab.

Table 16-1 Functions of the Admin Tab

Subtab	Description	Reference
Appliance	Manage WLSE system.	Managing the Appliance, page 16-2
System	View and manage supported AP firmware versions.	Managing Firmware Version Support, page 16-49
AAA Administration (WLSE Express only)	Internal authentication and authorization server.	Chapter 18, “Using the Internal AAA Server (WLSE Express Only)”
User Admin	Manage users and user roles.	Managing GUI Users, page 16-49
My Profile	Set password, email address, and customize Web interface per user.	Modifying Your Profile, page 16-55
Links	Set up links to other systems (such as CiscoWorks servers) and run the ACS failed login report.	Creating Links, page 16-57

Managing the Appliance

Options under the Appliance subtab allow you to manage the WLSE system and use connectivity tools. When you select **Admin > Appliance**, the following options are displayed.

**Note**

Your login determines whether you can use these options.

Table 16-2 Appliance Subtab Options

Option	Description	References
Status	Use WLSE log files. Restart the WLSE.	Using WLSE Log Files, page 16-4 Restarting the WLSE, page 16-7
Software	Manage WLSE system software.	Managing WLSE System Software, page 16-7

Table 16-2 **Appliance Subtab Options (continued)**

Option	Description	References
Security	Manage WLSE security: • Use authentication modules for WLSE users (alternative authentication server). • Obtain a certificate for secure Web access. • Configure Telnet and SSH access. • View the last 10 users who have logged on.	Managing Security, page 16-15
Backup and Restore	Back up and restore WLSE data.	Backing Up and Restoring Data, page 16-20
Master Configuration (WLSE Express only)	Export WLSE's configuration to a file.	Managing WLSE Master Configuration Files (WLSE Express Only), page 16-26
Redundancy	Manage redundant WLSEs. Two WLSEs can be managed as a high-availability cluster.	Managing WLSE Redundancy, page 16-28
Diagnostics	Diagnose WLSE: • Status reports • Self tests • Process management	Using WLSE Diagnostics Options, page 16-39
Splash Screen	Add a message to users at login.	Specifying a Splash Screen Message, page 16-43
Time/NTP/Name/Web Timeout	Set system parameters: • System time and NTP • Name servers • Web timeout period	Setting Time, Time Servers, Name Servers, and Web Session Timeout, page 16-43
Configure Mailroute	Specify a mail server for email forwarding.	Configuring the Mail Route, page 16-45
TFTP Management (WLSE Express only)	Manage files on the WLSE by using the internal TFTP server.	Managing Files for the WLSE TFTP Server (WLSE Express Only), page 16-45
Connectivity Tools	Test network connectivity.	Using Connectivity Tools, page 16-47

Using WLSE Log Files

This option allows you to view the contents of WLSE log files, download logs, search for data in logs, and email logs.

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **Admin > Appliance > Status > View Log File**. The following information is displayed:

Field	Description
Log file	Name of the log file. Name of the log file. To view a log file, click the name of the log file.
Directory	Location of log file on WLSE.
File Size	Size of file in bytes.
View	Displays a log file in a separate window.
Download	Saves a log file to your desktop or other location.

Step 2 To see a log file's details, click **View**. For a description of each file:

- For AAA server log files, see [Using AAA Server Log Files, page 18-28](#).

**Note**

The AAA server is available only on the [WLSE Express](#).

- For other log files, see [About Log Files, page 16-5](#).

Step 3 To download a log file, click **Download**.

**Note**

If this method of saving does not work, right-click **Download** and use the browser menu to save the file.

Step 4 To search within log files, select one or more files and enter a keyword into the Keyword text box. Click **Case Sensitive** if you want your search to be case sensitive, then click **Search**. A separate window displays the results of the search.

Step 5 To email log files, select one or more files and enter one or more comma-separated email addresses in the E-Mail Addresses textbox. Click **Send**.

Step 6 To clear old log files from the /var partition, you can use the **clearvar** CLI command. For more information on this command, see [clearvar, page A-12](#).

Related Topics

[Viewing System Information via CLI, page 17-15](#)

About Log Files

The WLSE maintains the following log files:

- Log files for the internal AAA server ([WLSE Express](#) only)—See [Using AAA Server Log Files](#), page 18-28.
- Log files for other functions—See [Table 16-3 General WLSE Log Files](#), page 16-5.

Table 16-3 **General WLSE Log Files**

File	Contents
AAA log files (WLSE Express only)	Logs for the internal AAA server. The internal AAA server is available only on the WLSE Express . For information on these log files, see Using AAA Server Log Files , page 18-28.
Repository.log	Actions performed by the repository web server.
access.log	Web server user access.
anismsnp.conf.log	Old SNMP community file, which is saved after you run the reset device-snmp command to reset the community string information on the WLSE. For more information, see reset device-snmp , page A-40.
backup.log	Appears after you back up WLSE data, restore data, or test the reachability of the backup location. To clear this log, which can become very large, see Clearing the Backup/Restore Log , page 16-23.
ciscoinstall.log	Information on upgrades of the WLSE software.
configbackup.log	The WLSE backs up the startup configuration once a day in order to detect any configuration changes. This log file contains information for that backup process. Information is kept for only the latest backup.
configexport.log	Information generated when a master configuration file is generated (WLSE Express only).
cwexport.log	Information about device exports to CiscoWorks RME.
daemons.log	Messages that dmgttd does not log.
dataUpdate.log	Appears after WLSE software is updated.
db2.log	Database startups due to installations or reboots.
db2runstat.last.log	Information on the latest run of the runstats facility, specifically size information on all the database tables and which tables were updated.
db2runstat.times.log	Summary of recent runs of the runstats facility, specifically which tables were updated and how long it took for the entire run to finish.
db2uext2.log	Generated by the database user exit script, which is part of the redundancy code. This file is for troubleshooting by TAC only.
device_events.log	Logs for the following device events detected by the WLSE: • Device reboots • Address changes on APs caused by reboots and DHCP • Changes between pending and managed states on devices
dhcp.log	Processing that occurs when a WLSE boots up and gets its startup configuration tar file from a TFTP server via DHCP.
diagnostic-info.log	Output of the diagnostic-info CLI command.

Table 16-3 General WLSE Log Files (continued)

File	Contents
dmgtd.log	Process management daemon log.
dumptcp.cap	Binary log file created by the dumptcp CLI command. To view this file, save it to the desktop. Then, use a utility such as tcpdump.
dumptech.tgz	Output of the dumptech CLI command. To view this file, save it to the desktop and unzip the file.
error.log	Web server errors.
faults.log	Device faults.
Health.xml.tgz	Displays the health of the WLSE appliance.
httpd_mod_security_audit_log	Logs details of every request (including POST) detected by ModSecurity (an intrusion detection and prevention engine) as carrying a possible attack.
httpd_mod_security_audit_log	Debug log of ModSecurity.
install.log	Software package installation.
jobvm.log	Errors and other information on scheduled jobs.
login.log	Lists who is logged in, the IP address of the machine from which the user is logged in, and the time the user logged in.
logs.tgz	Output of the tarlog CLI command (an archive of system logs). To view these logs, save this file to the desktop, then unzip the file.
mfgtest.log	Manufacturing tests.
mod_jk.log	Messages between Tomcat and Apache.
procps_last.log	Output from last running of the ps CLI command.
redundancy.log	Redundancy messages.
runstats.log	Output of utility that updates statistics on data in tables and indexes.
snmpd.log	SNMP agent log file.
ssl_request.log	Secure HTTPS socket layer web server events.
swan.log	Radio management log.
systemCheck.log	System checks performed.
tftp.log	Access points deployed by the Deployment Wizard (that is, access points that have downloaded the wlsestartup.ini file).
tomcat.log	Java servlet messages, including review and error information for configuration templates.
updateWLSE-x.x.log	Results of upgrading WLSE software; for example, updateWLSE-2.13.log.
var_logs.tgz	Output of the tarlog CLI command (an archive of system logs). To view these logs, save this file to the desktop, then unzip the file.

Restarting the WLSE

This option allows you to restart the WLSE. After restarting, discovery and inventory will resume at the next scheduled time.

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **Admin > Appliance > Status > Restart**.

Step 2 Click **OK** to restart the WLSE.

**Note**

To perform a manual soft restart (for example, when modifying a network interface) you can use the CLI commands. For information on CLI commands, see [Appendix A, “Command Line Interface \(CLI\) Commands.”](#)

Related Topics

- [Rebooting the WLSE via CLI, page 17-10](#)
- [Shutting Down and Powering Off the WLSE, page 17-10](#)
- [Administering Management Services via CLI, page 17-15](#)

Managing WLSE System Software

**Caution**

Before attempting to upgrade WLSE software, see the Readme files associated with the upgrade image in the Software Center on Cisco.com for the recommended procedure. Also, see the *Upgrading the CiscoWorks Wireless LAN Solution Engine, 2.13* on Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_installation_guides_list.html. Some procedures in this section may not be applicable to certain software upgrades.

**Caution**

Upgrading a redundant cluster of WLSEs requires special procedures, see [Upgrading Software on Redundant WLSEs, page 16-37](#).

**Caution**

You cannot upgrade from a pre-release version of WLSE software to a released version.

The options under **Admin > Appliance > Software** are:

- **Status**—View information on the installed software, such as software description, installation date, and installation status—See [Viewing Status of Installed Software, page 16-8](#).
- **Define Repository**—Specify the repository location. The repository provides software update services to the WLSE—See [Managing the Repository, page 16-9](#).

- **Upgrading Software**—Select and install a software image from the repository—See [Installing the Software Upgrade](#), page 16-12.
- **Browse Repository**—Browse the available complete images in the repository—See [Browsing the Repository](#), page 16-13.
- **Software Update History**—View information about current and previous versions of installed software, including version number, install date, and installation status—See [Viewing Software Update History](#), page 16-14.

The topics in this section are:

- [Viewing Status of Installed Software](#), page 16-8
- [Downloading the Upgrade Image](#), page 16-9
- [Creating the Repository](#), page 16-10
- [Defining the Repository](#), page 16-11
- [Installing the Software Upgrade](#), page 16-12
- [Viewing Software Update Logs](#), page 16-14
- [Managing Security](#), page 16-15

Viewing Status of Installed Software

You can view information about the software currently installed on the WLSE.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Appliance > Software > Status**. The Installed Software table contains the following information about the software versions that have been installed on the WLSE:

Field	Description
Software Name	Brief description of the software.
Installation Date	Date and time (UTC) the software was installed.
Status	Status of the installation: Success—Installed with no errors. Warning—Installed successfully with minor errors. Error—Installation was unsuccessful.
Details	Detailed install log for this software.

Last Installation Information shows the following information about the most recent software installation:

Field	Description
Name	Brief description.
Installation Status	Status of the installation: Success—Installed with no errors. Warning—Installed successfully with minor errors. Error—Installation was unsuccessful.
Log File	Detailed install log.

Step 2 To view details about an installation, click **View Log** in the Details field.

Result: The install log for the selected installation opens, showing information about the most recent software installation.

Related Topics

- [Viewing Software Update History, page 16-14](#)
- [Installing the Software Upgrade, page 16-12](#)
- [Managing WLSE System Software, page 16-7](#)

Managing the Repository

The software repository stores the available software updates for the WLSE. The repository can be either local (on the WLSE) or remote (on a Windows NT, Windows 2000, or Windows XP server). The tasks for managing the repository are:

Task	Reference
1. Download software from Cisco.com.	Downloading the Upgrade Image, page 16-9
2. Create repository.	Creating the Repository, page 16-10
3. Define repository.	Defining the Repository, page 16-11

Downloading the Upgrade Image

To locate the upgrade files, navigate to the Software Center for WLSE on Cisco.com or use the following URL:

<http://www.cisco.com/kobayashi/sw-center/cw2000/crypto/wlan-sol-eng/>



Note

WLSE update images are subject to import/export regulations on strong encryption. You may be directed to edit your Cisco.com profile to confirm that you are allowed to download such images before you can complete the download.

Download the relevant upgrade files:

- If you are using a local repository on the WLSE, download the zip file, the info file, and the readme to an FTP server. The upgrade zip file and the info file must be in the same directory on the FTP server. *Do not extract the zip file.*
- If you are using a Windows server as a repository, download the zip file and the readme file to the Windows server. *Do not extract the zip file.*

Creating the Repository

Adding files to the repository and deleting files from the repository require the use of CLI commands. For more information on CLI commands, see [Appendix A, “Command Line Interface \(CLI\) Commands.”](#)

The topics in this section are:

- [Creating a Local Repository, page 16-10](#)
- [Creating a Repository on a Windows Server, page 16-11](#)

Creating a Local Repository

To create a local repository on the WLSE:



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Open a [CLI](#) window to the WLSE, using Telnet or [SSH](#).
- Step 2** Specify the FTP site that will be the source of the software updates. Enter the following CLI command:

```
repository source ftp://hostname/path
```

where *hostname* is the name of the remote FTP server and *path* is the directory path on the remote FTP where you placed the zip file and info file.
- Step 3** Find the software you want on the FTP site by entering the following command. This command requires a valid username and password on the remote FTP server.

```
repository list remote
```
- Step 4** Download the software to the local repository using the following command. This command requires a valid username and password on the remote FTP server.

```
repository add package
```

For example, if the name of the zip file is WLSE-2.13-K9.zip, the *package* is WLSE-2.13-K9.

Creating a Repository on a Windows Server

A remote repository can serve as the repository for numerous WLSEs. You can create a repository on a Windows NT, Windows 2000, or Windows XP server.

**Note**

A remote repository created on a Windows server is temporary; it will not exist after the server reboots.

To set up a Windows server as a remote repository, see the relevant Readme.txt file on Cisco.com at <http://www.cisco.com/kobayashi/sw-center/cw2000/crypto/wlan-sol-eng/>.

Defining the Repository

By defining the repository, you are telling the WLSE where to look for available software updates.

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **Admin > Appliance > Software > Define Repository**.

Step 2 To define or redefine the repository, complete the following:

Text Box	Description
Host Name	Hostname or IP address of the repository. For a local repository, enter localhost . For a remote repository, enter the hostname or IP address of the repository.
Port Number	Port number used by the software on the repository. The default port number for a repository is 9851.
Description	(Optional) Description of the repository.

Step 3 Click **Connect to Repository** to verify that the hostname and port number you entered are correct. If the data is incorrect, an error message appears.

Step 4 Select **Admin > Appliance > Software > Browse Repository** to check the update image.

Related Topics

- [Installing the Software Upgrade, page 16-12](#)
- [Browsing the Repository, page 16-13](#)
- [Managing WLSE System Software, page 16-7](#)

Installing the Software Upgrade

**Caution**

Before attempting to upgrade WLSE software, see the Readme files associated with the upgrade image in the Software Center on Cisco.com and the *Upgrading the CiscoWorks Wireless LAN Solution Engine, 2.13* on Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_installation_guides_list.html. Some procedures in this section may not be applicable to certain software upgrades.

**Caution**

When you update or reinstall software, the WLSE stops and restarts. Therefore, you cannot access the WLSE during a software update, and you must log in again after updating software.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Appliance > Software > Install Software Updates**. The Install Software Updates window opens and displays information about the WLSE, the currently defined repository, and the compatible software available for updating.
- If an error message appears instead, you must define the repository before proceeding (**Admin > Appliance > Software > Define Repository**). For more information, see [Managing the Repository, page 16-9](#).

- Step 2** Select a software version from the Compatible Updates table, Compatible Reinstallations table, or Complete Images table.

These tables display the following information about the software you can install.

Field	Description
Name	Software identifier.
Version	Version number.
Summary	Brief description.
Release Date	Release date.
Details	Detailed description.

- Step 3** To view details on an image in the table, click **README** in the Details field.
- Step 4** To begin the installation, make a selection from the Compatible Updates table, Compatible Reinstallations table, or Complete Images table.
- Step 5** To install the selected software, click **Install**. The Install Software Updates window opens.
- Step 6** Click **Confirm** to continue the installation. Click **Cancel** to cancel the installation.
- Step 7** When the installation is complete, the WLSE will be unavailable for a few minutes while it restarts. If the Appliance Update window reappears, click the **Cancel** button to remove it.

- Step 8** To view details of the installation after the installation is complete, select **Admin > Appliance > Software > Status > View Log**.

Related Topics

- [Managing the Repository, page 16-9](#)
- [Viewing Status of Installed Software, page 16-8](#)
- [Viewing Software Update History, page 16-14](#)
- [Browsing the Repository, page 16-13](#)
- [Managing WLSE System Software, page 16-7](#)

Browsing the Repository

You can browse the available complete images and software upgrades on the repository using this option.



Note

A [repository](#) must be defined before you can browse software. To create and define a repository, see [Managing the Repository, page 16-9](#).



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Appliance > Software > Browse Repository**.

Information about the defined repository is displayed.

If an error message appears instead, you must define the repository before proceeding (**Admin > Appliance Software > Define Repository**). For more information see [Managing the Repository, page 16-9](#).

- Step 2** To view detailed information about a complete image or update, click **README** in the Complete Images table or Updates table. These tables display the following about all the software available on the repository:

Field	Description
Name	Software identifier.
Version	Version number.
Appliance Type	The appliance type that the software is designed for.
Release Date	Release date.
Summary	Brief description.
Details	Detailed description. Click README to display details.

Related Topics

- [Managing the Repository, page 16-9](#)
- [Installing the Software Upgrade, page 16-12](#)
- [Managing WLSE System Software, page 16-7](#)

Viewing Software Update History

This window shows only the update history, not a history of installed images. When you install a complete new image, the previous update history is erased.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Appliance > Software > Software Update History**. The following information is displayed:

Table 16-4 *Software Update History Window*

Field	Description
Name	Software identifier.
Version	Software version.
Summary	Summary of the installed software.
Install Date	Date and time (UTC) the software was installed.
Status	Status of the installed software.
Status	The status of the installation: Success—Software was installed with no errors. Warning—Software installed successfully with minor errors. Error—Software installation was unsuccessful.
Details	The detailed install log for this installation, including warning and error messages.

- Step 2** Click **View Log** in the Details field to view the detailed installation log (install.log file).

Related Topics

- [Viewing Status of Installed Software, page 16-8](#)
- [Managing WLSE System Software, page 16-7](#)

Viewing Software Update Logs

The WLSE maintains the following software update logs:

- ciscoinstall.log

- dataUpdate.log
- install.log
- updateWLSE-x.x.x.log

To view these logs, select **Admin > Appliance > Status > View Log File**. Some of these logs are not listed until you have performed an update of WLSE software. For information on these logs, see [Using WLSE Log Files, page 16-4](#).

Managing Security

You can manage the WLSE's by using the options under **Admin > Appliance > Security**:

- **Authentication Modules**—Set up the authentication module to be used (see [Using an Authentication Module, page 16-16](#)).
- **SSL (HTTPS)**—Obtain a permanent, signed Certificate Signed Request for secure Web access (see [Managing SSL \(HTTPS\), page 16-18](#)).
- **Telnet and SSH**—Configure Telnet and **SSH** settings (see [Enabling Telnet and Selecting SSH Type, page 16-19](#)).
- **Last 10 Logins**—View information about the last 10 users who have logged on to the WLSE (see [Viewing the Last 10 Logged-On Users, page 16-19](#)).

Related Topics

[Overview: Security, page 16-15](#)

Overview: Security

The WLSE provides the following security features:

- Optional secure connection through the Web browser—See [Managing SSL \(HTTPS\), page 16-18](#).
- Connection through the **CLI** via Telnet or SSH—See [Enabling Telnet and Selecting SSH Type, page 16-19](#).
- Authentication through the local database or alternative authentication services—See [Using an Authentication Module, page 16-16](#) and [Managing User Accounts, page 16-51](#).
- Flexible user access to managed devices and WLSE services through configurable roles—See [Managing Roles, page 16-49](#).

Overview: Authentication Modules

The WLSE provides a mechanism for authenticating users through the local authentication module and a local database of user IDs and passwords. Many network managers, however, already have an authentication service. To use your own authentication service instead of the local module, you can select one of the alternative modules:

- TACACS+
- RADIUS

**Note**

For any of the alternative modules listed above, if you select the **No Failover** option for authentication (**Admin > Appliance > Security > Authentication Modules**), the alternative authentication service only is used *and if the alternative authentication service is unavailable, no one will be able to log in to WLSE.*

**Note**

WLSE does not support MS NT Domain authentication.

After you select and configure a module, all authentication transactions are performed by the authentication service associated with that module. Users log in with the user ID and password associated with the current authentication module.

You must create all user roles on the Local authentication module. The WLSE ships with 4 default roles that you can use. If you want to create additional roles, you must define them locally. For more information about user roles, see [Managing Roles, page 16-49](#).

To configure WLSE using ACS as a TACACS+/RADIUS authentication module, see *Configuring the CiscoWorks Wireless LAN Solution Engine TACACS+/RADIUS Authentication Using Cisco Secure ACS* on cisco.com:

http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html

Related Topics

- [Using an Authentication Module, page 16-16](#)
- [Managing GUI Users, page 16-49](#)

Using an Authentication Module

You can use an existing RADIUS or TACACS+ authentication server to authenticate WLSE users by selecting and configuring the appropriate WLSE authentication module.

To configure an authentication module for users logging in to the CLI via Telnet or SSH, use the **auth** CLI command.

After you change the authentication module, you do not have to restart the WLSE. Changing the module does not affect users who are currently logged on. Users who log on after the change use the new module.

In WLSE releases prior to release 2.13, if you used an alternative authentication service, all users had to be in the local database of users. That is, for each user of the WLSE, you had to have a local user account matching the name of the user on the external authentication server. However, starting with WLSE 2.13, if you assign roles on the alternative authentication service, you do not have to create local user accounts.

Depending on the type of authentication server you use, you assign roles on the remote server in different ways as shown in the following table.

For Server Type	You must
RADIUS	Configure the attribute <i>cisco-av-pair</i> with the following attributes: <code>WLSE:groups="System Admin"</code>
TACACS+	Create a new service with the following attributes: <code>cmd=groups</code> <code>cmd-arg="Role Name"</code>

To configure WLSE using ACS as a TACACS+/RADIUS authentication module, see *Configuring the CiscoWorks Wireless LAN Solution Engine TACACS+/RADIUS Authentication Using Cisco Secure ACS* on [cisco.com](http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html):

http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html

Authentication is performed on the WLSE by enforcing the roles configured on the CiscoSecure ACS server, if you have configured it; otherwise, local user accounts are used. For information on adding users to the local database, see [Managing GUI Users, page 16-49](#).


Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Appliance > Security > Authentication Modules**.
- Step 2** Select an authentication module from the Select Module drop down list, then click **Submit**.
- Step 3** Enter the following data.

Table 16-5 Authentication Modules

Module	Parameters and Notes
Local	Use local user authentication only. This is the default setting. No configuration required.
RADIUS	Primary Server and Secondary Server—IP addresses or device names of the primary and secondary authentication servers. A secondary server is optional. Shared Secret—Secret key. Failover —If the remote authentication server becomes unreachable, local authentication is used. No Failover Authentication—By default, this option is not selected. If you select this option, the alternative authentication service only is used <i>and if the alternative authentication service is unavailable, no one will be able to log in to WLSE</i>. Local—Either local authentication or the alternative authentication service is used. If you defined a different password for local authentication and for the alternative authentication service, either will work.

Table 16-5 Authentication Modules

Module	Parameters and Notes
TACACS+	Primary Server and Secondary Server—IP addresses or device names of the primary and secondary authentication servers. A secondary server is optional. Shared Secret—Secret key. Failover —If the remote authentication server becomes unreachable, local authentication is used. No Failover Authentication—By default, this option is not selected. If you select this option, the alternative authentication service only is used <i>and if the alternative authentication service is unavailable, no one will be able to log in to WLSE.</i> Local—Either local authentication or the alternative authentication service is used. If you defined a different password for local authentication and for the alternative authentication service, either will work.

Step 4 Click **Submit** to save your changes.

Related Topics

- [Overview: Authentication Modules, page 16-15](#)
- [Setting Up TACACS+ or RADIUS Authentication for CLI Login, page 17-4](#)

Managing SSL (HTTPS)

SSL (secure socket layer) protocol provides a secure connection between Web clients and the WLSE. When you initially set up the WLSE, normally, an unsigned certificate and a CSR (Certificate Signed Request) are automatically generated and SSL is enabled. The unsigned certificate expires in one year. To obtain a permanent, signed certificate, use the following procedure.



Note

If you did not generate an unsigned certificate during initial installation and setup of the WLSE, you must log in to the CLI and use the **mkcert** command to generate an unsigned certificate, then log back in to the Web interface to complete the procedure for enabling SSL.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Appliance > Security > SSL (HTTPS)**.
- Step 2** Click **View CSR**. The encrypted CSR is displayed.
- Step 3** Copy the encrypted CSR (between the *begin* and *end* lines). Send the CSR to a certificate authority (such as Verisign), following the authority's procedure.
- Step 4** When you receive the signed certificate:
 - a. Copy it into an ASCII file on a client system.

- b. On the same client, select **Admin > Security**.
- c. Under SSL (HTTPS), type the path to the signed certificate or click **Browse** to locate the file, then click **Submit Certificate**.
- d. To use the new certificate, you need to restart the WLSE by logging on through the [CLI](#), running the **services stop** command to stop the system, then running the **services start** command to restart the system.

Step 5 You should block logins on the regular HTTP port (1741):

- a. Log in to the WLSE by using the console or by using Telnet or SSH.
- b. Enter the following CLI command:

```
# firewall eth0 1741
```

Step 6 To establish a connection to the WLSE by using SSL, use the prefix https instead of http when entering the URL into the browser and do not append a port number to the URL.

Enabling Telnet and Selecting SSH Type

Telnet can be used for connecting to the WLSE through the [CLI](#). By default, Telnet is disabled, which prevents unsecure connections through the CLI.

SSH is enabled by default. SSH provides a secure Telnet connection, encrypting all traffic, including passwords. By default, both SSH1 and SSH2 are used.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Appliance > Security > SSH and Telnet**.
- Step 2** To change the type of SSH used, select the desired SSH version from Select Protocol, then click **Change Protocol**.
- Step 3** To enable or disable Telnet, make a selection from Telnet, then click **Configure**.
Changes occur immediately.

Viewing the Last 10 Logged-On Users

To view information about the last 10 users who have logged on to the WLSE:



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Appliance > Security > Last 10 Logins**.

The Last 10 Logins table shows the following information for the last 10 logins:

Field	Description
Login Name	User's login name.
Logged In Since	Date and time the user logged in (UTC).
IP Address	IP address of the system from which the user logged in.
Associated role	Role assigned to the user.

Backing Up and Restoring Data

Backup and restore allows you to backup the WLSE's configuration and restore it if necessary.



Caution

You cannot restore a backup from a WLSE running pre-release (beta) software to a WLSE running released software.

The following options are provided for backup and restore:

- **Configure**—You must set the backup location before you can run backups (see [Specifying the Backup Location, page 16-21](#)).
- **Backup**—Schedule a backup of WLSE data or run an immediate backup (see [Scheduling and Running Backups, page 16-23](#)).
- **Restore**—Restore an available backup image (see [Restoring Data, page 16-24](#)).
- **Backup log**—The backup log (backup.log) appears after you back up WLSE data, restore data, or when you test the reachability of the backup location. To view the backup log, select **Admin > Appliance > Status**. For information on logs, see [Using WLSE Log Files, page 16-4](#). To clear the backup/restore log (which can become very large), see [Clearing the Backup/Restore Log, page 16-23](#).

Related Topics

- [About Backup and Restore, page 16-20](#)
- [Backing Up and Restoring via CLI, page 17-5](#)

About Backup and Restore

Backing up the WLSE saves its configuration data in case you need to restore the data. The backup operation backs up the entire WLSE database and configuration, which includes appliance setup, fault and performance data, device credentials, WLSE users, configuration templates, user-created groups, and jobs.

Backups are typically done on a regular basis (for example, weekly). However, you may choose to back up infrequently and use one or more of the data export mechanisms to gather interesting data from the WLSE.

The backup operation may take some time depending on the size of the database: the larger the database, the more the backup time will be required.

The restore operation includes all the information in the backup, including the information entered during initial configuration of the WLSE (setup program).

The restore process disrupts normal WLSE operation because the process shuts down the WLSE internal database and then restarts it.

You can restore data backed up on one WLSE to another WLSE. For information on restoring from one WLSE to another, see [Copying Configuration Data from One WLSE to Another, page 16-25](#).

Specifying the Backup Location

You must set the backup location before you can run backups. The backup location must be an FTP or SCP server.

Please observe the following cautions about the backup location:

- Backup has only been tested on the standard Windows 2000, Windows XP, and Unix FTP and SCP servers. Therefore, only these servers are explicitly supported for WLSE backups. However, any server that uses standard FTP or SCP commands and protocol should work.
- Make sure the target FTP or SCP directory has enough free space, especially if you are running frequent backups. If there is not enough space, the backup may fail or the backup data may be corrupted.
- If you are using a Windows 2000 or Windows XP server as the backup location, you must configure the server for UNIX directory mode. See [Configuring a Windows System as a Backup Location, page 16-22](#).
- SCP uses keys to identify the remote host and stores these keys on the WLSE. If the key on the remote host changes, the backup cannot be transferred. If you know that a key was legitimately changed on the remote host, you can use the **clearbackuphosts** CLI command to clear the stored keys. After that, the new keys can be stored.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Admin > Appliance > Backup and Restore > Configure**.

Step 2 Enter the following data:

Field	Description
Hostname/IP	Hostname or IP address for the backup location.
Username	Valid username on the backup location.
Password	Valid password on the backup location.
Verify Password	
Timeout	Timeout value, in seconds, for backup jobs. The default value is 7200 seconds. You can specify any value between 3600 and 43200 seconds. For large backup or restore jobs, you might need to increase this value. If you get a timeout error in the backup.log, increase this timeout value.

Field	Description
Path (Optional)	Path to the backup location. When specifying the path on a Windows 2000 or Windows XP server: • Use either forward slashes (/) or backslashes (\) as directory separators. • Do not include the drive specifier; for example, c:\. • Path is relative to the ftp root. • Backup mechanism can create multiple directory levels for you.  Note To specify a backup directory, you must specify a timeout value.
Use Secure Transfer	Select this to use secure copy (SCP) to move the backup files to the remote host. SCP is based on SSH. SCP uses keys to identify the remote host and stores these keys on the WLSE. If the key on the remote host changes, the backup cannot be transferred. If you know that a key was legitimately changed on the remote host, you can use the clearbackuphosts CLI command to clear the stored keys. After that, the new keys can be stored.

- Step 3** Click **Save**, or click **Erase** to clear your entries or remove the previously configured backup location.
- Step 4** Click **Test** to verify that the backup location is reachable and is configured as an FTP server.
- The message “Test OK” should be displayed. Any other response indicates a problem with the backup.
- Step 5** Click **Clear Log** to delete from the View Log File window the backup.log file that was created after the previous backup or restore operation.

Related Topics

- [Scheduling and Running Backups, page 16-23](#)
- [Restoring Data, page 16-24](#)
- [Configuring a Windows System as a Backup Location, page 16-22](#)
- [About Backup and Restore, page 16-20](#)
- [Backing Up and Restoring via CLI, page 17-5](#)

Configuring a Windows System as a Backup Location

You can use a Windows 2000 Server, Advanced Server, or Windows XP Professional system as a backup location. Before use, the system be configured as follows.



Note

Your login determines whether you can use this option.

Procedure

-
- Step 1** On the server, select **Start > Programs > Administrative Tools > Internet Services Manager**.
If this option is not available on the server, first enable it as follows:
- Select **Start > Settings > Control Panel > Add/Remove Programs**.
 - On the left side of the Add/Remove window, click **Add/Remove Windows Components**. The Windows Components wizard starts.
 - Select Internet Information Services, then click **Next**.
- Step 2** Right-click the FTP site for which you want to set the directory output style, then select **Properties**.
- Step 3** Select FTP Service from the Master Properties list and click **Edit**.
- Step 4** Select the Home Directory property sheet:
- Select **Write** under FTP Site Directory.
 - Select **UNIX** under Directory Listing Style.
 - Click **OK**.
-

Clearing the Backup/Restore Log

To remove the backup.log file from the View Log File window, select **Admin > Appliance > Backup and Restore > Configure**. Then, click **Clear Log**. This removes from the View Log File window the file created by the last backup or restore operation. This log file is called backup.log.

Scheduling and Running Backups

Data backed up includes role and user information, discovery configuration information, and other configuration information. The following procedure includes a verification step; it is recommended that you always verify that the backup succeeded. You can run an immediate backup or schedule regular backups.

Before scheduling backups, verify that the system time is set correctly. To set the system time, see [Set the Current Local and UTC Time, page 16-43](#).



Note Normal operations continue during backup.



Note You should perform a backup whenever you add users.



Note Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Appliance > Backup and Restore > Backup**.

If the message “Backup/restore is not configured” appears, you must specify the backup location. Select **Admin > Appliance > Backup and Restore > Configure**. For more information, see [Specifying the Backup Location, page 16-21](#).

Step 2 To run an immediate backup, click **Backup Now**.

Step 3 To schedule automatic backups:

- a. Enter the start date and time:
 - Select Every Month or a specific month.
 - Select Every Day, a day of the week, or a day of the month.
 - Select the time as hours (24-hour clock) and minutes (5-minute increments).
- b. Click **Schedule Backup**.

Step 4 To cancel a scheduled backup, click **Remove Scheduled Backup**.

Step 5 There are several ways to verify that the backup succeeded:

- Check the log file under backup.log file under **Admin > Appliance > Status > View Log File**.
- Select **Admin > Appliance > Backup and Restore > Restore**. The backup image should be listed in the Available Images list. Click **Cancel**.
- Log in to the backup location system and verify that there is a backup directory containing *WLSE hostname_date_time.inf* and *WLSE hostname_date_time.tar* files.

Related Topics

- [Restoring Data, page 16-24](#)
- [About Backup and Restore, page 16-20](#)
- [Backing Up and Restoring via CLI, page 17-5](#)

Restoring Data



Caution

If you are restoring a backup on a WLSE that is configured for redundancy, see the special instructions in [Backing Up and Restoring on Redundant WLSEs, page 16-37](#).

After you click **Restore** and **OK** in the following procedure, the following occur in sequence:

1. The WLSE shuts down automatically.
2. The data is restored.
3. The WLSE reboots.



Note

Your login determines whether you can use this option.

Procedure

To restore the WLSE’s configuration data from a backup:

Step 1 Select **Admin > Appliance > Backup and Restore > Restore**.

If the message “Backup/restore is not configured” appears, you must specify the backup location. Select **Admin > Appliance > Backup and Restore > Configure**. For more information, see [Specifying the Backup Location, page 16-21](#).

- Step 2** From the Available Images list, select a backup image. Images are listed by WLSE hostname and date and time of backup.
- Step 3** Click **Restore Appliance Network Information** if you want to restore the following information that is stored in flash memory:
- Network information—WLSE hostname, IP address, domain name, name servers, NTP server, and firewall settings.
 - Users’ CLI privileges.

**Caution**

Deselect **Restore Appliance Network Information** if you are restoring a backup created on another WLSE. For more information on restoring from one WLSE to another, see [Copying Configuration Data from One WLSE to Another, page 16-25](#).

- Step 4** Click **Restore**. The Restore Backup window opens.

- Step 5** Click **OK**.

Result: The WLSE shuts down, the data is restored, then the WLSE restarts.

Related Topics

- [Scheduling and Running Backups, page 16-23](#)
- [Specifying the Backup Location, page 16-21](#)
- [About Backup and Restore, page 16-20](#)
- [Backing Up and Restoring via CLI, page 17-5](#)

Copying Configuration Data from One WLSE to Another

You can back up data from one WLSE and copy it to another by using the backup and restore features. If you are replacing one WLSE with another, see the instructions in [Installing a Replacement WLSE, page 17-8](#).

- Step 1** Back up the data on the source WLSE. For more information, see [Backing Up and Restoring Data, page 16-20](#).
- Step 2** If you have installed a new WLSE and have not configured it yet, complete the initial configuration. For information on the setup program and initial configuration, see relevant installation guide for your WLSE hardware.
- Step 3** Restore configuration data to the destination WLSE, using the backup you made in Step 1.

**Caution**

Be sure to deselect **Restore Appliance Network Information**. Otherwise, the network information in flash memory will be overwritten and you will have to erase the WLSE’s configuration and run the setup program.

For more information on restoring backups, see [Restoring Data, page 16-24](#).

Related Topics

[Copying Configuration Data to another WLSE via CLI, page 17-9](#)

Managing WLSE Master Configuration Files (WLSE Express Only)

Using this option, you can create master configuration files that contain the current basic configuration data of a [WLSE Express](#) and use these files to configure other WLSEs.

For more information on the content of the master configuration files, see [About the Master Configuration Files, page 16-27](#).

Use the following procedure to create WLSE configuration files and download them from the WLSE to a TFTP server.

For details on the contents of the configuration files, editing the .xml file, parameters that can be saved, and procedures for using the master configuration to configure other WLSEs, see the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine Express, Release 2.13* on Cisco.com.



Note

Your login determines whether you can use this option. This option is available on the WLSE Express only.

Procedure

Step 1

To create configuration files:

- a. Configure the current (reference) WLSE with the data you want to save.
- b. Select **Admin > Appliance > Master Configuration**.
- c. Enter a filename in the Filename field.
- d. Click **Create New Config**.

Result: The types of data you can include in the configuration files are displayed.

- e. Select the data that you want to save. See [Table 16-6 on page 16-26](#) for more information about the data that is saved.
- f. Click **Create Config**.

Results: The .xml, .info, and .dat files are created and combined into a tar archive and stored on the WLSE. The name of the archive and the date it was created are added to the Saved Configurations list.

Table 16-6 **Data Saved in the Master Configuration Files ¹**

Type	Parameters	In .xml File	In .dat File
Faults	Default fault profile settings		X
	Notification settings	X	

Table 16-6 *Data Saved in the Master Configuration Files (continued)¹*

Type	Parameters	In .xml File	In .dat File
Discover	Discovery schedule, including seed devices and CDP distance setting	X	
	Device credentials	X	
	Advanced options (auto-manage, DNS lookup, and name format)	X	
	Inventory polling parameters	X	
	AAA server monitoring	X	
	Client tracking enable	X	
Rule Based Groups	User-defined rule-based groups		X
Configure	Templates ²	X	X
	Startup configuration assignments	X	
	Auto-managed template assignments	X	
Admin	Appliance Settings (redundancy, splash screen)	X	
	User role definitions		X
	Users	X	
Radio Management	AP locations	X	
	Radio management configuration	X	

1. For parameters that cannot be saved from the UI, you can add CLI commands to the .xml file. For example, settings for the internal AAA server are not saved from the UI.

2. Any custom commands in templates are saved to the .xml file. Template settings made from the UI are saved in the .dat file.

Step 2 To download the archive to your desktop:

- a. Select a configuration from the Saved Configurations list.
- b. Click **Download**.
- c. Specify the location, then download the file.

Step 3 To delete a saved configuration file from the WLSE, select the file from the Saved Configurations list and click **Delete**.

Related Topics

[About the Master Configuration Files, page 16-27](#)

About the Master Configuration Files

When you use the Master Configuration option, 3 files are created and combined into a tar archive. For example, if you specify the filename “config,” a tar archive called myconfig.tar is created. The archive contains the following files:

- config.xml—This file contains most of the WLSE configuration parameters in XML format, as shown in [Table 16-6 on page 16-26](#). You can edit this file.

The following parameters must be manually added to the .xml file as CLI commands:

- AAA Administration parameters (internal AAA server)
- Most of the settings in the Appliance subtab

You can also add other WLSE CLI commands to the .xml file.

For information on editing the .xml file, see the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine Express, Release 2.13*.

- config.dat—This file contains parameters that are saved as binary data, as shown in [Table 16-6 on page 16-26](#). This file cannot be edited.
- config.info—This file contains information about the other two files and identifies the tar file as a valid WLSE configuration.

Configuration files can be automatically downloaded to WLSEs by storing the file on a TFTP server and using DHCP to download the file. For more information on this method of configuring WLSEs, see the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine Express, Release 2.13* on Cisco.com at http://www.cisco.com/en/US/products/ps6379/prod_installation_guides_list.html.

Managing WLSE Redundancy

The redundancy feature allows you to enable high availability through a two-node cluster of WLSEs. If the WLSE designated as the primary node fails, fail-over occurs automatically to the secondary node. If, subsequently, the primary node is back in service and the secondary node fails, failback occurs to the primary node.

Configurable periodic synchronizations between primary and secondary nodes ensure that any data or configuration loss is minimal. During failover, all users are logged out and must log back in.



Tip

To force fail over from the active node to the standby node, see [Performing Manual Failover to the Standby Node, page 16-36](#).

Before enabling redundancy, see [Redundancy Requirements, page 16-29](#) for hardware and configuration prerequisites.

For details on how redundancy works, see [About Redundancy, page 16-30](#).

You can use the redundancy options to:

- Enable redundancy—See [Configuring Redundancy, page 16-32](#).
- Check redundancy settings—See [Checking Redundancy Settings, page 16-35](#).
- View the log of redundancy events—See [Viewing the Redundancy Event Log, page 16-36](#).

Related Topics

- [About Redundancy, page 16-30](#)
- [Redundancy Requirements, page 16-29](#)
- [Redundancy Email Messages, page 16-31](#)
- [Performing Manual Failover to the Standby Node, page 16-36](#)
- [Upgrading Software on Redundant WLSEs, page 16-37](#)
- [Replacing a Node, page 16-37](#)
- [Backing Up and Restoring on Redundant WLSEs, page 16-37](#)

- [Changing the Web Timeout Period on Redundant Nodes, page 16-38](#)
- [Controlling Access via HTTP/HTTPS on Redundant Nodes, page 16-38](#)

Redundancy Requirements

Following are the hardware, software, and network requirements for WLSE redundancy:

- You must have two operating WLSEs, which are installed and operating on the network.
- Both WLSEs must be running the same software version (2.9 or later).
- Both WLSEs must be the same hardware type:
 - You can pair two WLSE 1130 or WLSE 1130-19 systems.
 - You can pair two WLSE 1030 systems. This is the hardware type for the [WLSE Express](#).
- Both systems must be in the same IP subnet and connected to the same router.
- You must have a static (non-DHCP) IP addresses assigned to each node. These addresses are entered in the configuration screen.
- You must have a virtual IP address (VIP) for Ethernet interface eth0. This address is also entered in the configuration screen. If the nodes are of the WLSE 1130 series (which have two interfaces), you should enter a different virtual IP address for eth1. However, the VIP for eth1 is optional if redundancy functions will not be used via the eth1 interface. The VIP is a static (non-DHCP) address that must be officially allocated by your site's network administrator. The VIP must be in the same subnet as the base interface. That is, the VIP for eth0 must be in the same subnet as the IP address for eth0, and the VIP for eth1 must be in the same subnet as the IP address for eth1.

When the WLSEs are operating as a redundant pair, the VIP address is always assigned to the active node. If there is a failover, the VIP address moves to the new active node. All accesses to the redundant pair are performed by using the VIP address, so after a failover occurs, the active node always responds when addressed by the VIP address. Users can always use the VIP address to connect to the active node.

- Ethernet interface eth0 on both WLSEs must be in the same subnet. If ethernet interface eth1 is in use on both WLSEs, eth1 on both WLSEs must be in the same subnet. You can use either ethernet interface for redundancy.
- Both WLSEs must be using the same HTTP port. The default port is 1741. You can set this port to 1741 or 80 by using the **http-server port** CLI command. For more information, see [http-server, page A-21](#).
- The password for the [admin](#) user must be the same on both WLSEs.



Note

Any modifications to the admin user must be made on the *active* WLSE, and the change are propagated to the standby WLSEs. Any modifications you make to the admin user are rejected unless *both* WLSEs (active and standby) are operational.

- The mail route must be configured if you want to receive email notification of redundancy events. You can set the mail route by using the **mailroute** CLI command or by setting the mail route in Web interface (see [Configuring the Mail Route, page 16-45](#)).
- All redundancy users must have the Redundancy User ID role (**Admin > User Admin > Manage Roles**). For more information about users roles, see [Managing Roles, page 16-49](#).

**Note**

If you use a RADIUS authentication server, you must log on to both WLSEs at least once before you can configure redundancy.

About Redundancy

Redundancy is achieved by configuring a cluster of two WLSEs. One WLSE is in active mode, performing all normal WLSE functions. The other WLSE is in warm standby; that is, the system is up but no WLSE applications are running and only certain diagnostic operations are allowed.

The user interface on the standby node is restricted. The only features displayed are the Admin tab and the Appliance subtab. This prevents users from accidentally using the standby node for other operations.

For more information, see the following topics:

- [Redundancy Configuration, page 16-30](#)
- [Status Checking, page 16-30](#)
- [Failover, page 16-30](#)
- [Messages and Troubleshooting, page 16-31](#)
- [Changes in Certain Functions under Redundancy, page 16-31](#)

Redundancy Configuration

Redundancy can only be configured in the Web interface. However, after you have configured it, you can enable or disable redundancy by using the redundancy CLI command.

All redundancy configuration is performed on the primary node, which becomes the active WLSE after you set up redundancy. This configuration, plus all other data, is copied to the secondary node (the standby WLSE) automatically. Periodically, incremental changes are applied to the standby to keep it synchronized with the active node.

Status Checking

Under redundancy, the nodes synchronize with each other, the standby node checks the active node, and the active node checks itself.

Synchronization and checking intervals are configurable by the administrator. The minimum amount of time between data synchronizations is 15 minutes, and the maximum is 5 hours. The frequency of checks made to ensure that each node is functioning is from 15 seconds and 5 minutes.

If the system checks fail repeatedly on the active node, data will be synchronized with the standby node. Then the standby will become active and the original active node will reboot. This failover will not occur if the active node cannot reach the standby node. In that case, the active node will remain up and running until the standby comes back online.

Failover

If the active node goes down or experiences a transient failure, all users are logged out and must log back in. No matter which node is active, users always log in to the same IP address, called the virtual IP.

When the formerly active node comes back into service, it automatically becomes the standby node. If both WLSEs go down, the current active node may become the standby node if the standby node restarts first.

In case of failover, a small amount of data that has not been committed to the standby will be lost. The amount of potential data loss is limited to the data accumulated during the interval between synchronization of the two nodes. It will take a few minutes for the standby node to become active after it detects that the other node has failed.

Messages and Troubleshooting

Redundancy troubleshooting messages are logged to the redundancy.log file. System checks are logged to the systemCheck.log file. You can access these logs from **Admin > Appliance > Status**.

All significant redundancy events since the WLSE was started are logged to the redundancy event log. You can access the event log from **Admin > Appliance > Redundancy > Event Log**.

To troubleshoot a node, log in using the real IP address, instead of the virtual IP address.

Changes in Certain Functions under Redundancy

Certain WLSE functions require special treatment on a redundant cluster. See the following:

- [Upgrading Software on Redundant WLSEs, page 16-37](#)
- [Replacing a Node, page 16-37](#)
- [Backing Up and Restoring on Redundant WLSEs, page 16-37](#)
- [Changing the Web Timeout Period on Redundant Nodes, page 16-38](#)
- [Controlling Access via HTTP/HTTPS on Redundant Nodes, page 16-38](#)

Related Topics

- [Redundancy Requirements, page 16-29](#)
- [Redundancy Email Messages, page 16-31](#)
- [Performing Manual Failover to the Standby Node, page 16-36](#)

Redundancy Email Messages

The messages sent by the redundancy module are described in [Table 16-7 on page 16-31](#). The sender of all messages is WLSE@*ip_address*, where *ip_address* is the IP address of the WLSE that is sending the message.

These messages are logged in the redundancy.log file. For information on viewing this and other WLSE logs, see [Using WLSE Log Files, page 16-4](#).

Table 16-7 **Redundancy Email Messages**

Email Subject	Meaning
Lost connectivity with standby on <i>ip_address</i> .	Standby node is down.
Regained connectivity with standby on <i>ip_address</i> .	Standby node is up.
Lost connectivity with <i>ip_address</i> .	Node is down.
Redundancy active mode.	WLSE that sent this message is now active; that is, the WLSE is providing WLSE services.
Redundancy standby mode.	WLSE that sent this message is now in standby mode.

Table 16-7 **Redundancy Email Messages (continued)**

Email Subject	Meaning
Lost connectivity with router.	WLSE that sent this message was unable to ping the default router.
Regained connectivity with router.	WLSE that sent this message is now able to ping the default router.
Data may not have been successfully restored from active.	Standby WLSE detected failure of active WLSE and is becoming active before it successfully synchronized with the active node.
Redundancy turned off.	Redundancy has been disabled.
Failed to ship database file.	Active WLSE failed to synchronize database data with the standby (probably caused by standby node failure).
Failed to ship config file.	Active WLSE failed to synchronize configuration data with the standby (probably caused by standby node failure).
Failed to ship transaction log file.	Active WLSE failed to synchronize database data with the standby (probably caused by standby node failure).
DB restore failed. Will reinitialize the DB on <i>ip_address</i> .	Standby node failed to apply data received from active and will attempt to reinitialize and reboot and try the data synchronization again.
DB rollforward failed. Will reinitialize the DB on <i>ip_address</i> .	Standby node failed to apply data received from active and will attempt to reinitialize and reboot and try the data synchronization again.
System check failed on <i>ip_address</i> for reason: <i>reason</i> .	System check failure.

Related Topics

- [About Redundancy, page 16-30](#)
- [Redundancy Requirements, page 16-29](#)
- [Performing Manual Failover to the Standby Node, page 16-36](#)
- [Upgrading Software on Redundant WLSEs, page 16-37](#)
- [Replacing a Node, page 16-37](#)
- [Backing Up and Restoring on Redundant WLSEs, page 16-37](#)

Configuring Redundancy

Initial redundancy configuration is performed on the whichever WLSE is to be designated as primary. After configuration, the primary node becomes the active node.

Subsequent configuration changes can be done on whichever WLSE is in active mode, but the node IP addresses should remain the same as when they were initially configured. If you need to change the IP addresses, first turn redundancy off, then configure the node IP addresses.

**Caution**

When you enable and configure redundancy, all data on the standby system will be lost. Immediately after you complete the configuration and indicate that you wish to apply your changes, the active system is synchronized with the standby system. Thus, any existing data on the standby system is replaced by data from the active system.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Make sure that all prerequisites are met. See [Redundancy Requirements, page 16-29](#).
- Step 2** Log in to the primary node, which is the WLSE that will be active (that is, providing management services).
- Step 3** Select **Admin > Appliance > Redundancy > Manage Redundancy**.
- Step 4** To enable redundancy, select **Redundancy Enabled**.

**Note**

After redundancy is turned on, a backup and restore begins.

- Step 5** Enter data in the following fields.

Table 16-8 **Redundancy Parameters**

Field	Description
Redundancy Enabled	Enable or disable redundancy. When enable is selected, the other fields in the screen become active.
User ID	User ID. The user can be any user that has the Redundancy User ID attribute defined in its Role <i>and</i> has CLI privileges.
Password	User password on both the active and standby systems. The password must be identical on both systems.
HTTP Port	Port for client connections via HTTP. The default is 1741. The port must be the same on both systems. For information on setting the port, see the http-server port CLI command in Appendix A, “Command Line Interface (CLI) Commands.”
Notification Email	(Optional) Email address for notification of redundancy events. For information on notification, see Redundancy Email Messages, page 16-31 . For information on configuring email in general, see Configuring the Mail Route, page 16-45 .

Table 16-8 **Redundancy Parameters (continued)**

Field		Description
IP addresses ¹	Virtual IP eth0	Virtual IP address for the eth0 Ethernet interface must always be entered in this field. Virtual IP addresses are static (non-DHCP).
	Virtual IP eth1	If the WLSEs have two Ethernet interfaces, you should enter a different virtual IP address for eth1. However, the virtual IP address for eth1 is optional if redundancy functions will not be used via the eth1 interface.
	This Node IP ²	Static (non-DHCP) IP address of the primary node. If both Ethernet interfaces are configured, you can select the address/interface you want to use for redundancy communication.
	Other Node IP	Static IP address of the system that will become the standby node.
Minutes between sync		How often the active and standby WLSEs are synchronized. Synchronization consists of incrementally backing up the database on the active WLSE and restoring on the standby WLSE. Default is 60 minutes. Can be set between 15 minutes and 5 hours. On networks with more than 500 devices, it is not recommended that you set this to less than 30 minutes.
Seconds between check of other node		How often to check to make sure both nodes are functioning. Default is 60 seconds. Can be set between 15 seconds and 5 minutes. ³

1. For more information on IP addresses and virtual IP addresses, see [Redundancy Requirements, page 16-29](#). Changing parameters such as Virtual IP addresses and HTTP port numbers could cause undesirable behavior when using other management applications.
2. To change a node's IP address, first turn off redundancy, then configure the IP address, then turn on redundancy.
3. These checks are logged in the systemCheck.log. To view this log, select Admin > Appliance > Status.

Step 6 Click **Reset** to remove your current settings.

Step 7 Click **Verify** to verify that your settings are correct. The Redundancy Settings Verified screen appears.

- If there are errors, click **Fix Errors** to return to the Redundancy Settings screen to fix the errors.
- If there are no errors:
 - Click **Yes** to apply your changes. Redundancy mode will be turned on. A full backup begins; the backup will be restored to the standby node. Regular backups and restores will now begin, and the standby node will begin regular checking to make sure the active node is functioning.
 - Click **No** to return to the Redundancy Settings screen.

Related Topics

- [Checking Redundancy Settings, page 16-35](#)
- [Viewing the Redundancy Event Log, page 16-36](#)
- [About Redundancy, page 16-30](#)
- [Redundancy Email Messages, page 16-31](#)
- [Performing Manual Failover to the Standby Node, page 16-36](#)
- [Upgrading Software on Redundant WLSEs, page 16-37](#)

- [Replacing a Node, page 16-37](#)
- [Backing Up and Restoring on Redundant WLSEs, page 16-37](#)
- [Changing the Web Timeout Period on Redundant Nodes, page 16-38](#)

Checking Redundancy Settings



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Log in to the WLSE web interface of either the primary (active) node or the secondary (standby) node.
- Step 2** Select **Admin > Appliance > Redundancy > Redundancy Status**.
- Step 3** The redundancy settings described in [Table 16-9 on page 16-35](#) are displayed. If a field is blank, it has not been configured.

Table 16-9 **Redundancy Status Settings**

Field	Description
Redundancy Status	Active—Redundancy is enabled. This is the active node at the current time. Standby—Redundancy is enabled. This is the standby node at the current time. Not Configured—Redundancy is not enabled.
User ID	User ID. The user can be any user that has the Redundancy User ID attribute defined in its Role <i>and</i> has CLI privileges.
HTTP Port	HTTP port configured on both systems.
Notification Email	Email address to which notifications are sent.
Virtual IP eth0	Virtual IP address of Ethernet interface 0.
Virtual IP eth1	Virtual IP address of Ethernet interface 1 (if in use).
This Node IP	Static IP address of the current system.
Other Node IP	Static IP address of the other system.
Minutes between sync	Synchronization interval (how often data is copied from the active node to the standby node). Default: 60 minutes. Range: 15 minutes to 5 hours.
Seconds between check of other node	How often to check to make sure both nodes are functioning. Default: 60 seconds. Range: from 15 seconds to 5 minutes. ¹

1. These checks are logged in the systemCheck.log. To view this log, select Admin > Appliance > Status.

- Step 4** To reset parameters, see [Configuring Redundancy, page 16-32](#).

Related Topics

- [Configuring Redundancy, page 16-32](#)
- [Viewing the Redundancy Event Log, page 16-36](#)

- [About Redundancy, page 16-30](#)
- [Redundancy Email Messages, page 16-31](#)
- [Performing Manual Failover to the Standby Node, page 16-36](#)
- [Upgrading Software on Redundant WLSEs, page 16-37](#)
- [Replacing a Node, page 16-37](#)
- [Backing Up and Restoring on Redundant WLSEs, page 16-37](#)
- [Changing the Web Timeout Period on Redundant Nodes, page 16-38](#)

Viewing the Redundancy Event Log

The event log contains a listing of all significant redundancy events since the WLSE was started.

**Note**

Your login determines whether you can use this option.

Procedure

Select **Admin > Appliance > Redundancy > Event Log**.

The redundancy log is displayed; for example:

```
02:24:13 02/13/2004 Lost connectivity with standby on 192.161.98.53
02:24:13 02/13/2004 Regained connectivity with standby on 192.161.98.53
02:24:13 02/13/2004 Redundancy active mode
02:24:13 02/13/2004 Shipped file S0000147.LOG
02:24:12 02/13/2004 Shipped file wlse-configs.tgz
```

Related Topics

- [About Redundancy, page 16-30](#)
- [Redundancy Email Messages, page 16-31](#)
- [Messages and Troubleshooting, page 16-31](#)

Performing Manual Failover to the Standby Node

If you reboot the active node or stop services on it (preferred method), the standby node will automatically become active.

To reboot a WLSE, see [Restarting the WLSE, page 16-7](#).

To stop services on a WLSE, Telnet or SSH to the WLSE and enter the following CLI command:

```
services stop
```

To restart services, enter the following CLI command:

```
services start
```

Once restarted, the formerly active node will automatically become the standby node.

Related Topics

- [About Redundancy, page 16-30](#)

Upgrading Software on Redundant WLSEs

Both the active and standby node must run the same software release. You can either:

- Use standard WLSE upgrade procedures, which require that you disable redundancy, upgrade both nodes, and then enable redundancy.
- Upgrade while redundancy is enabled, by downloading the image to the local repository via the Software Image Management (SWIM) feature of Cisco Works Resource Manager Essentials (RME). After downloading the image, use the **redundancy** CLI command to install the image. This method is recommended.

For more information on both methods, see the document *Upgrading the CiscoWorks Wireless LAN Solution Engine, 2.13* on Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_13/index.htm.

Replacing a Node

If you need to replace a node:

- Turn off redundancy.
- Configure the replacement node.
- Turn on redundancy.

See [Configuring Redundancy, page 16-32](#) for information on turning redundancy on and off.

Related Topics

- [About Redundancy, page 16-30](#)
- [Checking Redundancy Settings, page 16-35](#)
- [Viewing the Redundancy Event Log, page 16-36](#)

Backing Up and Restoring on Redundant WLSEs

This section contains the following information:

- General information about backup and restore on redundant nodes—[About Backup and Restore on Redundant Nodes, page 16-37](#).
- How to restore on redundant nodes—[Restoring on Redundant Nodes, page 16-38](#).

About Backup and Restore on Redundant Nodes

When backing up and restoring on redundant nodes:

- If redundancy is not enabled, backup and restore are allowed.
- On the active node, backup is allowed; but restore fails and generates an error message asks you to first turn off redundancy.
- On the standby node, neither backup nor restore is allowed. If you try to run backup, an error message asks you to run backup on the active node.
- When restoring, if the backup was performed on the active node, redundancy will be automatically turned off after the restore. You will have to re-enable redundancy.

Restoring on Redundant Nodes

When restoring data from a previous backup on WLSEs that have been configured for redundancy, use the following procedure.

Procedure

- Step 1** Turn off redundancy.
- Step 2** Restore data on the primary WLSE, following the procedure in [Restoring Data, page 16-24](#).
- Step 3** Turn on redundancy.
-

Related Topics

- [About Redundancy, page 16-30](#)
- [Redundancy Email Messages, page 16-31](#)
- [Configuring Redundancy, page 16-32](#)
- [Checking Redundancy Settings, page 16-35](#)
- [Viewing the Redundancy Event Log, page 16-36](#)

Changing the Web Timeout Period on Redundant Nodes

If WLSE redundancy is in effect, you should stop and restart services on the standby WLSE. Otherwise, resetting the timeout will cause a switchover from the active server to the standby server and the new timeout period will not take effect.

Procedure

- Step 1** Telnet or SSH to the standby WLSE.
- Step 2** Enter the following CLI command on the standby server:
- ```
services stop
```
- Step 3** Change the web timeout period on the active server. For more information, see [Set the Web Timeout Period, page 16-44](#).
- Step 4** Enter the following CLI command on the standby server:
- ```
services start
```
-

Controlling Access via HTTP/HTTPS on Redundant Nodes

If you are implementing HTTP/HTTPS access control by using the **http-server accept** CLI command, you must add each server (node) to the other server's access list.

Assuming that the redundant WLSEs have IP addresses 209.165.202.100 and 209.165.202.200, enter the following CLI command on the WLSE with IP address 209.165.202.100:

```
http-server accept 209.165.202.200
```

Enter the following CLI command on the WLSE with IP address 209.165.202.200:

```
http-server accept 209.165.202.100
```

Using WLSE Diagnostics Options

The Diagnostics option provides tools to aid in troubleshooting. You can use these tools when you have a problem that might require assistance from the Cisco Technical Assistance Center (TAC).

The options under **Admin > Appliance > Diagnostics** are:

- **WLSE Info**—Gather troubleshooting information about the WLSE status and create status reports (see [Viewing and Creating a Status Report, page 16-39](#)).
- **Self Test**—Create and display self tests (see [Viewing and Creating a Self-Test Report, page 16-40](#)).
- **Processes**—View WLSE process status, stop and start processes (see [Managing Processes, page 16-40](#)).

Viewing and Creating a Status Report

This option provides a tool to aid in troubleshooting. The WLSE information and status report shows general WLSE status, log files, package information, database status, process status, web server information, Java class information, and log files.



Note Status reports show [UTC](#) time.



Note Your login determines whether you can use this option.

Procedure

-
Step 1	Select Admin > Appliance > Diagnostics > WLSE Info . Any existing reports are listed.
Step 2	To display a report, click its name.
Step 3	To create a new report, click Create . It will take five to seven minutes for the report to be complete. To display the new report, click its name. If the new report is not listed, click Refresh .
Step 4	To delete a report, select it and click Delete .
-

Related Topics

- [Viewing and Creating a Self-Test Report, page 16-40](#)
- [Managing Processes, page 16-40](#)

Viewing and Creating a Self-Test Report

This option provides a tool to aid in troubleshooting. Self-tests show the status of WLSE memory, database, DNS setup, and backup location configuration. Reports indicate whether the tests passed or failed. Self-tests are used mainly by the TAC when diagnosing problems.



Note Self-test reports show timestamps as [UTC](#) time.



Note Your login determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Appliance > Diagnostics > Self Test**. Any existing report is listed.
- Step 2** To display the report, click its name.
- Step 3** If no report is listed, you can create a new report by clicking **Create**.
- Step 4** To display the new report, click its name. If the report is not displayed, click **Refresh**.
- Step 5** To delete a report, select it and click **Delete**.

Related Topics

- [Viewing and Creating a Status Report, page 16-39](#)
- [Managing Processes, page 16-40](#)

Managing Processes

This option provides a tool to aid in troubleshooting. You can view the status of the major processes running on the WLSE, start and stop processes, and access complete reports.

If a process has failed a message (in red) is displayed in the top right corner of the Web interface. For example: **Following process failed: WirelessSvcManager.**



Note Your login determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Appliance > Diagnostics > Processes**. The Process Report displays the following information.

Column	Description
Process name	How a process is registered. For information on the processes displayed, see Processes Displayed, page 16-42 .
State	Process status and a summary of the log file entries for the process. A green up arrow shows that the process is running; a red down arrow shows that the process has failed. Click on the arrow for more information about process status.
Pid	Process ID. A unique number by which the operating system identifies each running program.
RC	Return code. “0” means normal program operation. Any other number typically represents an error. Refer to the error log.
Signo	Signal number. “0” means normal program operation. Any other number is the last signal delivered to the program before it terminated.
Start Time	Time (UTC) and date the process was started.
Stop Time	Time (UTC) and date the process was stopped.
Core	“Not applicable” means the program is running normally. “Core file created” means the program is not running normally and the operating system has created a core file. The core file stores important data about processes.
Information	What the process is doing. “Not applicable” means the program is not running normally.

Step 2 From the process table, you can do the following:

Task	Procedure
View details.	Click process name. See Daemon Information, page 16-42 .
View process status.	Click process state. See Process Status, page 16-42 .
Stop process.	Select process and click Stop . New status and other process information is displayed. The WebServer and Tomcat processes cannot be stopped.
Start process.	Select process and click Start . New status and other process information is displayed.
Update table with latest data.	Click Refresh . The table does not automatically update.
View all processes.	Click Complete Report . The system status is displayed.

Related Topics

[Administering Management Services via CLI, page 17-15](#)

Processes Displayed

The Process Report table displays the status of the following major WLSE processes:

Process Name	Description
TFTP	TFTP server.
WLSEIdleServer	Idle logout server for access to the CLI via Telnet or SSH.
WLSERepository	Local software repository server.
WirelessSvcMgr	Process that manages radio management tasks.
WLSEjobvm	Job virtual machine.
WLSEFaults	Fault manager.
WebServer	Web server.
Tomcat	Java servlet engine.
HaMibDaemon	HA MIB agent. Daemon process that listens to the redundancy switchover events and sends them to the SNMP agent.
ExcepReporter	Trap processes.
CDPbrdcast	CDP daemon that identifies Cisco devices to their immediate neighbors.

Daemon Information

The Daemon Information dialog box displays the following:

Field	Description
Process	Process name.
Path	File location.
Flags	Flags used to register process with the Daemon Manager.
Startup	Method used to start process.
Dependencies	Other processes that must be running for this process to run.

Process Status

The system log, which describes the status of the processes running in the system, displays the following:

Field	Description
Timestamp	Date and time the message is logged.
Process	Process that logged the message.
Type	Message type: INFO, WARNING, CRITICAL.
Information	Process status as known by the Daemon Manager.

Specifying a Splash Screen Message

The Splash Screen option allows you to set up a message that is displayed when a user logs in. After viewing the message, the user clicks **Agree** to continue logging in or **Disagree** to log out.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Appliance > Splash Screen**.
- Step 2** Enter the message to be displayed.
- Step 3** Check the **Enable** check box, then click **Apply**. The splash screen message is enabled.

**Note**

You *must* check **Enable** for the message to appear.

Setting Time, Time Servers, Name Servers, and Web Session Timeout

The **Admin > Appliance > Time/NTP/Name/Web Timeout** option allows you to:

- [Set the Current Local and UTC Time, page 16-43](#)
- [Specify NTP Time Servers, page 16-44](#)
- [Specify Name Servers, page 16-44](#)
- [Set the Web Timeout Period, page 16-44](#)

Set the Current Local and UTC Time

Current local (browser) time appears in most WLSE displays. Universal Coordinated Time ([UTC](#)) is the system time and appears in log files.

To set the time that appears in the Web interface, use the following procedure. Because there is a single system clock, setting the time here also updates the UTC time.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Appliance > Time/NTP/Name/Web Timeout**.
- Step 2** In the Current Time area, select the new time and date parameters from the lists and click **Update**.
-

Related Topics

[Setting the System Clock Manually via CLI, page 17-12](#)

Specify NTP Time Servers

This option allows you to maintain the current time on the WLSE by using [NTP](#) (Network Time Protocol) servers.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Appliance > Time/NTP/Name/Web Timeout**.
- Step 2** To remove an NTP server, select it from the Current Servers list and click Remove.
- Step 3** To add an NTP server, enter the server's IP address in the NTP Server IP Address text box and click **Enable**.
-

Related Topics

[Setting the System Clock Using NTP via CLI, page 17-11](#)

Specify Name Servers

You can specify the addresses of up to three name servers for name and address resolution.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Appliance > Time/NTP/Name/Web Timeout**.
- Step 2** To remove a name server, select it and click **Remove**.
- Step 3** To add a name server, enter its IP address in the Name Server IP Address textbox and click **Enable**.
-

Set the Web Timeout Period

The default timeout period for the Web interface is 30 minutes. If there is no input for 30 minutes, you will be logged out.

If WLSE redundancy is in effect, you should stop and restart services on the standby WLSE. Otherwise, resetting the timeout will cause a switchover from the active server to the standby server and the new timeout period will not take effect. For the procedure to reset the web timeout when using redundancy, see [Changing the Web Timeout Period on Redundant Nodes, page 16-38](#).

**Note**

Your login determines whether you can use this option.

To reset the timeout period for the Web interface:

Procedure

-
- Step 1** Select **Admin > Appliance > Time/NTP/Name/Web Timeout**.
- Step 2** To change the timeout period:
- Enter the new timeout setting (in seconds) in the **New Timeout** field.
 - Click **Set**.
-  **Note** After you click Set, the Web server will be restarted for the new timeout to take effect and you will be logged out.
-
- Step 3** To reset the timeout period to the default (30 minutes), click **Restore Default**.
-

Configuring the Mail Route

To ensure that WLSE email notifications reach their destinations, you can configure the WLSE's mail route by specifying an [SMTP](#) mail server. This setting affects emailing notifications about firmware and configuration jobs, emailing reports, and emailing fault notifications.



Note Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Appliance > Configure Mailroute**.
- Step 2** Enter the hostname or IP address of an SMTP mail server on your network and click **Save**.
- Step 3** To remove the mail route, click **Remove**.
-

Related Topics

[Configuring the Mail Route via CLI, page 17-15](#)

Managing Files for the WLSE TFTP Server (WLSE Express Only)



Note Your login determines whether you can use this option. This option is available on the [WLSE Express](#) only.

You can manage files in the /tftpboot/public directory of the WLSE Express by using the TFTP Management option. For example, you can download images for routers, switches, and other devices in the network and load the images on the devices. The space available in this directory for managing files is 1 gigabyte.

The root directory for the TFTP server is /tftpboot. However, when sending files to the WLSE TFTP server, use a pathname starting with /public (instead of /tftpboot/public).

The following file management operations are permitted:

- Uploading files from the desktop or other systems and downloading files to the desktop or other systems.
- Deleting files.
- Creating an empty file to allow file *put* operations from TFTP clients and importing files from devices.


Note

User files in the /tftpboot/public directory will be backed up and restored by the normal WLSE backup/restore processes and files will be synchronized when operating in redundancy mode.

Procedure

Step 1 Select **Admin > Appliance > TFTP Management**. A listing of files currently in the /tftpboot/public directory is displayed.

Step 2 To import a file from the desktop:

- Enter the path in the text box or click **Browse** to locate the file.
- Click **Upload**.

Result: The file will be copied to the /tftpboot/public directory and listed in the file table. The file table includes information about the total amount of space that has been used and contains the following fields for each stored file:

Field	Description
Name	Filename
Size	Size of file
Last Modified	Date and time created or last modified
Trashcan icon	Deletes the file.
Rename icon	Allows you to rename the file.
Save icon	Allows you to view or download the file.

Step 3 To create an empty file for TFTP *put* operations:

- Enter the filename in the text box.
- Click **Create**.

Result: An empty file will be created in the /tftpboot/public directory and listed in the file table.


Note

The /tftpboot directory is the root directory for the TFTP server. Therefore, to transfer a file to the WLSE, include the subdirectory in the command: `tftp://wlse_ip_address/public/filename`.

Step 4 To download a file to the desktop:

- Click the save icon in the file table.

- b. In the Downloading dialog box, click **Open** or **Save**.
- c. Browse to the location where you want to save the file.

Step 5 To rename a file:

- a. Click the Rename icon in the file list.
- b. Enter the new name, then click **OK**.

Step 6 To delete a file, click the trashcan. To delete all files, click **Select All**, then click **Delete**.

To deselect a file, click its checkbox in the file table. To deselect all files, click **Deselect All**.

Using Connectivity Tools

When you select **Admin > Appliance > Connectivity Tools**, the following options for testing device connectivity and reachability are displayed:

- **Network Tools**—ping, traceroute, nslookup, TCP port scan, SNMP reachability (see [Using Network Tools, page 16-47](#)).
- **SNMP Query Tool**—query a device's SNMP variables (see [Using the SNMP Query Tool, page 16-48](#)).
- **Telnet/SSH Tool**—Telnet and SSH reachability (see [Using the Telnet/SSH Tool, page 16-48](#)).

Using Network Tools

The Network Tools option offers several tools for testing device connectivity.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Admin > Appliance > Connectivity Tools**.

Step 2 Enter a device name or IP address in the Device text box.

When you select an option button, the results window tells you whether the connectivity test was successful. Pressing **Enter** will not work. You *must* click a button.

Table 16-10 **Connectivity Tools**

Button	Description	Results
Ping	Tests device reachability.	If successful, statistics are displayed on the packets transmitted and received.
Traceroute	Detects routing errors between the WLSE and a device.	If successful, the routes to the device are displayed.
NSLookup	Looks up hostname or IP address information via the name server.	If successful, displays the name server name and IP address and the device name and IP address.

Table 16-10 **Connectivity Tools (continued)**

Button	Description	Results
TCP Port Scan	Finds the active ports on a device.	Displays the active ports.
SNMP Reachable	Tries to reach a device by using SNMP and tests read/write SNMP strings. To reach a device by using SNMP, the device's credentials must be in the WLSE database. To check credentials, select Devices > Discover > Device Credentials > SNMP Communities .	If the device is reachable, its sysObjID is displayed. If no sysObjID is returned: • The query may be timing out because the device is busy or is remotely located. • The SNMP agent in the device may not be functioning.

Step 3 Click **Close** to close the results window.

Using the SNMP Query Tool

This tool allows you to find the value of a specified SNMP variable. Normally, this tool is used under the direction of Cisco TAC when they are assisting you with troubleshooting a problem.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Appliance > Connectivity Tools > SNMP Query Tool**.
- Step 2** Enter the device's IP address or hostname and the OID of the SNMP variable.
- Step 3** Click **Get** to display a single-value variable.
- Step 4** Click **Get Table** to display a variable that consists of a table.
- Step 5** Click **Clear** to clear your entries.

Using the Telnet/SSH Tool



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Appliance > Connectivity Tools > Telnet/SSH Tool**.
- Step 2** Enter a device name or IP address in the Device text box.
- Step 3** Click **Telnet** to verify Telnet connectivity to the WLSE.

Step 4 Click **SSH** to verify SSH connectivity to the WLSE.

**Note**

If the Telnet or SSH credentials fail, go to **Devices > Discover > Device Credentials > Telnet/SSH User/Password** and modify the credentials. See [Entering Device Credentials, page 4-5](#).

Step 5 Click **Clear** to clear your entries.

Managing Firmware Version Support

You can use the WLSE to view the versions currently supported by the WLSE.

**Note**

Your login determines whether you can use this option.

Procedure

To display firmware versions currently supported by the WLSE:

Step 1 Select **Admin > System > Firmware Supported Versions**.

Step 2 The access point firmware versions that are supported by the WLSE Firmware module are displayed.

Step 3 To import updated firmware support, see [Managing Firmware Version Support, page 16-49](#).

**Note**

For a list of the devices supported by WLSE, see the Supported Devices Table on Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_device_support_tables_list.html

Managing GUI Users

The options displayed when you select **Admin > User Admin** allow you to manage user roles and logins:

- [Managing Roles, page 16-49](#)—Add, modify, and delete user roles.
- [Managing User Accounts, page 16-51](#)—Add, modify, and delete user accounts.

Related Topics

- [Modifying Your Profile, page 16-55](#)
- [Overview: Authentication Modules, page 16-15](#)

Managing Roles

Use this option to add, modify, and delete user-defined roles and to modify predefined roles. A user's role determines the tabs and subtabs the user can access. Users who have access to a subtab can perform all of the tasks under the subtab.

This section contains the following topics:

- Adding, modifying, and deleting roles—See [Adding, Modifying, and Deleting Roles, page 16-51](#).
- About roles—See [Overview: Roles, page 16-50](#).

Overview: Roles

A user's role grants access privileges to WLSE functions. The role determines the tabs and subtabs the user can access. Users who have access to a subtab can perform all of the tasks under the subtab. Although you cannot delete predefined roles, you can modify them. The predefined roles and their default privileges are:

- System administrator—Allows access to all WLSE tasks. You can change the password using the console or the WLSE's Manage Users option (see [Managing User Accounts, page 16-51](#)). You cannot modify the privileges of the System Admin role. A user who has the System Admin role can modify other user roles.
- Network administrator—Monitoring authority, device configuration authority, and discovery configuration authority.
- Network operator—Monitoring and device configuration authority.
- Help desk—Monitoring authority only.

You can use these predefined roles to control which features staff members are allowed to access. Less skilled, front-line technical support can be assigned the Help Desk role. More skilled and experienced support staff might be given the Network Operator or Network Administrator roles. The most skilled and experienced staff with direct responsibility for the WLSE should be given the System Admin role.

The following privileges have special functions:

- [About XML API Privileges, page 16-50](#)
- [About Debug Tools Privileges, page 16-50](#)
- [About Redundancy User Role Attributes, page 16-50](#)

About XML API Privileges

The XML API privileges are for users who will be using the XML application programming interface (API). If you are using the API, you should create different users for this purpose, and grant such users access to the API only. Access to the API is authenticated and authorization is checked. For more information about the XML API, see the *Developer Guide for the CiscoWorks Wireless LAN Solution Engine*. This guide is included with the XML API SDK (Software Developer Kit) in the Software Center on Cisco.com.

About Debug Tools Privileges

The Debug Tools privilege determines whether users can run the debug tools, which are not needed in normal customer environments. These tools are sometimes used in cases involving Cisco support personnel.

About Redundancy User Role Attributes

Any user that is used as the redundancy user must have the Redundancy attributes in their role. See [Adding, Modifying, and Deleting Roles, page 16-51](#) for more information about modifying user-defined roles.

Adding, Modifying, and Deleting Roles

You can edit the predefined roles, or you can create new, user-defined roles. You can modify or delete any user-defined roles.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** To access the role management window, select **Admin > User Admin > Manage Roles**. Role names are displayed in the center pane. To view the subtabs to which the role has access, select the role.
- The [admin](#) user and users who have the System Administrator role can view all roles.
 - The admin user and a user who has the System Administrator role can modify all of the other roles.
 - Other users can only view the roles assigned to them and roles that they have created.
- Step 2** To add a role:
- a. Replace the text *New Role* with the name you have chosen for the new role.
 - b. Select the check boxes next to the features the role will access. Click **Add**.
-  **Note** When you select a feature (for example, Display Faults), the role is granted access to the corresponding subtab (for example, **Faults > Display Faults**).
- c. The new role appears in the list of roles.
- Step 3** To modify a role, select the role. Select the check boxes for the features you want to add to the role and deselect the check boxes next to the features you want to remove from the role. Then click **Modify** to save the changes.
- Step 4** To delete a user-defined role, select the role, then click **Delete**.

Related Topics

- [Naming Guidelines, page B-1](#)
- [Managing User Accounts, page 16-51](#)

Managing User Accounts

Using the options under this tab, you can create new user accounts, modify existing users, and delete users. The topics in this section are:

- [Adding Users, page 16-52](#)
- [Modifying Users, page 16-54](#)
- [Deleting Users, page 16-55](#)
- [Overview: User Accounts, page 16-52](#)

Related Topics

- [Overview: Authentication Modules, page 16-15](#)
- [Modifying Your Profile, page 16-55](#)
- [Naming Guidelines, page B-1](#)
- [User Management via CLI, page 17-3](#)

Overview: User Accounts

Each new user must be assigned at least one role and assigned a privilege level for accessing the WLSE CLI. There are three possible privilege levels for the WLSE CLI:

- None—No access to the CLI.
- Level 0—Access to a small subset of CLI commands.
- Level 15—Full WLSE CLI access. Typically, level 15 privileges should only be given to the most skilled systems administration level users.

The default user (admin) is created during initial setup of the WLSE. The admin user has the System Administrator role and level 15 CLI privileges. This user cannot be deleted.

User accounts that you add by using the CLI commands do not have Web interface privileges. You can modify such users in the Web interface and add the appropriate roles to give them access to the Web interface.

Except for the admin user and users with the System Administrator role, only the logins created by you are displayed. If logins were created by another user, they are not visible; only their creator can display them. However, the admin user and any user with the System Administrator role can view all users, no matter who created them.

Adding Users

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > User Admin > Manage Users**. The Users list displays the current users.
- The [admin](#) user can view and modify all existing users.
 - Users who have the System Administrator role can view all users that have been created, no matter who created them. Other users can view their own logins and any users they have created.
 - When creating other users, a user can only assign his role or a role with lesser privileges. For example, userA has only the network administrator role. Users created by userA can have only the network administrator role or roles with fewer privileges.
- Step 2** Enter the following information, in the order shown in [Table 16-11 on page 16-53](#).

Table 16-11 Adding Users

Field	Information to Enter
User Name	Name of the new user. Usernames can be up to 32 characters in length and are case-sensitive. Most characters are allowed, except for the colon, comma, single quote, double quote, or space. For more information on the allowable characters, see Appendix B, “Naming Guidelines.” Note Usernames must begin with a character and cannot begin with a number. However, if the user is <i>not</i> using the CLI (that is, CLI Access is set to <i>None</i>), the username can begin with a number.
User Password	Password for the new user.
Confirm Password	Passwords are unlimited in length and are case-sensitive. You can use most characters, except for the single quote or double quote. For more information on the allowable characters, see Appendix B, “Naming Guidelines.”
Email	Email address of the user (optional).
CLI Access	User’s level of access to the WLSE CLI: None, Level 0, or Level 15. Users with privilege level 15 can use all commands, and users with privilege level 0 can use a small subset of commands. ¹
Roles	One or more roles for the user. Roles determine the user’s access to tabs and subtabs in the Web interface. - To add a role, select it from the pulldown list. - To view a role, select it and click show role. - To remove a role, select it and click remove.

1. For information on CLI commands, see [Appendix A, “Command Line Interface \(CLI\) Commands.”](#)

Step 3 To clear your entries and start over, click **Clear**.

Step 4 To add the new user, click **Add**. The new username is added to the Users list. To discard your changes, click **Clear**.

Step 5 After you add users, it is recommended that you run a backup. See [Scheduling and Running Backups, page 16-23](#).

Related Topics

- [Modifying Your Profile, page 16-55](#)
- [Naming Guidelines, page B-1](#)
- [Managing Roles, page 16-49](#)

Modifying Users

**Note**

Your login determines whether you can use these options.

Procedure

To modify a user:

- Step 1** Select **Admin > User Admin > Add/Modify/Delete**. The Users list displays the current users.

**Note**

Except for the [admin](#) user and users with the System Administrator role, only the logins created by you are displayed. If logins were created by another user, they are not visible; only their creator can display them. However, the admin user and any user with the System Administrator role can view all users.

- Step 2** Select the user from the Users list and make the desired changes, using the field descriptions in [Table 16-12 on page 16-54](#).

Table 16-12 **Modifying Users**

Field	Information to Enter
User Name	User's name. Usernames can be up to 32 characters in length and are case-sensitive. Usernames must begin with a character and cannot begin with a number. Note If the user is <i>not</i> using the CLI (that is, CLI Access is set to <i>None</i>), the username can begin with a number. For information on the allowable characters, see Appendix B, "Naming Guidelines."
User Password	New password for user.
Confirm Password	Passwords are unlimited in length and are case sensitive. You can use any character except for the single quote, double quote, and dollar sign.
Email	Enter or change the user's email address.
CLI Access	User's access to the WLSE CLI : None, Level 0, or Level 15. By default, Level 15 is selected for the System Administrator role, and None is selected for others. Users with privilege level 15 can use all commands, and users with privilege level 0 can use a subset. For information on commands that are available for each privilege level, see Appendix A, "Command Line Interface (CLI) Commands."

Table 16-12 **Modifying Users**

Field	Information to Enter
Roles	The user's roles. Roles determine the user's access to tabs and subtabs in the Web interface. • To add a role, select it from the pulldown list. • To view a role, select it and click show role. • To remove a role, select it and click remove.

Step 3 Click **Modify** to save your changes or **Clear** to discard your changes.

Related Topics

- [Naming Guidelines, page B-1](#)
- [Managing Roles, page 16-49](#)
- [Modifying Your Profile, page 16-55](#)

Deleting Users

Use the following procedure to delete users.

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **Admin > User Admin > Manage Users**.

Step 2 Select the username from the Users list, then click **Delete**. After you click **OK**, the user is deleted.

Modifying Your Profile

Use the My Profile tab to:

- Change your password—See [Changing Your Password, page 16-56](#).
- Change your email address—See [Changing Your Email Address, page 16-56](#).
- Set your home page preferences—See [Changing the Default Tab and Subtab, page 16-56](#).

Changing Your Password

The user password is set when the user is created. Use the following procedure to change your password.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > My Profile > Change password**.
- Step 2** To change your password, enter a new password in the New Password and Re-enter New Password fields. For information on allowable characters, see [Naming Guidelines, page B-1](#).
- Step 3** Click **Apply** to save your changes or **Reset** to discard your changes.
-

Related Topics

- [Modifying Users, page 16-54](#)
- [Naming Guidelines, page B-1](#)

Changing Your Email Address

The email address is set initially when a user is created. To change your email address, use the following procedure.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > My Profile > Change Email Address**.
- Step 2** Enter a new email address.
- Step 3** Click **Save** to save your changes or **Reset** to discard your changes.
-

Related Topics

- [Modifying Users, page 16-54](#)

Changing the Default Tab and Subtab

By default, an overview that provides information about all the main tabs is displayed when you log in. When you select a tab, an overview of the subtabs is displayed.

Use the following procedure to select a tab as your home page and select default subtabs for each main tab.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > My Profile > Set Tab Defaults**.
- Step 2** Select the home page you want displayed when you log in. For example, you may want your most frequently used tab to be displayed first.
- Selecting Overview restores the defaults.
 - Selecting a main tab makes that tab your default home page.
- Step 3** Select default subtabs for any or all main tabs:
- Selecting Overview displays information about the contents of the subtab.
 - Selecting a subtab makes that subtab the default tab that appears first when you select the main tab.
- Step 4** Click **Save** to save your changes or **Reset** to discard them.
-

Creating Links

You can link to other systems and display their desktops in the right pane or in a separate window. For example, you could link to a CiscoWorks server, to Cisco Secure Access Control Server (ACS), or to another WLSE.

The special link called ACS Failed Login Report generates a report about failed logins on an ACS server.

This section contains the following topics:

- Creating a link to another system, such as a CiscoWorks server or another WLSE—See [Creating a Link to Another System, page 16-57](#).
- Configuring the ACS Failed Login Report link and recreating the link if it has been deleted—See [Configuring the ACS Failed Login Report Link, page 16-58](#).
- Running the ACS Failed Login Report—See [Running the ACS Failed Login Report, page 16-60](#).

**Note**

This feature is available to all users.

Creating a Link to Another System

**Note**

The following characters are unsupported and cannot be entered in this dialog: double quote, single quote, and angle brackets (< >).

Procedure

-
- Step 1** Select **Admin > Links**. The Add Links window and current links appear.

- Step 2** To add a link:
- Enter the name of the link and the URL of the system in the Add Link window; for example: `http://cw_server:1741` creates a link to the CiscoWorks server called `cw_server`.
 - To display the system's desktop in the right pane of the WLSE interface, deselect **Open in New Window**. Otherwise, the display opens in a separate window. It is recommended that you display the desktop in a separate window.
 - Click **Save**. The link is added to the Links list in the left pane.
- Step 3** To edit a link:
- Click **Edit** under the name of the link in the Links list.
 - Make your changes and click **Save**.
- Step 4** To delete a link, select the link name in the Links list and click **Delete**.
- Do not delete the ACS Failed Login Report link. If you accidentally delete it and want to recreate it, see [Replacing a Deleted Link, page 16-59](#).
- Step 5** To connect to the other system, click the link name in the left pane.
-

Configuring the ACS Failed Login Report Link

This section contains the following topics:

- [Configuring the Link, page 16-58](#) (the link must be configured before you can display a report).
- [Replacing a Deleted Link, page 16-59](#) (use this procedure if the link is missing from the list of current links).

Configuring the Link



Note

The following characters are unsupported and cannot be entered in this dialog: double quote, single quote, and angle brackets (< >).

The link must be configured before you display a report.

Procedure

- Step 1** On the ACS server, enable Web access for the admin user.
- Step 2** On the WLSE, select **Admin > Links**. The Add Links window and current links appear.
- Step 3** Click **Edit** under ACS Failed Login Report and enter the following information:

Field	Description
URL	URL of the ACS server, in the format <code>http://ACS_server:port</code> or <code>https://ACS_server:port</code> . For ACS server 3.x for Windows, the port number is 2002.
Username	Administrator username created when ACS software was installed on the ACS server.
Password	Password for the administrator username.

Step 4 To display the report in the right pane of the WLSE interface, deselect **Open in New Window**. Otherwise, the report opens in a separate window.

Step 5 Click **Save**.

Related Topics

[Running the ACS Failed Login Report, page 16-60](#)

Replacing a Deleted Link

If the link has been deleted, use the following procedure to create it again.

Procedure

- Step 1** Navigate to **Admin > Links** and click **Add to Links ...**
- Step 2** In the Name field, enter **ACS Failed Login Report**, then click **Save**. The ACS Failed Login Report link appears in the list of current links.
- Step 3** Click **Edit** under ACS Failed Login Report and enter the following information:

Field	Description
URL	URL of the ACS server, in the format <code>http://ACS_server:port</code> . For ACS server 3.x for Windows, the port number is 2002.
Username	Administrator username created when ACS software was installed on the ACS server.
Password	Password for the administrator username.

Step 4 To display the report in the right pane of the WLSE interface, deselect **Open in New Window**. Otherwise, the report opens in a separate window.

Step 5 Click **Save**.

Related Topics

[Running the ACS Failed Login Report, page 16-60](#)

Running the ACS Failed Login Report

The ACS failed login report shows failed logins on a specified Cisco Access Control Server (ACS).

**Note**

Only a single link is supported; therefore, you cannot add a second link that points to a second ACS server.

To run an ACS failed login report:

Procedure

-
- Step 1** Select **Admin > Links**. The ACS Failed Login Report link is displayed in the list of current links:
- If the link is missing, see [Replacing a Deleted Link, page 16-59](#).
 - If no report is displayed, see [Configuring the ACS Failed Login Report Link, page 16-58](#).
- Step 2** To run the report, click **ACS Failed Login Report**.
-



Managing the WLSE System via the CLI

This chapter describes some of the system administration tasks that you can perform by using the command line interface (CLI).

For information about performing system administration tasks from the the Web interface, see [Chapter 16, “Managing the WLSE System.”](#)

This chapter contains the following topics:

- [Using CLI Commands, page 17-1](#)
- [Using a Console with the WLSE, page 17-2](#)
- [Logging In and Out via CLI, page 17-2](#)
- [User Management via CLI, page 17-3](#)
- [Backing Up and Restoring via CLI, page 17-5](#)
- [Upgrading WLSE Software via CLI, page 17-10](#)
- [Shutting Down and Powering Off the WLSE, page 17-10](#)
- [Rebooting the WLSE via CLI, page 17-10](#)
- [Setting WLSE System Date and Time via CLI, page 17-11](#)
- [Configuring Ethernet Interfaces, page 17-12](#)
- [Administering Management Services via CLI, page 17-15](#)
- [Viewing System Information via CLI, page 17-15](#)
- [Managing Disk Space, page 17-17](#)
- [Recovery Management, page 17-17](#)

Using CLI Commands

Any user with CLI access can log in to the command-line interface. Most CLI commands require access level 15. This access can be assigned in the Web interface (**Admin > User Admin > Manage Users**) or through the CLI (**username** CLI command).

For details on all of the CLI commands, see [Appendix A, “Command Line Interface \(CLI\) Commands.”](#)

Using a Console with the WLSE

Some of the procedures in this chapter require that you connect a console to the console/serial port.

Procedure

-
- Step 1** If there is a monitor or keyboard connected to the WLSE, remove it.
- Step 2** Connect a console terminal or PC running Hyper Terminal to the WLSE's console/serial port. Use the cable supplied with the WLSE and, if necessary, the DB-9-to-RJ-45 console adapter.
- For the [WLSE 1130 series](#), use the serial port on the back panel.
 - For the WLSE 1030, use the console/serial port on the back panel.



Note

Use the console/serial port; do not use the video port.

For more information on the console/serial port, see the relevant *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine* on Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_installation_guides_list.html.

Logging In and Out via CLI

Use the following commands to log in and out of the WLSE via the CLI. By using this method of logging in, you can use the WLSE's CLI commands.



Note

The CLI has a pre-set timeout of 15 minutes. This is not configurable. After 15 minutes of inactivity, you will be logged out of the CLI.

Logging In

To use the CLI to log in:

Procedure

-
- Step 1** Attach a console or connect via Telnet or SSH to the WLSE.
- If you are using a console:
- For the [WLSE 1130 series](#), use the serial port on the back panel.
 - For the WLSE 1030 (WLSE express), use the console/serial port on the back panel.
- Step 2** At the login prompt, enter **admin** or use another account that has CLI privileges.
- Step 3** At the password prompt, enter the password.

Result: The system prompt appears.

**Note**

Users must have CLI privileges to use the CLI. Users who have only level 0 privileges can use only a small subset of the CLI commands. Users who have level 15 privileges can use all commands. For information on setting these privileges via CLI, see [Managing User Accounts, page 17-3](#). For information on setting CLI privileges via the Web interface, see [Managing User Accounts, page 16-51](#).

Logging Out

To log out, use the **exit** command.

User Management via CLI

This section contains the following topics:

- [Managing User Accounts, page 17-3](#)
- [Setting Up TACACS+ or RADIUS Authentication for CLI Login, page 17-4](#)

Managing User Accounts

You can create users via the CLI and grant them CLI privileges. Such users appear in the user management screens of the Web interface, but they do not have access to the Web interface features unless you modify them in the Web interface to add access.

Creating and Modifying User Accounts

**Note**

Your login determines whether you can use this command.

To create or modify user accounts, use the following command for each user account you want to add or modify:

```
username name password password privilege 0 | 15
```

where:

- *name* is the username of the account.

Username can be up to 32 characters in length, are case sensitive, and must not begin with a number. Passwords cannot contain a colon, semi-colon, comma, single quote, double quote, or space.

- *password* is the user's password.

Passwords are unlimited in length and are case sensitive. You can use any character except for the single quote or double quote.

- **privilege 0** allows access to a subset of the CLI commands (see [CLI Command Details, page A-7](#)). This is the default and is assigned to the account even if you omit this argument.
- **privilege 15** allows access to all CLI commands.

To allow access to the Web interface, log into the Web interface and modify the user's account to add roles and privileges (see [Managing User Accounts, page 16-51](#) or the online help).

Deleting User Accounts

To delete a user, enter the following command:

```
no username name
```

where *name* is the user to be deleted.

Setting Up TACACS+ or RADIUS Authentication for CLI Login

You can use an authentication server for logging in through Telnet or SSH. This requires configuring the authentication server and setting up the authentication module on the WLSE.

To configure the authentication server, add the WLSE as a client, configure the shared secret, and add the users. The users must also exist on the WLSE; see [Creating and Modifying User Accounts, page 17-3](#).

**Note**

WLSE does not support MS NT Domain authentication.

**Note**

Your login determines whether you can use this command.

To set up the WLSE's RADIUS module, enter the following command:

```
auth cli failover radius secret server
```

where *secret* is the shared secret and *server* is the hostname or IP address of the authentication server.

To set up the WLSE's TACACS+ module:

```
auth cli failover tacacs secret server
```

where *secret* is the shared secret and *server* is the hostname or IP address of the authentication server.

**Note**

If you use CLI remote authentication, you must create a local user on the WLSE. You do not need to create a local user on the WLSE for HTTP authentication.

For more information about using alternative authentication, see [auth, page A-7](#), and [Overview: Authentication Modules, page 16-15](#).

Backing Up and Restoring via CLI

You should backup the WLSE at regular intervals and before software updates or system recoveries.

Before attempting to backup or restore your WLSE, make sure you have the following:

- A remote FTP or SCP host to serve as the backup location.
- A valid username and password on the backup location.
- A backup directory on the backup location that has the proper permissions for the username and password you will be using.

Backups preserve the database, flash memory (network information and users' CLI privileges), and the user configuration (including users, roles, templates, firmware images, device credentials, policies, and threshold settings).

Backups do not preserve startup templates, the mail route, and AAA server trend data. Also, the four system-defined user roles will be reset to their default privileges.

This section contains procedures for specifying the backup location, backing up the WLSE, and restoring the WLSE. For an example backup sequence, see the description of the **backup** CLI command in [backup](#), page A-8.

**Note**

You can replace one WLSE with another by backing up and restoring the data from the old WLSE to the new one. See [Installing a Replacement WLSE](#), page 17-8.

**Note**

You can restore a backup made on one WLSE to another WLSE. For information, see [Copying Configuration Data to another WLSE via CLI](#), page 17-9.

Setting Up the Backup Location

Before backing up, you must specify an FTP or SCP server as the backup location. Please observe the following cautions about the backup location:

- Backup has been tested on the standard Windows 2000, Windows XP, and Unix FTP and SCP servers only. Therefore, only these servers are explicitly supported for WLSE backups. However, any server that uses standard FTP commands and protocol should work.
- Make sure the target FTP or SCP directory has enough free space, especially if you are running frequent backups. If there is not enough space, the backup may fail or the backup data may be corrupted.
- If you are using a Windows 2000 or Windows XP server as the backup location, you must configure the server for UNIX directory mode. See [Configuring a Windows System as a Backup Location](#), page 16-22.
- SCP uses keys to identify the remote host and stores these keys on the WLSE. If the key on the remote host changes, the backup cannot be transferred. If you know that a key was legitimately changed on the remote host, you can use the **clearbackuphosts** CLI command to clear the stored keys. After that, the new keys can be stored.

**Note**

Your login determines whether you can use the commands described in this section.

Specifying the Backup Location

To specify the backup location, enter the following command:

```
backupconfig hostname username password {FTP|SCP} [timeout [directory]]
```

where:

- *hostname* is the hostname or IP address of the backup system.
- *username* is the username of a user on the backup system.
- *password* is the password of the user on the backup system.
- *FTP* or *SCP* is the protocol used for the backup transfer
- *timeout* is the timeout value in seconds for backup restore jobs. The default is 7200seconds, You can enter any value between 3600 and 43200 seconds.
- *directory* is the pathname of the backup directory, if different from user's default directory.



Note To specify a backup directory, you must specify a timeout value.

This backup location information will be used by the **backup**, **listbackup**, and **restore** commands.

Displaying the Backup Location

If a backup location has been specified, you can display the hostname and username by entering the following command:

```
show backupconfig
```

Removing the Backup Location

To remove the backup location, enter the following command:

```
no backupconfig
```

Backing Up the WLSE

When backing up via the CLI, you can perform manual, one-time backups. To schedule regular backups, use the Web interface; for information, see [Backing Up and Restoring Data, page 16-20](#).



Note WLSE operations continue during the backup.



Note Your login determines whether you can use this command.

Procedure

To back up the WLSE:

-
- Step 1** Make sure the backup location has been configured. See [Setting Up the Backup Location, page 17-5](#).
- Step 2** To test the availability of the backup location enter:
- ```
backup test
```
- Step 3** To backup the WLSE, enter:
- ```
backup
```

Result: The WLSE will be backed up to the location you specified in the **backupconfig** command.

Restoring WLSE Configuration

During the restore procedure, the following occur in sequence:

1. The WLSE shuts down automatically.
2. Data is restored.
3. The WLSE reboots.

**Note**

The WLSE shuts down during the restore operation and reboots afterwards.

**Note**

Your login determines whether you can use these commands.

To restore the WLSE configuration:

- Step 1** Set up the backup location by using the **backupconfig** command.
- Step 2** To list the available backups, enter:
- ```
listbackup
```
- Step 3** Enter the following command:

```
restore backup_name
```

where *backup\_name* is the name of the backup you want to restore.

To restore without overwriting the WLSE flash memory, use the following command:

```
restore -n backup_name
```

The flash memory contains the WLSE's network settings (WLSE hostname, IP address, domain name, name servers, NTP server, and firewall settings) and users' CLI privileges.

---

For information about restoring from one WLSE to another, see:

- [Installing a Replacement WLSE, page 17-8](#)

- [Copying Configuration Data to another WLSE via CLI, page 17-9](#)

## Installing a Replacement WLSE

This section describes tasks you should perform when installing a replacement WLSE (replacing an existing WLSE with a new one). If you are simply using a backup from one WLSE to restore data on another WLSE, see [Copying Configuration Data to another WLSE via CLI, page 17-9](#).

## Removing the Old WLSE



### Note

Your login determines whether you can use these commands.

### Procedure

Before removing the old WLSE:

- 
- Step 1** Record the WLSE's configuration (the information that you entered when you initially set up the WLSE). Use the following command to display the configuration:
- ```
show config
```
- Step 2** Back up the data from the old WLSE. See [Backing Up and Restoring via CLI, page 17-5](#) for details.
- Step 3** Enter the following command:
- ```
shutdown
```
- Step 4** Power down and remove the old system.
- 

## Installing the Replacement WLSE



### Note

Your login determines whether you can use this command.

### Procedure

To install the replacement WLSE:

- 
- Step 1** Install and power on the new WLSE, using the instructions in the *Installation and Configuration Guide*.
- Step 2** For the [WLSE 1130 series](#):
- If you are using the same basic network information (for example, IP address and hostname) that you used on the old WLSE:
    - Run the setup program.
    - Enter the following command to restore all the configuration data from the old system, including the basic network information:

```
restore backup_name
```

- If you are *not* using the same basic configuration (for example, IP address and hostname) that you used on the old WLSE:
  - Run the setup program.
  - Enter the following command to restore all the configuration data from the old system except the basic network information:

```
restore -n backup_name
```

**Step 3** For the WLSE 1030 Express:

- a. Configure the new WLSE, using the instructions in the *Installation and Configuration Guide*.
- b. If you are using the same basic network information (for example, IP address and hostname), enter the following command to restore all the configuration data from the old system:

```
restore backup_name
```

- c. If you are *not* using the same basic network configuration, enter the following command to restore all configuration data except the basic network information:

```
restore -n backup_name
```

## Copying Configuration Data to another WLSE via CLI

You can back up data from one WLSE and copy it to another by using the backup and restore features. If you are replacing one WLSE with another, see [Installing a Replacement WLSE, page 17-8](#).



### Note

Your login determines whether you can use this command.

### Procedure

To restore a backup from one WLSE to another:

- Step 1** Back up the data on the original WLSE. For more information, see [Backing Up and Restoring via CLI, page 17-5](#).
- Step 2** If you installed a new WLSE and have not yet configured it, perform the initial setup. For information on initial setup, see the relevant *Installation and Configuration Guide* for your WLSE hardware on Cisco.com at [http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_installation_guides_list.html).
- Step 3** Restore the configuration data from your backup by entering the following command. Use the backup image name as the argument.

```
restore -n backup_name
```

**Note**

Be sure to use the **-n** option. Otherwise, the network information in flash memory will be overwritten and you will have to erase the WLSE's configuration and run the setup program to reenter the network information.

## Upgrading WLSE Software via CLI

For information about installing software updates on the WLSE by using the CLI, see the the following documents:

- *Upgrading CiscoWorks Wireless LAN Solution Engine Software, 2.13* on Cisco.com at [http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_installation_guides_list.html)
- The Readme.txt files on Cisco.com at <http://www.cisco.com/kobayashi/sw-center/cw2000/crypto/wlan-sol-eng/>

## Rebooting the WLSE via CLI

**Caution**

All processes running on the system stop and restart when you run the **reload** command. The WLSE will not respond while it is reloading.

Rebooting the system restarts its management services, even if the services were stopped prior to the reboot.

**Note**

Your login determines whether you can use this command.

To restart the WLSE, enter the following command:

```
reload
```

Result: You are prompted to verify the reload. Enter **yes** to confirm or **no** to cancel the reload.

## Shutting Down and Powering Off the WLSE

**Caution**

If you power off the WLSE improperly, you might disable the system.

**Note**

Your login determines whether you can use this command.

To shut down the WLSE:

**Step 1**

Enter the following command:

**shutdown**

**Step 2** Power off the WLSE.

---

## Setting WLSE System Date and Time via CLI

The WLSE uses Universal Coordinated Time (UTC) for the system time and date. The WLSE uses UTC to display the time and date when you are connected via Telnet/SSH or the console and when you are viewing log files. The WLSE uses the client's local time to display the time and date when connected via the Web interface.

You can set and maintain the system date and time by:

- [Setting the System Clock Using NTP via CLI, page 17-11](#) (the recommended method).
- [Setting the System Clock Manually via CLI, page 17-12](#).



### Note

You can also set the current time by using the Web interface. For information, see [Setting Time, Time Servers, Name Servers, and Web Session Timeout, page 16-43](#).

---

To display the system time, use the **show clock** command. For more information on this command, see [clock set, page A-12](#).

## Setting the System Clock Using NTP via CLI

NTP is the recommended method for configuring time and date on the system. If your network uses NTP to set the date and time on devices, you can specify the NTP servers on the WLSE. If NTP is not enabled, you can set the system clock to UTC manually as described in [Setting the System Clock Manually via CLI, page 17-12](#).



### Note

Your login determines whether you can use this command.

---

To specify NTP servers, enter the following command:

```
ntp server ip-address
```

where *ip-address* is the IP address of an NTP server.

To remove NTP servers and disable NTP, enter the following command for each NTP server that you specified:

```
no ntp server ip_address
```



### Caution

If you do not set the system clock manually after disabling NTP, the system clock might become inaccurate.

---

## Setting the System Clock Manually via CLI

If your network does not use NTP to set the system time on devices and the time is not set correctly, set the date and time manually.

**Note**

Your login determines whether you can use this command.

To set the date and time manually:

**Step 1** Stop services:

```
services stop
```

**Step 2** Enter the following command:

```
clock set hh:mm:ss month day year
```

where:

- *hh:mm:ss* is the current time (for example, 13:32:00).
- *month* is the current month (for example, December).
- *day* is the day of the month (for example, 31).
- *year* is the current year (for example, 2003).

**Step 3** Restart services:

```
services start
```

For more information about the **clock set** command, see [clock set](#), page A-12.

## Configuring Ethernet Interfaces

This section contains the following topics:

- [WLSE 1130 Series Interfaces](#), page 17-13
- [WLSE 1030 Interface](#), page 17-13
- [Configuring Protocols on Ethernet Interfaces](#), page 17-13
- [Configuring Interface Parameters](#), page 17-14
- [Changing the WLSE's IP Address](#), page 17-14
- [Using Both Interfaces on the WLSE 1130 Series](#), page 17-14

## WLSE 1130 Series Interfaces

The [WLSE 1130 series](#) have two 10/100/1000 Mbps Ethernet interfaces. The Ethernet 0 interface is configured during initial setup of the WLSE, and all protocols are enabled on the Ethernet 0 interface.

For the WLSE 1130 platform, the Ethernet interface labeled “A” on the back panel corresponds to Ethernet 0 in software (such as CLI commands). The Ethernet interface labeled “B” corresponds to Ethernet 1 in software.

For the WLSE 1130-19, the interfaces are labeled 0 and 1.

## WLSE 1030 Interface

The WLSE 1030 (WLSE Express) has one 10/100/1000 Mbps Ethernet connector. The Ethernet interface is configured by default to use DHCP to retrieve network parameters for configuring the WLSE.

## Configuring Protocols on Ethernet Interfaces

All protocols are enabled by default on the Ethernet 0 interface. On the Ethernet 1 interface of dual-interface WLSEs, all protocols except for CDP are enabled.

Any Ethernet interface can be individually configured to allow or prevent connections via the following protocols:

- Cisco Discovery Protocol (CDP)
- Hypertext transfer protocol (HTTP)
- Hypertext transfer protocol secure (HTTPS)
- Internet Control Message Protocol (ICMP)
- Secure shell (SSH) 1 and 2
- Simple network management protocol (SNMP)
- Telnet



### Note

---

Your login determines whether you can use this command.

---

To allow CDP on an interface, enter the following command:

```
cdp run port
```

where *port* is the Ethernet interface, for example, eth0.

To disable CDP, enter the following command:

```
no cdp run port
```

For more information on this command, see [cdp](#), page A-10.

To allow or prevent any of the other protocols on an interface, use the **firewall** command. For information on this command, see [firewall](#), page A-19.

## Configuring Interface Parameters

To enable or disable Ethernet interfaces and set parameters on the interfaces, use the following commands.

```
interface eth[ernet][0-5] [up | down]

interface eth[ernet][0-5] dhcp

interface eth[ernet][0-5] ipaddress netmask [default-gateway address]
[up | down] [auto | speed [10|100|1000] duplex [half | full]
mtu [46-1500]
```

For more details on these commands, see [interface, page A-25](#).



### Note

Your login determines whether you can use this command.

## Changing the WLSE's IP Address

If you use the **interface** command to change the IP address, append **up** to the command line if the interface is down. Append **down** if the interface is up when you change the IP address:

```
interface eth0 209.165.201.8 255.255.255.224 default-gateway 209.165.201.1 up
```

## Using Both Interfaces on the WLSE 1130 Series



### Note

Your login determines whether you can use the commands described in this section.

The Ethernet 0 interface is configured by the setup program when you initially install and set up the WLSE. The Ethernet 1 interface is not automatically configured, but you can configure it manually by using the **interface** and **cdp run** commands.

You can connect each interface to a different network and use both interfaces to manage devices, or use one interface to manage devices and use the other interface to communicate with a network management system.

The **interface** command creates a routing table entry that directs traffic to the correct interface. For example, when you configure Ethernet 1 with the gateway address 192.168.1.0 and the IP address 192.168.1.1, the **interface** command also creates an entry in the routing table that directs all 192.168.1.0 subnet traffic to Ethernet 1. Subsequently, if you use the **route** command to add new routes, packets for the second interface will still be properly routed.

If you are using both interfaces to manage devices, you must configure the second interface as follows:

- Make sure CDP is enabled on the Ethernet 1 interface—See [Configuring Protocols on Ethernet Interfaces, page 17-13](#).
- Configure Ethernet 1 interface parameters—See [Configuring Interface Parameters, page 17-14](#).



### Note

If you have configured both the Ethernet 0 and Ethernet 1 interfaces with IP addresses and you are using an AAA server in the network, you must configure both IP addresses as clients on the AAA server.



## Configuring the Mail Route via CLI

To ensure that email arrives at its proper destination, you can specify an SMTP server. This affects email notifications about firmware and configuration jobs, emailing reports, and emailing fault notifications.

**Note**

Your login determines whether you can use this command.

To specify a mail server, enter the following command:

```
mailroute server
```

where *server* is the IP address or hostname of your email server.

## Administering Management Services via CLI

The WLSE allows you to stop and start all management services at once. All commands that affect management services affect all of them, and the logs that collect services information collect information about all of them.

You can stop and restart the management services if the system is not responding correctly. This should cause the services to reset and function properly again. Management services are restarted automatically when you reboot the WLSE.

**Note**

Your login determines whether you can use this command.

To stop management services, enter the following command:

```
services stop
```

To start management services, enter the following command:

```
services start
```

To view management services status, enter the following command:

```
services status
```

## Viewing System Information via CLI

To view system information, you can use the CLI commands listed in [Table 17-1 on page 17-15](#).

**Table 17-1**      *Commands for Viewing System Information*

| Command                       | Information Displayed                                   |
|-------------------------------|---------------------------------------------------------|
| <a href="#">apptyp</a>        | Type of hardware platform—WLSE 1130 series or WLSE 1030 |
| <a href="#">dumptcp</a>       | Displays the content of TCP/IP packets                  |
| <a href="#">ps</a>            | Linux processes running on the WLSE                     |
| <a href="#">show auth-cli</a> | Type of authentication used for secure CLI access       |

**Table 17-1** *Commands for Viewing System Information (continued)*

| Command                  | Information Displayed                                                                             |
|--------------------------|---------------------------------------------------------------------------------------------------|
| <b>show auth-http</b>    | Type of authentication used for secure HTTP access                                                |
| <b>show backupconfig</b> | Current backup and restore location and username                                                  |
| <b>show backuplog</b>    | Contents of backup log                                                                            |
| <b>show bootlog</b>      | Messages from the last system boot                                                                |
| <b>show cdp neighbor</b> | The WLSE's nearest neighbor on the network                                                        |
| <b>show cdp run</b>      | CDP configuration of the WLSE                                                                     |
| <b>show clock</b>        | System data and time (UTC)                                                                        |
| <b>show config</b>       | System information and network configuration                                                      |
| <b>show daemonslog</b>   | Daemons log                                                                                       |
| <b>show dmgtldlog</b>    | Daemon manager log                                                                                |
| <b>show domain-name</b>  | WLSE's domain name                                                                                |
| <b>show hosts</b>        | Information about the hosts file                                                                  |
| <b>show http-server</b>  | Access control settings for HTTP and HTTPS                                                        |
| <b>show import hosts</b> | Imported hosts file                                                                               |
| <b>show install</b>      | Installation log files or names and descriptions of software updates and images in the repository |
| <b>show interfaces</b>   | Network interface information                                                                     |
| <b>show ipchains</b>     | IP chains for Ethernet interface                                                                  |
| <b>show maillog</b>      | Email log                                                                                         |
| <b>show mailroute</b>    | Current mailroute                                                                                 |
| <b>show proc[ess]</b>    | Statistics for active processes                                                                   |
| <b>show redundancy</b>   | Redundancy status and settings of redundancy parameters                                           |
| <b>show repository</b>   | Status or access log of repository                                                                |
| <b>show route</b>        | Routes that are currently configured                                                              |
| <b>show securitylog</b>  | Security log                                                                                      |
| <b>show snmp-server</b>  | WLSE's SNMP configuration                                                                         |
| <b>show ssh-server</b>   | SSH access control information                                                                    |
| <b>show ssh-version</b>  | Type of SSH enabled on the WLSE                                                                   |
| <b>show syslog</b>       | Syslog                                                                                            |
| <b>show tech</b>         | Information necessary for Cisco TAC to assist you                                                 |
| <b>show telnetenable</b> | Telnet status                                                                                     |
| <b>show time</b>         | Time zone and NTP server                                                                          |
| <b>show tomcatlog</b>    | Tomcat log                                                                                        |
| <b>show version</b>      | Currently installed software and hardware information                                             |
| <b>show webaccesslog</b> | Web access log                                                                                    |

**Table 17-1** *Commands for Viewing System Information (continued)*

| Command                              | Information Displayed |
|--------------------------------------|-----------------------|
| <a href="#">show weberrorlog</a>     | Web error log         |
| <a href="#">show websslaccesslog</a> | Web SSL log           |

## Managing Disk Space

To view disk use, use the **df** command; for example:

```
df
Filesystem Size Used Avail Use% Mounted on
/dev/hda12 298M 78M 220M 26% /
/dev/hda1 53M 5.1M 45M 10% /boot
/dev/hda7 2.7G 338M 2.2G 13% /extra
/dev/hda11 596M 33M 564M 6% /home
/dev/hda6 2.8G 269M 2.5G 10% /opt
none 1.5G 0 1.4G 0% /dev/shm
/dev/hda5 1.9G 33M 1.8G 2% /tftpboot
/dev/hda9 596M 33M 563M 6% /tmp
/dev/hda10 571M 254M 288M 47% /usr
/dev/hda13 27G 1.8G 25G 7% /var
```

To remove old system log files from the /var partition, use the **clearvar** command.



### Caution

This command stops services before purging old log files. Upon completion, system services restart.

#### **clearvar**

```
Warning: This command will restart all services.
Continue? (Y/N):y
Daemon Management stopping. This may take a few minutes.
INFO: All processes are terminated.
INFO: All processes are terminated.
```

#### Database Connection Information

```
Database server = DB2/LINUX 7.2.9
SQL authorization ID = CASUSER
Local database alias = WLSEDB
```

```
DB20000I The PRUNE command completed successfully.
DB20000I The SQL command completed successfully.
```

## Recovery Management

Use the following procedures to recover from problems:

- [Erasing System Configuration and Resetting to Factory Defaults](#), page 17-18
- [Using the Maintenance Image](#), page 17-18.
- [Using the Recovery CD](#), page 17-19.
- [Using the Rescue Image](#), page 17-21

- [Recovering from the Loss of All Administrator Passwords, page 17-21](#)

## Erasing System Configuration and Resetting to Factory Defaults

**Note**

Your login determines whether you can use these commands.

**Note**

The following commands stop and restart system services.

To reset the WLSE to factory defaults, but leave the database and logs in place, enter the following command:

```
erase config
```

To purge the database, enter the following command:

```
reinitdb
```

## Using the Maintenance Image

The WLSE's maintenance image consists of an operating system image and default system configuration stored in flash memory. You can use the maintenance image to recover from serious problems.

The following commands are available while the WLSE is running the maintenance image:

- **reload**
- **erase config**
- **fsck**—This command is available only in the maintenance and rescue images.

While the maintenance image is running, you can do the following tasks, which you cannot do when the system is booted normally from the disk:

- Recover from loss of all administrative passwords. See [Recovering from the Loss of All Administrator Passwords, page 17-21](#).
- Perform disk filesystem integrity checks or recover from filesystem corruption. See [fsck, page A-73](#).

## Booting from the Maintenance Image

As a security measure, you can boot from the maintenance image only while connected to the system console.

- 
- Step 1** Connect a console to the WLSE, using the procedure in [Using a Console with the WLSE, page 17-2](#).
- Step 2** Log in as **admin**.
- For the [WLSE 1130 series](#), use the serial port on the back panel.
  - For the WLSE 1030 (WLSE express), use the console/serial port on the back panel.
- Step 3** Reboot the system by doing one of the following:
- Enter the following command to reload the system if it is running:

```
reload
```

- Power on the system, if it is powered off.
- Power the system off and then back on if you have lost all passwords.

**Step 4** When the `GRUB boot :` prompt appears, press the Tab key.

**Step 5** When the `boot :` prompt appears, enter:

```
CiscoBreR
```

**Step 6** After you complete all necessary tasks, reboot the system by entering the following command and allowing the system to boot from the disk (the default boot order)

```
reload
```

## Using the Recovery CD

With the Recovery CD included with your WLSE, you can:

- Reimage the WLSE—See [Reimaging the WLSE—Local Installation Method, page 17-19](#) or [Reimaging the WLSE—Remote Installation Method, page 17-20](#).
- Boot from the rescue image—See [Using the Rescue Image, page 17-21](#).



### Caution

Before using the Recovery CD, check the relevant Readme file on the CD for possible changes to procedures, for example, WLSE-2.13.ISO-Readme-v1.txt.



### Note

If you do not have a recovery CD, you can create one by downloading recovery disk files from Cisco.com and reassembling them. Before attempting to make a recovery CD, check the relevant Readme file, for example WLSE-2.13.ISO-Readme-v1.txt. The recovery CD files are located on Cisco.com at <http://www.cisco.com/cgi-bin/tablebuild.pl/wlan-sol-eng>.

## Reimaging the WLSE—Local Installation Method

Please review the following notes and cautions before using this method to reimage a WLSE:

- This procedure will destroy all data and install a new image. You will need to replace the data by restoring a backup. For information on backups, see [Backing Up the WLSE, page 17-6](#).
- Although every effort has been made to validate the accuracy of the software version on the Recovery CD, you must review the WLSE's software versions on <http://www.cisco.com> and download any necessary earlier software updates. See the Readme files included with the updates to perform the update procedure.
- Reimaging the WLSE by using the recovery CD and the local installation method does not erase the network information in flash memory. After installing the recovery CD, network details and the admin password do not get erased. If you need to erase this information, run the [erase config](#) command either before or after reimaging.

### Procedure

To reimage your WLSE, perform the following steps:

- 
- Step 1** Connect a console to the WLSE, using the procedure in [Using a Console with the WLSE, page 17-2](#).
- Step 2** Log in as the **admin** user, and enter the password created when the WLSE was configured.
- Step 3** Put the Recovery CD in the WLSE's CD drive.  
The CD drive is located on the front panel, under the bezel.
- Step 4** Enter the following command. The WLSE will reboot.  
`reload`
- Step 5** At the following prompt, enter **yes** to start the Recovery CD:  
Do you wish to continue (Yes/[No]/Rescue) **yes**

**Caution**

If you do not want to re-image the WLSE, enter **rescue**. For more information about the rescue image, see [Using the Rescue Image, page 17-21](#).

- 
- Step 6** When the WLSE ejects the Recovery CD, remove it.
- Step 7** At the following prompt, enter **yes**:  
Do you wish to reload and start the install?(yes/[no]) **yes**  
  
Result: The WLSE is re-imaged and reboots.
- Step 8** When the Recovery CD ejects from the CD drive, remove it.  
When the installation completes, the login prompt appears on the console.
- 

## Reimaging the WLSE—Remote Installation Method

**Note**

Although every effort has been made to validate the accuracy of the software version on the Recovery CD, you must review the WLSE's software versions on <http://www.cisco.com> and download any necessary software updates. See the Readme files included with the updates to perform the update procedure.

**Caution**

This procedure will destroy all data and install a new image. You will need to replace the data by restoring a backup. For information on backups, see [Backing Up the WLSE, page 17-6](#).

To reimage your WLSE, perform the following steps:

- 
- Step 1** Insert the Recovery CD into the CD drive of a system running Microsoft Windows 2000.
- Step 2** Double-click on the CD drive to display the contents of the Recovery CD.
- Step 3** Double-click on the autorun.bat file.  
A command prompt window appears and as well as a pop-up window displaying instructions for installing the Recovery CD.
- Step 4** Follow the installation instructions in the pop-up window.

**Note**

Make sure you keep both the command prompt window and pop-up window open until the installation finishes.

## Using the Rescue Image

The rescue image is similar to the maintenance image, but is accessible via the Recovery CD. The rescue image is mainly used to aid technical support when diagnosing issues. Use the rescue image if you cannot use the maintenance image, but need to. You can use the rescue image to boot the system to perform some system administration tasks and disaster recovery. For information about the uses of the maintenance image, see [Using the Maintenance Image, page 17-18](#).

You are limited to the following commands while the system is running the rescue image: **reload**, **erase config**, and **fsck**.

To boot from the rescue image, perform the following steps:

- Step 1** Connect a console, using the procedure in [Using a Console with the WLSE, page 17-2](#).
- Step 2** Log in as the **admin** user. The **admin** user's password was created when the WLSE was initially configured.
- Step 3** Put the Recovery CD in the WLSE's CD drive.  
The CD drive is located on the front panel, under the bezel.
- Step 4** Enter the following command. The WLSE will reboot.  
**reload**
- Step 5** At the following prompt, enter **rescue**.  
A prompt appears, and you can run the following CLI commands:

| Command             | Description                                                  |
|---------------------|--------------------------------------------------------------|
| <b>fsck</b>         | Check and repair the file system.                            |
| <b>reload</b>       | Reboot the WLSE.                                             |
| <b>erase config</b> | Erase the configuration in flash memory and reload the WLSE. |

For more information on these commands, see [Appendix A, "Command Line Interface \(CLI\) Commands."](#)

## Recovering from the Loss of All Administrator Passwords

If you cannot log on to the system and perform administrative tasks, perform the following procedure.

**Procedure**

- 
- Step 1** Connect a console, using the procedure in [Using a Console with the WLSE, page 17-2](#).
- Step 2** Power the system off, then power it back on. Boot messages appear, and then following prompt appears:

```

0: CiscoBre
1: CiscoBreR

```

- Step 3** Use the Up Arrow and Down Arrow keys to select **1** for CiscoBreR and press **Enter**. The following prompt appears:

```
bash-2.05a#
```

- Step 4** Enter the following command. This erases the WLSE's configuration, returns the WLSE to factory defaults, and reloads the WLSE.

```
bash-2.05a# erase config
```

- Step 5** After the WLSE starts up, a login prompt appears.

- For the [WLSE 1130 series](#), log in as setup, and use the setup program to configure the system. This allows you to add a password for the admin user.

For more information about the setup program, see the relevant *Installation and Configuration Guide for the Wireless LAN Solution Engine* on Cisco.com at

[http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_installation_guides_list.html).

---





## Using the Internal AAA Server (WLSE Express Only)

---

WLSE 2.13 includes an integrated authentication and authorization server that provides LEAP, Cisco-PEAP, MS-PEAP, EAP-FAST, and EAP-TLS authentication for access points.

The internal AAA server is available on the Wireless LAN Solution Engine Express (WLSE 1030) only.

The AAA server Web interface is accessible by selecting **Admin > AAA Administration**.

This chapter provides overview information and procedures for using the internal AAA server:

- [About the AAA Server, page 18-1](#)
- [Configuring the AAA Server—Overview, page 18-6](#)
- [Using AAA Server Screens, page 18-7](#)
- [Using AAA Server Log Files, page 18-28](#)
- [Monitoring the AAA Server, page 18-28](#)
- [Using AAA Server CLI Commands, page 18-30](#)
- [RADIUS Attributes for the AAA Server, page 18-46](#)

### About the AAA Server

The AAA server is a RADIUS (Remote Authentication Dial-In User Service) server that allows multiple devices to use a common authentication and authorization database.

The server receives requests from users attempting to access clients and authenticates and/or authorizes users.

This section includes the following descriptions of AAA server features:

- [Basic Authentication and Authorization, page 18-2](#)
- [RADIUS Attributes of the AAA Server, page 18-2](#)
- [Supported Services, page 18-3](#)
- [Methods of Storing User Information, page 18-3](#)
- [Extensible Authentication Services, page 18-4](#)
- [Methods of Configuring the AAA Server, page 18-4](#)
- [Backup/Restore and Software Upgrades, page 18-5](#)

- [Ports Used by the AAA Server, page 18-5](#)
- [Fault Monitoring and Trend Reports, page 18-5](#)
- [Certificates and RSA Keys, page 18-5](#)

## Basic Authentication and Authorization

The WLSE AAA server allows you to better manage access to your network, as it allows you to store all security information in centralized databases instead of distributing the information around the network.

The AAA server is based on a client/server model. The client passes information to the AAA server and acts on the response from the server. The server receives user access requests, authenticating the user and returning any available configuration information for the client to pass on to the user.

The AAA server handles the following tasks:

- Authentication—determines the identity of users and whether they may be allowed to access the network.
- Authorization—determines the level of network services available to authenticated users after they are connected.
- Session and resource management—tracks user sessions and allocates dynamic resources

The protocol is a simple packet exchange in which the client sends a request packet to the AAA server with a name and password. The AAA server looks up the name and password to verify that it is correct and returns an accept packet. The AAA server can also reject the request packet. To ensure network security, the client and server use a shared secret, which is known to both. Also, user passwords are encrypted between the client and the server.

Three participants (user, client, and AAA server) are involved in this interaction as follows:

1. The user contacts the client and supplies a name and password.
2. The client begins the session:
  - a. The client receives the name and password.
  - b. The client formats this information into an access-request packet.
  - c. The client forwards this packet to the AAA server.
3. The AAA server determines which client sent the request and parses the request. The server chooses a service to authenticate and/or authorize the user.
4. The AAA server's authentication service verifies that the name and password are in the database.
5. The AAA server's authorization service creates the response packet with the appropriate attribute's for the user's session.
6. The AAA server formats the response and sends the response to the client.
7. The client receives the response and communicates with the user.

## RADIUS Attributes of the AAA Server

The AAA server comes with the standard RADIUS attributes (as defined by RFC 2865). For more information about AAA server attributes, see [RADIUS Attributes for the AAA Server, page 18-46](#).

## Supported Services

The AAA server supports the following services:

- Windows active directory—see [Domain Authentication, page 18-3](#)
- Lightweight Directory Access Protocol (LDAP)—see [Lightweight Directory Access Protocol \(LDAP\), page 18-3](#)
- Extensible authentication services (EAP)—see [Extensible Authentication Services, page 18-4](#)

## Methods of Storing User Information

When configuring an authentication service, you need to specify the user service; that is, where the user profile information is stored. This information can be stored locally on the AAA server or on an LDAP server. When the AAA server receives a request, it directs the request to the specified service. Then the service looks up the user and authenticates or authorizes the user.

As an alternative to LDAP or the local service, you can use the Domain Authentication method and store user information in Windows Active Directory.

This section briefly describes these services:

- [Local User Database, page 18-3](#)
- [Lightweight Directory Access Protocol \(LDAP\), page 18-3](#)
- [Domain Authentication, page 18-3](#)

### Local User Database

When using this service, you must enter each user and password on the AAA server. You can assign RADIUS attributes to each user. With the local service, you can have the AAA server perform authentication and/or authorization using a specific user list. For more information, see [Managing AAA Users, page 18-24](#).

### Lightweight Directory Access Protocol (LDAP)

LDAP servers store directory information about users in order to authenticate them.

You can designate both a central LDAP server and local LDAP servers. The local LDAP server is primary, and the centralized server is secondary.

For more information about LDAP, see [Managing the LDAP Central Server, page 18-11](#) and [Managing the LDAP Local Server, page 18-12](#).

### Domain Authentication

The AAA server can authenticate against the user database in Windows Active Directory on a Windows domain controller (WDC). Using this service requires that you download and configure a remote agent from Cisco.com and install the remote agent on the domain controller system.

To use domain authentication, you must install a remote agent on the WDC. You can download the remote agent from Cisco.com.

For information on downloading the remote agent and using domain authentication, see [Configuring Windows Domain Authentication, page 18-15](#).

## Extensible Authentication Services

You can configure and use more than one of the following authentication services at the same time. If more than one service is configured, the WLSE negotiates which one to use.

The AAA server supports Extensible Authentication Protocol (EAP) to provide a common protocol for differing authentication mechanisms. EAP enables the dynamic selection of the authentication mechanism at authentication time based on information transmitted in the Access-Request. The AAA server supports the following EAP authentication methods.

The supported EAP methods are described in [Table 18-1 on page 18-4](#). You enable each EAP method by configuring it, using the WLSE UI or WLSE CLI commands.

**Table 18-1 Supported EAP Methods**

| EAP Method | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LEAP       | LEAP (Lightweight Extensible Authentication Protocol) is a Cisco-proprietary protocol that was defined and implemented for Cisco's Aironet product family.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| PEAP       | <p>Protected EAP (PEAP) is an authentication method that was designed to mitigate several weaknesses of EAP. PEAP leverages TLS to achieve certificate-based authentication of the server (and optionally the client) and creation of a secure session that can then be used to authenticate the client. The AAA server supports the following versions of PEAP:</p> <ul style="list-style-type: none"> <li>• Cisco-PEAP (PEAP Version 1)</li> <li>• MS-PEAP (Microsoft PEAP, PEAP Version 0)</li> </ul> <p>PEAP can be used for authentication between wireless clients, such as inventory devices, and access points (either WDS access points or <a href="#">infrastructure access points</a>).</p> |
| EAP-FAST   | <p>EAP-FAST is a two-phase authentication protocol:</p> <ul style="list-style-type: none"> <li>• Phase 0, provisioning. Provision client with a credential called PAC (Protected Access Credential).</li> <li>• Phase 1, authentication. Use the PAC to establish a tunnel with the server and authenticate the username and password.</li> </ul> <p>The PAC is a security credential that is used to establish a shared secret between clients and the server. For EAP-FAST on the WLSE's AAA server, the PAC is created automatically.</p>                                                                                                                                                           |
| EAP-TLS    | EAP Transport Level Security (EAP-TLS) is an authentication method that was designed to mitigate several weaknesses of EAP. EAP-TLS leverages TLS, described in RFC 2246, to achieve certificate-based authentication of the server and (optionally) the client. EAP-TLS provides many of the same benefits as PEAP but differs from it in the lack of support for legacy authentication methods.                                                                                                                                                                                                                                                                                                      |

## Methods of Configuring the AAA Server

For this release, the AAA server is pre-configured with appropriate parameters, so initial configuration is minimal. A WLSE user with system administration privileges can configure the AAA server. The configuration methods for the AAA server are WLSE CLI commands and the WLSE web interface. For information on the AAA Web interface, see [Using AAA Server Screens, page 18-7](#).

Most of the functions of the AAA server's Web interface can be performed by using command-line interface (CLI) commands. Additional functions that are not in the Web interface are provided through CLI commands: generating certificates, configuring logging method, reinitializing the database, and starting or stopping daemons. For details on CLI commands, see [Using AAA Server CLI Commands, page 18-30](#).

## Backup/Restore and Software Upgrades

Backup and restore of the AAA server database is handled by the normal WLSE backup and restore functions—See [Backing Up and Restoring Data, page 16-20](#). Upgrade of the AAA server is performed during a normal WLSE software upgrade—See [Managing WLSE System Software, page 16-7](#).

## Ports Used by the AAA Server

The AAA server requires sole use of the following ports on the WLSE:

- UDP ports 1812 and 1813—for RADIUS
- TCP ports 2785 and 2786—for internal process communication

## Fault Monitoring and Trend Reports

The RADIUS, LEAP, and Cisco-PEAP protocols are monitored by the WLSE's fault mechanism. MS-PEAP and EAP-FAST are not monitored.

After configuring the AAA server and setting up AAA server monitoring, you can view faults, configure fault monitoring, and run reports for the authentication protocol that you select. A given WLSE can only monitor one protocol per AAA server. For information on configuring the WLSE to monitor the AAA server, see [Monitoring the AAA Server, page 18-28](#).

### Related Topics

- [Using AAA Server Screens, page 18-7](#)
- [Configuring the AAA Server—Overview, page 18-6](#)
- [Fault Monitoring, page 3-1](#)
- [Using Reports, page 10-1](#)

## Certificates and RSA Keys

A self-signed certificate is automatically generated by the WLSE during initial startup and is placed in a location where it can be used by the AAA server. A self-signed certificate is required; the AAA server will not operate without a self-signed certificate.

If you need to obtain a more secure certificate from a certificate authority, obtain an RSA key, or regenerate the self-signed certificate in order to make changes in it, you will need to enter the pathnames of the certificates and the key in the relevant AAA server screens.

When you request a certificate from the certificate authority you receive an RSA key and two certificates: your certificate for your site and a certificate that certifies the issuing authority.

The self-signed certificate is not as secure as a certificate issued by a certificate authority, but may be adequate if your network is not accessible from the outside. Also, you may wish to generate your own self-signed certificate that contains the name of your organization and other identifying information.



**Note**

For detailed information about how to generate certificates to be used with the WLSE, and how to configure AAA certificates to be used on the WLSE, see the *WLSE AAA Server Certificate Configuration Guide* on Cisco.com.

# Configuring the AAA Server—Overview

This section contains the following topics:

- [Naming Guidelines, page 18-6](#)
- [Configuration Methods, page 18-6](#)
- [Configuration Tasks, page 18-6](#)
- [Reconfiguration Tasks, page 18-7](#)

## Naming Guidelines

For AAA server usernames, group names, and client names, you can use up to 255 characters and any character except for the forward slash (/).

## Configuration Methods

You can configure the AAA server by using the screens in the Web interface ([Using AAA Server Screens, page 18-7](#)) or the CLI commands ([Using AAA Server CLI Commands, page 18-30](#)).

## Configuration Tasks

To configure the AAA server, perform the tasks in [Table 18-2 on page 18-6](#).

**Table 18-2**      **Tasks for Configuring the AAA Server**

| Task Description                                                                                  | Reference                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure the authentication services you are going to use.                                       | <a href="#">Configuring LEAP Settings, page 18-18</a><br><a href="#">Configuring Cisco-PEAP Settings, page 18-18</a><br><a href="#">Configuring MS-PEAP Settings, page 18-19</a><br><a href="#">Configuring EAP-TLS Settings, page 18-21</a><br><a href="#">Configuring EAP-FAST Settings, page 18-21</a> |
| If you are using the local user database, add users.                                              | <a href="#">Managing AAA Users, page 18-24</a>                                                                                                                                                                                                                                                            |
| If you are using LDAP as the user database, configure LDAP parameters on the WLSE. <sup>1 2</sup> | <a href="#">Managing the LDAP Central Server, page 18-11</a><br><a href="#">Managing the LDAP Local Server, page 18-12</a>                                                                                                                                                                                |

**Table 18-2**      *Tasks for Configuring the AAA Server (continued)*

| Task Description                                                                                                                                 | Reference                                                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| If you are using domain authentication (Windows Active Directory) for the user database, configure domain authentication parameters on the WLSE. | <a href="#">Configuring Windows Domain Authentication, page 18-15</a> |
| If you are using domain authentication groups, you can create local groups and map them to groups on the WDC.                                    | <a href="#">Managing Groups, page 18-26</a>                           |
| Add clients. <sup>3</sup>                                                                                                                        | <a href="#">Managing AAA Clients, page 18-23</a>                      |
| (Optional) Configure the WLSE to monitor the internal AAA server.                                                                                | <a href="#">Monitoring the AAA Server, page 18-28</a>                 |
| (Optional) Configure logging (syslog or local)                                                                                                   | <a href="#">aaa-server logging, page 18-40</a>                        |

1. You can use LDAP or domain authentication for one service and use the local database for another.
2. If you are using LDAP, you need to add a WLSE user on the LDAP server.
3. The WLSE appliance must be added as a client of the AAA server.

## Reconfiguration Tasks

If you change any of the information listed in [Table 18-3 on page 18-7](#) after initial configuration, you will need to make corresponding changes on the WLSE.

**Table 18-3**      *Reconfiguring the AAA Server*

| Change                                  | Reference                                                                                                                  |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| LDAP server characteristics             | <a href="#">Managing the LDAP Central Server, page 18-11</a><br><a href="#">Managing the LDAP Local Server, page 18-12</a> |
| IP address of a client device           | <a href="#">Managing AAA Clients, page 18-23</a>                                                                           |
| RADIUS shared secret of a client device | <a href="#">Managing AAA Clients, page 18-23</a>                                                                           |
| Addition of devices or users            | <a href="#">Managing AAA Clients, page 18-23</a><br><a href="#">Managing AAA Users, page 18-24</a>                         |

## Using AAA Server Screens



### Note

If you are using the WLSE redundancy feature, AAA screens are not displayed on the standby WLSE.

This section contains procedures for configuring the AAA server and includes the following topics:

- [AAA Server Administration Subtab Functions, page 18-8](#)
- [Displaying AAA Server Status, page 18-9](#)
- [Setting AAA Server Trace Level and Viewing Trace Logs, page 18-10](#)
- [Managing the LDAP Central Server, page 18-11](#)
- [Managing the LDAP Local Server, page 18-12](#)

- [Configuring Windows Domain Authentication, page 18-15](#)
- [Configuring LEAP Settings, page 18-18](#)
- [Configuring Cisco-PEAP Settings, page 18-18](#)
- [Configuring MS-PEAP Settings, page 18-19](#)
- [Configuring EAP-TLS Settings, page 18-21](#)
- [Configuring EAP-FAST Settings, page 18-21](#)
- [Managing AAA Clients, page 18-23](#)
- [Managing AAA Users, page 18-24](#)
- [Managing Groups, page 18-26](#)
- [Viewing and Releasing Sessions, page 18-27](#)

## AAA Server Administration Subtab Functions



### Note

The AAA Administration subtab may not be visible to some users; whether you see the Admin tab or its subtabs depends on the user roles assigned to your login.

The options under the AAA Administration subtab are:

**Table 18-4**      **AAA Server Subtab Functions**

| Option                     | Function                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AAA Server Status          | Display status of server processes— <a href="#">Displaying AAA Server Status, page 18-9</a>                                                                                                                                                                                                                                                             |
| AAA Server Trace Level     | Set level of trace logging— <a href="#">Setting AAA Server Trace Level and Viewing Trace Logs, page 18-10</a>                                                                                                                                                                                                                                           |
| LDAP Central Server        | Configure LDAP if using LDAP for user database:<br><a href="#">Managing the LDAP Central Server, page 18-11</a><br><a href="#">Managing the LDAP Local Server, page 18-12</a>                                                                                                                                                                           |
| LDAP Local Server          |                                                                                                                                                                                                                                                                                                                                                         |
| Windows Domain Auth Server | Configure domain authentication— <a href="#">Configuring Windows Domain Authentication, page 18-15</a>                                                                                                                                                                                                                                                  |
| LEAP Settings              | Configure the AAA protocols you are using:<br><a href="#">Configuring LEAP Settings, page 18-18</a><br><a href="#">Configuring Cisco-PEAP Settings, page 18-18</a><br><a href="#">Configuring MS-PEAP Settings, page 18-19</a><br><a href="#">Configuring EAP-TLS Settings, page 18-21</a><br><a href="#">Configuring EAP-FAST Settings, page 18-21</a> |
| Cisco-PEAP Settings        |                                                                                                                                                                                                                                                                                                                                                         |
| MS-PEAP Settings           |                                                                                                                                                                                                                                                                                                                                                         |
| EAP-TLS Settings           |                                                                                                                                                                                                                                                                                                                                                         |
| EAP-FAST Settings          |                                                                                                                                                                                                                                                                                                                                                         |
| Clients                    | Add, modify, and delete clients— <a href="#">Managing AAA Clients, page 18-23</a>                                                                                                                                                                                                                                                                       |
| Users                      | Add modify and delete users if you are using the local user database— <a href="#">Managing AAA Users, page 18-24</a>                                                                                                                                                                                                                                    |



**Table 18-4 AAA Server Subtab Functions (continued)**

| Option   | Function                                                                                 |
|----------|------------------------------------------------------------------------------------------|
| Groups   | Manage groups for domain authentication— <a href="#">Managing Groups</a>                 |
| Sessions | Display and release sessions— <a href="#">Viewing and Releasing Sessions, page 18-27</a> |

## Displaying AAA Server Status

To display information on AAA server processes, select **Admin > AAA Admin > AAA Server Status**. The status of the following processes (running or not) and the PID of each process is displayed.

In addition, the health of the AAA server is displayed. The message *Server is Running, its health is 10 out of 10* means that the AAA server is running optimally. If this health indicator decreases, you should inspect the AAA server logs for any anomalous behavior. For example, if the percent of rejected requests grows significantly over time, the health indicator will decrease. For information on these logs, see [Using AAA Server Log Files, page 18-28](#).

For information on any outstanding AAA server faults, select **Faults > Display Faults**. Faults and reports on the AAA server are only displayed after the WLSE has been configured to monitor the AAA server. For more information, see [Monitoring the AAA Server, page 18-28](#).

**Table 18-5 AAA Server Processes**

| Process                   | Function                                                                                                                                                                   |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AAA server                | Processes AAA packets, listening for RADIUS requests, deciding what to do with them (may include making an <a href="#">LDAP</a> query), and then sending RADIUS responses. |
| AAA daemon manager        | Similar to the WLSE daemon manager. Restarts any of the other processes when necessary and coordinates orderly startup and shutdown of the other processes.                |
| AAA database lock manager | Controls access to the database process by multiple clients. In particular, the server, CLI, and Web interface all need to access the database and must be coordinated.    |
| AAA database              | Maintains AAA configuration data, including any internal users that have been defined.                                                                                     |

### Related Topics

- [About the AAA Server, page 18-1](#)
- [Displaying Fault Information, page 3-1](#)
- [Monitoring the AAA Server, page 18-28](#)

## Setting AAA Server Trace Level and Viewing Trace Logs

The AAA Server Trace Level page displays the current trace level for the AAA server. Trace information can be used for debugging or validating the behavior of the AAA server. The trace level governs how much information is logged about the contents of a packet. The higher the trace level, the more information is logged. Trace levels are inclusive, so if you set trace level to 3, you log all of the information for trace levels 1 and 2.

Tracing is meant to be temporary, and you should not leave tracing turned on for more than a brief period of time. If tracing is left on, it will quickly fill up available disk space. The rate of consumption of disk space depends on the trace level selected and the current traffic rate (that is, the number of access points authenticating per second).

For information on the trace levels and the information logged at each level, see [Trace Levels and Information Logged](#), page 18-10.

**Note**

If you have configured the WLSE to monitor the AAA server, you can display information on any outstanding AAA server faults in **Faults > Display Faults**.

The AAA-server-trace.log file contains the results of tracing; the file contains data only when tracing is turned on. To use this file, select **Admin > Appliance > Status > View Log File**.

**Procedure**

- Step 1** Select **Admin > AAA Administration > AAA Server Trace Level**.
- Step 2** Select the desired trace level, from 0 (no tracing) to 5 (most verbose).
- Step 3** Click **Submit**.

**Related Topics**

- [About the AAA Server](#), page 18-1
- [Displaying Fault Information](#), page 3-1
- [Monitoring the AAA Server](#), page 18-28

## Trace Levels and Information Logged

lists the trace levels and the information logged at each level. This information is logged in the AAA-server-trace.log, accessible by **Admin > AAA Administration > View Log File**. Trace levels are inclusive; for example, if trace level is set at 3, the information from trace levels 2 and 3 are also logged.

**Table 18-6** Trace Levels and Information Logged

| Trace Level | Information Returned                                                                             |
|-------------|--------------------------------------------------------------------------------------------------|
| 0           | No trace performed                                                                               |
| 1           | Reports when packet is sent or received or when there is a change in the remote server's status. |

**Table 18-6**      **Trace Levels and Information Logged (continued)**

| Trace Level | Information Returned                                                                                                                                                                                                                                                                                                                                                                  |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2           | Logs the following: <ul style="list-style-type: none"> <li>• Services and session managers used to process a packet</li> <li>• Client and vendor objects used to process a packet</li> <li>• Remote server details for LDAP and RADIUS, such as sending packets and timing out</li> <li>• Details about poorly formed packets</li> <li>• Details included in trace level 1</li> </ul> |
| 3           | Logs the following: <ul style="list-style-type: none"> <li>• Error traces in TCL scripts when referencing invalid RADIUS attributes</li> <li>• Scripts that were executed</li> <li>• Details about local UserList processing</li> <li>• Details included in trace levels 1 and 2</li> </ul>                                                                                           |
| 4           | Logs the following: <ul style="list-style-type: none"> <li>• Information about advanced duplication detection processing</li> <li>• Details about creating, updating, and deleting sessions</li> <li>• Trace details about scripting APIs called</li> <li>• Details included in trace levels 1, 2, and 3</li> </ul>                                                                   |
| 5           | Logs the following: <ul style="list-style-type: none"> <li>• Details about use of the policy engine: rules that were run, what the rules did, whether the rule passed or failed, which policies were called</li> <li>• Details included in trace levels 1, 2, 3, and 4</li> </ul>                                                                                                     |

## Managing the LDAP Central Server



### Note

If you are using the default method of having LEAP query the internal database, you do not need to configure LDAP servers. For PEAP, the default is to use LDAP.

The Lightweight Directory Access Protocol (LDAP) screens allow you to enter information about local and central LDAP servers. LDAP servers store directory information about users in order to authenticate them.

The WLSE must also be added to the LDAP server.

### Procedure

To modify the properties of the LDAP central server:

**Step 1**      Select **Admin > AAA Administration > LDAP Central Server**.

The Configure LDAP Central Server screen has two parts: the top part is for setting general parameters, and the bottom part is for creating LDAP-to-RADIUS attribute mappings.

- Step 2** Enter or modify the information in the screen. For details on the fields and how the parameters are used, see [About LDAP Parameters, page 18-13](#).
- Step 3** (Optional) LDAP-to-RADIUS attribute mapping. You can add or delete mappings as follows. For information on the RADIUS attributes that are native to the AAA server, see [RADIUS Attributes for the AAA Server, page 18-46](#).



**Note** Once entered, a mapping cannot be modified. To modify a mapping, you must first delete the mapping and then add it again.

#### To add a mapping:

- a. Select **Add**.  
Result: The LDAP Attribute and Maps to RADIUS Attribute text boxes appear, along with an **Apply** button.
- b. Enter the desired mapping.
- c. Click **Apply**.

#### To delete a mapping:

- a. Select the mapping from the **LDAP Attributes to RADIUS Attributes** list.
- b. Click **Delete**.

**Step 4** To save your changes, click **Submit**.

**Step 5** To cancel your changes, click **Cancel**.

#### Related Topics

- [About the AAA Server, page 18-1](#)
- [About LDAP Parameters, page 18-13](#)
- [Managing the LDAP Local Server, page 18-12](#)
- [Configuring the AAA Server—Overview, page 18-6](#)

## Managing the LDAP Local Server



**Note** If you are using the default method of having LEAP query the internal database, you do not need to configure LDAP servers. The default for PEAP is to use LDAP.

Use the Lightweight Directory Access Protocol (LDAP) screens to enter information about local and central LDAP servers. LDAP servers store authentication and authorization information.

The WLSE must also be added to the LDAP server.

#### Procedure

To modify the attributes of a LDAP local server:

**Step 1** Select **Admin > AAA Administration > LDAP Local Server**.

The Configure LDAP Local Server screen has two parts: the top part is for setting general parameters, and the bottom part is for creating LDAP-to-RADIUS attribute mappings.

- Step 2** Enter or modify the general information in the top part of the screen. For details on the fields and how the parameters are used, see [About LDAP Parameters, page 18-13](#).
- Step 3** (Optional) LDAP-to-RADIUS attribute mapping. You can add or delete mappings as follows. For information on the RADIUS attributes that are native to the AAA server, see [RADIUS Attributes for the AAA Server, page 18-46](#).



**Note** Once a mapping has been added, you cannot modify it. You must first delete the mapping and then add it again.

#### To add a mapping:

- a. Select **Add**.

Result: The LDAP Attribute and RADIUS Attribute text boxes appear, along with an **Apply** button.

- b. Enter the desired mapping.
- c. Click **Apply**.

#### To delete a mapping:

- a. Select the mapping from the **LDAP Attributes to RADIUS Attributes** list.
- b. Click **Delete**.

- Step 4** To save your changes, click **Submit**.

- Step 5** To cancel your changes, click **Cancel**.

#### Related Topics

- [About the AAA Server, page 18-1](#)
- [About LDAP Parameters, page 18-13](#)
- [Managing the LDAP Central Server, page 18-11](#)
- [Configuring the AAA Server—Overview, page 18-6](#)

## About LDAP Parameters

This section contains:

- Details on the LDAP parameters in the LDAP screens—See [LDAP Parameter Details, page 18-13](#).
- How the parameters are used—See [How LDAP Settings are Used, page 18-15](#).

#### LDAP Parameter Details

The LDAP parameters you can set in the AAA server LDAP server screens are described in [Table 18-7 on page 18-14](#). All parameters are required, except as indicated. The values you enter are used as described in [How LDAP Settings are Used, page 18-15](#).

**Table 18-7 LDAP Parameters**

| Field                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name                | Host name or IP address of the LDAP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Port                     | Port on the LDAP server for the bind (usually, port 389). The port number must be an integer between 1 and 65536.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Bind Name (optional)     | The distinguished name (DN) (administrator name) to use when establishing a connection between the LDAP and AAA servers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Bind Password (optional) | Password associated with the Bind Name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Search Path              | <p>Path that indicates where in the LDAP database to start the search for user information. The path is specified is a distinguished name (DN). LDAP references an LDAP object by its distinguished name.</p> <p>Specifying a DN (such as ou=Engineering, o=cisco.com) as the Search Path restricts user queries to objects that match those property values.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Search Filter            | Search filter used by the AAA server when querying the LDAP server for user information. Use the notation %s to indicate where the user ID should be inserted. For example, a typical value for this property is (uid=%s), which means that when querying for information about user joe, use the filter uid=joe. <i>uid</i> is the name of the LDAP property that contains the same values as the RADIUS User Name attributes that are being authenticated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| User Password            | LDAP property that contains the passwords to use for authentication. This property must be a property of all objects that match the Search Path.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Password Encryption      | <p>Select an encryption method for the user password:</p> <ul style="list-style-type: none"> <li>• None—no encryption (the default).</li> <li>• Dynamic—This setting instructs the AAA server to choose the encryption mechanism on a case-by-case basis after the server determines the presence of a known prefix, which the server prepends to the password attribute.</li> <li>• Crypt—AAA server encryption using the Unix crypt algorithm.</li> <li>• SHA-1 or SSHA-1— Secure Hash Algorithm; a hashing algorithm that produces a 160-bit digest based upon the input. The algorithm produces SHA passwords that are irreversible or prohibitively expensive to reverse. Enables the AAA server to authorize users whose passwords are stored in an LDAP server and hashed by using the SHA-1 encoding scheme. SSHA-1 is Netscape's (iPlanet) enhancement of the SHA-1 algorithm which includes salted password data.</li> </ul> |
| Timeout                  | Timeout for bind attempts. How long (in seconds) the AAA server will wait for a response from the LDAP server. The default is 15 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

**Table 18-7**      **LDAP Parameters (continued)**

| Field                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LDAP to RADIUS mappings (optional) | <p>List of name/value pairs. The name is an LDAP attribute to retrieve from the user record, and the value is the RADIUS attribute to set to the value of the LDAP attribute.</p> <p>An error message is displayed:</p> <ul style="list-style-type: none"> <li>• If you attempt to map the same attribute more than once, an error message will be displayed.</li> <li>• If you enter an incorrect RADIUS attribute.</li> </ul> <p>See the relevant vendor documentation for information about which attributes you may need to enter. The AAA server will operate properly with no authorization attributes; however, the client device may not provide the appropriate service because of the lack of certain authorization attributes. For a list of the RADIUS attributes native to the AAA server, see <a href="#">RADIUS Attributes for the AAA Server, page 18-46</a>.</p> |

**How LDAP Settings are Used**

The LDAP settings that you configure in the LDAP screens are used as follows.

The AAA server connects as an LDAPv3 client to the LDAP server on the named Port. The AAA server uses the Bind Name and Bind Password to connect. If the LDAP server does not respond within the number of seconds specified as the Timeout, the server times out. This connection is made once at startup and again if the connection is dropped.

Each time an Access-Request is received, the AAA server queries the subtree rooted at the Search Path, using the Search Filter (substituting the RADIUS User-Name for %s) to specify an object in the subtree. If such an object is found, the User Password Attribute and specified LDAP Attribute values are returned.

On the AAA server, the RADIUS User-Password attribute value is encrypted, using the Password Encryption technique, and is then compared to the returned User Password Attribute value (which must be encrypted using the same technique). If these values match, the other LDAP Attribute values that are returned are mapped as specified to RADIUS attributes. These composed attribute-value pairs are added to the Access-Accept packet.

**Related Topics**

- [Managing the LDAP Central Server, page 18-11](#)
- [Managing the LDAP Local Server, page 18-12](#)

## Configuring Windows Domain Authentication

Use this option to configure the AAA server to use Windows domain authentication service as the user database. This service uses a user database stored in Windows Active Directory on a Windows Domain Controller. Use of this service requires that you download and configure a remote agent and install it on the Windows Domain Controller.

**Note**

To use domain authentication service, you must first download a remote agent and install it on the Windows Domain Controller. The remote agent provides a secure tunnel between Active Directory and the WLSE. For information about downloading and installing the remote server, see [Installing the Remote Server for Domain Authentication, page 18-17](#).

A user can optionally specify the domain name along with a user ID while logging on. The domain name is used for authentication:

- If the domain is not specified, authentication is first performed with the WDC/AD default domain and then with all the other trusted domain controllers until the user is found.
- If the domain is specified, authentication is performed only on that domain, which could be the local WDC/AD or one of the trusted WDC/ADs.

If you want to map RADIUS attributes to values in Active Directory, you can create AAA server groups and map them to Active Directory groups.

Optionally, users can be authorized using WDC/AD. The list of groups to which the user belongs in the WDC/AD is used. You map this list of groups to an internal group in the AAA server by means of a group map. The group map is a map between a list of external groups in WDC/AD and an internal AAA user group. You can configure an optional default group, which is used when there is no mapping found or when there is no hit in the maps. When a hit is encountered, the corresponding group is used. For example, if the user is in groups A, B, C, and D and a map for ABC is found before the map for ABCD, the ABC map is used.

**Procedure**

**Step 1** Select **Admin > AAA Administration > Windows Domain Auth Server**.

**Step 2** Enter the following information.

| Field                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name                | Set the hostname for the local WDC/AD.<br>Default is localhost.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Port                     | Set the port number.<br>Default is 2004.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Default Domain           | (Optional) Sets the default domain name.<br>The default domain is used to locate the user if the user does not specify a domain when logging in.                                                                                                                                                                                                                                                                                                                                                   |
| Group mapping:           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Default AAA Server Group | Select an AAA server group to be mapped to WDC/AD groups. A default AAA server group is provided (domain-auth-usergroup), or you can create your own default group to be mapped to all WDC/AD groups.<br>If you are not mapping groups, select None.<br><br><b>Note</b> To configure RADIUS attributes in the default user group, create another default group, or create other groups to be mapped to WDC/AD groups, you use the Groups option. See <a href="#">Managing Groups, page 18-26</a> . |



| Field                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AAA User Group to Windows Group Mappings | <p>(Optional) If you are using group maps, map the AAA groups to WDC/AD groups as needed:</p> <ol style="list-style-type: none"> <li>1. Click <b>Add</b>.</li> <li>2. Two fields appear at the bottom of the screen: AAA User Group and Maps to Windows Group.</li> <li>3. Enter a group name and click <b>Apply</b>. Repeat this step to add more groups. After you click <b>Apply</b>, the group is added to the list under Default AAA Server Group.</li> </ol> <p><b>Note</b> The AAA server groups must first be defined under <b>Admin &gt; AAA Administration &gt; Groups</b>.</p> |

**Step 3** To save your changes, click **Submit**. To discard your changes, click **Cancel**.

### Installing the Remote Server for Domain Authentication

Use the following instructions to download and install the mandatory remote server on a Windows Domain Controller (WDC). The remote server should be installed on a WDC that has access to your Active Directory server.

### Procedure

- Step 1** Navigate to the following URL on Cisco.com and log in:  
<http://www.cisco.com/cgi-bin/tablebuild.pl/acs-soleng-3des>
- Step 2** Download Remote-Agent-ACSse-win-v3.3.2.2-K9.zip.
- Step 3** Unzip the archive and run Setup.exe:
- At the prompt for an ACS appliance, enter the IP address or hostname of the WLSE.
  - At the prompt for the software to be installed, select windows authentication.
- Step 4** Finish the installation

### Related Topics

- [Installing the Remote Server for Domain Authentication, page 18-17](#)
- [Configuring the AAA Server—Overview, page 18-6](#)
- [About the AAA Server, page 18-1](#)
- [Managing Groups, page 18-26](#)

## Configuring LEAP Settings

The AAA server uses LEAP to authenticate repeater access points via a WDS access point. By default, user information is stored locally in the AAA server.

### Procedure

- 
- Step 1** Select **Admin > AAA Administration > LEAP Settings**
- Step 2** Select the service to use after LEAP negotiation. This specifies the location of user information for authentication and authorization. When the AAA server receives a request, it directs the request to the specified service. Then the service looks up the user and authenticates or authorizes the user.
- Local—authenticates against user information stored locally.
  - [LDAP](#)—authenticates against user information on the LDAP server.
  - Windows Domain-Auth—authenticates against WDC/AD.
- Step 3** To save your changes, click **Submit**. To discard your changes, click **Cancel**.
- 

### Related Topics

- [About the AAA Server, page 18-1](#)
- [Configuring the AAA Server—Overview, page 18-6](#)
- [Configuring Windows Domain Authentication, page 18-15](#)
- [Managing AAA Users, page 18-24](#)
- [Managing the LDAP Central Server, page 18-11](#)
- [Managing the LDAP Local Server, page 18-12](#)

## Configuring Cisco-PEAP Settings

The AAA server uses PEAPV1 tunneling EAP-GTC for authentication and authorization of wireless supplicants via access points. User profile information is stored in [LDAP](#) by default.

### Procedure

- 
- Step 1** Select **Admin > AAA Administration > Cisco-PEAP Settings**.
- Step 2** Enter the following information.

| Field                        | Description                                   |
|------------------------------|-----------------------------------------------|
| Private Key Password         | The server's private key password for PEAPV1. |
| Confirm Private Key Password |                                               |

| Field                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                             |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Certificate Upload    | Enter the absolute pathname of the file that contains your enterprise's certificate or browse for the file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | You will need to upload these certificates and the RSA key if you obtain an official certificate from a certificate authority. For information on obtaining an official certificate, see <a href="#">Managing SSL (HTTPS)</a> , page 16-18. |
| RSA Key Upload        | Enter or browse for the absolute pathname of the file that contains the RSA private key.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                             |
| CA Certificate Upload | Enter or browse for the absolute pathname of the file that contains the certificate authority's certificate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                             |
| Inner Service         | Select the source of user information for authentication and authorization. <ul style="list-style-type: none"><li>• Local—authenticates against user information stored locally. All users must be entered on the AAA server. See <a href="#">Managing AAA Users</a>, page 18-24.</li><li>• LDAP—authenticates against user information on the LDAP server. This is the default. See <a href="#">Managing the LDAP Central Server</a>, page 18-11 and <a href="#">Managing the LDAP Local Server</a>, page 18-12.</li><li>• Windows Domain-Auth—authenticates against user information in an Active Directory database on a Windows Domain Controller. See <a href="#">Configuring Windows Domain Authentication</a>, page 18-15.</li></ul> |                                                                                                                                                                                                                                             |

**Step 3** To save your changes, click **Submit**. To discard your changes, click **Cancel**.

#### Related Topics

- [About the AAA Server](#), page 18-1
- [Configuring the AAA Server—Overview](#), page 18-6
- [Managing AAA Users](#), page 18-24
- [Configuring Windows Domain Authentication](#), page 18-15
- [Managing the LDAP Central Server](#), page 18-11
- [Managing the LDAP Local Server](#), page 18-12

## Configuring MS-PEAP Settings

This option allows you to set PEAP V0 parameters for AAA. User profile information is stored in [LDAP](#) by default.



#### Note

The AAA server cannot monitor MS-PEAP; therefore, there is no fault monitoring and reports are not available for this protocol.

#### Procedure

**Step 1** Select **Admin > AAA Administration > MS-PEAP Settings**.

**Step 2** Enter the following information.

| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                             |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Private Key Password         | The server’s private key password for PEAPv0. The password must match the ServerRSAKeyFile certificate file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                             |
| Confirm Private Key Password |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                             |
| Certificate Upload           | Enter absolute pathname of file that contains your enterprise’s certificate or browse for the file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | You will need to upload these certificates and the RSA key if you obtain an official certificate from a certificate authority. For information on obtaining an official certificate, see <a href="#">Managing SSL (HTTPS)</a> , page 16-18. |
| RSA Key Upload               | Enter or browse for absolute pathname of file that contains the RSA private key.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                             |
| CA Certificate Path          | Enter or browse for absolute pathname of file that contains the certificate authority’s certificate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                             |
| Inner Service                | Select the source of user information for authentication and authorization. When the AAA server receives a request, it directs the request to the specified service. Then the service looks up the user and authenticates or authorizes the user. <ul style="list-style-type: none"><li>• Local—authenticates against user information stored locally. All users must be entered on the AAA server. See <a href="#">Managing AAA Users</a>, page 18-24.</li><li>• LDAP—authenticates against user information on an LDAP server. This is the default. See <a href="#">Managing the LDAP Central Server</a>, page 18-11 and <a href="#">Managing the LDAP Local Server</a>, page 18-12.</li><li>• Windows Domain-Auth—authenticates against under information in a Windows active directory database on a Windows domain authentication server. See <a href="#">Configuring Windows Domain Authentication</a>, page 18-15.</li></ul> |                                                                                                                                                                                                                                             |

**Step 3** To save your changes, click **Submit**. To discard your changes, click **Cancel**.

#### Related Topics

- [Configuring the AAA Server—Overview](#), page 18-6
- [About the AAA Server](#), page 18-1
- [Managing AAA Users](#), page 18-24
- [Managing the LDAP Central Server](#), page 18-11
- [Managing the LDAP Local Server](#), page 18-12
- [Configuring Windows Domain Authentication](#), page 18-15

## Configuring EAP-TLS Settings

This option allows you to set PEAP V0 parameters for AAA. User profile information is stored in [LDAP](#).

### Procedure

**Step 1** Select **Admin > AAA Administration > EAP-TLS Settings**.

**Step 2** Enter the following information; all fields are required.

| Field                        | Description                                                                                                                                   |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Private Key Password         | The server's private key password.                                                                                                            |
| Confirm Private Key Password |                                                                                                                                               |
| Certificate Upload           | If you obtain a certificate from a certificate authority, enter the absolute pathname of the certificate files or browse for them.            |
| RSA Key Upload               | If you obtain a certificate from a certificate authority, enter the absolute pathname of the file that contains the RSA key or browse for it. |

**Step 3** To save your changes, click **Submit**. To discard your changes, click **Cancel**.

## Configuring EAP-FAST Settings

Use this option to configure EAP-FAST settings for the AAA server.



### Note

The AAA server cannot monitor EAP-FAST on the internal AAA server; therefore, there is no fault monitoring and reports are not available for this protocol.

### Procedure

**Step 1** Select **Admin > AAA Administration > EAP-FAST Settings**.

**Step 2** Enter the following information.



### Note

The fields that are grayed out are not currently supported.

**Table 18-8** *EAP-FAST Parameters*

| Field               | Description                                                                                                                                            |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Always Authenticate | If selected, provisioning always rolls over into authentication without relying on a separate setting. Wireless performs better when this is selected. |

**Table 18-8** *EAP-FAST Parameters (continued)*

| Field                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authority Identifier  | Set the authority identifier. Must be a single string that uniquely identifies this server; spaces and quotation marks are not allowed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Authority Information | Enter the authority information, which provides human-readable descriptive text for the credential issuer; for example the enterprise and/or server name. The value might be displayed to the client for identification purposes. Uniquely identifies the PAC issuer. Can contain spaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Credential Lifetime   | Set the lifetime of the credential: <ul style="list-style-type: none"> <li>• <b>Forever</b>—Credential never expires.</li> <li>• <b>Timespan</b>—Click <b>Timespan</b> to activate the following fields. Click <b>Forever</b> to delete the values of the following fields and deactivate them (gray them out). <ul style="list-style-type: none"> <li>– weeks</li> <li>– days</li> <li>– hours</li> <li>– minutes</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                        |
| Provisioning Mode     | Set the provisioning mode. Only <b>Anonymous</b> is supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Inner Service         | Select the service to use after LEAP negotiation. This specifies the location of user information for authentication and authorization. When the AAA server receives a request, it directs the request to the specified service. Then the service looks up the user and authenticates or authorizes the user. <ul style="list-style-type: none"> <li>• <b>Local</b>—authenticates against user information stored locally. All users must be entered on the AAA server; see <a href="#">Managing AAA Users, page 18-24</a>.</li> <li>• <b>LDAP</b>—authenticates against user information on the LDAP server.</li> <li>• <b>Windows Domain-Auth</b>—authenticates against user information in an Active Directory database on a Windows Domain Controller. See <a href="#">Configuring Windows Domain Authentication, page 18-15</a>.</li> </ul> |

**Step 3** To save your changes, click **Submit**. To discard your changes, click **Cancel**.

#### Related Topics

- [About the AAA Server, page 18-1](#)
- [Configuring the AAA Server—Overview, page 18-6](#)
- [Managing AAA Users, page 18-24](#)
- [Configuring Windows Domain Authentication, page 18-15](#)
- [Managing the LDAP Central Server, page 18-11](#)
- [Managing the LDAP Local Server, page 18-12](#)

## Managing AAA Clients

In the context of the AAA server, a client is a device that submits a request for authorization on behalf of infrastructure access points. Clients that should be added under this option are:

- Devices that provide Wireless Domain Services (WDS). These include WDS access points, Wireless LAN Services Modules (WLSMs), or routers running an image that includes WDS capabilities.
- If you are *not* using WDS, all of the [infrastructure access points](#) with users who should be authenticated should be added as clients.
- The WLSE itself (for monitoring the internal AAA server).

To set up the WLSE to monitor the internal AAA server, see [Monitoring the AAA Server, page 18-28](#).

- Any other device that communicates directly with the AAA server.

By using address ranges or wildcards (\*), you can add multiple clients at the same time.

### Procedure

**Step 1** Select **Admin > AAA Administration > Clients**.

**Step 2** Add the WLSE as a client. If you are using a redundant pair of WLSEs, add both WLSEs to the list of clients.

**Writer question: For the redundant pair, do you use the VIPs?**

- Click **Add Client**.
- Enter the IP address of the WLSE.
- Enter a shared secret.



#### Note

You will need this shared secret when configuring the WLSE to monitor the AAA server—See [Monitoring the AAA Server, page 18-28](#).

**Step 3** Add other clients:

- Click **Add Client**.
- Enter the following information.

| Field         | Description                                                                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name          | Name for the client.                                                                                                                                                                                                                     |
| IP Address    | Client IP address. You can enter: <ul style="list-style-type: none"> <li>• A single address; for example 191.168.168.5.</li> <li>• Ranges; for example, 192.168.168.3-5.</li> <li>• The * wildcard; for example, 192.168.*.*.</li> </ul> |
| Shared Secret | RADIUS shared secret set on the client.                                                                                                                                                                                                  |

- Click **Submit**.
- Click **Cancel** to cancel submission of the new client.

- Step 4** To modify a client:
- Click the client name.
  - Edit the client as desired.
  - Click **Submit**.
  - Click **Cancel** to cancel your changes to the client.
- Step 5** To delete a client:
- Click the client name. The Edit Client screen appears.
  - Click **Delete**.
- 

### Related Topics

[About the AAA Server, page 18-1](#)

## Managing AAA Users

In the context of the AAA server, a user is any entity that is being authenticated by a client; for example, a person, an infrastructure access point, or a MAC address.

Enter all users in this screen unless you are using LDAP or Windows domain authentication as the source of user information.

If you have chosen “local” as the Inner Service for a protocol, enter all users to be authenticated in this screen.

Possible users include:

- Users on any of the devices that are using the AAA server to authenticate or authorize those users.
- Administrators who are using authentication to access APs through Telnet.
- A WLSE user, if you are using the WLSE to monitor the performance of the internal AAA server. For more information about using the WLSE to monitoring the internal AAA server, see [Monitoring the AAA Server, page 18-28](#).

You can [Add a User](#), [Modify a User](#), and [Delete a User](#).

### Add a User

---

- Step 1** Select **Admin > AAA Administration > Users**.
- Step 2** Click **Add User**. The Add User page appears.
- Step 3** Enter the user name and user password and confirm the password.
- These are the values that will be assigned to the RADIUS User-Name and User-Password attributes when the access point authenticates with WDS.
- A user name can have up to 255 characters. You can use any character except the forward slash (/).
- Step 4** (Optional) In the “RADIUS attributes to value mappings” section, add RADIUS attribute mappings as follows.



**Note**

See the relevant vendor documentation for information about which attributes you may need to enter. The AAA server will operate properly with no authorization attributes; however, the client device may not provide the appropriate service because of the lack of certain authorization attributes. For a list of the RADIUS attributes native to the AAA server, see [RADIUS Attributes for the AAA Server, page 18-46](#).

- a. Select **Add**.

Result: The RADIUS Attribute and Attribute Value text boxes appear.

- b. Enter the desired mappings.
- c. Click **Apply**.

**Note**

Mappings cannot be modified. To change a mapping, first delete it from the RADIUS Attributes to Values list, then create a new mapping.

**Step 5** To add the user, click **Submit**. To cancel the creation of the user, click **Cancel**.

**Note**

If you entered an incorrect RADIUS attribute in Step 4, or you attempt to map the same attribute more than once, an error message will be displayed after you click **Submit**. The user will not be added. Click **Back** to make corrections in the mappings.

### Modify a User

**Step 1** Select **Admin > AAA Administration > Users**.

**Step 2** Click the user name. The User Edit screen appears.

**Step 3** To change the name, enter a new name in the Name field.

**Step 4** To change the password, click **Change Password**. Then, enter the new password and confirm it.

**Step 5** To add RADIUS attribute mappings, see [Modify a User, page 18-25](#) for details.

**Step 6** To delete a RADIUS attribute mapping, select the mapping from the RADIUS Attributes to Values list, then click **Delete**.

**Note**

Mappings cannot be modified. To change a mapping, first delete it, then create a new mapping.

**Step 7** Click **Submit**. To cancel your changes to the user, click **Cancel**.

### Delete a User

**Step 1** Select **Admin > AAA Administration > Users**.

**Step 2** Click the user name. The Edit User page appears.

**Step 3** Click **Delete**.

---

**Related Topics**

- [Configuring the AAA Server—Overview, page 18-6](#)
- [About the AAA Server, page 18-1](#)

## Managing Groups

When you select **Admin > AAA Administration > Groups**, the Groups List screen displays.

In this screen, you define the user groups to be mapped to WDC/AD groups in the Windows Domain Auth screen. You can define a default group to be mapped to all WDC/AD groups.

You must define AAA server groups in this screen before you can map AAA server groups to WDC/AD groups (unless you are using the default AAA server group). The group mapping feature is used to assign RADIUS attributes to groups of users stored in an Active Directory database on a Windows Domain Controller. For more information on mapping groups, see [Configuring Windows Domain Authentication, page 18-15](#).

You can add groups, edit existing groups, or delete existing groups.

**Procedure**

---

**Step 1** To add a group, click **Add Group** in the Groups List page.

**Step 2** Enter the group name in the Name field.

A group name can have up to 255 characters. You can use any character except the forward slash (/).

**Step 3** (Optional) Add RADIUS attribute values as follows.



**Note** See the relevant vendor documentation for information about which attributes you may need to enter. For a list of the RADIUS attributes native to the AAA server, see [RADIUS Attributes for the AAA Server, page 18-46](#)

---

a. Select **Add**.

Result: The RADIUS Attribute and Value text boxes appear.

b. Enter the desired mappings.

c. Click **Apply**.

d. Repeat steps a-c to add more mappings.

**Step 4** After you have finished creating the group, click **Submit**.



**Note** If you entered an incorrect RADIUS attribute in Step 2d, or you attempt to map the same attribute more than once, an error message will be displayed after you click **Submit**. The user will not be added. Click **Back** to make corrections in the mappings.

---

**Step 5** To modify a group:

a. Click the group name. The Group Edit screen appears.

- b. To change the name, enter a new name in the Name field.
- c. To add or delete RADIUS attribute mappings, see Step 3 for details.
- d. To delete a RADIUS mapping, select the mapping, then click **Delete**.
- e. Click **Submit**.

**Step 6** To delete a group:

- a. Click the group name. The Edit Group page appears.
- b. Click **Delete**.

**Step 7** To cancel your changes, click **Cancel**.

---

#### Related Topics

[Configuring Windows Domain Authentication, page 18-15](#)

## Viewing and Releasing Sessions

The Sessions screen allows you to:

- Display information about a user session by entering a username or session ID: Username, Time the session started and session ID.
- Release all sessions.

#### Procedure

---

**Step 1** Select **Admin > AAA Administration > Sessions**.

Result: A list of all the currently active sessions is displayed.

**Step 2** To query for a session, enter a session ID or username.

- The Username, Time, and Session ID of the query or the message that no session was found is displayed. The Username is the RADIUS username. The Time is the time the session began.
- To release the session, Click **Release**.
- To return to the main Sessions page, click **Cancel**.

**Step 3** To release all sessions, select **Release All**.

---

#### Related Topics

- [About the AAA Server, page 18-1](#)
- [Configuring the AAA Server—Overview, page 18-6](#)

## Using AAA Server Log Files

The AAA server log files, and log files for other WLSE functions can be accessed through **Admin > Appliance > Status > View Log File**. For detailed information on how to download, search, and email log files (and information about other WLSE log files), see [Using WLSE Log Files, page 16-4](#).

**Table 18-9** Log Files for the Internal AAA Server

| Log File               | Content                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AAA-accounting.log     | Formatted accounting records received from the access points, generated for each accounting request. For example:<br><br>Mon, 26 Jan 2004 12:12:56<br>User-Name = user1<br>NAS-IP-Address = 127.0.0.1<br>NAS-Port = 1<br>Framed-IP-Address = 1.1.1.1<br>Called-Station-Id = 14085271703<br>Calling-Station-Id = 14085271703<br>NAS-Identifier = localhost<br>Acct-Status-Type = Stop<br>Acct-Session-Id = 1 |
| AAA-cli.log            | Information on AAA server CLI commands that have been executed.                                                                                                                                                                                                                                                                                                                                             |
| AAA-daemon-manager.log | Output from watchdog and AAA database daemon processes.                                                                                                                                                                                                                                                                                                                                                     |
| AAA-database.log       | Information on AAA database activity.                                                                                                                                                                                                                                                                                                                                                                       |
| AAA-server-trace.log   | Output from AAA server tracing, when tracing is enabled.                                                                                                                                                                                                                                                                                                                                                    |
| AAA-server.log         | Output from RADIUS daemon processes.                                                                                                                                                                                                                                                                                                                                                                        |
| AAA-status.log         | Startup and shutdown history of AAA processes. Also, AAA server installation and deinstallation history.                                                                                                                                                                                                                                                                                                    |

## Monitoring the AAA Server

You can use the WLSE's fault-monitoring feature to monitor a single protocol on the AAA server (either RADIUS, Cisco-PEAP, or LEAP).

The WLSE does not monitor MS-PEAP or EAP-FAST on the WLSE's built-in AAA server.

A given WLSE can only monitor one protocol per AAA server.

The WLSE monitors the following for the selected protocol:

- Server availability
- Server state (for example, degraded, overloaded, or OK)
- Server authentication errors

After configuring the AAA server and the WLSE as described in the following procedure, you can monitor the performance of the internal AAA server by selecting **Faults > Display Faults** and view reports about the AAA server by selecting **Reports > Trends**. For more information on faults and reports, see [Chapter 3, "Fault Monitoring"](#) and [Chapter 10, "Using Reports."](#)



### Note

The WLSE must also be added to the AAA server as a client.

### Procedure

- 
- Step 1** You will need the name and password of a WLSE user. If necessary, add a user—see [Managing GUI Users, page 16-49](#). You will need this data in Steps 3 and 4.
- Step 2** Select **Admin > AAA Administration > Clients**.  
Add the WLSE as a client.
- Step 3** Add the WLSE user to the user database:
- If you are using the local database for users, add the WLSE user to the list of AAA server users under **Admin > AAA Administration > Users**.
  - If you are using LDAP, add the WLSE user to the LDAP database of users.
- Step 4** Select **Devices > Discover > AAA Server**:
- a. Select RADIUS from the Server Type list.
  - b. Enter the hostname or IP address of the WLSE in the Server Name field.
  - c. Enter 1812 in the Server Port field.
  - d. Enter the username and password of the WLSE user from Step 1 in the Username and Password fields.
  - e. Enter the shared secret of the WLSE in the Secret field.  
This is the shared secret that you entered when adding the WLSE as a client of the AAA server.
  - f. Click **Save**.
- Step 5** If the WLSE is a member of a redundant pair, repeat Step 4 for the second WLSE.
- Step 6** Select **Faults > Manage Fault Settings**:
- a. Select the Default profile, then click **Edit**.
  - b. Select **AAA SERVER > RADIUS Response Time**.
  - c. Select **Enable**.
  - d. Set the Poll Interval to 1 minute.
  - e. Set consecutive polling cycles to 2 for the “Server is unavailable” Setting.



---

**Note** Leave the consecutive polling cycles at the default of 1 for the remaining settings in this window.

---

- f. Click **Apply**.
- 

### Related Topics

- [Configuring the AAA Server—Overview, page 18-6](#)
- [Monitoring AAA Servers, page 4-14](#)

## Using AAA Server CLI Commands

This section provides details on the AAA server CLI commands. [Table 18-10 on page 18-30](#) lists all of the commands. Most of the features provided in the Web interface are also available via CLI commands. Some functions that are not provided in the Web interface are provided through CLI commands; such as generating self-signed certificates, configuring logging method, reinitializing the database, and starting or stopping daemons.

For general information about using WLSE CLI commands, see [Appendix A, “Command Line Interface \(CLI\) Commands.”](#)

When AAA server CLI are executed, these events are logged in the AAA-cli.log. You can access this log from **Admin > Appliance > Status > View Log File**.

**Table 18-10 AAA Server CLI Commands**

| Command                       | Privilege Level | Description                                                          | Reference                                          |
|-------------------------------|-----------------|----------------------------------------------------------------------|----------------------------------------------------|
| <b>aaa-server cisco-peap</b>  | 15              | Configures <a href="#">PEAP server</a> on the AAA server.            | <a href="#">aaa-server cisco-peap, page 18-32</a>  |
| <b>aaa-server client</b>      | 15              | Manages AAA server clients.                                          | <a href="#">aaa-server client, page 18-33</a>      |
| <b>aaa-server domain-auth</b> | 15              | Configures <a href="#">WDC domain authentication</a> .               | <a href="#">aaa-server domain-auth, page 18-34</a> |
| <b>aaa-server eap-fast</b>    | 15              | Configures EAP-FAST.                                                 | <a href="#">aaa-server eap-fast, page 18-35</a>    |
| <b>aaa-server eap-tls</b>     | 15              | Configures EAP-TLS.                                                  | <a href="#">aaa-server eap-tls, page 18-37</a>     |
| <b>aaa-server ldap</b>        | 15              | Configures <a href="#">LDAP server</a> parameters on the AAA server. | <a href="#">aaa-server ldap, page 18-37</a>        |
| <b>aaa-server leap</b>        | 15              | Specifies AAA service to use after LEAP negotiation.                 | <a href="#">aaa-server leap, page 18-39</a>        |
| <b>aaa-server logging</b>     | 15              | Configures AAA server logging (local or syslog).                     | <a href="#">aaa-server logging, page 18-40</a>     |
| <b>aaa-server ms-peap</b>     | 15              | Configures MS-PEAP.                                                  | <a href="#">aaa-server ms-peap, page 18-41</a>     |
| <b>aaa-server reinit</b>      | 15              | Reinitializes AAA server database.                                   | <a href="#">aaa-server reinit, page 18-42</a>      |
| <b>aaa-server session</b>     | 15              | Deletes or displays current AAA server sessions.                     | <a href="#">aaa-server session, page 18-43</a>     |
| <b>aaa-server start</b>       | 15              | Starts or stops AAA server daemons.                                  | <a href="#">aaa-server start, page 18-43</a>       |
| <b>aaa-server status</b>      | 15              | Displays status of AAA server.                                       | <a href="#">aaa-server status, page 18-44</a>      |

**Table 18-10**      **AAA Server CLI Commands (continued)**

|                             |    |                                                        |                                                  |
|-----------------------------|----|--------------------------------------------------------|--------------------------------------------------|
| <b>aaa-server trace</b>     | 15 | Sets or displays the AAA server trace level.           | <a href="#">aaa-server trace, page 18-44</a>     |
| <b>aaa-server user</b>      | 15 | Manages AAA server users (access points).              | <a href="#">aaa-server user, page 18-45</a>      |
| <b>aaa-server usergroup</b> | 15 | Manages user groups for Windows domain authentication. | <a href="#">aaa-server usergroup, page 18-45</a> |

## aaa-server cisco-peap

This command displays and configures Cisco PEAP parameters: the server’s password, certificates and RSA private key, and AAA service to use after PEAP negotiation.

### Syntax Description

|                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aaa-server cisco-peap private-key-password</b> <i>password</i><br><b>aaa-server cisco-peap private-key-password</b>  | Sets or displays server’s private key password for PEAPv1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>aaa-server cisco-peap inner-service</b><br><b>aaa-server cisco-peap inner-service { ldap   local   domain-auth }</b> | Displays or specifies the service to use after LEAP negotiation. This command specifies the location of user information for authentication and authorization. When the AAA server receives a request, it directs the request to the specified service. Then the service looks up the user and authenticates or authorizes the user. <ul style="list-style-type: none"> <li>local—authenticates against user information stored locally. This is the default. Enter the users in the AAA server.</li> <li>LDAP—authenticates against user information on the LDAP server. This is the default.</li> <li>domain-auth—authenticates against user information stored in an Active Directory database on a Windows Domain Controller.</li> </ul> |
| <b>aaa-server cisco-peap mkcert</b>                                                                                     | Generates a self-signed certificate. A self-signed certificate is automatically generated by the WLSE, but you can use this command to generate another one if you need to make changes. This command is interactive, and requests the following optional information: country, organization and organizational unit, and server or installation name.                                                                                                                                                                                                                                                                                                                                                                                       |

### Related Commands

- [aaa-server user, page 18-45](#)
- [aaa-server domain-auth, page 18-34](#)
- [aaa-server ldap, page 18-37](#)



## aaa-server client

This command adds, deletes, and displays clients or resets a client's parameters. The clients of the AAA server might be infrastructure access points (if not using WDS) or WDS devices. The WLSE itself should be added as a client of the AAA server if you will use the WLSE to monitor the AAA server.

### Syntax Description

|                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aaa-server client</b>                                                                                | Displays all properties of all clients: name, IP address, shared secret, and authorization type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>aaa-server client</b> <i>name</i>                                                                    | Displays name, IP address, shared secret, and authorization type for a client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>aaa-server client</b> <i>name</i><br><b>ip-address</b> <i>ip-address</i> <b>secret</b> <i>secret</i> | <p>Adds a client or resets a client's IP address, shared secret, and authorization type.</p> <ul style="list-style-type: none"> <li><i>name</i> is chosen by the administrator to identify the client and must be a single string, without spaces or surrounding quotation marks.</li> <li><i>secret</i> is a single string, without spaces or surrounding quotation marks.</li> <li><i>ip-address</i> can be a single IP address, or can include ranges and the * wildcard.</li> </ul> <p>All arguments are required. The properties are overwritten if a client exists with the same name.</p> |
| <b>no aaa-server client</b> <i>name</i>                                                                 | Deletes a client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

### Examples

This command adds a client. All arguments are required.

```
aaa-server client ap001 ip-address 10.10.10.1 secret boo
aaa-server client ap001 ip-address 10.10.10.1 secret boo
```

This command displays information about a client:

```
aaa-server client
aaa-server client ap001 ip-address 10.10.10.1 secret boo
```

# aaa-server domain-auth

This command configures the domain authentication/authorization service. Configure this service if you are using Windows Domain Controller/Active Directory (WDC/AD) as your user database for the AAA server.

## Syntax Description

|                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aaa-server domain-auth host-name</b><br><i>ad-host-name</i>                  | Sets or displays the hostname of the WDC/AD server. <i>ad-host-name</i> must be a single string, without spaces or surrounding quotation marks.                                                                                                                                                                                                                                                                                      |
| <b>aaa-server domain-auth port</b> <i>portnumber</i>                            | Sets the port number. Must be a valid number between 1 and 65535.                                                                                                                                                                                                                                                                                                                                                                    |
| <b>aaa-server domain-auth port</b>                                              | Displays the port number.                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>aaa-server domain-auth defaultusergroup</b><br><i>group-name</i>             | Sets the default user group name (must be the name of an existing group), displays the default user group name, or clears the default user group.                                                                                                                                                                                                                                                                                    |
| <b>no aaa-server domain-auth defaultusergroup</b>                               | To create a default AAA user group, use the <a href="#">aaa-server usergroup</a> command.                                                                                                                                                                                                                                                                                                                                            |
| <b>aaa-server domain-auth groupmap</b><br><i>group-name=windows-group-names</i> | Maps a single AAA group to one or more WDC/AD groups. The group name must be an existing group. If you are listing more than one WDC/AD group, separate the group names by commas.<br><br>The group mapping feature is used to assign RADIUS attributes to groups of users stored in an Active Directory database on a Windows Domain Controller.<br><br>To create AAA groups, use the <a href="#">aaa-server usergroup</a> command. |
| <b>no aaa-server domain-auth groupmap</b><br><i>groupnum</i>                    | Removes a group mapping. <i>groupnum</i> must be valid group number. To obtain group numbers, use the following command to display all of the group mappings.                                                                                                                                                                                                                                                                        |
| <b>aaa-server domain-auth groupmap</b>                                          | Displays group mappings.                                                                                                                                                                                                                                                                                                                                                                                                             |

## Usage Guidelines

Use the [aaa-server usergroup](#) command to define AAA user groups.

## Examples

To display the hostname of the active directory server:

```
aaa-server domain-auth host-name
aaa-server domain-auth host-name adhost
```

To add group mappings:

```
aaa-server domain-auth groupmap aaagroup1=wingroup2,wingroup3
```

To display group mappings:

```
aaa-server domain-auth groupmap
 1. aaagroup1=wingroup2,wingroup3
 2. aaagroup2=wingroup3,wingroup4
```

To remove a group mapping:

```
no aaa-server domain-auth groupmap 1
```

#### Related Commands

[aaa-server usergroup](#), page 18-45

## aaa-server eap-fast

This command configures EAP-FAST parameters.

### Syntax Description

|                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aaa-server eap-fast always-authenticate</b><br><b>{ true   false }</b><br><b>aaa-server eap-fast always-authenticate</b> | Sets or displays the flag indicating whether provisioning should always roll over into authentication without relying on a separate session. Most environments (including wireless) perform better when this parameter is set to true.                                                                                                                                                                                                                                 |
| <b>aaa-server eap-fast authority-identifier</b> <i>name</i><br><b>aaa-server eap-fast authority-identifier</b>              | Sets or displays the authority identifier. <i>name</i> must be a single string, without spaces or quotation marks.                                                                                                                                                                                                                                                                                                                                                     |
| <b>aaa-server eap-fast authority information</b> <i>description</i><br><b>aaa-server eap-fast authority information</b>     | Sets or displays the authority information. <i>description</i> is human-readable descriptive text for this credential issuer and may be displayed to the client for identification purposes. If the description contains spaces, it must be surrounded by double-quotes.                                                                                                                                                                                               |
| <b>aaa-server eap-fast credential lifetime</b> <i>lifetime</i><br><b>aaa-server eap-fast credential lifetime</b>            | Sets or displays the credential lifetime. <i>lifetime</i> is specified as a string consisting of pairs of numbers and units. Units may be one of the following: <ul style="list-style-type: none"> <li>• M, minute, or minutes</li> <li>• H, hour, or hours</li> <li>• D, day, or days</li> <li>• W, week or week</li> </ul> If the credential never expires, specify <i>lifetime</i> as forever. If lifetime contains spaces, it must be surrounded by double-quotes. |

|                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aaa-server eap-fast inner service</b><br><b>[ ldap   local   domain-auth ]</b><br><b>aaa-server eap-fast inner service</b> | <p>Sets or displays the service to use after LEAP negotiation. This determines the location of user information for authentication and authorization. When the AAA server receives a request, it directs the request to the specified service. Then the service looks up the user and authenticates or authorizes the user.</p> <ul style="list-style-type: none"> <li>• <b>local</b>—authenticates against user information stored locally. Enter the users in the AAA server.</li> <li>• <b>LDAP</b>—authenticates against user information on the LDAP server. This is the default.</li> <li>• <b>domain-auth</b>—authenticates against user information stored in an Active Directory database on a Windows Domain Controller.</li> </ul> |
| <b>aaa-server eap-fast adhp-mode</b><br><b>[ anonymous   signed ]</b>                                                         | <p>Sets or displays the ADHP (provisioning) mode. Only <b>anonymous</b> is supported.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Examples

To set the authority information:

```
aaa-server eap-fast authority-information "some descriptive text"
aaa-server eap-fast authority-information "some descriptive text"
```

To set the credential lifetime:

```
aaa-server eap-fast credential-lifetime "8 days 4 hours"
aaa-server eap-fast credential-lifetime "8 days 4 hours"
```

```
aaa-server eap-fast credential-lifetime forever
aaa-server eap-fast credential-lifetime forever
```

### Related Commands

[aaa-server domain-auth, page 18-34](#)

[aaa-server user, page 18-45](#)

[aaa-server ldap, page 18-37](#)

## aaa-server eap-tls

This command sets EAP-TLS parameters.

### Syntax Description

|                                                                   |                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aaa-server eap-tls private-key-password</b><br><i>password</i> | Sets or displays the server's private key password. The password must be a single string, without spaces or surrounding quotation marks.                                                                                                                                                                                                                       |
| <b>aaa-server eap-tls private-key-password</b>                    |                                                                                                                                                                                                                                                                                                                                                                |
| <b>aaa-server eap-tls mkcert</b>                                  | Generates a self-signed certificate. A self-signed certificate is automatically generated by the WLSE, but you can use this command to generate another certificate if you need to make changes. This command is interactive, and requests the following optional information: country, organization and organizational unit, and server or installation name. |

## aaa-server ldap

This command configures [LDAP](#) server parameters.

### Syntax Description

In the following commands, specify **local** for the LDAP local server or **central** for the LDAP central server.

|                                                                                      |                                                                                                                                                                     |
|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aaa-server ldap</b>                                                               | Displays LDAP settings for both the central and local LDAP servers.                                                                                                 |
| <b>aaa-server ldap { local   central }</b>                                           | Displays LDAP settings for either the local or central server.                                                                                                      |
| <b>aaa-server ldap { local   central } timeout</b><br><i>timeout</i>                 | Sets or displays the timeout (in seconds) for bind attempts or displays current timeout setting, how long the AAA server waits for a response from the LDAP server. |
| <b>aaa-server ldap { local   central } timeout</b>                                   |                                                                                                                                                                     |
| <b>aaa-server ldap { local   central } host-name</b><br><i>[ ipaddr   hostname ]</i> | Sets or displays hostname or IP address of the LDAP server. The hostname must be all lower-case. The hostname is not checked to make sure it is a valid hostname.   |
| <b>aaa-server ldap { local   central } host-name</b>                                 |                                                                                                                                                                     |
| <b>aaa-server ldap { local   central } port</b><br><i>portnumber</i>                 | Sets or displays port of the LDAP server. The port number must be an integer between 1 and 65536. The validity of the number is not checked.                        |
| <b>aaa-server ldap { local   central } port</b>                                      |                                                                                                                                                                     |
| <b>aaa-server ldap { local   central } bind-name</b><br><i>bindname</i>              | Sets or displays administrator name with which to bind. The bindname must be a single string, without spaces or surrounding quotation marks.                        |
| <b>aaa-server ldap { local   central } bind-name</b>                                 |                                                                                                                                                                     |

|                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aaa-server ldap { local   central } bind-password</b> <i>password</i><br><b>aaa-server ldap { local   central } bind-password</b>                                                   | Sets or displays (in clear text) administrator password with which to bind. The password must be a single string, without spaces or surrounding quotation marks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>aaa-server ldap { local   central } search-path</b> <i>path</i><br><b>aaa-server ldap { local   central } search-path</b>                                                           | Sets or displays root of the search tree in LDAP. The path must be a single string, without spaces or surrounding quotation marks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>aaa-server ldap { local   central } search-filter</b> [ <i>filter</i> ]<br><b>aaa-server ldap { local   central } search-filter</b>                                                 | <p>Sets or displays the search filter (uid=%s), where uid is the name of the LDAP property that contains the same values as the RADIUS User Name attributes that are being authenticated.</p> <p>The search filter must be in the form “(somename=%s)”. The value must be surrounded by double quotes, and spaces are not allowed. The LHS (somename) is not validated.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>aaa-server ldap { local   central } user-password</b> [ <i>property-name</i> ]<br><b>aaa-server ldap { local   central } user-password</b>                                          | Sets or displays LDAP property name that contains user passwords. The property name must be a single string, without spaces or surrounding quotation marks. Must be a property of all objects that match the search path.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>aaa-server ldap { local   central } use-ssl</b> [ true   false ]<br><b>aaa-server ldap { local   central } use-ssl</b>                                                              | <i>This option has not been implemented and will be removed in a future release.</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>aaa-server ldap { local   central } user-password-encryption { dynamic   none   crypt   sha-1   ssha-1 }</b><br><b>aaa-server ldap { local   central } user-password-encryption</b> | <p>Sets or displays the encryption style for the user password property:</p> <p><b>dynamic</b>—instructs the AAA server to choose the encryption mechanism on a case-by-case basis after the server determines the presence of a known prefix, which the server prepends to the password attribute.</p> <p><b>none</b>—no encryption (the default).</p> <p><b>crypt</b>—AAA server encryption using the Unix crypt algorithm.</p> <p><b>sha-1</b> or <b>ssha-1</b>—Secure Hash Algorithm; a hashing algorithm that produces a 160-bit digest based upon the input. The algorithm produces SHA passwords that are irreversible or prohibitively expensive to reverse. Enables the AAA server to authorize users whose passwords are stored in an LDAP server and hashed by using the SHA-1 encoding scheme. SSHA-1 is Netscape's (iPlanet) enhancement of the SHA-1 algorithm which includes salted password data.</p> |

|                                                                                                                      |                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>aaa-server ldap { local   central }<br/>attribute-mapping</b>                                                     | Adds, resets, or displays mapping between an LDAP property and a RADIUS authorization attribute.               |
| <b>aaa-server ldap { local   central }<br/>attribute-mapping</b> <i>ldap-property</i><br>[ <i>radius-attribute</i> ] | The no form deletes the mapping.                                                                               |
| <b>no aaa-server ldap { local   central }<br/>attribute-mapping</b> <i>ldap-property</i>                             | For information on AAA server attributes, see <a href="#">RADIUS Attributes for the AAA Server, page 18-46</a> |

## Examples

To display all of the properties of the local LDAP server:

```
aaa-server ldap local
host-name = 127.0.0.1
port = 389
bind-name =
bind-password =
search-path = o=cisco.com
search-filter = (uid=%s)
user-password = userpassword
user-password-encryption = Dynamic
timeout = 15
use-ssl = FALSE
attribute-mapping =
```

To set the timeout for bind attempts (in seconds) on the central LDAP server:

```
aaa-server ldap central timeout 15
aaa-server ldap central timeout 15
```

To display the root of the search tree in LDAP:

```
aaa-server ldap local search-path
aaa-server ldap local search-path o-cisco.com
```

To set the search filter:

```
aaa-server ldap local search-filter "(top=%s)"
aaa-server ldap local search-filter (top=%s)
```

## aaa-server leap

To specify or display the AAA service to use after LEAP negotiation, use the following command:

```
aaa-server leap inner-service
```

```
aaa-server leap inner-service { ldap | local | domain-auth }
```

### Syntax Description

Specify the service to use after LEAP negotiation. This specifies the location of user information for authentication and authorization. When the AAA server receives a request, it directs the request to the specified service. Then the service looks up the user and authenticates or authorizes the user.

- **local**—authenticates against user information stored locally. This is the default. Enter the users in the AAA server.

- **LDAP**—authenticates against user information on an LDAP server.
- **domain-auth**—authenticates against user information in an Active Directory database on a Windows domain controller.

### Example

To display information about the currently configured AAA service to use after LEAP negotiation, use the following command:

```
aaa-server leap inner-service
aaa-server leap inner-service local
```

#### Related Commands

[aaa-server domain-auth](#), page 18-34

[aaa-server ldap](#), page 18-37

[aaa-server user](#), page 18-45

## aaa-server logging

The following commands configure syslog and local logging for the AAA server. Syslog logging is disabled by default. Local logging is enabled by default.

Syslog logging requires a UNIX host running a syslog daemon as a receiver for the AAA messages.

### Syntax Description

|                                                                                                                                |                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aaa-server logging</b>                                                                                                      | Displays current values for logging: <ul style="list-style-type: none"> <li>• Whether syslog and local logging are enabled.</li> <li>• Syslog server IP address and facility local number, if configured.</li> </ul> |
| <b>aaa-server logging syslog</b><br><b>no aaa-server logging syslog</b>                                                        | Enables or disables syslog logging. Causes the AAA server to stop and restart.                                                                                                                                       |
| <b>aaa-server logging local</b><br><b>no aaa-server logging local</b>                                                          | Enables or disables local logging. Causes the AAA server to stop and restart.                                                                                                                                        |
| <b>aaa-server logging syslog ip-address</b> <i>address</i><br><b>aaa-server logging syslog ip-address</b>                      | Sets or displays the current IP address used by the syslog server.                                                                                                                                                   |
| <b>aaa-server logging syslog facility-local-number</b> <i>number</i><br><b>aaa-server logging syslog facility-local-number</b> | Sets or displays the syslog facility local number. The number must be in the range 0-16. If the facility local number is changed and syslog is enabled, the AAA server will be restarted.                            |



## Usage Guidelines



### Note

The AAA server stops before modifications to logging settings are made and restarts afterward.

Multiple settings cannot be combined into one command.

Syslog logging will not work unless you provide both the server IP address and facility local number.

Syslog logging and local logging are independent of each other.

## Example

The following command shows that syslog logging is disabled and local logging is enabled:

```
aaa-server logging
no aaa-server logging syslog
aaa-server logging local
```

The following command stops local logging and restarts the AAA server:

```
no aaa-server logging local
no aaa-server logging local
restarting the AAA server...
```

The following command changes the syslog facility local number and restarts the AAA server:

```
aaa-server logging syslog facility-local-number 10
aaa-server logging syslog facility-local-number 10
restarting the AAA server...
```

## aaa-server ms-peap

The following commands configure MS-PEAP.

### Syntax Description

|                                                                   |                                                                                                                                                                                                       |
|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aaa-server ms-peap private-key-password</b><br><i>password</i> | Sets or displays the server's private key password for PEAPv0. The password must be a single string without spaces or quotation marks. The password must match the ServerRSAKeyFile certificate file. |
| <b>aaa-server ms-peap private-key-password</b>                    |                                                                                                                                                                                                       |

|                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aaa-server ms-peap inner service</b><br><b>[ ldap   local   domain-auth ]</b> | <p>Specifies the service to use after LEAP negotiation. This determines the location of user information for authentication and authorization. When the AAA server receives a request, it directs the request to the specified service. Then the service looks up the user and authenticates or authorizes the user.</p> <ul style="list-style-type: none"> <li>• <b>local</b>—authenticates against user information stored locally. Enter the users in the AAA server.</li> <li>• <b>LDAP</b>—authenticates against user information on the LDAP server. This is the default.</li> <li>• <b>domain-auth</b>—authenticates against user information stored in an Active Directory server on a Windows domain controller.</li> </ul> |
| <b>aaa-server ms-peap mkcert</b>                                                 | <p>Generates a self-signed certificate. A self-signed certificate is automatically generated by the WLSE, but you can use this command to generate another certificate if you need to make changes. This command is interactive, and requests the following optional information: country, organization and organizational unit, and server or installation name.</p>                                                                                                                                                                                                                                                                                                                                                                |

**Related Commands**

[aaa-server user, page 18-45](#)

[aaa-server ldap, page 18-37](#)

[aaa-server domain-auth, page 18-34](#)

# aaa-server reinit

The following command reinitializes the AAA server database to its starting configuration:

**aaa-server reinit**

## Example

To reinitialize the AAA server database:

```

aaa-server reinit
Rollforward recovery using "/opt/CSCOar/data/db/vista.tjf" started Thu Dec 30 02:00:21
2004
Rollforward recovery using "/opt/CSCOar/data/db/vista.tjf" finished Thu Dec 30 02:00:21
2004

Waiting for these processes to die (this may take some time):
AAA server running (pid: 1374)
AAA daemon manager running (pid: 1309)
AAA database lock running (pid: 1316)
AAA database running (pid: 1315)
4 processes left.....k2 processes left.0 processes left

AAA Daemon Manager shutdown complete.
```

```
execute /opt/CSCOar/conf/add-on/pre-fixup-symlink
Starting AAA Daemon Manager..completed.
```

## Usage Guidelines

This command causes AAA server processes to stop and then restart.

## aaa-server session

The following commands delete or display current sessions. If no name or session ID is specified, all sessions are listed.

## Syntax Description

|                                           |                                           |
|-------------------------------------------|-------------------------------------------|
| <b>no aaa-server session <i>name</i></b>  | Deletes a session.                        |
| <b>no aaa-server session</b>              | Deletes all sessions.                     |
| <b>aaa-server session</b>                 | Displays all sessions.                    |
| <b>aaa-server session <i>name</i></b>     | Displays the named session.               |
| <b>aaa-server session id <i>id</i></b>    | Displays a session by session identifier. |
| <b>no aaa-server session id <i>id</i></b> | Deletes a session by session identifier.  |

## Example

To display all current sessions:

```
aaa-server session
aaa-server session ap008 id 1 start-time 02/14/1990 15:38.54
aaa-server session ap005 id 2 start-time 02/15/1990 05:10:40
aaa-server session ap005 id 3 start-time 02/15/1990 05:11:14
```

## aaa-server start

The following command starts or stops the AAA server daemons:

```
aaa-server { start | stop }
```

## Usage Guidelines

If the AAA server is already up and you attempt to start it, the following messages are displayed:

```
aaa-server start
WARNING: Some AAA Server components are already running.

AAA server running (pid: 1374)
AAA daemon manager running (pid: 1309)
AAA database lock running (pid: 1316)
AAA database running (pid: 1315)
```

Use "aaa-server stop" to terminate these processes.

Nothing started.

If you attempt to stop the AAA server and another user is active and running a CLI command, for example, the following is displayed:

```
aaa-server stop
WARNING: You can not shut down AAA server while the
CLI is being used. Current list of running CLI with process id is:
26342 aregcmd
Shutdown failed.
```

## Related Commands

[aaa-server status, page 18-44](#)

## aaa-server status

The following command displays the status of the AAA server:

```
aaa-server status
```

## Example

Example output:

```
aaa-server status
AAA server running (pid: 1127)
AAA daemon manager running (pid: 1111)
AAA database running (pid: 1117)
AAA database lock running (pid: 1118)
```

## Related Commands

[aaa-server start, page 18-43](#)

## aaa-server trace

The following command sets or displays the trace level:

```
aaa-server trace [0 | 1 | 2 | 3 | 4 | 5]
```

There are 6 levels of tracing; 0 means no tracing; 5 is complete tracing (most verbose).

For more information about trace levels, see [Trace Levels and Information Logged, page 18-10](#).

## Usage Guidelines

Trace output can only be viewed in the Web interface. Select **Administration > Appliance > View Log Files** and view AAA-server-trace.log.

## aaa-server user

The following commands configure, delete, or modify AAA server users in the local user database. AAA server users are the infrastructure access points (the access points that register with the WDS access point).

### Syntax Description

|                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aaa-server user</b> <i>name</i> <b>password</b> <i>password</i>                  | Adds user or resets name or password of user. The name and password must be a single string, without spaces or surrounding quotation marks.<br><br>User names can be up to 255 characters in length and any character is allowed, except for the forward slash (/).                                                                                                                                                                                                                                                                             |
| <b>no aaa-server user</b> <i>name</i>                                               | Deletes a user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>aaa-server user</b>                                                              | Displays all properties of all users.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>aaa-server user</b> <i>name</i>                                                  | Displays properties of named user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>aaa-server user</b> <i>name</i> <b>attribute</b> <i>radius-attr</i> <i>value</i> | Adds or resets a RADIUS authorization attribute of the user. All arguments are required. <ul style="list-style-type: none"> <li><i>name</i> must be an existing user.</li> <li><i>radius-attr</i> must be an existing attribute. For information on the native attributes, see <a href="#">RADIUS Attributes for the AAA Server</a>, page 18-46.</li> <li><i>value</i> must be a single string, with no spaces or surrounding quotation marks. If the attribute is already defined for this user, the previous value is overwritten.</li> </ul> |
| <b>no aaa-server user</b> <i>name</i> <b>attribute</b> <i>radius-attr</i>           | Deletes RADIUS attribute from an existing user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

### Examples

The following command displays all users:

```
aaa-server user
aaa-server user ap008 password <encrypted>
aaa-server user ap005 password <encrypted>
 attributes =
 Framed-Ip-Address = 1.1.11.1
```

The following example command displays a single user:

```
aaa-server user ap008
aaa-server user ap008 password <encrypted>
```

## aaa-server usergroup

The following commands display, add, modify or delete AAA server user groups. These groups are mapped to WDC/AD groups for authorizing users. To map AAA groups to WDC/AD groups, use the [aaa-server domain-auth](#) command.

|                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aaa-server usergroup</b>                                                          | Displays all properties of all user groups.                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>aaa-server usergroup</b> <i>name</i>                                              | Creates a user group.<br><br>Group names can be up to 255 characters in length and any character is allowed, except for the forward slash (/).                                                                                                                                                                                                                                                                                                   |
| <b>no aaa-server usergroup</b> <i>name</i>                                           | Deletes a user group.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>aaa-server usergroup</b> <i>name</i> <b>attribute</b> <i>radius-attr value</i>    | Adds a RADIUS authorization attribute to an existing user group. <ul style="list-style-type: none"> <li><i>name</i> must be an existing user group.</li> <li><i>radius-attr</i> must be an attribute native to the AAA server. For information on RADIUS attributes, see <a href="#">RADIUS Attributes for the AAA Server, page 18-46</a>.</li> <li><i>value</i> must be a single string; spaces and quotation marks are not allowed.</li> </ul> |
| <b>no aaa-server usergroup</b> <i>name</i> <b>attribute</b> <i>radius-attr value</i> | Deletes RADIUS authorization attribute from a user group.                                                                                                                                                                                                                                                                                                                                                                                        |

## Examples

To display user groups:

```
aaa-server usergroup
 aaa-server usergroup aaagroup1
 attributes =
 user-name = buster
 called-station-id = 77
 aaa-server usergroup aaagroup2
```

To add an attribute to an existing user group:

```
aaa-server usergroup aaagroup1 attribute called-station-id 77
```

### Related Commands

[aaa-server domain-auth, page 18-34](#)

# RADIUS Attributes for the AAA Server

This section lists the RADIUS attributes supported by the internal AAA server. RADIUS attributes carry the specific authentication and authorization information, and configuration details for requests and replies.

All RADIUS requests and responses consist of one or more attributes, such as the user's name, user's password, and type of service the client should provide to the user.

The attribute dictionary contains prefigured authentication, authorization, and accounting attributes that can be part of a client's or user's configuration. The dictionary entries translate an attribute into a value the AAA server uses to parse incoming requests and generate responses.

Each vendor has its own list of supported attributes. See the vendor's documentation for information about these attributes.

For more detailed information about specific attributes, refer to the appropriate RFC as listed in [Table 18-11](#). You can find RFCs on the world wide web at [www.ietf.org](http://www.ietf.org).

This section contains the following information:

- List of all attributes of the internal AAA server—See [Table 18-12 on page 18-47](#).
- How to set tunnel attributes—See [Setting Tunnel Attributes, page 18-50](#).

**Table 18-11** *RFCs for RADIUS Attributes*

| RFC Subject                                          | RFC Number |
|------------------------------------------------------|------------|
| Standard RADIUS Attributes                           | 2865       |
| RADIUS Accounting Attributes                         | 2866       |
| Accounting Modifications for Tunnel Protocol Support | 2867       |
| Attributes for Tunnel Protocol Support               | 2868       |
| RADIUS Extensions                                    | 2869       |
| RADIUS for IPv6                                      | 3162       |

The standard, non vendor-specific RADIUS attributes supported by the AAA server are listed in [Table 18-12](#).

**Table 18-12** *RADIUS Attributes Supported by the AAA Server*

| Attribute Name              | Attribute Number |
|-----------------------------|------------------|
| Acct-Authentic              | 45               |
| Acct-Delay-Time             | 41               |
| Acct-Input-Gigawords        | 52               |
| Acct-Input-Octets           | 42               |
| Acct-Input-Packets          | 47               |
| Acct-Interim-Interval       | 85               |
| Acct-Link-Count             | 51               |
| Acct-Multi-Session-Id       | 50               |
| Acct-Output-Gigawords       | 53               |
| Acct-Output-Octets          | 43               |
| Acct-Output-Packets         | 48               |
| Acct-Session-Id             | 44               |
| Acct-Session-Time           | 46               |
| Acct-Status-Type            | 40               |
| Acct-Terminate-Cause        | 49               |
| Acct-Tunnel-Connection      | 68               |
| Acct-Tunnel-Packets-Lost    | 86               |
| Acquire-group-session-limit | 280              |
| ARAP-Challenge-Response     | 84               |

**Table 18-12** *RADIUS Attributes Supported by the AAA Server (continued)*

| <b>Attribute Name</b>    | <b>Attribute Number</b> |
|--------------------------|-------------------------|
| ARAP-Features            | 71                      |
| ARAP-Password            | 70                      |
| ARAP-Security            | 73                      |
| ARAP-Security-Data       | 74                      |
| ARAP-Zone-Access         | 72                      |
| Callback-Id              | 20                      |
| Callback-Number          | 19                      |
| Called-Station-Id        | 30                      |
| Calling-Station-Id       | 31                      |
| Change-Password          | 17                      |
| CHAP-Challenge           | 60                      |
| CHAP-Password            | 3                       |
| Class                    | 25                      |
| Configuration-Token      | 78                      |
| Connect-Info             | 77                      |
| Digest-Attributes        | 207                     |
| Digest-Response          | 206                     |
| EAP-Message              | 79                      |
| Error-Cause              | 101                     |
| Event-Timestamp          | 55                      |
| Filter-Id                | 11                      |
| Framed-AppleTalk-Link    | 37                      |
| Framed-AppleTalk-Network | 38                      |
| Framed-AppleTalk-Zone    | 39                      |
| Framed-Compression       | 13                      |
| Framed-Interface-Id      | 96                      |
| Framed-IP-Address        | 8                       |
| Framed-IP-Netmask        | 9                       |
| Framed-IPv6-Pool         | 100                     |
| Framed-IPv6-Prefix       | 97                      |
| Framed-IPv6-Route        | 99                      |
| Framed-IPX-Network       | 23                      |
| Framed-MTU               | 12                      |
| Framed-Pool              | 88                      |
| Framed-Protocol          | 7                       |
| Framed-Route             | 22                      |



**Table 18-12** *RADIUS Attributes Supported by the AAA Server (continued)*

| <b>Attribute Name</b>   | <b>Attribute Number</b> |
|-------------------------|-------------------------|
| Framed-Routing          | 10                      |
| Idle-Timeout            | 28                      |
| Login-IP-Host           | 14                      |
| Login-IPv6-Host         | 98                      |
| Login-LAT-Group         | 36                      |
| Login-LAT-Node          | 35                      |
| Login-LAT-Port          | 63                      |
| Login-LAT-Service       | 34                      |
| Login-Service           | 15                      |
| Login-TCP-Port          | 16                      |
| Message-Authenticator   | 80                      |
| NAS-Identifier          | 32                      |
| NAS-IP-Address          | 4                       |
| NAS-IPv6-Address        | 95                      |
| NAS-Port                | 5                       |
| NAS-Port-ID             | 87                      |
| NAS-Port-Type           | 61                      |
| Originating-Line-Info   | 94                      |
| Password-Expiration     | 21                      |
| Password-Retry          | 75                      |
| Port-Limit              | 62                      |
| Prompt                  | 76                      |
| Proxy-State             | 33                      |
| Reply-Message           | 18                      |
| Service-Type            | 6                       |
| Session-Timeout         | 27                      |
| State                   | 24                      |
| Termination-Action      | 29                      |
| Text-Ascend-Data-Filter | 225                     |

**Table 18-12** *RADIUS Attributes Supported by the AAA Server (continued)*

| Attribute Name                                                                                                                   | Attribute Number |
|----------------------------------------------------------------------------------------------------------------------------------|------------------|
| For special instructions on setting the following tunnel attributes, see <a href="#">Setting Tunnel Attributes</a> , page 18-50. |                  |
| Tunnel-Assignment-ID                                                                                                             | 82               |
| Tunnel-Client-Auth-ID                                                                                                            | 90               |
| Tunnel-Client-Endpoint                                                                                                           | 66               |
| Tunnel-Medium-Type                                                                                                               | 65               |
| Tunnel-Password                                                                                                                  | 69               |
| Tunnel-Preference                                                                                                                | 83               |
| Tunnel-Private-Group-ID                                                                                                          | 81               |
| Tunnel-Server-Auth-ID                                                                                                            | 91               |
| Tunnel-Server-Endpoint                                                                                                           | 67               |
| Tunnel-Type                                                                                                                      | 64               |
| User-Name                                                                                                                        | 1                |
| User-Password                                                                                                                    | 2                |
| Vendor-Specific Attributes                                                                                                       | 26               |

## Setting Tunnel Attributes

When using the tunnel attributes listed in [Table 18-13 on page 18-50](#), attach a tag consisting of **\_tag** followed by a value from 1 to 31. For example, Tunnel-Client-Endpoint\_tag3.

**Table 18-13** *Tunneling Attributes Supported by the AAA Server*

| Attribute Number | Attribute               |
|------------------|-------------------------|
| 64               | Tunnel-Type             |
| 65               | Tunnel-Medium-Type      |
| 66               | Tunnel-Client-Endpoint  |
| 67               | Tunnel-Server-Endpoint  |
| 69               | Tunnel-Password         |
| 81               | Tunnel-Private-Group-ID |
| 82               | Tunnel-Assignment-ID    |
| 83               | Tunnel-Preference       |
| 90               | Tunnel-Client-Auth-ID   |
| 91               | Tunnel-Server-Auth-ID   |



## Command Line Interface (CLI) Commands

---

This appendix summarizes the WLSE's command line interface (CLI) commands.



**Note**

---

When you use CLI commands to make a configuration change, the system configuration is updated immediately.

---

This appendix contains the following sections:

- [Using the CLI, page A-1](#)
- [CLI Conventions, page A-2](#)
- [Command Privileges, page A-2](#)
- [Checking Command Syntax, page A-2](#)
- [Command History Feature, page A-2](#)
- [Help for CLI Commands, page A-2](#)
- [Command Summary, page A-3](#)
- [Command Description Conventions, page A-3](#)
- [CLI Command Details, page A-7](#)
- [Maintenance Image Commands, page A-73](#)

## Using the CLI

You can use the CLI by:

- Attaching a console to the WLSE, or
- Accessing the WLSE using Telnet or SSH.



**Note**

---

Telnet is disabled by default. Use the **telnetenable** command to enable Telnet. See [telnetenable, page A-69](#).

---

## CLI Conventions

The command-line interface (CLI) uses the following conventions:

- The key combination **^c** or **Ctrl-c** means hold down the **Ctrl** key while you press the **c** key.
- A string is defined as a non-quoted set of characters.
- Use single-quotes (') to surround a series of parameters; do not use double-quotes



**Note**

---

Although the WLSE CLI is similar to the IOS CLI, they are not identical.

---

## Command Privileges

Access to CLI commands is controlled by your user account privilege level. Users with privilege level 15 can use all commands. Users with privilege level 0 can use only a subset of the commands. Most commands require privilege level 15.

## Checking Command Syntax

The user interface provides several types of responses to incorrect command entries:

- `Command not found`—You entered a command line that does not contain a valid command.
- `Incomplete command`—You entered a valid command but omitted required arguments.
- `Invalid input`—You entered a valid command but provided invalid arguments or parameters.

In addition, some commands have command-specific error messages that notify you that a command is valid but cannot run correctly.

## Command History Feature

The CLI provides a command history feature. To display previously entered commands, press the up arrow key. After pressing the up arrow key, you can press the down arrow key to display the commands in reverse order. To run a command, press the **Enter** key while the command is displayed on the command line. You can also edit commands before pressing the **Enter** key.



**Note**

---

Pressing **Ctrl-c** erases the history.

---

## Help for CLI Commands

For a list of all commands and their syntax, type **help** and press **Enter**.

For help on a specific command, use either of the following methods:

- Type the command name, a space, **help**; then press **Enter**. For example, **ntp help**.
- Type **help**, a space, and the command name; then press **Enter**. For example, **help ntp**.

The help provides command usage information and syntax.

## Command Description Conventions

Command descriptions in this document and in the CLI help system use the following conventions:

- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ( [ ] ) indicate optional elements.
- Braces ( { } ) indicate a required choice. Braces within square brackets ( [ { } ] ) indicate a required choice within an optional element.
- Boldface indicates commands and keywords that are entered literally as shown.
- Italics indicate arguments for which you supply values.

## Command Summary

Table A-1 lists the CLI commands.

**Table A-1** Command Summary

| Command                    | Privilege Level                                                                                                                                                                                                      | Description                                                        | Reference                                   |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|---------------------------------------------|
| <b>aaa-server</b> commands | These commands are for the internal AAA server, which is available on the WLSE Express only. For information on these commands, see <a href="#">Chapter 18, “Using the Internal AAA Server (WLSE Express Only).”</a> |                                                                    |                                             |
| <b>apptyp</b>              | 0                                                                                                                                                                                                                    | Shows the hardware type.                                           | <a href="#">apptyp, page A-7</a>            |
| <b>auth</b>                | 15                                                                                                                                                                                                                   | Enables remote authentication of WLSE users.                       | <a href="#">auth, page A-7</a>              |
| <b>backup</b>              | 15                                                                                                                                                                                                                   | Backs up WLSE database configuration.                              | <a href="#">backup, page A-8</a>            |
| <b>backupconfig</b>        | 15                                                                                                                                                                                                                   | Sets backup file location for all backup and restore operations.   | <a href="#">backupconfig, page A-9</a>      |
| <b>cdp</b>                 | 15                                                                                                                                                                                                                   | Enables or disables Cisco Discovery Protocol (CDP).                | <a href="#">cdp, page A-10</a>              |
| <b>clear</b>               | 0                                                                                                                                                                                                                    | Clears terminal settings for the shell.                            | <a href="#">clear, page A-11</a>            |
| <b>clearbackuphosts</b>    | 15                                                                                                                                                                                                                   | Clears the stored key for using SCP for backups.                   | <a href="#">clearbackuphosts, page A-11</a> |
| <b>clearvar</b>            | 15                                                                                                                                                                                                                   | Purges log and core files from /var partition.                     | <a href="#">clearvar, page A-12</a>         |
| <b>clock set</b>           | 15                                                                                                                                                                                                                   | Sets system date and time.                                         | <a href="#">clock set, page A-12</a>        |
| <b>debug</b>               | 15                                                                                                                                                                                                                   | Enables debugging mode for CLI commands.                           | <a href="#">debug, page A-13</a>            |
| <b>df</b>                  | 15                                                                                                                                                                                                                   | Displays current storage usage.                                    | <a href="#">df, page A-14</a>               |
| <b>diagnostic-info</b>     | 15                                                                                                                                                                                                                   | Gathers diagnostic information.                                    | <a href="#">diagnostic-info, page A-15</a>  |
| <b>dumpcores</b>           | 15                                                                                                                                                                                                                   | Compresses the core files and saves them to the user's directory.  | <a href="#">dumpcores, page A-15</a>        |
| <b>dumptcp</b>             | 15                                                                                                                                                                                                                   | Displays TCP/IP packet content and dumps packet content to a file. | <a href="#">dumptcp, page A-16</a>          |

Table A-1 Command Summary (continued)

| Command                             | Privilege Level  | Description                                                                          | Reference                                     |
|-------------------------------------|------------------|--------------------------------------------------------------------------------------|-----------------------------------------------|
| <a href="#">dumptechn</a>           | 15               | For diagnostics.                                                                     | <a href="#">dumptechn</a> , page A-17         |
| <a href="#">erase config</a>        | 15 <sup>1</sup>  | Erases configuration in flash memory and reloads the WLSE.                           | <a href="#">erase config</a> , page A-17      |
| <a href="#">exit</a>                | 0                | Logs user out.                                                                       | <a href="#">exit</a> , page A-18              |
| <a href="#">firewall</a>            | 15               | Implements port filtering.                                                           | <a href="#">firewall</a> , page A-19          |
| <a href="#">fsck</a>                | N/A <sup>2</sup> | Checks and repairs file system.                                                      | <a href="#">fsck</a> , page A-73              |
| <a href="#">gethostbyname</a>       | 15               | Displays IP address of a known domain name.                                          | <a href="#">gethostbyname</a> , page A-20     |
| <a href="#">hostname</a>            | 15               | Changes system host name.                                                            | <a href="#">hostname</a> , page A-21          |
| <a href="#">http-server</a>         | 15               | Controls access via HTTP and HTTPS                                                   | <a href="#">http-server</a> , page A-21       |
| <a href="#">import</a>              | 15               | Imports host files or maps IP addresses to host names.                               | <a href="#">import</a> , page A-22            |
| <a href="#">install</a>             | 15               | Configures repository for installing software updates and installs software updates. | <a href="#">install</a> , page A-23           |
| <a href="#">interface</a>           | 15               | Configures Ethernet interfaces.                                                      | <a href="#">interface</a> , page A-25         |
| <a href="#">ip domain-name</a>      | 15               | Defines default domain name.                                                         | <a href="#">ip domain-name</a> , page A-26    |
| <a href="#">ip name-server</a>      | 15               | Specifies address of name servers.                                                   | <a href="#">ip name-server</a> , page A-27    |
| <a href="#">listbackup</a>          | 15               | Lists all current backups at the configured site.                                    | <a href="#">listbackup</a> , page A-28        |
| <a href="#">mail</a>                | 15               | Debugs and tests email settings.                                                     | <a href="#">mail</a> , page A-28              |
| <a href="#">mailcntrl</a>           | 15               | Lists size of or deletes mail log, send queue, or user queue.                        | <a href="#">mailcntrl</a> , page A-30         |
| <a href="#">mailroute</a>           | 15               | Forwards email to specified server.                                                  | <a href="#">mailroute</a> , page A-30         |
| <a href="#">mkcert</a>              | 15               | Generates Certificate Signed Request (CSR) for HTTPS.                                | <a href="#">mkcert</a> , page A-31            |
| <a href="#">nslookup</a>            | 15               | Translates device name to IP address or IP address to device name.                   | <a href="#">nslookup</a> , page A-32          |
| <a href="#">ntp server</a>          | 15               | Allows system clock to be synchronized by a time server.                             | <a href="#">ntp server</a> , page A-32        |
| <a href="#">ping</a>                | 0                | Sends ICMP echo_request packets for diagnosing basic network connectivity.           | <a href="#">ping</a> , page A-34              |
| <a href="#">ps</a>                  | 15               | Shows running processes.                                                             | <a href="#">ps</a> , page A-35                |
| <a href="#">radiomanager</a>        | 15               | Enables/disables radio manager processes.                                            | <a href="#">radiomanager</a> , page A-35      |
| <a href="#">redundancy</a>          | 15               | Turns redundancy on or off, performs software upgrade on redundant cluster.          | <a href="#">redundancy</a> , page A-36        |
| <a href="#">reinitdb</a>            | 15               | Reinitializes database.                                                              | <a href="#">reinitdb</a> , page A-37          |
| <a href="#">reload</a> <sup>3</sup> | 15 <sup>1</sup>  | Reboots WLSE.                                                                        | <a href="#">reload</a> , page A-38            |
| <a href="#">repository</a>          | 15               | Manages local repository for installing software updates.                            | <a href="#">repository</a> , page A-38        |
| <a href="#">reset device-snmp</a>   | 15               | Resets WLSE's community string.                                                      | <a href="#">reset device-snmp</a> , page A-40 |

Table A-1 Command Summary (continued)

| Command                           | Privilege Level | Description                                                                                        | Reference                                     |
|-----------------------------------|-----------------|----------------------------------------------------------------------------------------------------|-----------------------------------------------|
| <a href="#">restore</a>           | 15              | Restores backed up configuration from the configured location.                                     | <a href="#">restore</a> , page A-41           |
| <a href="#">route</a>             | 15              | Adds a route.                                                                                      | <a href="#">route</a> , page A-42             |
| <a href="#">services</a>          | 15              | Manages WLSE services.                                                                             | <a href="#">services</a> , page A-42          |
| <a href="#">setup</a>             | 15              | Configure network parameters of WLSE Express                                                       | <a href="#">setup</a> , page A-43             |
| <a href="#">show auth-cli</a>     | 15              | Displays type of authentication used for secure CLI access.                                        | <a href="#">show auth-cli</a> , page A-44     |
| <a href="#">show auth-http</a>    | 15              | Displays type of authentication used for secure HTTP access.                                       | <a href="#">show auth-http</a> , page A-44    |
| <a href="#">show backupconfig</a> | 15              | Displays current backup/restore location.                                                          | <a href="#">show backupconfig</a> , page A-44 |
| <a href="#">show backuplog</a>    | 15              | Displays contents of backup log.                                                                   | <a href="#">show backuplog</a> , page A-45    |
| <a href="#">show bootlog</a>      | 15              | Displays messages logged during last system boot.                                                  | <a href="#">show bootlog</a> , page A-45      |
| <a href="#">show cdp neighbor</a> | 15              | Displays nearest neighbor on the network.                                                          | <a href="#">show cdp neighbor</a> , page A-46 |
| <a href="#">show cdp run</a>      | 15              | Displays Cisco Discovery Protocol (CDP) configuration.                                             | <a href="#">show cdp run</a> , page A-47      |
| <a href="#">show clock</a>        | 15              | Displays current UTC date and time.                                                                | <a href="#">show clock</a> , page A-47        |
| <a href="#">show config</a>       | 15              | Displays configuration.                                                                            | <a href="#">show config</a> , page A-48       |
| <a href="#">show daemonslog</a>   | 15              | Displays daemons log.                                                                              | <a href="#">show daemonslog</a> , page A-48   |
| <a href="#">show dmgtldlog</a>    | 15              | Displays daemon manager log.                                                                       | <a href="#">show dmgtldlog</a> , page A-49    |
| <a href="#">show domain-name</a>  | 15              | Displays domain name                                                                               | <a href="#">show domain-name</a> , page A-50  |
| <a href="#">show hosts</a>        | 15              | Displays host file.                                                                                | <a href="#">show hosts</a> , page A-50        |
| <a href="#">show http-server</a>  | 15              | Shows HTTP and HTTP access control information.                                                    | <a href="#">show http-server</a> , page A-51  |
| <a href="#">show import hosts</a> | 15              | Displays imported host files.                                                                      | <a href="#">show import hosts</a> , page A-51 |
| <a href="#">show install</a>      | 15              | Displays software updates and images available on configured repository and logs of installations. | <a href="#">show install</a> , page A-51      |
| <a href="#">show interfaces</a>   | 0               | Displays information about network interface.                                                      | <a href="#">show interfaces</a> , page A-53   |
| <a href="#">show ipchains</a>     | 15              | Displays IP chains for selected interface.                                                         | <a href="#">show ipchains</a> , page A-53     |
| <a href="#">show maillog</a>      | 15              | Displays mail log.                                                                                 | <a href="#">show maillog</a> , page A-54      |
| <a href="#">show mailroute</a>    | 15              | Displays SMTP mail server.                                                                         | <a href="#">show mailroute</a> , page A-55    |
| <a href="#">show proc[ess]</a>    | 0               | Displays information about processes running on WLSE.                                              | <a href="#">show proc[ess]</a> , page A-55    |
| <a href="#">show redundancy</a>   | 15              | Displays information about redundancy status and configuration.                                    | <a href="#">show redundancy</a> , page A-56   |
| <a href="#">show repository</a>   | 15              | Displays status or access log of configured repository.                                            | <a href="#">show repository</a> , page A-57   |

Table A-1 Command Summary (continued)

| Command                              | Privilege Level                                                        | Description                                                                 | Reference                                        |
|--------------------------------------|------------------------------------------------------------------------|-----------------------------------------------------------------------------|--------------------------------------------------|
| <a href="#">show route</a>           | 15                                                                     | Displays routes currently configured.                                       | <a href="#">show route</a> , page A-57           |
| <a href="#">show securitylog</a>     | 15                                                                     | Displays secure log information.                                            | <a href="#">show securitylog</a> , page A-58     |
| <a href="#">show snmp-server</a>     | 15                                                                     | Displays SNMP configuration.                                                | <a href="#">show snmp-server</a> , page A-59     |
| <a href="#">show ssh-server</a>      | 15                                                                     | Displays SSH access control information                                     | <a href="#">show ssh-server</a> , page A-59      |
| <a href="#">show ssh-version</a>     | 15                                                                     | Displays type of SSH enabled.                                               | <a href="#">show ssh-version</a> , page A-59     |
| <a href="#">show syslog</a>          | 15                                                                     | Displays syslog information.                                                | <a href="#">show syslog</a> , page A-60          |
| <a href="#">show tech</a>            | 15                                                                     | Displays information for Cisco's Technical Assistance Center.               | <a href="#">show tech</a> , page A-61            |
| <a href="#">show telnetenable</a>    | 15                                                                     | Displays Telnet status.                                                     | <a href="#">show telnetenable</a> , page A-61    |
| <a href="#">show time</a>            |                                                                        |                                                                             | <a href="#">show time</a> , page A-62            |
| <a href="#">show tomcatlog</a>       | 15                                                                     | Displays Tomcat log.                                                        | <a href="#">show tomcatlog</a> , page A-62       |
| <a href="#">show version</a>         | 0                                                                      | Displays information about current software installed on WLSE.              | <a href="#">show version</a> , page A-63         |
| <a href="#">show webaccesslog</a>    | 15                                                                     | Displays Web access log.                                                    | <a href="#">show webaccesslog</a> , page A-63    |
| <a href="#">show weberrorlog</a>     | 15                                                                     | Displays Web error log.                                                     | <a href="#">show weberrorlog</a> , page A-64     |
| <a href="#">show websslaccesslog</a> | 15                                                                     | Displays Web SSL log.                                                       | <a href="#">show websslaccesslog</a> , page A-65 |
| <a href="#">shutdown</a>             | 15                                                                     | Shuts down WLSE in preparation for powering it off.                         | <a href="#">shutdown</a> , page A-65             |
| <a href="#">snmp-server</a>          | 15                                                                     | Configures SNMP agent.                                                      | <a href="#">snmp-server</a> , page A-66          |
| <a href="#">ssh host</a>             | 15                                                                     | Connects to an external host by using SSH.                                  | <a href="#">ssh host</a> , page A-67             |
| <a href="#">ssh-server accept</a>    | 15                                                                     | Controls SSH access.                                                        | <a href="#">ssh-server accept</a> , page A-67    |
| <a href="#">ssh-version</a>          | 15                                                                     | Enables Secure Shell (SSH) 1, SSH 2, or both SSH 1 and SSH 2.               | <a href="#">ssh-version</a> , page A-68          |
| <a href="#">tarlog</a>               | 15                                                                     | Tars log files.                                                             | <a href="#">tarlog</a> , page A-68               |
| <a href="#">telnet</a>               | 15                                                                     | Telnets to an external host.                                                | <a href="#">telnet</a> , page A-68               |
| <a href="#">telnetenable</a>         | 15                                                                     | Configures Telnet access.                                                   | <a href="#">telnetenable</a> , page A-69         |
| <a href="#">tftpserver</a>           | 15                                                                     | Allows the TFTP server to be used for general purposes (WLSE Express only). | <a href="#">tftpserver</a> , page A-70           |
| <a href="#">traceroute</a>           | 0                                                                      | Displays route to specified host and identifies faulty gateways.            | <a href="#">traceroute</a> , page A-70           |
| <a href="#">username</a>             | 15                                                                     | Creates new user account or changes account properties.                     | <a href="#">username</a> , page A-71             |
| <a href="#">webtimeout</a>           | 15                                                                     | Changes session timeout for the Web interface.                              | <a href="#">webtimeout</a> , page A-72           |
| <a href="#">wlseconfig</a>           | <i>Do not use this command. This command is for internal use only.</i> |                                                                             |                                                  |

1. This command is also available in the maintenance image.
2. This command is available only in the maintenance image.
3. This command is also available in the maintenance image.



# CLI Command Details

This section provides an alphabetical listing of all CLI commands, along with options, examples, and usage guidelines.



## Note

The maintenance image includes a small set of CLI commands. For information on these commands, see [Maintenance Image Commands, page A-73](#).

## aaa-server

The aaa-server CLI commands are available on the WLSE Express only. For information on these CLI commands, see [Chapter 18, “Using the Internal AAA Server \(WLSE Express Only\).”](#)

## apptyp

Use this command to show the type of WLSE hardware.

**apptyp**

## Example

This command shows that the WLSE is an 1130:

```
apptyp
1130
```

## auth

Use this command to enable secure authentication through a remote authentication server.

```
auth { cli | http } { local | tacacs { failover | nofailover | local } secret server1 [server2] | radius {
failover | nofailover | local } secret server1[:port] [server2[:port]] }
```

## Syntax Description

|              |                                                                                                                                                     |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>cli</b>   | Enables authentication when using the CLI.<br><b>Note</b> If you use CLI remote authentication, you must create a local user on the WLSE.           |
| <b>http</b>  | Enables authentication when using HTTP.<br><b>Note</b> When you use HTTP authentication, you do <i>not</i> need to create a local user on the WLSE. |
| <b>local</b> | Enables local authentication.                                                                                                                       |

|                   |                                                                                                                                                                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>tacacs</b>     | Enables authentication using TACACS+ (Terminal Access Controller Access Control System).<br><b>Note</b> If you select this module, only the users configured on the TACACS+ server and the <a href="#">admin</a> user can log into the WLSE. |
| <b>radius</b>     | Enables authentication using RADIUS (Remote Dial-In User Service).                                                                                                                                                                           |
| <b>failover</b>   | If remote authentication server becomes unreachable, use local authentication.                                                                                                                                                               |
| <b>nofailover</b> | Use remote authentication only.<br><br><b>Caution</b> If remote authentication server goes down, no one will be able to log in.                             |
| <b>local</b>      | Use either remote or local authentication.                                                                                                                                                                                                   |
| <i>secret</i>     | Shared secret code of server.                                                                                                                                                                                                                |
| <i>server1</i>    | IP address or device name of server from which authentication will occur.                                                                                                                                                                    |
| <i>server2</i>    | IP address or device name of optional secondary server from which authentication could occur.                                                                                                                                                |
| <i>port</i>       | Optional port number of RADIUS authentication server.                                                                                                                                                                                        |

## Example

This command enables secure remote authentication from a remote server using TACACS.

```
auth http tacacs tr5e43 209.165.200.224
```

## Related Commands

[show auth-cli](#), page A-44

[show auth-http](#), page A-44

# backup

Use this command to back up the WLSE.

```
backup [test]
```

## Syntax Description

|             |                                                                      |
|-------------|----------------------------------------------------------------------|
| <b>test</b> | Tests configured backup hostname, username, password, and directory. |
|-------------|----------------------------------------------------------------------|

## Usage Guidelines

The **backup** command backs up the WLSE configuration to the location specified by the **backupconfig** command.

## Example

A typical backup proceeds as follows:

1. Run **backupconfig** (see [backupconfig, page A-9](#)) to specify the location for storing the backups.
2. Run **backup test** to make sure the credentials specified in **backupconfig** and the user can write to the target location:

```
admin@sj-wlse:backup test
test OK
```

The **backup test** command creates a small file called test.tar at the target location under a sub-directory of BACKUP (the default directory created by the backup process). If the backup test does not return OK, the backup command will fail.

3. Run the **backup** command to start the backup process. Depending upon the amount of data, this can take a few minutes. Do not interrupt the process:

```
admin@sj-wlse:backup
backupfile: sj-wlse_02142004_222801.taraa
sj-wlse_02142004_222801.inf
admin@sj-wlse
```

The backup process creates a .taraa file and .inf file named for the WLSE hostname and the date and time of the backup.

4. Log in to the backup location system and verify that there is a backup directory under the BACKUP/WLSE hostname\_date\_time subdirectory and that it contains the two files created by the backup process.

## Related Commands

[backupconfig, page A-9](#)

[listbackup, page A-28](#)

[restore, page A-41](#)

[show backupconfig, page A-44](#)

## backupconfig

Use the **backupconfig** command to specify the location for all backup and restore operations. To delete the backup configuration, use the **no backupconfig** command.

**backupconfig** *hostname username password* { **FTP** | **SCP** } [*timeout* [ *directory* ] ]

**no backupconfig**

## Syntax Description

|                 |                                                    |
|-----------------|----------------------------------------------------|
| <i>hostname</i> | Host name or IP address of the backup host system. |
| <i>username</i> | Username of the backup host system.                |
| <i>password</i> | Password of the backuphost system.                 |

|                  |                                                                                                                                                                                              |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FTP SCP</b>   | Protocol to use for transferring the backup to the backup host system: <ul style="list-style-type: none"> <li>FTP (File Transfer Protocol)—the default</li> <li>SCP (Secure Copy)</li> </ul> |
| <i>timeout</i>   | Optional timeout value for backup restore jobs. Allowed values are 3600 to 43200 seconds (default = 7200 seconds).                                                                           |
| <i>directory</i> | Optional path to specific backup directory, if different from user's default directory.<br><b>Note</b> If you specify a <i>directory</i> , you must also supply a <i>timeout</i> value.      |

## Usage Guidelines

If you are using SCP for file transfer, the WLSE stores a shared key for the remote host. If the key changes on the remote host, files cannot be transferred. To clear the key and allow the WLSE to use the new key, use the **clearbackuphosts** command.

## Example

The following command causes all backup and restore operations to use the host with IP address 209.165.200.224, username user1, and password pass:

```
backupconfig 209.165.200.224 user1 pass
```

The following command clears all backup and restore configuration information:

```
no backupconfig
```

## Related Commands

[backup, page A-8](#)

[clearbackuphosts, page A-11](#)

[listbackup, page A-28](#)

[restore, page A-41](#)

[show backupconfig, page A-44](#)

# cdp

Use the **cdp** command to configure the Cisco Discovery Protocol (CDP). Allows the WLSE to recognize, and be recognized by, other Cisco devices.

```
cdp run { [interface] | timer seconds | holdtime seconds }
```

```
no cdp { run [interface] | timer | holdtime }
```

## Syntax Description

|              |                                                                                                |
|--------------|------------------------------------------------------------------------------------------------|
| <b>run</b>   | Starts the WLSE sending out CDP signals to other devices.                                      |
| <b>timer</b> | Set CDP packet retransmission time, the amount of time, in seconds, that CDP signals are sent. |

|                  |                                                                                                                                                                                                                                                                                                                                              |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>holdtime</b>  | Set CDP packet information hold time, the amount of time a device will recognize another device without receiving a signal. For example, if your system's holdtime is set to 30 seconds, and another device that has already been recognized by yours does not send a signal within that 30 seconds, your system will cease to recognize it. |
| <i>interface</i> | Ethernet port on which CDP will be enabled. Acceptable range of values is eth0-eth5. On the WLSE 1130, eth0 corresponds to the port labeled A on the back panel, and eth1 corresponds to the port labeled B.                                                                                                                                 |
| <i>seconds</i>   | Amount of time, in seconds, that the system takes to either transmit the CDP packet information or to hold another system's CDP packet information.                                                                                                                                                                                          |

### Usage Guidelines

After you use the **no cdp** command, the **timer** and **holdtime** values are set to their default values.

### Example

This command sets the CDP packet's retransmission time at 10 seconds:

```
cdp timer 10
```

This command sets the CDP packet's retransmission to its default time.

```
no cdp timer
```

### Related Commands

[show cdp run, page A-47](#)

## clear

Use this command to clear the terminal settings for the shell.

```
clear
```

## clearbackuphosts

Use this command to clear the stored key when using SCP for backups.

### Syntax

```
clearbackuphosts
```

### Usage Guidelines

When you use SCP to transfer backup files to a remote host, the WLSE stores keys to identify the remote hosts. If the key on a remote host changes, the backup files cannot be transferred. This command clears the stored keys and allows the WLSE to store a new key.

## Related Commands

[backupconfig](#), page A-9

# clearvar

Use this command to delete old log and core files from the /var partition.

**clearvar**

## Usage Guidelines



### Caution

This command stops all services on the WLSE before purging old log files. Upon completion, the command restarts all services.

The normal operation of the WLSE does not delete backup logs; it overwrites them. However, the **clearvar** command does delete backup files. It also deletes other files (var\_logs\_tgz, logs\_tgz, etc.) which are created by commands such as dumptech, etc.



### Note

The WLSE automatically performs a rollover of logs which can cause backups to be overwritten. For example, if the file redundancy.log grows too large (default 10000 lines), then the WLSE's automatic rollover mechanism will rename the current file to redundancy.log\_backup, and create a new file called redundancy.log. When the new file is filled up, the process repeats. This means that the new redundancy.log file is copied over as redundancy.log\_backup, and the previous contents of redundancy\_backup.log are overwritten, and therefore lost.

# clock set

Use this command to set the system date and time. See the following usage guidelines before using this command.

**clock set** { *hh:mm:ss month day year* }

## Syntax Description

|                 |                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------|
| <b>set</b>      | Sets the system clock.                                                                                |
| <i>hh:mm:ss</i> | Current time (for example, 13:32:00).                                                                 |
| <i>month</i>    | Current month, as full month name or at least the first 3 characters of the month (for example, jan). |
| <i>day</i>      | Day of the month (1 to 31).                                                                           |
| <i>year</i>     | Current year (for example, 2000).                                                                     |

## Usage Guidelines

When setting the system time, set the time to UTC.

When resetting the time, you must stop and restart WLSE services. Otherwise, scheduled configuration and firmware jobs will not run properly.

To reset the time:

- 
- Step 1** Stop services:  
**services stop**
- Step 2** Change the time.
- Step 3** Start services:  
**services start**
- 

If you configure the system to use Network Time Protocol (NTP), you do not need to set the system clock manually using the **clock** command. When setting the clock, enter the current time in Coordinated Universal Time (UTC).

For more information about the system time, see the [Understanding WLSE Time Displays, page 1-10](#).

### Example

This command sets the date and time:

```
clock set 16:00:00 dec 11 2001
```

```
Tue Dec 11 16:00:00 UTC 2001
```

### Related Commands

[ntp server, page A-32](#)

[clock set, page A-12](#)

## debug

Use this command to enable or disable debugging mode, which displays detailed information when parsing CLI commands.

### Syntax

```
debug
```

### Example

When debug is enabled, the output of the **df** command is:

```
admin@wlse1:df
DEBUG:linePtr=---df---
DEBUG:execStrPtr=---/opt/appliance/enable/df ---
DEBUG:Command /opt/appliance/enable/df
Token: /opt/appliance/enable/df
Token: (null)
DEBUG: progArgV /opt/appliance/enable/df
DEBUG: progArgV (null)
Filesystem Size Used Avail Use% Mounted on
```

```

/dev/hda12 298M 111M 187M 38% /
/dev/hda1 53M 14M 36M 27% /boot
/dev/hda7 2.7G 1.3M 2.5G 1% /extra
/dev/hda11 596M 33M 564M 6% /home
/dev/hda6 2.8G 278M 2.5G 10% /opt
none 1.5G 0 1.4G 0% /dev/shm
/dev/hda5 1.9G 33M 1.8G 2% /tftpboot
/dev/hda9 596M 33M 563M 6% /tmp
/dev/hda10 571M 254M 288M 47% /usr
/dev/hda13 27G 502M 26G 2% /var
DEBUG:Error returned from command: 19
DEBUG:arg 0:/opt/appliance/enable/df
DEBUG:/opt/appliance/enable/df

```

## df

Use this command to display the current storage usage on the WLSE.

### df

### Usage Guidelines

This command is intended as a debugging tool for problems with full partitions.

### Example

The following command displays the current storage usage on the WLSE:

```

df
Filesystem Size Used Avail Use% Mounted on
/dev/sda12 151M 59M 92M 39% /
/dev/sda1 49M 2.8M 44M 6% /boot
/dev/sda7 985M 24M 911M 3% /extra
/dev/sda8 601M 32M 569M 5% /home
/dev/sda6 1001M 136M 865M 14% /opt
/dev/sda13 9.7G 32M 9.7G 0% /tftpboot
/dev/sda9 601M 32M 569M 5% /tmp
/dev/sda10 591M 212M 350M 38% /usr
/dev/sda5 2.9G 450M 2.5G 15% /var

```

### Related Commands

[fsck, page A-73](#)



## diagnostic-info

Use this command to gather diagnostic information and place the information in the diagnostic-info.log file.

### Syntax Description

**diagnostic-info**

### Usage Guidelines

You can view and download the diagnostic-info.log file by selecting **Admin > Appliance > View Log File**.

## dumpcores

Use this command to check for core files, tar and compress these files into /var/adm/CSCOets/logdumpcores.tgz, and ftp or scp the .tgz file to the specified host and directory.

**dumpcores** *username remote-host remote-directory* [ **ftp** | **scp** ]

### Syntax Description

|                         |                                                                                                                                                                                              |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>username</i>         | The user name (required to access the FTP- or SCP-accessible host).                                                                                                                          |
| <i>remote-host</i>      | The name of the FTP- or SCP-accessible host.                                                                                                                                                 |
| <i>remote-directory</i> | The directory in which to save the file on the FTP- or SCP-accessible host.                                                                                                                  |
| <b>ftp</b>   <b>scp</b> | The protocol to use when transferring the log file to the host system: <ul style="list-style-type: none"> <li>FTP (File Transfer Protocol)</li> <li>SCP (Secure Copy)—the default</li> </ul> |

### Usage Guidelines

The dumpcores command will prompt for the host's password before transferring the file.

### Example

```
admin@app3:dumpcores foo foo-pc /home/foo
Core files found. Continue? (Y/N): Y
foo@foo-pc's password:
dumpcores.tgz 100% 111 0.1KB/s 00:00
admin@app3:
```

## dumptcp

Use this command to display TCP/IP network protocol packet content.

```
dumptcp proto { snmp snmp-trap ip icmp tcp udp | port port }
[interface eth[ernet]0 ... 5] [host host [host2 host2]]
[packets packets] [log]
```

### Syntax Description

|                           |                                                                                                                                                                                                                                                                       |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>proto</b>              | Name of protocol. Enter <b>snmp</b> , <b>snmp-trap</b> , <b>ip</b> , <b>icmp</b> , <b>tcp</b> , or <b>udp</b> to specify the protocol for which you want to view the packet content. You must specify either a protocol or a port.                                    |
| <b>port</b>               | Use the port number to specify the protocol to observe, instead of specifying the protocol name. You must specify either a protocol or a port.                                                                                                                        |
| <i>port</i>               | Port number.                                                                                                                                                                                                                                                          |
| <b>interface eth[0-5]</b> | The interface to observe. On the WLSE 1130, eth0 corresponds to the port labeled A on the back panel, and eth1 corresponds to the port labeled B.                                                                                                                     |
| <b>host, host2</b>        | The host(s) to observe.                                                                                                                                                                                                                                               |
| <i>host</i>               | The host name(s).                                                                                                                                                                                                                                                     |
| <b>packets packets</b>    | Maximum number of packets to be captured (up to 10,000).                                                                                                                                                                                                              |
| <b>log</b>                | Logs the output of the command in a file in a dumptcp.cap file. You can retrieve the file from the web interface— <b>Admin &gt; Appliance &gt; Status &gt; View Log File</b> . Use a utility such as tcpdump or Ethereal to view the file, which is in binary format. |

### Usage Guidelines

You can either specify a protocol by name or specify a port; you must specify one or the other. Optionally, you can specify the interface and specify one or two hosts to observe.

The command allows you to continuously observe the packets. Enter **Ctrl C** to terminate the command.

### Examples

The following command listens displays the SNMP packets in the interface:

```
dumptcp proto snmp interface eth0
```

The following command listens to packets from port 161 only with abc.com as either the source or destination host:

```
dumptcp port 161 host abc.com
```

The following command limits the capture to 1000 packets:

```
dumptcp proto tcp packets 1000
```

### Related Commands

[interface, page A-25](#)

## dumptech

Use this command for diagnostic purposes. It calls the **diagnostic-info** and **tarlog** commands and sends the output via **SCP** (secure copy) to a user on a remote host. The output is saved in the dumptech.tgz file in the specified directory. The dumptech.tgz file can also be downloaded from **Admin > Appliance > Status > View Log Files**.

This command is useful for getting the files to an FTP server when the Web interface is not accessible.

**dumptech** *username remote-host remote-directory*

### Syntax

|                         |                                                      |
|-------------------------|------------------------------------------------------|
| <i>username</i>         | Name of the user on the remote host.                 |
| <i>remote-host</i>      | Name or IP address of the remote host.               |
| <i>remote-directory</i> | Name of the directory in which to save the log file. |

### Usage Guidelines and Examples

The correct usage of the **dumptech** command and the output displayed during the transfer process is shown in the following examples.

In the first case, the user has a valid SCP server setup and can access the file from the specified directory on the FTP server or from the WLSE Web interface.

```
dumptech userA hostA /users/userA
cmd=/opt/appliance/scripts/dumptech.sh userA@hostA:/users/userA
The authenticity of host 'hostA (209.165.200.11)' can't be established.
RSA key fingerprint is 8b:b0:41:00:d5:e4:7a:66:d3:b3:c2:47:f9:1b:7c:38.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'hostA (209.165.200.11)' (RSA) to the list of known hosts.
userA@hostA's password: password
dumptech.tgz 100% |*****| 691 KB 00:01
```

If you do not have an SCP server or do not know whether your FTP server supports SCP, you can enter non-existent parameters, as shown in the following example. In this case, you can access the file from the WLSE Web interface.

```
dumptech nouser nowhere /nodirectory
cmd=/opt/appliance/scripts/dumptech.sh nouser@nowhere:/nodirectory
ssh: nowhere: Name or service not known
lost connection
```

### Related Commands

[diagnostic-info](#), page A-15

[tarlog](#), page A-68

## erase config

Use this command to erase the configuration in flash memory and reload the WLSE with its default settings.

## erase config

### Syntax Description

This command has no arguments or keywords.

### Usage Guidelines

When you enter the command, you are prompted for confirmation. Enter **yes** to confirm, or press **Enter** to accept the default response **no**.



#### Caution

When you confirm this command, the system configuration in flash memory is set to the defaults and the system reboots automatically. The system will not operate until you reconfigure it.

When the system reboots, you must reconfigure it. For information about configuring the basic network settings, see the relevant *Installation and Configuration Guide* for your WLSE on Cisco.com at [http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw\\_1105/wlse/2\\_12/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm).

The results of running this command are:

1. All settings in flash memory are erased.
2. The default settings are restored to flash memory. This includes setting all Ethernet interfaces to “down” and setting **firewall private** for all interfaces
3. The WLSE shuts down and restarts.

### Example

This command erases the system configuration:

```
erase config
```

```
This will erase your configuration, return device to factory defaults, and reload the device
```

```
Do you want to continue?[no]:yes
```

## exit

Use this command to log out of the CLI command interface.

```
exit
```

### Syntax Description

This command has no arguments or keywords.

### Example

The following command logs you out of the system:

```
exit
```

## firewall

Use this command to configure port access for each interface. This command provides flexibility in securing the WLSE. The WLSE can be configured for secure or public network environments. In previous releases, the **http** argument was **1741**, and **1741** is allowed in this release for backward compatibility; for more information, see the **Syntax Description** for **http**.

```
firewall eth[ernet]0-5 { [public | private] |
[icmp | telnet | ssh | snmp | https | http | tftp | REPOSITORY NONE] }
```

### Syntax Description

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>eth [0-5]</b>  | Interface to be configured. Acceptable values are eth0-eth5. On the WLSE 1130, eth0 corresponds to the port labeled A on the back panel, and eth1 corresponds to the port labeled B.                                                                                                                                                                                                                                                             |
| <b>public</b>     | Denies access via Internet Control Message Protocol (ICMP), Telnet, SNMP, TFTP, and REPOSITORY.<br>Allows access via SSH, HTTPS, and HTTP.                                                                                                                                                                                                                                                                                                       |
| <b>private</b>    | No access is denied.<br>Allows connections via ICMP, Telnet, SSH, SNMP, HTTPS, and HTTP.                                                                                                                                                                                                                                                                                                                                                         |
| <b>icmp</b>       | Ignores ICMP ping messages. With this option set, the WLSE will not respond to external ICMP ping messages but you will still be able to use <b>traceroute</b> and <b>ping</b> commands.                                                                                                                                                                                                                                                         |
| <b>telnet</b>     | Ignores incoming Telnet connections.                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>ssh</b>        | Ignores incoming SSH connections.                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>snmp</b>       | Ignores incoming SNMP requests.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>https</b>      | Denies all connections to the SSL HTTP port used by the SSL Web interface.                                                                                                                                                                                                                                                                                                                                                                       |
| <b>http</b>       | Denies all connections to the HTTP port used by the Web interface. This is the port that is configured for HTTP access; it could be port 80 or port 1741, depending on the configuration. The default port is 1741; you can change this by using the <b>http-server port port</b> command.<br><br><b>Note</b> Instead of the <b>http</b> argument, you can use <b>1741</b> . This option is provided for backward compatibility in this release. |
| <b>tftp</b>       | Ignores all connections to the TFTP host.                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>REPOSITORY</b> | Prevents access to the the local software repository from the network. Ignores all connections to WLSE port 9851.                                                                                                                                                                                                                                                                                                                                |
| <b>NONE</b>       | Accepts all connections.                                                                                                                                                                                                                                                                                                                                                                                                                         |

### Usage Guidelines

To configure an Ethernet port for secured public access, use the **public** option.

To configure an Ethernet port for local access, via a LAN or VLAN, use the **private** option.

To disable ICMP, Telnet, SSH, SNMP, HTTPS, or to deny connections to the SSL HTTP port or the HTTP 1741 port, use the corresponding option.

## Example

The following is an example of a secure Ethernet port configuration:

- Ethernet port 0 is connected to the Internet, and is configured to be accessible only via HTTPS by entering:

```
firewall eth0 public ssh 1741
```

- Ethernet port 0 is connected to an internal LAN or VLAN, and is configured to be accessible via any of the supported protocols by entering:

```
firewall eth0 private
```

An on-site user has full access to the WLSE, but an external user can only access it using a secure connection.

## Related commands

[show interfaces, page A-53](#)

[interface, page A-25](#)

[http-server, page A-21](#)

# gethostbyname

Use this command to display the IP address of a known hostname.

```
gethostbyname host
```

## Syntax Description

|      |                      |
|------|----------------------|
| host | Domain name of host. |
|------|----------------------|

## Example

This command displays the IP address of example.com

```
gethostbyname example.com
209.165.200.224
```

# help

Use this command to display help for all of the CLI commands.

## hostname

Use this command to change the system host name.

**hostname** *name*

### Syntax Description

|             |                                                                                                                                                                |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i> | New hostname for the WLSE. The name is case-sensitive and may be from 1 to 24 alphanumeric characters (A-Z, a-z, 0-9), the minus sign (-), and the period (.). |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

The following example changes the hostname to sandbox:

```
hostname sandbox
```

## http-server

Use this command to control:

- HTTP and HTTPS access to the WLSE by specifying the IP addresses from which connections are accepted. The default behavior is to accept all connections. If you specify IP addresses, connections are only accepted from matched addresses. The **no** form of the command removes an address.
- The port used for HTTP access.

```
http-server accept ip_address [netmask] | port { 80 | 1741 }
```

```
no http-server accept ip_address [netmask]
```

```
http-server port { 80 | 1741 }
```

### Syntax Description

|                                         |                                                                                                                                        |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>accept</b> <i>ip_address netmask</i> | An address and optional netmask from which connections are accepted or an address and optional netmask to remove from the access list. |
| <b>port</b> { 80   1741 }               | Port to use for HTTP access.                                                                                                           |

### Usage Guidelines

You can add one address per command line.

The **no** form of the command removes HTTP/HTTPS access one address at a time. The **no** form of the command must exactly match the rule it is deleting.

In a redundant cluster of WLSEs, if you are using an HTTP/HTTPS access list, you must enter a command on each WLSE to allow access by the other WLSE in the cluster.

## Example

To accept HTTP and HTTPS connections from the host 192.168.12.12 with the netmask 255.255.255.0:

```
http-server accept 192.168.12.12 255.255.255.0
```

To use port 80 for HTTP access instead of the default port 1741:

```
http-server port 80
```

## Related Commands

[firewall, page A-19](#)

[show http-server, page A-51](#)

# import

Use this command to add a single host for IP address mapping or import a UNIX-style hosts file from a remote FTP server.

**import host** *hostname ipaddress*

**no import host** *hostname ipaddress*

**import hosts** *ftp-host username password pathname*

**no import hosts**

## Syntax Description

|                  |                                                    |
|------------------|----------------------------------------------------|
| <b>host</b>      | Imports a single hostname mapped to an IP address. |
| <i>hostname</i>  | Hostname to import.                                |
| <i>ipaddress</i> | IP address to map hostname to.                     |
| <b>hosts</b>     | Imports host file from an FTP-accessible host.     |
| <i>password</i>  | Password used to access an FTP-accessible host.    |
| <i>pathname</i>  | Path to the file to be imported.                   |
| <i>ftp-host</i>  | IP address or hostname of the FTP-accessible host. |
| <i>username</i>  | username use to access the FTP-accessible host.    |

## Usage Guidelines

To import a single host:

**import hosts** *hostname ipaddress*

To import host files from an external, FTP- accessible server:

**import hosts** *ftp-host username password path*

To remove an individual IP address from the imported host file:

**no import host** *hostname ipaddress*



To remove an imported host file:

**no import hosts**

## Example

The following command imports host files from the FTP- accessible server ftpserver\_1. Ftpserver\_1 has the username admin, the password pass, and the path /ftpserver\_1/hosts.

```
import hosts ftpserver_1 admin pass /ftpserver_1/hosts
```

The following command deletes the hosts imported in the example above:

```
no import hosts
```

## Related Commands

[show import hosts, page A-51](#)

# install

Use this interactive command to install software updates on the WLSE.

**install configure** { **URL** *URL* | **default** | **save** }

**install update** *package*

**install list** [ **all** | **full** | **page** | **updates** ]

**install current**

**install help**



### Caution

Before upgrading WLSE software, check the readme.txt file associated with the software image. You can find this file along with the software image in the Software Center on Cisco.com.

## Syntax Description

|                  |                                                                                                                             |                                                                                                                       |
|------------------|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>configure</b> | Defines the repository from which to install software updates or complete images. A repository is a remote or local server. |                                                                                                                       |
|                  | <b>URL</b>                                                                                                                  | Sets the URL of the repository. Only HTTP is supported.                                                               |
|                  | <i>URL</i>                                                                                                                  | The URL of the repository. The URL should take the form of <code>http://host:port/path</code> (the path is optional). |
|                  | <b>default</b>                                                                                                              | Configures the WLSE to be its own repository. The URL is <code>http://localhost:9851</code> .                         |
|                  | <b>save</b>                                                                                                                 | Saves the current configuration in the install.ini file.                                                              |
| <b>update</b>    | Installs the specified software update package.                                                                             |                                                                                                                       |
|                  | <i>package</i>                                                                                                              | Name of an installable update package                                                                                 |

|                |                                                              |                                                                                                                                                                                                                                                                                                                        |
|----------------|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>current</b> | Lists the currently installed packages on the WLSE.          |                                                                                                                                                                                                                                                                                                                        |
| <b>list</b>    | Lists software updates and images on the defined repository. |                                                                                                                                                                                                                                                                                                                        |
|                | <b>all</b>                                                   | Lists all software on the defined repository. This command displays software name, version, requirements, type, and summary information.                                                                                                                                                                               |
|                | <b>full</b>                                                  | Lists only the complete images on the defined repository. Displays name of image, version, requirements, type, and summary information                                                                                                                                                                                 |
|                | <b>page</b>                                                  | Displays first page of command output. To display more: <ul style="list-style-type: none"> <li>Press the Return key to display the next line of output.</li> <li>Press the Space bar to display the next screen of output</li> </ul> Press <b>q</b> or <b>Q</b> to exit paged output and return to the command prompt. |
|                | <b>updates</b>                                               | Lists only the updates on the configured repository. Displays software name, version, requirements, type, and summary information                                                                                                                                                                                      |
| <b>exit</b>    | Exit from interactive use of the <b>install</b> command.     |                                                                                                                                                                                                                                                                                                                        |

## Usage Guidelines

The **install** command is designed as an interactive command, although you can use it in non-interactive mode. For example, to list the images on the repository in interactive mode:

```
wlse-1130: install
install: list all
```

To exit from interactive mode, type **exit**.

To list the images on the repository in non-interactive mode:

```
wlse-1130: install list all
```

## Examples

The following command configures the WLSE to use port 9851 on the system with IP address 209.165.200.22, as the repository:

```
wlse-1130: install
Install URL not configured
install: configure URL http://209.165.200.224:9851
```

The following command installs the update package named WLSE-2.0:

```
install: update WLSE-2.0
```

The following command lists all software updates in the repository:

```
install: list all
```

| Name        | Version | Requires | Type     | Summary                   |
|-------------|---------|----------|----------|---------------------------|
| WLSE-2.7.1  | 2.7.1   | WLSE-2.7 | UPDATE   | Wireless LAN Solution ... |
| WLSE-2.7u   | 2.7     | WLSE-2.0 | UPDATE   | Wireless LAN Solution ... |
| WLSE-2.5FCS | 2.5     | WLSE-2.0 | UPDATE   | Wireless LAN Solution ... |
| WLSE-2.0.2  | 2.0.2   | WLSE-2.0 | UPDATE   | Wireless LAN Solution ... |
| WLSE-2.0    | 2.0     |          | COMPLETE | Wireless LAN Solution ... |

The following command lists all the packages and patches currently installed on the WLSE:

```
wlse-1130:install current
URL=http://209.165.200.224:9851
Initializing install: Success
```

| Name        | Version | Requires    | Type     | Summary                   |
|-------------|---------|-------------|----------|---------------------------|
| WLSE-2.7.1  | 2.7.1   | WLSE-2.7    | UPDATE   | WLSE 2.7.1 Upgrade        |
| WLSE-2.7u   | 2.7     | WLSE-2.0    | UPDATE   | WLSE 2.7 Upgrade          |
| WLSE-2.5a   | 2.5a    | WLSE-2.5FCS | UPDATE   | Wireless Lan Solution ... |
| WLSE-2.5FCS | 2.5     | WLSE-2.0    | UPDATE   | WLSE 2.5FCS Upgrade       |
| WLSE-2.0.2  | 2.0.2   | WLSE-2.0    | UPDATE   | WLSE 2.0.2 Upgrade        |
| WLSE-2.0a   | 2.0a    | WLSE-2.0    | UPDATE   | Wireless Lan Solution ... |
| WLSE-2.0    | 2.0     |             | COMPLETE | WLSE Solution Engine      |

## Related Commands

[repository](#), page A-38

[show install](#), page A-51

[show version](#), page A-63

## interface

Use this command to configure an Ethernet interface.

**interface eth[ernet][0-5] { up | down }**

**interface eth[ernet][0-5] dhcp**

**interface eth[ernet][0-5] *ipaddress netmask* [ default-gateway address ]**  
**[ up | down ] [ auto | speed [ 10 | 100 | 1000 ] duplex [ half | full ]**  
**[ mtu 46-1500 ]**

## Syntax Description

|                        |                                                                                                                                                                                                                                                                                                                                             |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>eth[0-5]</b>        | Name of the interface port to be configured. Acceptable values are eth0-eth5. On the WLSE 1130, eth0 corresponds to the port labeled A on the back panel, and eth1 corresponds to the port labeled B.                                                                                                                                       |
| <b>up</b>              | Enables the interface (the default).<br><br><b>Note</b> If you include the <i>ipaddress</i> parameter and want to enable the interface in the same command, either enter the <b>up</b> parameter after <i>ipaddress</i> and its required parameters, or do not specify the <b>up</b> or <b>down</b> parameters ( <b>up</b> is the default). |
| <b>down</b>            | Disables the interface. If you include the <i>ipaddress</i> parameter and want to disable the interface in the same command, enter the <b>down</b> parameter after <i>ipaddress</i> and its required parameters.                                                                                                                            |
| <b>dhcp</b>            | The WLSE acquires network information from a DHCP server. This is the default setting on the WLSE Express (WLSE 1030 hardware).                                                                                                                                                                                                             |
| <i>ipaddress</i>       | The IP address of the interface. When changing the WLSE's IP address, append the <b>up</b> option to the command line.                                                                                                                                                                                                                      |
| <i>netmask</i>         | The netmask of the interface IP address.                                                                                                                                                                                                                                                                                                    |
| <b>default-gateway</b> | The IP address of the default gateway that connects the WLSE to the network.                                                                                                                                                                                                                                                                |
| <i>address</i>         | The default gateway IP address.                                                                                                                                                                                                                                                                                                             |

|                           |                                                          |
|---------------------------|----------------------------------------------------------|
| <b>up</b>                 | See the preceding description of <b>up</b> .             |
| <b>down</b>               | See the preceding description of <b>down</b> .           |
| <b>auto</b>               | Allow the interface speed to be set automatically.       |
| <b>speed</b>              | Set the interface speed to 10, 100, or 1000 megabits.    |
| <b>duplex half   full</b> | Set interface to half-duplex or full-duplex mode.        |
| <b>mtu 46-1500</b>        | Set the maximum packet size within this range, in bytes. |

## Usage Guidelines

When you enter the **interface** command, the interface that you specify is enabled by default. If you want to disable an enabled interface or leave a disabled interface disabled, you must specify the **down** option.

If the interface is down when you change the IP address or hostname, append **up** to the command line. If the interface is up, append **down** to the command line. For example:

```
interface eth0 209.165.201.8 255.255.255.224 default-gateway 209.165.201.1 up
```

## Example

The following command disables the Ethernet 1 interface:

```
interface eth1 down
```

The following command sets the Ethernet 0 IP address, netmask, and gateway IP address:

```
interface eth0 209.165.200.224 255.255.255.224 default-gateway 209.165.201.31 up
```

## Related Commands

[show interfaces, page A-53](#)

## ip domain-name

Use this command to define a default domain name. To remove the default domain name, use the **no** form of the command.

A default domain name allows the system to resolve any unqualified host names. Any IP hostname that does not contain a domain name will have the configured domain name appended to it. If you are using a DNS server, this appended name is resolved by the DNS server, and then added to the host table.

**ip domain-name** *name*

**no ip domain-name** *name*

## Syntax Description

|             |                                       |
|-------------|---------------------------------------|
| <i>name</i> | Domain name (for example, cisco.com). |
|-------------|---------------------------------------|

## Example

This command defines the default domain name to be cisco.com:

```
ip domain-name cisco.com
```

This command removes the default domain name abc.com:

```
no ip domain-name abc.com
```

## Related Commands

[show domain-name, page A-50](#)

[ip domain-name, page A-26](#)

## ip name-server

Use this command to specify the addresses of up to three name servers for name and address resolution. To remove a name server, use the **no** form of the command.

```
ip name-server ip-address
```

```
no ip name-server ip-address
```

## Syntax Description

|                   |                                        |
|-------------------|----------------------------------------|
| <i>ip-address</i> | Name server IP address (maximum of 3). |
|-------------------|----------------------------------------|

## Usage Guidelines

Use the **ip name-server** command to point the WLSE to a specific DNS server. You may configure up to three servers. If you attempt to configure a fourth name server, the following error message appears:

```
Name-server table is full.
```

The WLSE must be able to contact a functional DNS server to operate correctly. If it does not, in most cases it will not correctly process requests from management applications that use it. If the system cannot obtain DNS services from the network, Telnet connections to the system will fail or Telnet interaction with the system will become extremely slow.

## Example

This command assigns a name server for the system to use for name-to-address resolution:

```
ip name-server 209.165.200.224
```

This command disables the name server; the system will not use it for name-to-address resolution:

```
no ip name-server 209.165.200.224
```

## Related Commands

[ip domain-name, page A-26](#)

## listbackup

Use this command to list all available backups at the defined location. Backup names are created by using the WLSE hostname and the backup date and time.

**listbackup**

### Syntax Description

This command has no arguments or keywords.

### Usage Guidelines

You must first define the backup location by using the **backupconfig** command.

### Example

The following command lists all current backups at the configured site:

```
listbackup
ex1_06042001_170640: Hostname: ex1 Date: 06042001 time: 1700
ex1_06052001_124543: Hostname: ex1 Date: 06052001 time: 1243
ex1_06052001_155148: Hostname: ex1 Date: 06052001 time: 1558
ex1_06202001_145704: Hostname: ex1 Date: 06202001 time: 1454
```

### Related Commands

[backup, page A-8](#)

[backupconfig, page A-9](#)

[restore, page A-41](#)

[show backupconfig, page A-44](#)

## mail

Use this command to send and receive mail and to debug and test email settings.

**mail** [ *to user@host* [ **debug** ] ]

### Syntax Description

To read email, enter the command with no arguments. To send email, enter the command with the following arguments:

|                  |                                         |
|------------------|-----------------------------------------|
| <b>to</b>        | Sends email to the expressed recipient. |
| <i>user@host</i> | Recipient of the email.                 |
| <b>debug</b>     | Debug email problems.                   |

### Usage Guidelines

When sending a message, enter a period on a line by itself to terminate the message body.

When listing the mail queue, enter **exit** to return to the CLI command prompt.

## Example

The following command sends an email message:

```
mail to operator@sj_wlse
Subject: test
This is a test mail
.
Cc:
```



### Note

You must end the mail message with a period (.) on a line by itself.

The following command debugs email problems:

```
admin@magellan.com:mail to operator@cisco.com DEBUG
Subject: testing
testing
.
Cc:
operator@cisco.com... Connecting to inbound.cisco.com. via esmtp...
220 inbound.cisco.com ESMTP Sendmail 8.12.11/8.11.2; Mon, 19 Jul 2004 13:24:00 -0700 (PDT)
>>> EHLO magellan.cisco.com
250-inbound.cisco.com Hellomagellan.cisco.com [192.168.65.120], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-EXPN
250-VERB
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-DELIVERBY
250 HELP
>>> MAIL From:<admin@magellan.cisco.com> SIZE=45
250 2.1.0 <admin@magellan.cisco.com>... Sender ok
>>> RCPT To:<operator@cisco.com>
250 2.1.5 <operator@cisco.com>... Recipient ok
>>> DATA
354 Enter mail, end with "." on a line by itself
>>> .
250 2.0.0 i6JK00im006330 Message accepted for delivery
operator@cisco.com... Sent (i6JK00im006330 Message accepted for delivery)
Closing connection to inbound.cisco.com.
>>> QUIT
221 2.0.0 inbound.cisco.com closing connection
admin@magellan.com:
```

## Related Commands

[mailcntrl, page A-30](#)

[mailroute, page A-30](#)

## mailcntrl

Use this command to display the size of the email log, send queue, or user queue or delete the email log, send queues, or user queues.

```
mailcntrl list { logsize | sendqueueusize | userqueueusize }
```

```
mailcntrl clear { log | sendqueue | userqueue }
```

### Syntax Description

|              |                         |                        |
|--------------|-------------------------|------------------------|
| <b>list</b>  | Displays the following: |                        |
|              | <b>logsize</b>          | Size of the mail log.  |
|              | <b>sendqueueusize</b>   | Size of the sendqueue. |
|              | <b>userqueueusize</b>   | Size of the userqueue. |
| <b>clear</b> | Deletes the following:  |                        |
|              | <b>log</b>              | WLSE email log.        |
|              | <b>sendqueue</b>        | WLSE send queues.      |
|              | <b>userqueue</b>        | WLSE user queues.      |

### Example

The following command clears the WLSE's email log.

```
mailcntrl clear log
```

### Related Commands

[show maillog, page A-54](#)

## mailroute

To forward email to a specified SMTP server, use the following command to specify the server. If no server is specified, the WLSE will use DNS to determine the correct email server in your local domain. To stop forwarding mail to the SMTP server, use the **no mailroute** command to remove the defined mail server information.

```
mailroute { hostname | ip-address }
```

```
no mailroute
```

### Syntax Description

|                   |                                |
|-------------------|--------------------------------|
| <i>hostname</i>   | Host name of an email server.  |
| <i>ip-address</i> | IP address of an email server. |



## Example

The following command forwards email to a server with the hostname mailserver:

```
mailroute mailserver
```

## Related Commands

[show mailroute, page A-55](#)

# mkcert

Use this command to generate or regenerate the SSL self-signed certificate for enabling secure socket layer protocol (SSL). SSL provides a secure HTTPS connection between Web clients and the WLSE.

When you initially set up the WLSE, a private key, a self-signed certificate, and a certificate signing request (CSR) are generated.

This command enables SSL.

The unsigned certificate expires in one year; use the procedure described below to obtain and install a permanent certificate from a certificate authority.



### Note

When you wish to establish an SSL connection to the WLSE, use the https prefix instead of http when entering the URL into the browser. Do not append a port number to the URL.

## Syntax Description

**mkcert**

## Usage Guidelines

When you run **mkcert**, the following prompts are displayed. For some fields, there is a default name. If you enter a period (.), the field will be left blank.

| Prompt                      | Response                                                                                                                                                         |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Country Name             | Country, state or province, and city in which the WLSE is located.<br>Use the 2-character code for the country and the full names of state or province and city. |
| 2. State or Province Name   |                                                                                                                                                                  |
| 3. Locality Name            |                                                                                                                                                                  |
| 4. Organization Name        | Full name of organization that owns the WLSE.                                                                                                                    |
| 5. Organizational Unit Name | (Optional) Section of organization that is using the WLSE.                                                                                                       |
| 6. Common Name              | Fully qualified domain name of organization.                                                                                                                     |
| 7. Email Address            | Email address of organization.                                                                                                                                   |

After generating the certificate, view it in the Web interface (**Administration > Security > SSL (HTTPS)**). Copy everything between the BEGIN CERTIFICATE REQUEST and END CERTIFICATE REQUEST lines and send it to a certificate authority (such as Verisign). Use the authority's procedure for sending the certificate.

When you receive the signed certificate:

- 
- Step 1** Copy the certificate into an ASCII file on a client system.
  - Step 2** Start the WLSE Web interface from the same client system.
  - Step 3** Select **Admin > Security > SSL (HTTPS)**.
  - Step 4** Enter the path to the certificate or click **Browse** to locate it. Then click **Submit Certificate**.
  - Step 5** To use the new certificate, restart the WLSE by running the following commands:

```
services stop
services start
```

---

## nslookup

Use this command to translate a device name to its IP address or an IP address to its device name.

```
nslookup { dns-name | ip-address }
```

### Syntax Description

|                   |                                       |
|-------------------|---------------------------------------|
| <i>dns-name</i>   | Device name of a host on the network. |
| <i>ip-address</i> | IP address of a host on the network.  |

### Example

The following command translates the device name hostname to its IP address:

```
nslookup hostname
Server: dns.ex1.com
Address: 209.165.200.224
Name: ex1.com
Address: 209.165.201.0
```

## ntp server

Use this command to configure the Network Time Protocol (NTP) and allow the system clock to be synchronized by a time server. To disable this function, use the **no** form of this command.

```
ntp server ip-address
```

```
no ntp server ip-address
```

### Syntax Description

|                   |                                    |
|-------------------|------------------------------------|
| <i>ip-address</i> | IP address of the NTP time server. |
|-------------------|------------------------------------|

## Usage Guidelines

Use the **ntp server** command to synchronize the system clock with the specified NTP server. If you configure multiple NTP servers, the system will synchronize with the first working NTP server it finds. There is no limit to the number of NTP servers that you can configure.

The **ntp server** command validates the NTP server that you specify. The possible results are:

- If the server is a valid NTP server, a message similar to the following appears:

```
19 Jan 00:43:48 ntpdate[1437]: step time server 209.165.200.224 offset 999.257304
```

- If no NTP server with the name or IP address you specified exists, a message similar to the following appears:

```
19 Jan 00:43:40 ntpdate[1431]: no server suitable for synchronization found
```

In this case, remove the NTP server by using the **no** form of the command, then configure a valid NTP server.

- If the system time is set to a time later than the time on the NTP server, a message similar to the following appears:

```
19 Jan 00:43:58 ntpdate[1265]: Can't adjust the time of day: Invalid argument.
```

In this case, the **ntp server** command is entered into the system configuration, but NTP will not function. Follow these steps to remove the command and configure NTP correctly:

- 
- Step 1** Remove the **ntp server** command from the configuration by entering the **no** form of the command. For example:

```
no ntp server ip-address
```

where *ip-address* is the IP address of the NTP server.

- Step 2** Set the system clock to a time that is behind the time on the NTP server using the **clock set** command. For more information about the clock command, see [clock set, page A-12](#).

- Step 3** Enter the **ntp server** command again to configure the NTP server on the system. For example:

```
ntp server ip-address
```

---

## Example

This command configures the system to use an NTP server:

```
ntp server 209.165.201.0
```

This command configures the system to stop using the NTP server:

```
no ntp server 209.165.201.0
```

## Related Commands

[clock set, page A-12](#)

# ping

Use this command to send ICMP echo\_request packets for diagnosing basic network connectivity.

```
ping [-n] [-c count] [-i wait] [-s packetsize] { hostname | ip-address }
```

## Syntax Description

|                   |                                                                                   |
|-------------------|-----------------------------------------------------------------------------------|
| <b>-n</b>         | Disables reverse DNS lookup.                                                      |
| <b>-c</b>         | Sets the number of echo packets to send.                                          |
| <i>count</i>      | Number of echo packets to send.                                                   |
| <b>-i</b>         | Sets the amount of time to wait between sending each packet.                      |
| <i>wait</i>       | Amount of time to wait between sending each packet, in seconds. The default is 1. |
| <b>-s</b>         | Sets the size of each echo packet.                                                |
| <i>packetsize</i> | The size of each echo packet, in bytes. The default is 56.                        |
| <i>hostname</i>   | Host name of system to ping.                                                      |
| <i>ip-address</i> | IP address of system to ping.                                                     |

## Usage Guidelines

To use this command with the *hostname* argument, DNS must be configured on the system.

To force the time-out of a nonresponsive host or to eliminate a loop cycle, press **Ctrl-c**.

## Example

This command sends 4 echo packets to the host otherhost with a wait time of 5 seconds between each packet:

```
ping -c 4 -i 5 209.165.200.224
PING 209.165.200.224 (209.165.200.224) from 209.165.201.0 : 56(84) bytes of data.
64 bytes from dns-sjl.cisco.com (209.165.200.224): icmp_seq=0 ttl=246 time=16.3 ms
64 bytes from dns-sjl.cisco.com (209.165.200.224): icmp_seq=1 ttl=246 time=2.0 ms
64 bytes from dns-sjl.cisco.com (209.165.200.224): icmp_seq=2 ttl=246 time=2.1 ms
64 bytes from dns-sjl.cisco.com (209.165.200.224): icmp_seq=3 ttl=246 time=2.1 ms
```

## Related Commands

[traceroute, page A-70](#)

## ps

Use this command to show running processes.

**ps** [ **help** ] [ **info** ] [ **options** ]

### Syntax Description

This is a standard Linux command.

|                |                                                                                      |
|----------------|--------------------------------------------------------------------------------------|
| <b>help</b>    | Displays the Linux manual page.                                                      |
| <b>info</b>    | Prepends additional information about /proc and socket status.                       |
| <b>options</b> | Use Unix98, BSD, and GNU options that are displayed when use the <b>help</b> option. |

### Usage Guidelines

The output of the **ps** command is sent to the `procps_last.log` file. You can view or download this file from the Web interface: **Admin > Status > View Log File**.

## radiomanager

Use this command to disable or enable the Radio Management processes. Radio Management processes are enabled by default. If you disable the Radio Management processes, the Intrusion Detection System (IDS), Radio Manager (Radio Mgr), and Site planning features (Sites, including Location Manager) will be unavailable. However, the Manage Remaining IDS Settings feature will be available. The message `Radio Management Disabled` is displayed near the top of the screen when Radio Management is disabled.

**radiomanager** [ **enable** | **disable** | **show** | **help** ]

### Syntax Description

|                |                                                                                                                                                |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>enable</b>  | Radio Management options (IDS, Radio Mgr, Sites, client tracking) are running and available for use in the Web interface. This is the default. |
| <b>disable</b> | Radio Management options do not run and are not shown in the Web interface.                                                                    |
| <b>show</b>    | Displays Management status (enabled or disabled).                                                                                              |
| <b>help</b>    | Displays help for the <b>radiomanager</b> command.                                                                                             |

### Usage Guidelines



#### Caution

All processes running on the WLSE will stop and restart when you run **radiomanager enable** or **radiomanager disable**. The WLSE will not respond while it is reloading.

Enabling or disabling Radio Management causes the WLSE to reload. You are asked to confirm before executing the command; for example:

**radio manager disable**

radio manager will be disabled and WLSE will reload [ok]

Radio Management faults that were issued before Radio Management was disabled will not be automatically cleared. You can clear these faults manually.

Location-based groups that were created before processes were disabled cannot be modified or deleted. You can enable Radio Management processes and then modify or delete these groups.

## redundancy

Use this command to turn redundancy on or off.

**redundancy { on | off }**

**redundancy status**

**redundancy config**

**redundancy upgrade** *package\_name*

### Syntax Description

|                                    |                                                                                                                                                                                         |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>on</b>                          | Turn on redundancy mode after validating current redundancy settings.                                                                                                                   |
| <b>off</b>                         | Turn off redundancy mode.                                                                                                                                                               |
| <b>status</b>                      | Show redundancy status; that is, whether or not redundancy is configured.                                                                                                               |
| <b>config</b>                      | Show redundancy status and redundancy configuration. For information on the setting the redundancy configuration parameters, see <a href="#">Managing WLSE Redundancy, page 16-28</a> . |
| <b>upgrade</b> <i>package_name</i> | Upgrade WLSE software on a redundant cluster of WLSEs. Upgrades both nodes without requiring that redundancy be turned off during the upgrade.                                          |

### Examples

This command upgrades a WLSE from an upgrade image that has been downloaded to the local repository via RME SWIM:

```
admin@wlse1: redundancy upgrade WLSE-2.13u
```

This command shows that redundancy is not configured on the WLSE:

```
admin@wlse1: redundancy status
Redundancy Status: Not Configured
HTTP Port: 1741
Notification Email:
Virtual IP eth0:
Virtual IP eth1:
This Node IP: 172.19.28.158
Other Node IP:
Minutes between sync: 30
Seconds between check of other node: 60
```

## Usage Guidelines

When you run **redundancy on**, the current redundancy settings are validated. Error messages are displayed if any parameters are not configured, and errors must be corrected before you can turn on redundancy mode. To correct validation errors, use the Web interface. For more information, see [Managing WLSE Redundancy, page 16-28](#).

The validation failure messages are:

```
Notification email is not specified
Admin Password not set
Failed to decrypt admin password
Primary IP not specified
Secondary IP not specified
Sync interval not specified or invalid
Check interval not specified or invalid
Invalid HTTP port specified. Must be 1741 or 80
HTTP port not set
Virtual IP not specified
```

The **upgrade** option can be used to upgrade a redundant cluster after downloading the image to the local WLSE repository via the Software Image Management (SWIM) option of CiscoWorks RME. This command looks for the specified software image in the local repository on either the active or standby WLSE. It is preferable to run the command from the active node. By using this method of upgrading, downtime is minimized because one node is running while the other is being upgraded. For more information on this method of upgrading, see the document *Upgrading CiscoWorks Wireless LAN Solution Engine Software, 2.13* on Cisco.com at [http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw\\_1105/wlse/2\\_13/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_13/index.htm).

## Related commands

[show redundancy, page A-56](#)

[repository, page A-38](#)

## reinitdb

Use this command to reinitialize the database. This command erases all information in the database (except for SNMP community strings entered under **Device > Discover > Device Credentials > SNMP Communities**), stops and restarts system services, and reboots the WLSE.

**reinitdb**



### Note

This command stops and restarts system services.

## Usage Guidelines

After the database is reinitialized, the WLSE reboots.

## Syntax Description

This command has no arguments or keywords.

## Example

This command reinitializes the database:

```
reinitdb
```

## reload

Use this command to reboot the WLSE.

```
reload [force]
```

## Syntax Description

The **force** option causes a reload without asking for confirmation.

## Usage Guidelines

You will be prompted to verify the reload. Enter **yes** to confirm or **no** to cancel the reload.



**Caution**

All processes running on the system stop when you run the **reload** command. The WLSE will not respond while it is reloading.

## Example

This command reboots the system:

```
reload
```

## Related Commands

[shutdown, page A-65](#)

## repository

Use this command to manage the local repository, from which the WLSE downloads its software updates. You can add, delete, or list software packages in the repository; specify the location from the local repository downloads images, and control the status of the repository.

```
repository add package [rate Kbytes/second]
```

```
repository delete [package | all]
```

```
repository list { local | remote } [detail] [page]
```

```
repository source URL
```

```
repository server [stop | start | status]
```



## Syntax Description

|                           |                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>add</b> <i>package</i> | Transfers a software update image named <i>package</i> from a remote server to the local repository.                                                                                                                                                                                                                                                          |
| <b>rate</b>               | Rate of transfer of the image in Kbytes/second.                                                                                                                                                                                                                                                                                                               |
| <b>delete</b>             | Deletes a package from local repository.                                                                                                                                                                                                                                                                                                                      |
| <b>all</b>                | Deletes all packages from local repository.                                                                                                                                                                                                                                                                                                                   |
| <b>list</b>               | List software images and packages in configured local or remote repository.                                                                                                                                                                                                                                                                                   |
| <b>local</b>              | Lists software updates and packages in local repository.                                                                                                                                                                                                                                                                                                      |
| <b>remote</b>             | Lists software updates and packages in remote repository.                                                                                                                                                                                                                                                                                                     |
| <b>detail</b>             | Includes details of software updates and images displayed.                                                                                                                                                                                                                                                                                                    |
| <b>page</b>               | Displays first page of command output. To display more: <ul style="list-style-type: none"> <li>Press the Return key to display the next line of output.</li> <li>Press the Space bar to display the next screen of output</li> </ul> Press <b>q</b> or <b>Q</b> to exit paged output and return to the command prompt.                                        |
| <b>source</b> <i>URL</i>  | Configure WLSE to serve as repository and to download software updates and images from external server whose IP address is <i>URL</i> (restricted to the FTP protocol). This command only configures the WLSE to be a repository. To configure the WLSE to install software updates and images from this repository, see <a href="#">install, page A-23</a> . |
| <b>server</b>             | Start, stop, or display status of the WLSE's local repository.                                                                                                                                                                                                                                                                                                |
| <b>stop</b>               | Stop local repository.                                                                                                                                                                                                                                                                                                                                        |
| <b>start</b>              | Start local repository.                                                                                                                                                                                                                                                                                                                                       |
| <b>status</b>             | Display status of local repository.                                                                                                                                                                                                                                                                                                                           |

## Usage Guidelines

You will be prompted to enter a username and password if they are needed to access the remote server.

## Examples

The following command transfers the update EX\_2.0 from an update server to the local repository:

```
repository add ex_2.0
```

The following command deletes the update EX\_2.0 from the local repository:

```
repository delete EX_2.0
```

The following command lists the software updates and images available on the configured local repository, with details and one page at a time:

```
repository list local detail page
```

The following command configures the WLSE to be a repository, and to download software updates and images from http:// 209.165.200.224:

```
repository source ftp://209.165.200.224
```

The following command stops the local repository:

```
repository server stop
```

## Related Commands

[install, page A-23](#)

[show repository, page A-57](#)

## reset device-snmp

Use this command to reset the WLSE's community strings to the default.



### Caution

This command is intended as a last resort; use it only if you cannot restart the WLSE in any other way. You will lose the community strings and must re-enter them as described below under **Usage Guidelines**.

## Syntax Description

```
reset [device-snmp | help]
```

## Usage Guidelines

This command is intended for restarting the WLSE if the tomcat process fails and the cause for the failure was corruption of the SNMP community string file. In that case, the Web interface will not be available, but the CLI will be available. The procedure follows.

- 
- Step 1** Log in to the CLI as [admin](#) or as another user who has the System Administrator role.
- Step 2** Run the **service status** command to check the status of the tomcat process. If the status is “Failed to run”, proceed to the next step.
- Step 3** Run the **show tomcatlog** command. It should contain these error messages about the SNMP community file:
- ```
MESSAGE: SnmpLibHandler: About to initialize SNMP Errors found while parsing community strings.
FATAL ERROR: SnmpLibHandler: unable to read SNMP communities file:
/var/adm/CSCOets/config/cwsi/anisnmp.conf
```
- Step 4** Run the **reset device-snmp** command.
- The file is reset and previously defined communities are lost.
 - The community strings are reset to *.*.*:public::10:1:::public.
 - The old SNMP community file is placed in the WLSE's log area. To view the file, select **Admin > Appliance > Status > View Log File**. Select the anisnmp.conf.log file.
- Step 5** Log into the Web interface as [admin](#) or as another user who has the System Administrator role.
- Step 6** Select **Devices > Discover > Device Credentials > SNMP Communities** and re-enter your community strings.
-

Example

```
reset device-snmp
Warning: This command will restart all services.
Continue? (Y/N):
```

Related Commands

[services, page A-42](#)
[show tomcatlog, page A-62](#)
[snmp-server, page A-66](#)
[show snmp-server, page A-59](#)

restore

Use this command to restore a backed up configuration of the WLSE.

```
restore -n backup_name
```

Syntax Description

<i>backup_name</i>	Name of backup.
-n	Restores without overwriting the flash memory, which contains network information (hostname, IP address, domain name, name servers, NTP server) and users' CLI privileges.

Usage Guidelines

The restore command shuts down services on the WLSE, restores the data, and then reboots the WLSE. Backups are restored from the location that you specified. To specify the backup location, use the **backupconfig** command.

You can restore configuration data from one WLSE to another; for example, if you want to replace one WLSE with another. For more information see the backup procedures in [Backing Up and Restoring Data, page 16-20](#).

Example

The following command restores the backup called **backup1** from the configured backup location:

```
restore backup1
```

Related Commands

[backup, page A-8](#)
[backupconfig, page A-9](#)
[listbackup, page A-28](#)

[show backupconfig, page A-44](#)

route

Use this command to add a route through a gateway device. To delete a route, use the **no** version of the command.

route *network-address netmask gateway-address*

no route *network-address netmask gateway-address*

Syntax Description

<i>network-address</i>	IP address of the network.
<i>netmask</i>	Value of the network netmask.
<i>gateway-address</i>	IP address of router or gateway.

Example

The following command adds a route:

```
route 209.165.201.0 255.255.255.224 209.165.200.224
```

The following command deletes the above route:

```
no route 209.165.201.0 255.255.255.224 209.165.200.224
```

services

Use this command to list, start, or stop the management services running on the WLSE.

services { **status** | **start** | **stop** }

Syntax Description

status	Displays management services status.
start	Starts management services.
stop	Stops management services.

Usage Guidelines

Management services are the software installed on the system by network management applications. Use this command to stop and restart management services if the system is not responding correctly to a management application. This should cause the services to reset and function properly again.

Example

This command stops management services:

```
services stop
```

This command starts management services:

```
services start
```

This command shows services status:

```
services status
```

```
Process= WirelessSvcMgr
  State = Program started - No mgt msgs received
  Pid   = 1567
  RC     = 0
  Signo  = 0
  Start  = 09/28/04 21:56:11
  Stop   = Not applicable
  Core   = Not applicable
  Info   = Application started by administrator request.

Process= WLSEjobvm
  State = Program started - No mgt msgs received
  Pid   = 1573
  RC     = 0
  Signo  = 0
  Start  = 09/28/04 21:56:11
  Stop   = Not applicable
  Core   = Not applicable
  Info   = Application started by administrator request.
.
.
.
```

Related Commands

[show proc\[ess\], page A-55](#)

setup

Use this command to configure the WLSE Express if you are not using DHCP.

```
setup
```

Usage Guidelines

For details on using the **setup** command, see the *WLSE Installation and Configuration Guides* on Cisco.com
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm.

show auth-cli

Use this command to display the type of authentication used for secure CLI access.

```
show auth-cli
```

Syntax Description

This command has no arguments or keywords.

Example

This command and response shows that local authentication is being used for the CLI:

```
show auth-cli  
local
```

Related Commands

[auth, page A-7](#)

show auth-http

Use this command to display the type of authentication used for secure HTTP access.

```
show auth-http
```

Syntax Description

This command has no arguments or keywords.

Example

This command and response shows that the WLSE's local authentication is being used for the CLI:

```
show auth-http
```

Related Commands

[auth, page A-7](#)

show backupconfig

Use this command to display the current backup and restore configuration.

```
show backupconfig
```

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

If the backup location is not set, the host and username fields display `NONE`.

Example

The following command displays the current backup and restore configuration:

```
show backupconfig
Hostname: 209.165.201.0
Username: user1
```

Related Commands

[backup, page A-8](#)

[backupconfig, page A-9](#)

[listbackup, page A-28](#)

[restore, page A-41](#)

show backuplog

Use this command to display the contents of the backup log.

```
show backuplog
```

show bootlog

Use this command to display the messages logged during the last system boot.

```
show bootlog [ page ]
```

Syntax Description

page	Displays first page of command output.

Usage Guidelines

When using paged output:

- Press the Return key to display the next line of output.
- Press the Space bar to display the next screen of output
- Press **q** or **Q** to exit paged output and return to the command prompt.

Example

This command displays the messages logged during the last system boot:

```
show bootlog page
Linux/UID32 version 2.2.16-13bipsec.uid32 (gcc version egcs1
```

```
Console: colour VGA+ 80x25
Calibrating delay loop... 1133.77 BogoMIPS
start low memory: 0xc0001000 i386_endbase: 0xc009f000
addresses range:: 0xc0f00000 0xc1000000
start memory: c04f8000 end_memory: d0000000
Memory: 257688k/262144k available (988k kernel code, 416k reserved, 2992k data,)
Dentry hash table entries: 262144 (order 9, 2048k)
Buffer cache hash table entries: 262144 (order 8, 1024k)
Page cache hash table entries: 65536 (order 6, 256k)
vmdump: setting dump_execute() as dump_function_ptr ...
VFS: Diskquotas version dquot_6.4.0 initialized
CPU: Intel Pentium III (Coppermine) stepping 06
Checking 386/387 coupling... OK, FPU using exception 16 error reporting.
Checking 'hlt' instruction... OK.
POSIX conformance testing by UNIFIX
mtrr: v1.35a (19990819) Richard Gooch (rgooch@atnf.csiro.au)
:
```

Related Commands

[reload, page A-38](#)

show cdp neighbor

Use this command to display the nearest neighbor on the network.

show cdp neighbor

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

CDP neighbor information is usually broadcasted at 3- to 5-minute intervals, so there may be a delay in displaying neighbor information.

Example

This command shows the nearest neighbor on the network.

```
show cdp neighbor
cdp neighbor device: Switch
    device type: cisco WS-C2924-XL
    port: FastEthernet0/12
    address: 209.165.201.0
```


show cdp run

Use this command to display the Cisco Discovery Protocol (CDP) configuration.

show cdp run

Syntax Description

This command has no arguments or keywords.

Example

The following command displays the CDP configuration:

```
show cdp run
CDP protocol is enabled ...
    broadcasting interval is every 60 seconds.
    time-to-live of cdp packets is 180 seconds.
    CDP is enabled on port eth0.
```

Related Commands

[cdp, page A-10](#)

show clock

Use this command to display the system date and time in Coordinated Universal Time (UTC).

show clock

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

For more information about the system time, see [Understanding WLSE Time Displays, page 1-10](#).

Example

This command displays the system date and time:

```
show clock
12:43:47 Jun 20 2001
```

Related Commands

[clock set, page A-12](#)

[ntp server, page A-32](#)

show config

Use this command to display network configuration and user information. Only the users who have CLI access are shown. Users with Web interface access only are not listed.

show config

Syntax Description

This command has no arguments or keywords.

Example

This command displays the system configuration, including any users who have CLI access:

```
show config
hostname ex1
interface ethernet0 209.165.201.0 255.255.255.224 default-gateway 209.165.202.128
interface ethernet1 up
ip domain-name cisco.com
ip name-server 209.165.202.158
ntp server 209.165.202.108
username admin epassword ***** privilege 15
username jpxl11 epassword ***** privilege 15
firewall ethernet0 NONE
snmp-server configuration:
    RW community string: private
    RO community string: public
    sysLocation: your site information
    sysContact: your contact information
telnet disabled
CLI auth: local
HTTP auth: local
```

show daemonslog

Use this command to display the daemons log.

show daemonslog [**page** | **include** *matchstring1* [*matchstring2*]]

Syntax Description

page	Displays first page of command output.
include	Filters the command output to display only the records that contain the specified string of characters.
<i>matchstring1</i> <i>matchstring2</i>	Strings of characters to search for in the command output.

Usage Guidelines

When using paged output:

- Press the Return key to display the next line of output.

- Press the Space bar to display the next screen of output
- Press **q** or **Q** to exit paged output and return to the command prompt.

Example

The following command displays the daemons log, one page at a time:

```
show daemonslog page
[dmgrDbg] getenv(PX_DBG)=NULL
[dmgrDbg] getenv(PX_MY_DEBUG)=NULL
[dmgrDbg] getenv(PX_MY_TRACE)=NULL
[dmgrDbg] getenv(PX_DBG_LEVEL)=NULL
[dmgrDbg] [Tue Sep 28 21:55:30 2004]##### INFO ##### re-evaluate DbgLevel=0x0
+++>it(1) = 80782f0 <WirelessSvcMgr>
+++>it(1) = 8077f10 <WLSEjobvm>
+++>it(1) = 8077e00 <WLSEFaults>
+++>it(1) = 8077c00 <WebServer>
+++>it(1) = 8077d00 <Tomcat>
+++>it(1) = 8077ab0 <Snmptrapd>
+++>it(1) = 8077960 <ExcepReporter>
+++>it(1) = 8077850 <CDPbrdcast>
+++>it(1) = 80776e0 <PerfMon>
:
```

show dmgtldlog

Use this command to display the daemon manager log.

show dmgtldlog [**page** | **include** *matchstring1* [*matchstring2*]]

Syntax Description

page	Displays first page of command output.
include	Filters the command output to display only the records that contain the specified string of characters.
<i>matchstring1</i> <i>matchstring2</i>	Strings of characters to search for in the command output.

Usage Guidelines

When using paged output:

- Press the Return key to display the next line of output.
- Press the Space bar to display the next screen of output
- Press **q** or **Q** to exit paged output and return to the command prompt.

Example

The following command displays the daemon manager log, one page at a time:

```
show dmgtldlog page
/var/adm/CSOets/log/dmgtld.log
```

```
Dec 20 13:42:56 ex dmgt[712]: #3001:TYPE=INFO:Using port: tcp/42340.  
Dec 20 13:42:56 ex dmgt[714]: #3007:TYPE=INFO:Started application(HSEC  
ollector) "/bin/nice -n 19 /opt/CSCOets/bin/collector" pid=715.  
Dec 20 13:42:56 ex dmgt[714]: #3007:TYPE=INFO:Started application(HSEA  
:  
:
```

show domain-name

Use this command to display the WLSE's current domain name. This command uses DNS to perform a reverse DNS lookup.

show domain-name

Syntax Description

This command has no arguments or keywords.

Example

This command displays the system domain name:

```
show domain-name  
cisco.com
```

Related Commands

[ip domain-name, page A-26](#)

show hosts

Use this command to display the WLSE's host file.

show hosts [page]

Syntax Description

page	Displays first page of command output.

Usage Guidelines

When using paged output:

- Press the Return key to display the next line of output.
- Press the Space bar to display the next screen of output
- Press **q** or **Q** to exit paged output and return to the command prompt.

Example

The following command displays the host file one page at a time:

```
show hosts page
```

```
127.0.0.1 localhost localhost.localdomain
192.19.28.169 wlse-2.cisco.com
(END)
```

Related Commands

[import, page A-22](#)

show http-server

Use this command to display HTTP and HTTPS access control information.

show http-server

Syntax Description

This command has no arguments or keywords.

Related Commands

[http-server, page A-21](#)

show import hosts

Use this command to display the imported host file.

show import *hosts*

Syntax Description

<i>hosts</i>	Name of server that host files were imported from.

Example

This command displays the imported host file that was imported from the host ftpserver_1:

```
show import ftpserver_1
```

Related Commands

[import, page A-22](#)

show install

Use this command to display the names of software updates available on the configured repository or installation log files.

show install

show install logs [detail] [page]

Syntax Description

detail	Displays names and descriptions of software updates and images on the configured repository.
page	Displays first page of command output.

Usage Guidelines

After running the **show install logs** command, you must press q to exit to the CLI prompt.

When using paged output:

- Press the Return key to display the next line of output.
- Press the Space bar to display the next screen of output
- Press **q** or **Q** to exit paged output and return to the command prompt.

Example

The following command displays the names of the software updates installed on the WLSE:

```
admin@wlse:show install logs page
2
NAME=WLSE-2.11
(END)
```

The following command displays names and descriptions of software installed on the WLSE:

```
admin@wlse:show install logs detail page
3
+++++
INFO: System related content of "hwdata"
=====
/usr/X11R6/lib/X11/Cards
/usr/share/doc/hwdata-0.14.1
/usr/share/doc/hwdata-0.14.1/COPYING
/usr/share/doc/hwdata-0.14.1/LICENSE
/usr/share/hwdata
/usr/share/hwdata/CardMonitorCombos
/usr/share/hwdata/Cards
/usr/share/hwdata/MonitorsDB
/usr/share/hwdata/pci.ids
/usr/share/hwdata/pcitable
:
```

Related Commands

[install, page A-23](#)

[repository, page A-38](#)

show interfaces

Use this command to display information about the system network interfaces.

show interfaces

Syntax Description

This command has no arguments or keywords.

Example

This command displays information about system network interfaces:

```
show interfaces
eth0      Link encap:Ethernet  HWaddr 00:02:B3:35:FD:CC
          inet addr:209.165.200.224 Bcast:209.165.201.0 Mask:255.255.255.224
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:80309 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22451 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:5 Base address:0xef00 Memory:d0c7e000-d0c7ec40
          RX bytes:116826221 (111.4 Mb)  TX bytes:59923827 (57.1 Mb)
          Interrupt:5 Base address:0xef00 Memory:febfb000-febfb038

          Speed: 100Mb/s
          Duplex: Full

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:28836 errors:0 dropped:0 overruns:0 frame:0
          TX packets:28836 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:13419821 (12.7 Mb)  TX bytes:13419821 (12.7 Mb)
```

Related Commands

[interface, page A-25](#)

show ipchains

Use this command to display the IP chains for the selected interface.

show ipchains eth[0-5]

Syntax Description

eth[0-5]	Interface to be displayed. Acceptable values are eth0-eth5. On the WLSE 1130, eth0 corresponds to port labeled A on the back panel, and eth1 corresponds to port labeled B.

Example

The following command displays the IP chains for the ethernet 0 interface:

```
show ipchains eth0
Chain ineth0 (1 references):
target      prot opt  source                destination          ports
ACCEPT      tcp  -y--l-  anywhere              ex.help             any ->  telt
ACCEPT      tcp  ----- anywhere              ex.help             any ->  telt
ACCEPT      tcp  ----- anywhere              ex.help             any ->  3345
ACCEPT      tcp  -y--l-  anywhere              ex.help             any ->  ssh
```

Related Commands

[interface, page A-25](#)

show maillog

Use this command to display the mail log.

```
show maillog [ page | include matchstring1 [ matchstring2 ] ]
```

Syntax Description

page	Displays first page of command output.
include	Filters command output to display only records that contain the specified string of characters.
<i>matchstring1</i> <i>matchstring2</i>	Strings of characters to search for in command output.

Usage Guidelines

When using paged output:

- Press the Return key to display the next line of output.
- Press the Space bar to display the next screen of output
- Press **q** or **Q** to exit paged output and return to the command prompt.

Example

The following command displays the collector log, one page at a time:

```
show maillog page
/var/log/maillog
Dec 21 04:02:06 ex sendmail[11643]: EAA11643: from=root, size=307, class=0, pri=30307,
nrcpts=1, msgid=<200112210402.EAA11643@ex.help>, relay=root@localhost
Dec 21 04:02:06 ex sendmail[11660]: EAA11643: SYSERR(root): Cannot exec /usr/bin/procmail:
No such file or directory
Dec 21 04:02:06 ex sendmail[11643]: EAA11643: to=root, ctladdr=root (0/0), delay=00:00:06,
xdelay=00:00:00, mailer=local, stat=Operating system error
:
```


Related Commands

[mailcntrl](#), page A-30

show mailroute

Use this command to show the current mail route.

show mailroute

Syntax Description

This command has no arguments or keywords.

Related Commands

[mailroute](#), page A-30

show proc[ess]

Use this command to display active process statistics.

show proc [page]

Syntax Description

page	Displays first page of command output.

Usage Guidelines

When using paged output:

- Press the Return key to display the next line of output.
- Press the Space bar to display the next screen of output
- Press **q** or **Q** to exit paged output and return to the command prompt.

Example

The following command displays the active process statistics one page at a time:

```
show proc page
PID      ELAPSED    SZ      STARTED  TTY  COMMAND
1        22:29:10   277    Thu Dec 20 13:42:29 2001 ?    init
2        22:29:10    0    Thu Dec 20 13:42:29 2001 ?    kflushd
3        22:29:10    0    Thu Dec 20 13:42:29 2001 ?    kupdate
4        22:29:10    0    Thu Dec 20 13:42:29 2001 ?    kpiod
5        22:29:10    0    Thu Dec 20 13:42:29 2001 ?    kswapd
6        22:29:03    0    Thu Dec 20 13:42:36 2001 ?    kreiserfsd
85       22:29:00    0    Thu Dec 20 13:42:39 2001 ?    kreiserfsd
86       22:29:00    0    Thu Dec 20 13:42:39 2001 ?    kreiserfsd
87       22:28:59    0    Thu Dec 20 13:42:40 2001 ?    kreiserfsd
88       22:28:59    0    Thu Dec 20 13:42:40 2001 ?    kreiserfsd
```

```

      89      22:28:59      0 Thu Dec 20 13:42:40 2001 ? kreiserfsd
     208      22:28:57     290 Thu Dec 20 13:42:42 2001 ? watchdog
     322      22:28:51     342 Thu Dec 20 13:42:48 2001 ? idled
     510      22:28:51     290 Thu Dec 20 13:42:48 2001 ? syslogd
     519      22:28:50     361 Thu Dec 20 13:42:49 2001 ? klogd
     637      22:28:48     327 Thu Dec 20 13:42:51 2001 ? crond
     651      22:28:48     286 Thu Dec 20 13:42:51 2001 ? inetd
    17076      18:23      364 Fri Dec 21 11:53:16 2001 ? \_ in.telnetd
    17077      18:23      575 Fri Dec 21 11:53:16 2001 0 | \_ login
:

```

show redundancy

Use this command to display the current redundancy configuration or status.

```
show redundancy { config | status }
```

Usage Guidelines

Although redundancy settings can be displayed with this CLI command, redundancy parameters can only be configured in the Web interface. After you configure redundancy in the Web interface, you can turn it on or off with the **redundancy** command.

Syntax Description

config	Shows settings of redundancy parameters and whether the WLSE is in redundancy mode.
status	Shows whether WLSE is in redundancy mode.

Example

This command shows an example of the current settings of the redundancy parameters:

```

show redundancy config
Redundancy Status: Not Configured
HTTP Port: 1741
Notification Email:
Virtual IP eth0:
This Node IP: 172.20.114.31
Other Node IP:
Minutes between sync: 30
Seconds between check of other node: 60

```

The following command output shows that the WLSE is not in redundancy mode:

```

show redundancy status
not configured

```

Related Commands

[redundancy, page A-36](#)

show repository

Use this command to display the status or access log of a configured repository.

```
show repository { status | access-log } [ page ]
```

Syntax Description

status	Displays the status of the local repository
access-log	Displays the access-log of the local repository
page	Displays first page of command output.

Usage Guidelines

When using paged output:

- Press the Return key to display the next line of output.
- Press the Space bar to display the next screen of output.
- Press **q** or **Q** to exit paged output and return to command prompt.

Example

This command displays the status of the configured repository:

```
show repository status
Repository Source: 171.69.212.146:9851
repository is running.
```

Related Commands

[repository](#), page A-38

show route

Use this command to display the routes that are currently configured.

```
show route
```

Syntax Description

This command has no arguments or keywords.

Example

This command displays the currently configured routes:

```
show route
Destination      Gateway Genmask          Flags Metric Ref    Use Iface
209.165.200.224  0.0.0.0 255.255.255.224 UH    0      0      0 eth0
209.165.200.225  0.0.0.0 255.255.255.224 U      0      0      0 eth0
209.165.200.254  0.0.0.0 255.255.255.224 U      0      0      0 lo
```

```
209.165.202.128 0.0.0.0 255.255.255.224 UG 0 0 0 eth0
```

Related Commands

[route](#), page A-42

show securitylog

Use this command to display security log information.

```
show securitylog [ page | include matchstring1 [ matchstring2 ]]
```

Syntax Description

page	Displays first page of command output.
include	Filters command output to display only records that contain specified string of characters.
<i>matchstring1</i> <i>matchstring2</i>	Strings of characters to search for in command output.

Usage Guidelines

When using paged output:

- Press the Return key to display the next line of output.
- Press the Space bar to display the next screen of output
- Press **q** or **Q** to exit paged output and return to command prompt.

Example

The following command displays the security log, one page at a time:

```
show securitylog page
/var/log/secure
Dec 20 13:45:23 ex in.tftpd[1381]: connect from 209.165.200.224
Dec 20 13:45:27 ex in.tftpd[1383]: connect from 209.165.200.224
Dec 20 13:45:31 ex in.tftpd[1385]: connect from 209.165.200.224
Dec 20 13:45:35 ex in.tftpd[1387]: connect from 209.165.200.224
Dec 20 13:45:39 ex in.tftpd[1389]: connect from 209.165.200.224
Dec 20 13:45:44 ex in.tftpd[1391]: connect from 209.165.200.224
Dec 20 13:45:48 ex in.tftpd[1393]: connect from 209.165.200.224
Dec 20 13:45:52 ex in.tftpd[1395]: connect from 209.165.200.224
Dec 20 13:45:56 ex in.tftpd[1397]: connect from 209.165.200.224
Dec 20 13:46:00 ex in.tftpd[1399]: connect from 209.165.200.224
Dec 20 13:46:04 ex in.tftpd[1412]: connect from 209.165.200.224
Dec 20 13:46:27 ex in.tftpd[1424]: connect from 209.165.200.224
Dec 20 13:46:31 ex in.tftpd[1426]: connect from 209.165.200.224
Dec 20 13:46:35 ex in.tftpd[1428]: connect from 209.165.200.224
:
```

show snmp-server

Use this command to display the SNMP configuration.

show snmp-server

Syntax Description

This command has no arguments or keywords.

Example

The following command displays the WLSE's SNMP configuration:

```
show snmp-server
RW community string: private
RO community string: public
sysLocation: your site information
sysContact: your contact information
trap-forwarding is disabled
```

Related Commands

[snmp-server, page A-66](#)

show ssh-server

Use this command to display SSH access control information.

show ssh-server

Syntax Description

This command has no arguments or keywords.

Related Commands

[ssh-server accept, page A-67](#)

show ssh-version

Use this command to display the type of SSH that is enabled:

show ssh-version

Syntax Description

This command has no arguments or keywords.

Example

This command displays the type of SSH that is enabled:

```
show ssh-version
SSH1, SSH2
```

Related Commands

[ssh-version, page A-68](#)

show syslog

Use this command to display syslog information.

```
show syslog [ page ] [ include matchstring1 [ matchstring2 ]
```

Syntax Description

page	Displays first page of command output.
include	Filters the command output to display only the records that contain the specified string of characters.
<i>matchstring1</i> <i>matchstring2</i>	Strings of characters to search for in the command output.

Usage Guidelines

When using paged output:

- Press the Return key to display the next line of output.
- Press the Space bar to display the next screen of output.
- Press **q** or **Q** to exit paged output and return to command prompt.

To filter command output to include only the records that contain a specified string(s) of characters, use the **include** option with one or two character strings to search for.

If you include two strings, the command outputs only those records that contain both character strings.

Example

This command displays syslog information:

```
show syslog
Jun 20 16:04:23 ex syslogd 1.3-3: restart.
Jun 20 16:04:23 ex syslog: syslogd startup succeeded
Jun 20 16:04:23 ex kernel: klogd 1.3-3, log source = /proc/kmsg start.
Jun 20 16:04:23 ex kernel: Inspecting /boot/System.map-2.2.16-13bipse2
Jun 20 16:04:23 ex syslog: klogd startup succeeded
:
```

Related Command

[interface, page A-25](#)

show tech

Use this command to display information necessary for Cisco's Technical Assistance Center to assist you:

show tech [**page**]

Syntax Description

page	Displays first page of command output.

Usage Guidelines

When using paged output:

- Press the Return key to display the next line of output.
- Press the Space bar to display the next screen of output.
- Press **q** or **Q** to exit paged output and return to the command prompt.

Example

```
show tech page
/bin/cat: /var/log/secure: Permission denied
Copyright (c) 1999-2000 by Cisco Systems, Inc.
Build Version (166) Mon Jun 11 16:56:23 PDT 2001
Linux/UID32 version 2.2.16-13bipsec.uid32 (gcc version egcs1
Uptime: 0 days 18 hours 35 mins

2 Ethernet interfaces
hostname ex
interface ethernet0 209.165.200.224 255.255.255.224 default-gateway 209.165.202.128
ip name-server 209.165.201.0
username admin epassword ***** privilege 15
eth0      Link encap:Ethernet  HWaddr 00:02:B3:35:FD:CC
          inet addr:209.165.200.224 Bcast:209.165.201.31 Mask:255.255.255.224
:
```

show telnetenable

Use this command to display the WLSE's Telnet status.

show telnetenable

Syntax Description

This command has no arguments or keywords.

Example

The following command shows whether Telnet is enabled or disabled:

```
show telnetenable
```

```
telnet enable for: ALL
```

Related Commands

[telnetenable](#), page A-69

[telnet](#), page A-68

show time

Use this command to display time zone configuration and NTP server (if any).

show tomcatlog

Use this command to display the Tomcat log.

```
show tomcatlog [ page ] [ include matchstring1 [ matchstring2 ]
```

Syntax Description

page	Displays first page of command output.
include	Filters the command output to display only the records that contain the specified string of characters.
<i>matchstring1</i> <i>matchstring2</i>	Strings of characters to search for in the command output.

Usage Guidelines

When using paged output:

- Press the Return key to display the next line of output.
- Press the Space bar to display the next screen of output
- Press **q** or **Q** to exit paged output and return to the command prompt.

Example

The following command displays the tomcat log, one page at a time:

```
show tomcatlog page
/var/adm/CSCOets/log/tomcat.log
2001-12-20 01:43:06 - ContextManager: Adding context Ctx( /examples )
2001-12-20 01:43:06 - ContextManager: Adding context Ctx( /admin )
Starting tomcat. Check logs/tomcat.log for error messages
2001-12-20 01:43:06 - ContextManager: Adding context Ctx( )
getUIProperties(): unhandled error could be a bad ui.properties
java.lang.NullPointerException
    at java.io.Reader.<init>(Reader.java:68)
    at java.io.InputStreamReader.<init>(InputStreamReader.java:96)
:
```


show version

Use this command to display information about the current software, hardware type, and details about the hardware.

show version

Syntax Description

This command has no arguments or keywords.

Example

The command displays information about software and hardware and limits on the number of access points that can be managed; for example:

```
show version
(C) Copyright 2005 by Cisco Systems Inc.
WLSE 1030 Release 2.11FCS Mon Mar 7 12:59:06 UTC 2005
Device Limit = 100
Build Version (66) Tue Mar 8 06:47:27 UTC 2005
Uptime: 0 days 1 hour 34 mins
Linux version 2.4.28-5_WLSE (root@app20.cisco.com) (gcc version 2.96 20000731 (Red Hat
Linux 7.3 2.96-113)) #1 Mon Jan 31 16:16:56 PST 2005

1030
VIA CPU at 1000.058 Mhz with 1025592K bytes of memory.
1 Ethernet interfaces

18.464Gb on disk
```

show webaccesslog

Use this command to display the Web access log.

```
show webaccesslog [ page ] [ include matchstring1 [ matchstring2 ]
```

Syntax Description

page	Displays first page of command output.
include	Filters the command output to display only the records that contain the specified string of characters.
<i>matchstring1</i> <i>matchstring2</i>	Strings of characters to search for in the command output.

Usage Guidelines

To display more:

- Press the Return key to display the next line of output.
- Press the Space bar to display the next screen of output.

- Press **q** or **Q** to exit paged output and return to the command prompt.

Example

The following command displays the Web access log, one page at a time:

```
show webaccesslog page
/var/adm/CSCOets/log/access_log
209.165.200.224 - - [21/Dec/2001:10:38:54 +0000] "GET / HTTP/1.0" 302 276 "-"
"Mozilla/4.76 [en]C-CCK-MCD (Windows NT 5.0; U)"
209.165.200.224 - - [21/Dec/2001:10:38:54 +0000] "GET /perl/login-form.cgi HTTP/1.0" 200
2268 "-" "Mozilla/4.76 [en]C-CCK-MCD (Windows NT 5.0; U)"
209.165.200.224 - - [21/Dec/2001:10:38:55 +0000] "GET /icons/hse.gif HTTP/1.0" 200 5554
"http://209.165.201.0:1741/perl/login-form.cgi" "Mozilla/4.76 [en]C-CCK-MCD (Windows NT
5.0; U)"
209.165.200.224 - - [21/Dec/2001:10:38:55 +0000] "GET /icons/left_top.gif HTTP/1.0" 200
324 "http://209.165.201.0:1741/perl/login-form.cgi" "Mozilla/4.76 [en]C-CCK-MCD (Windows
NT 5.0; U)"
:
```

show weberrorlog

Use this command to display the Web error log.

```
show weberrorlog [ page ] [ include matchstring1 [ matchstring2 ] ]
```

Syntax Description

page	Displays first page of command output.
include	Filters the command output to display only the records that contain the specified string of characters.
<i>matchstring1</i> <i>matchstring2</i>	Strings of characters to search for in the command output.

Usage Guidelines

When using paged output:

- Press the Return key to display the next line of output.
- Press the Space bar to display the next screen of output
- Press **q** or **Q** to exit paged output and return to the command prompt.

Example

The following command displays the Web error log, one page at a time:

```
show weberrorlog page
/var/adm/CSCOets/log/error_log
[Thu Dec 20 13:43:00 2001] [error] (22)Invalid argument: <Perl>: Invalid command 'secret',
perhaps mis-spelled or defined by a module not included in the server configuration
[Thu Dec 20 13:43:00 2001] [error] (22)Invalid argument: <Perl>: Invalid command 'line',
perhaps mis-spelled or defined by a module not included in the server configuration
[Thu Dec 20 13:43:00 2001] [error] (22)Invalid argument: <Perl>:
```

:

show websslaccesslog

Use this command to display the Web SSL log.

```
show websslaccesslog [ page | include matchstring1 [ matchstring2 ]]
```

Syntax Description

page	Displays first page of command output.
include	Filters the command output to display only the records that contain the specified string of characters.
<i>matchstring1</i> <i>matchstring2</i>	Strings of characters to search for in the command output.

Usage Guidelines

When using paged output:

- Press the Return key to display the next line of output.
- Press the Space bar to display the next screen of output
- Press **q** or **Q** to exit paged output and return to the command prompt.

Example

The following command displays the Web SSL log, one page at a time:

```
show websslaccesslog page
```

shutdown

Use this command to shut down the system in preparation for powering it off.

```
shutdown
```

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

All processes running on the WLSE will stop, and the WLSE will not respond until you power it off and back on.

You are prompted to verify the shutdown. Enter **yes** to continue, or **no** to cancel the shutdown.

**Caution**

Never power the system off without running the **shutdown** command first. Doing so can destroy data and prevent the system from booting.

Example

This command shuts down the system:

```
shutdown
```

Related Commands

[reload, page A-38](#)

snmp-server

Use this command to configure the simple network management protocol (SNMP) community string, contact information, and location information. Use the **no** forms to delete the community string, location information, or contact information.

```
snmp-server { community community-name [ RO | RW ] |  
              location sysLocation-info | contact sysContact-info }
```

```
no snmp-server community community-name
```

```
no snmp-server contact
```

```
no snmp-server location
```

Syntax Description

community <i>community-name</i>	Sets a community string.
RO	Makes the community string read-only.
RW	Makes the community string read/write.
location <i>sysLocation-info</i>	Sets the system location string.
contact <i>sysContact-info</i>	Sets the contact string.

Example

This command sets the SNMP contact string:

```
snmp-server contact Dial System Operator at Beeper # 27345
```

Related Commands

[show snmp-server, page A-59](#)

ssh host

Use this command to use SSH to connect to an external host.

```
ssh host [ -l username ]
```

Syntax Description

host	Name or IP address of host to which to connect.
-l username	

Example

Enter the following command to connect to an external host using SSH:

```
ssh 209.165.200.224
```

ssh-server accept

Use this command to control access to the WLSE via SSH. The default behavior is to accept all connections. If you specify an IP address, connections will be accepted from matching addresses only. Use the **no** form to remove SSH access control for the specified IP address.

```
ssh-server accept ip_address [ netmask ]
```

```
no ssh-server accept ip_address [ netmask ]
```

Syntax Description

<i>ip_address</i>	IP address to be allowed access.
<i>netmask</i>	Netmask for the IP address.

Usage Guidelines

The **no** form of the command must match exactly the rule it is deleting.

Related Commands

[show ssh-server, page A-59](#)

ssh-version

Use this command to enable Secure Shell (SSH) 1 or SSH 2, or both.

```
ssh-version { ssh1 | ssh2 | both }
```

Syntax Description

ssh1	Enables SSH 1
ssh2	Enables SSH 2
both	Enables both SSH 1 and SSH2

Example

This command enables ssh1:

```
ssh-version ssh1
```

Related Commands

[show ssh-version, page A-59](#)

tarlog

Use this command to create two archives of system log files.

```
tarlog
```

Usage Guidelines

When you run the tarlog command, system log files are archived to var_logs.tgz and logs.tgz.

These files can only be accessed from the web interface:

1. Run the **tarlog** command. The var_logs.tgz and logs.tgz archive files are created.
2. Select **Administration > Appliance > Status > View Log File**.
3. Save the desired file to the desktop.
4. Unzip the file.

telnet

Use this command to Telnet to an external host.

```
telnet { hostname | ip-address } [ portnumber ]
```

Syntax Description

<i>hostname</i>	Hostname of the external host.
<i>ip-address</i>	IP address of the external host.
<i>portnumber</i>	portnumber of the external host.

Example

Enter the following command to telnet to port 9851 of a system with the IP address 209.165.200.224:

```
telnet 209.165.200.224 9851
```

Related Commands

[telnetenable](#), page A-69

telnetenable

Use this command to control Telnet access to the WLSE. The default is disabled.

```
telnetenable { status | disable | enable [ ip-address [ ip-address ... ] | domain [] ] }
```

Syntax Description

enable	Enables Telnet access to the system.
disable	Disables Telnet access to the system. This is the default.
status	Displays current access status.
<i>ip-address</i>	IP addresses of systems allowed Telnet access. If this argument is used, no other machines will be allowed access. Multiple IP address are allowed.
<i>domain</i>	Domains of systems allowed Telnet access. If this argument is used, machines with domains other than the specified domain will be denied Telnet access. Multiple domains are allowed.

Usage Guidelines

To enable Telnet access to the system for *all* IP source addresses, use the **telnetenable enable** command alone. To enable *only specific* IP addresses, use the **telnetenable enable** command followed by the IP addresses.

Example

This command enables Telnet for all IP source addresses:

```
telnetenable enable
```

Related Commands

[show telnetenable](#), page A-61

tftpserver

Use this command to use the WLSE's TFTP server for general purposes. This command is available only on the WLSE Express.

```
tftpserver [ list | create file | delete file | rename file1 file2 |  
              upload URL ]
```

Syntax Description

list	Lists the contents of the TFTP server's public repository.
create <i>file</i>	Creates an empty file, which is required for importing files from devices to the WLSE.
delete <i>file</i>	Delete a file from the TFTP server's public repository.
rename <i>file1 file2</i>	Rename <i>file1</i> (source) to <i>file2</i> (destination).
upload <i>URL</i>	Upload file from the desktop. The URL is one of the following: • http://hostname/file • ftp://hostname/file • tftp://hostname/file]

traceroute

Use this command to display the network route to a specified host and identify faulty gateways.

```
traceroute [ -f first_ttl ] [ -m max_ttl ] [ -w waittime ] -n host [ packetlength ]
```

Syntax Description

-f <i>first_ttl</i>	Maximum time-to-live (maximum number of hops) of first outgoing probe packet. Default: 1 hop.
-m <i>max_ttl</i>	Maximum time-to-live for outgoing probe packets. Default: 30 hops.
-w <i>waittime</i>	Time to wait for a response to a probe, in seconds. Default: 5.
-n	Do not use DNS lookup for hostnames.
<i>host</i>	Name or IP address of host to which to connect.
<i>packetlength</i>	Length of packet to send, in bytes. Default and minimum: 40.

Usage Guidelines

This command displays a list of the hosts that receive probe packets as they travel to the destination host. Hosts are displayed in the order in which the receiving hosts receive the packets. Asterisks (*) appear as the entry for hosts that do not respond correctly to probing.

Example

This command displays the network route to the host otherhost with a packet time-to-live value of 2, a wait time of 5 seconds, and 50-byte packets:

```
traceroute -m 20 -w 10 cisco.com 50
traceroute to example.com (209.165.200.224), 20 hops max, 50 byte packets
 1  ex1.com (209.165.200.225)  0.981 ms  0.919 ms  0.926 ms
 2  ex2.com (209.165.200.254)  1.528 ms  0.747 ms  0.661 ms
 3  ex3.com (209.165.200.255)  0.887 ms  0.770 ms  0.744 ms
 4  ex4.com (209.165.201.0)    0.932 ms  0.789 ms  0.679 ms
 5  ex5.com (209.165.201.1)    1.066 ms  1.052 ms  0.983 ms
 6  ex6.com (209.165.201.30)   1.472 ms  1.247 ms  1.847 ms
 7  ex7.com (209.165.201.31)   1.738 ms  1.424 ms  1.658 ms
 8  ex8.com (209.165.202.128)  3.728 ms  2.429 ms  2.804 ms
 9  ex9.com (209.165.202.129)  6.283 ms  5.499 ms  3.285 ms
10  ex10.com (209.165.202.158) 9.926 ms 73.463 ms 3.895 ms
11  ex11.com (209.165.202.159) 70.967 ms * 47.106 ms
```

Related Commands

[ping, page A-34](#)

username

Use this command to create a new user account or change account properties. Use the **no** form of the command to remove a user account.

username *name* [**password** | **epassword**] *password* [**privilege** { **0** | **15** }]

no username *name*

Syntax Description

<i>name</i>	Name of the user account to create or remove: • Usernames can be up to 32 characters long. • Usernames must begin with a character (cannot begin with a number). • You can use any character except for the colon, comma, single quote, double quote, or space. Note If the user is <i>not</i> using the CLI (that is, privilege is set to 0), the username can begin with a number.
password <i>password</i> epassword <i>password</i>	Password for the account. • Passwords are unlimited in length and are case sensitive. • You can use any character except for the single quote or double quote.

privilege	(Optional) CLI privilege level.
0	Level 0 privileges. This is the default.
15	Level 15 privileges.

Usage Guidelines

The default privilege level is 0 if you do not use the privilege option.

For information on the allowable characters in user names and passwords, see [Appendix B, “Naming Guidelines.”](#)

Users that you create by using this command do not automatically have the HTTP access that is required for using the WLSE’s web interface. To provide such users with HTTP access:

-
- Step 1** Log into the Web interface as [admin](#) or as another user who has the System Administrator role.
 - Step 2** Select **Administration > User Admin**, then select **Manage Users**.
 - Step 3** For each user you added by using the CLI:
 - a.** Select the username, then select the relevant role(s).
 - b.** Click **Modify**.
-

For more information about managing users, see [Managing GUI Users, page 16-49](#).

For more information about the characters allowed in usernames and passwords, see [Appendix B, “Naming Guidelines.”](#)

Example

This command creates a user account named user1 with password password1 and privilege level 15:

```
username user1 password password1 privilege 15
```

This command removes the user account:

```
no username user1
```

webtimeout

Use this command to set the timeout period for the Web interface. After the timeout expires, you are logged out. The default is 30 minutes (1800 seconds).

webtimeout [**status** | **time** *seconds* | **default**]

Syntax Description

status	Shows the current web session timeout setting.
time <i>seconds</i>	Sets the web session timeout period.
default	Resets web session timeout to the default 30 minutes (1800 seconds).

Example

```
webtimeout time 3600 seconds
```

Maintenance Image Commands

This section describes the commands that are available when the system is booted from the maintenance image. For more information about the maintenance image, see [Using the Maintenance Image, page 17-18](#).

erase config

This command is identical to the level-15 **erase config** command. For a description, see [erase config, page A-17](#).

fsck

Use this command to check and repair the filesystem.

```
fsck
```

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

This command might prompt you for confirmation before making certain repairs.

Example

The following command checks and repairs the filesystem:

```
fsck
```

reload

This command is identical to the level 15 **reload** command. For a description, see [reload, page A-38](#).



Naming Guidelines

Revised: May 24, 2006, OL-8374-01

This appendix provides information about:

- [Naming Rules for Users and Roles, page B-1.](#)
- [Naming Rules for Hostnames and Device Names, page B-2.](#)
- [Naming Rules for Other Names and Descriptions, page B-2.](#)
- [Naming Rules for Domain Names, page B-3](#)
- [Naming Rules for the Built-In AAA Server \(WLSE Express Only\), page B-3](#)
- [Naming Rules for Authentication Modules, page B-4](#)

Naming Rules for Users and Roles

[Table B-1](#) lists the rules for WLSE usernames, passwords, and roles. These rules apply to WLSE users configured in the **Administration > User Admin** subtab and to users configured by using the CLI **username** command.

Table B-1 **Allowable Characters for Users and Roles**

Type	Rules
User Name	• No more than 32 characters. • Case-sensitive. • The following characters are not permitted: – Cannot start with a number, unless the user is not using the CLI. If the user is <i>not</i> using the CLI (that is, the user's CLI access privilege is set to <i>None</i>), the username can begin with a number. – Cannot contain a colon, semi-colon, comma, single-quote, double-quote, or space. • Other than the restrictions noted above, any character from Table B-2 is permitted.
User Password	• No limit on length. • Case sensitive. • Any character except for the single quote or double quote.

Table B-1 Allowable Characters for Users and Roles (continued)

Type	Rules
User Role	• No more than 32 characters. • Case-sensitive. • Cannot contain a hyphen (dash, minus sign) or a full stop (period). • Other than the restrictions noted above, any character from Table B-2 is permitted.

Naming Rules for Hostnames and Device Names

The naming rules for hostnames and device names are:

- Blank spaces are not allowed.
- The first character in a name must be alphanumeric.
- The only valid characters are the alphanumeric characters, the minus sign (-), the period (.), and the underscore (_).

Naming Rules for Other Names and Descriptions

[Table B-2](#) lists the allowable characters for names and descriptions in most WLSE dialogs. There are restrictions on the following types of names:

- Users and roles—See [Naming Rules for Users and Roles, page B-1](#).
- Device names and hostnames—See [Naming Rules for Hostnames and Device Names, page B-2](#).

The number of characters allowed are:

- Names
 - For templates, up to 56 characters are allowed.
 - For faults settings, up to 60 characters are allowed.
 - For all other names, up to 64 characters are allowed.
- Descriptions—up to 256 characters are allowed

**Note**

Each job name (configuration job, firmware job, or AP radio scan) must be unique.

There are additional rules for some WLSE screens. These rules are included in the online help for those screens.

**Note**

Do not use the Enter key in any description fields.

Table B-2 Allowable Characters for Names and Descriptions

Character Description	Characters
alphanumeric—upper and lower case	A-Z, a-z, 0-9
space	
Note Do not use for usernames.	
exclamation mark	!
percent sign	%
left and right parenthesis	()
asterisk	*
comma	,
Note Do not use for usernames.	
hyphen, dash, minus sign	-
Note Do not use for roles.	
full stop (period)	.
Note Do not use for roles.	
solidus (forward slash)	/
Note Do not use in the built-in AAA server.	
colon	:
Note Do not use for usernames.	
semicolon	;
Note Do not use for usernames or for domain names.	
equals	=
question mark	?
low line (underscore)	_
left and right square bracket	[]
left and right curly bracket	{ }
vertical line	
tilde	~
dollar sign	\$

Naming Rules for Domain Names

You cannot use a semicolon (;) in a domain name.

Naming Rules for the Built-In AAA Server (WLSE Express Only)

The built-in AAA server on the WLSE Express allows up to 255 characters and any character except for the forward slash (/) in client names, group names, and usernames.

Naming Rules for Authentication Modules

You cannot use a pound (#) sign in the shared secret for RADIUS or TACACS+ authentication modules, which are defined under **Admin > Appliance > Security > Authentication Modules**.



Ports and Protocols

This appendix provides information about:

- [Table C-1 Ports Used by WLSE, page C-1](#)
- [Ports Hosted by the WLSE, page C-2.](#)
- [Transport Protocols and Authentication Methods Used by the WLSE, page C-2](#)

Ports Used by the WLSE

[Table C-1](#) lists the ports that are hosted by other devices and servers and used by WLSE services.



Note

The NAT protocol is not used by the WLSE.

Table C-1 *Ports Used by WLSE*

Destination Port Number	Protocol and WLSE Service	Port Hosted By
TCP 21	FTP—IOS AP configuration	FTP server
TCP 22	SSH—IOS AP configuration	Access point
TCP 23	TELNET—IOS AP configuration	Access point
TCP 25	SMTP—fault notification	SMTP server
UDP 53	DNS—IOS AP configuration	DNS server
TCP 80	HTTP/HTTPS—access point configuration	Access point
TCP 9851	WHISK—repository for upgrading WLSE software	Windows repository server
UDP 161	SNMP—discovery, inventory, configuration of APs, configuration archive	Access point, other devices
UDP 162	SNMP—Traps received from APs	Trap receiver
UDP 514	SYSLOG—fault notification	Syslog server
UDP 1645 and 1646	RADIUS—AAA synthetic authentication (ACS versions prior to 3.2.3)	Cisco ACS server

Table C-1 Ports Used by WLSE (continued)

Destination Port Number	Protocol and WLSE Service	Port Hosted By
UDP 1812 and 1813	RADIUS—AAA synthetic authentication (ACS 3.2.3 version)	Cisco ACS server
UDP 2887	WLCCP—Wireless Domain Service (WDS) radio management	Master WDS access point

Ports Hosted by the WLSE

Table C-2 lists the ports hosted by the WLSE and used by other devices and servers.

Table C-2 Ports Hosted by WLSE

Destination Port Number	Protocol and WLSE Service	Source
TCP 443	HTTPS—WLSE secure Web port	Client browser
TCP 1741	HTTP—WLSE Web port	Client browser
TCP 2004	Default port used by remote agent for built-in AAA server. Used only for Windows domain authentication on the WLSE Express.	Windows domain controller
UDP ephemeral	TFTP—Firmware image transfer	Access point
UDP 69	TFTP—Firmware image transfer, configuration archive	Access point
UDP 162	SNMP—Traps received from APs	Access point
UDP 1620	SNMP—Traps received from APs	Access point

Transport Protocols and Authentication Methods Used by the WLSE

Table C-3 lists the protocols and authentication methods that WLSE uses for its network management functions.

Table C-3 WLSE Transport Protocol and Authentication Methods

Function	Telnet/SSH	Enable Password ¹	SNMP-RO Community	SNMP-RW Community	TFTP	HTTP
Discovery	--	-	X	-	-	-
Inventory	-	-	X	-	-	-
Config—Regular Job	X	X	-	-	X	-
Archive—Regular Job	-	-	X	X	X	-
Config—Auto Job	X	X	-	-	-	-

Table C-3 *WLSE Transport Protocol and Authentication Methods (continued)*

Function	Telnet/SSH	Enable Password ¹	SNMP-RO Community	SNMP-RW Community	TFTP	HTTP
Startup Config	-	-	-	-	X	-
Firmware Upgrade	X	X	-	X	X	-
Faults	-	-	X	-	-	-

1. The enable password is used only if the access point is configured with an enable password.



Revised: June 5, 2006, OL-8374-01

Numerics

- 802.11a** The IEEE standard that governs the deployment of 5-GHz OFDM systems. It specifies the implementation of the physical layer for wireless UNII bands (see UNII, UNII 1, and UNII 2) and provides four channels per 100 MHz of bandwidth.
- 802.11b** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5- and 11-Mbps 2.4-GHz wireless LANs.
- 802.11g** The IEEE standard that specifies carrier sense media access control and physical layer specifications for high-speed 2.4 GHz wireless networking

A

- AAA** Authentication, Authorization, and Accounting. The WLSE monitors LEAP, PEAP, EAP-MD5, RADIUS, and EAP-FAST AAA services provided by some AAA servers, including the built-in AAA server on the WLSE Express.
See also [EAP-MD5 server](#), [LEAP server](#), [PEAP server](#), [RADIUS](#), [EAP-FAST](#).
- access point** Access points are wireless LAN transceivers that serve as the center point of a standalone wireless network or as the connection point between wireless and wired networks. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network.
- ad-hoc network** See [IBSS](#).
- admin** The default user on the WLSE, created during initial setup of the WLSE. The admin user has the System Administrator role and level 15 CLI privileges. The admin user cannot be deleted.
- ARP** Address resolution protocol. An Internet protocol used to map an IP address to a MAC address. Defined in RFC 826.
- AVVID** Cisco Architecture for Voice, Video and Integrated Data. Cisco provides the baseline infrastructure that enables enterprises to design networks that scale to meet Internet business demands. Cisco AVVID delivers business infrastructure and intelligent network services.

B

BDPU	Bridge Protocol Data Unit. <i>See</i> STP .
black hole mitigation	Radio Manager feature that recommends the optimal beacon interval for an AP based on data collected from AP radio scan and client walkabout.
BOOTP	Bootstrap Protocol. The protocol used by a network node to determine the IP address of its Ethernet interfaces to affect network booting.
bridge	<i>See</i> wireless bridge .
BSS	Basic Service Set—a set of 802.11 stations associated with a single AP.
BSSID	Basic Service Set Identifier (see BSS)

C

CAC	Call Admission Control—An AP feature that determines whether to admit or reject a job request based on the amount of resources (including CPU, memory, and network bandwidth) at its disposal. The capacity of the system at a given time is defined by the number of jobs it is servicing at that time plus the additional number of jobs it can accept without compromising the quality of service of the jobs in the system.
CCK	Complementary Code Keying. Modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 5.5 and 11 Mbps.
CCMP	Based on the Advanced Encryption Standard (AES) defined in the National Institute of Standards and Technology's FIPS Publication 197, AES-CCMP is a symmetric block cipher that can encrypt and decrypt data using keys of 128, 192, and 256 bits. AES-CCMP is superior to WEP encryption and is defined in the IEEE 802.11i standard.
CKIP	Cisco Key Integrity Protocol. Cisco's WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group.
CCKM	Cisco Centralized Key Management. Using CCKM, authenticated client devices can roam from one access point to another without any perceptible delay during re-association. An access point or WLSM (Wireless LAN Services Module) on your network provides wireless domain services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS's cache of credentials dramatically reduces the time required for re-association when a CCKM-enabled client device roams to a new access point.
CDP	Cisco Discovery Protocol. Media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment, including routers, access servers, bridges, and switches. Using Cisco Discovery Protocol, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN. Runs on all media that support SNAP, including LANs, Frame Relay, and ATM media.

CDP distance	The CDP distance determines the depth of the discovery and applies to all seed devices. If CDP distance is 1, only the immediate neighbors of the seed device are discovered. If CDP distance is 2, devices A and B that are directly connected to the seed devices are discovered and the immediate neighbors of A and B are also discovered.
CLI	The command line interface for administering the WLSE. You use the CLI through a console attached to the WLSE's console port or by opening a Telnet connection to the WLSE. CLI commands are described in the <i>User Guide for the CiscoWorks Wireless LAN Solution Engine</i> —from the online help, click PDF .
client	A wireless user, such as a laptop with a wireless card.
CMIC	Cisco Message Integrity Check. MIC prevents bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The client's adapter driver must support MIC functionality, and MIC must be enabled on the access point.
codecs	Coder/decoder—a device that encodes or decodes a signal. For example, codecs can be used to convert binary signals transmitted on digital networks to the analog signals that are transmitted on analog networks.
community strings	Text strings that act as passwords to authenticate communication with devices that contain an SNMP agent.
CoS	Class or Service. An indication of how an upper-layer protocol requires a lower-layer protocol to treat its messages.
CSR	Certificate Signed Request. Request sent to a certificate authority for using HTTPS.
CSV	Comma-separated values. A file format used by CiscoWorks application, such as Resource Manager Essentials, to exchange information on managed devices.
D	
DFS	Dynamic Frequency Selection. Anti-contention rules for critical radar applications (for mostly military and weather operations) imposed by the ETSI and the FCC.
DHCP	Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

DNS Domain Name System. An Internet service that translates domain names into IP addresses. Domain names are a clear way of representing an Internet address. The Internet, however, is actually based on IP addresses. For example, the URL `http://www.website.com` might actually point to the IP address `http://123.456.789.0`. Because maintaining a central list of domain name/IP address correspondences would be impractical, the lists of domain names and IP addresses are distributed throughout servers on the Internet in the Domain Name System. If one DNS server cannot translate a particular domain name, it contacts another one, and so on, until the correct IP address is returned.

downlink Transmissions from AP to client.

DTIM Deliver Traffic Indication Message. Used by access points to tell power-save client devices that a packet is waiting for them.

DSCP Differentiated Services Code Point is a model in which traffic is treated by intermediate systems with relative priorities based on the type of services.

DSP Digital signal processor.

E

EAP ‘Extensible authentication protocol.

EAP-MD5 server Servers running EAP and providing dynamic, session-specific wireless encryption keys, central user administration, and authentication between clients and access points. EAP-MD5 uses MD5 hashing on client and challenge passwords. The WLSE monitors EAP-MD5 servers.

See also [AAA](#).

EAP-FAST EAP-FAST is a two-phase authentication protocol:

- Phase 0, provisioning. Provision client with a credential called PAC (Protected Access Credentials).
- Phase 1, authentication. Use the PAC to establish a tunnel with the server and authenticate the username and password.

The WLSE monitors EAP-FAST servers. *See also* [AAA](#).

EAP-TLS EAP with Transport Level Security.

EAPOL Extensible Authentication Protocol Over LAN

exception A group of related faults.

F

fast secure roaming Cisco software feature that allows Cisco and Cisco-compatible clients to layer-2 roam in under 150ms (under 10ms in most cases). Fast secure roaming uses a complex key hierarchy that is closely based on industry-standard WPA, and improves on WPA by adding WDS and establishing trust between the WDS and wireless APs and clients. This allows clients to re-establish WEP keys when roaming.

See also [WDS](#), [WPA](#), [WEP keys](#).

G

GMT Greenwich Mean Time. Mean solar time at the meridian of Greenwich, England, formerly used as a basis for standard time throughout the world.

See also [UTC](#).

GPR Gratuitous Probe Response—To detect the presence of a WLAN, dual mode phones that support cellular and WLAN modes of operation consume significant battery power due to the amount of time the phone must wait passively while listening for beacons on each channel. Because beacon intervals are typically on the order of hundreds of milliseconds, these scans require that the phone's receiver is enabled for at least a typical beacon interval on each channel. The Gratuitous Probe Response feature helps to conserve battery power by providing a high rate packet on the order of 10ms. The GPR packet is transmitted from the AP at a predefined time interval (at intervals between 10 and 50ms).

GRE Generic Routing Encapsulation. A tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multi protocol subnetworks in a single-protocol backbone environment, IP tunneling that uses GRE allows network expansion across a single-protocol backbone environment.

H

HA High availability. Another term for WLSE redundancy. For more information, see [Managing WLSE Redundancy, page 16-28](#).

HSRP Hot Standby Router Protocol. Provides high network availability and transparent network topology changes. HSRP creates a Hot Standby router group with a lead router that services all packets sent to the Hot Standby address. The lead router is monitored by other routers in the group, and if it fails, one of these standby routers inherits the lead position and the Hot Standby group address.

HTTP	Hypertext Transfer Protocol. The protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.
HTTPS	Secure HTTP with SSL (secure socket layer). <i>See also</i> SSL .
I	
IBSS	Independent Basic Service Set. A local network configuration that is set up by clients and in which the clients communicate directly with each other. This ad-hoc network mode is specified by the 802.11 standard for client radio network interface cards (NIC).
ICMP	Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing.
IGMP	Internet Group Membership Protocol. Used by IP hosts to report their multicast group memberships to an adjacent multicast router.
infrastructure access points	The access points that participate in WDS and register with a WDS device. <i>See also</i> WDS devices .
J	
jitter	A variation in the delay of received packets.
L	
LDAP	Netscape Lightweight Directory Access Protocol. Provides a standard way for Internet clients, applications, and WWW servers to access directory information across the Internet, such as user names, e-mail addresses, security certificates, and other contact information.
LEAP server	Light EAP server, which combines centralized two-way authentication with dynamically generated wireless equivalent privacy keys or WEP keys. <i>See also</i> AAA and WEP keys .
M	
managed APs	APs that participate in the SWAN architecture, so that their channel and transmit powers, along with other parameters, can be inspected and controlled by WLSE.

MHAE Mobile home authentication extension. Mobile IP uses a strong authentication scheme to protect communications to and from visiting clients. All registration messages between a visiting client and the home agent must contain the MHAE. Proxy Mobile IP also implements this requirement in the registration messages sent by the access point on behalf of the visiting clients to the home agent.

See also [proxy mobile IP](#).

MIC Message integrity check. MIC prevents bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The client adapter's driver must support MIC functionality, and MIC must be enabled on the access point.

MOK A type of modulation used before the IEEE finished high-speed 802.11 standard and may still be used in older wireless networks.

N

non-serving channel One or more channels on which an AP is *not* transmitting. Non-serving channel monitoring means that the channels the AP is not transmitting on are monitored. By monitoring non-serving channels, Radio Manager can detect rogue APs that you might not have discovered had it monitored only the channel the AP is transmitting on (the serving channel). See [serving channel](#).

nslookup The NSLookup tool is used to look up device or host information via the name server. You must enter a device name, not an IP address, to use this function. You must have a DNS server in order to look up network servers.

NTP Network Time Protocol. Protocol built on top of TCP that ensures accurate local timekeeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

O

OFDM Orthogonal Frequency Division Multiplexing. A radio modulation technique that provides 54 Mbps in the 5 GHz band.

P

PAC Protected access credentials. Credentials that are either automatically or manually provisioned and used to perform mutual authentication with the RADIUS server during EAP-FAST authentication. PACs are created by the Cisco Secure ACS server and are identified by an ID. The user obtains a copy of the PAC from the server, and the ID links the PAC to the profile created in ACU. When manual PAC provisioning is enabled, the PAC file is manually copied from the server and imported onto the client device.

See also [EAP-FAST](#).

PEAP server Protected EAP server, which combines centralized two-way authentication with dynamically generated wireless equivalent privacy keys or WEP keys.

See also [AAA](#) and [WEP keys](#).

ping A common method for troubleshooting the accessibility of devices.

A ping tests an ICMP echo message and its reply. Because ping is the simplest test for a device, it is the first to be used. If ping fails, try using traceroute.

Run ping to view the packets transmitted, packets received, percentage of packet loss, and round-trip time in milliseconds.

proxy mobile IP An access point feature that works in conjunction with the Mobile IP feature on Cisco devices on the wired network. When you enable proxy Mobile IP on your access point and on your wired network, the access point helps client devices from other networks remain connected to their home networks. The visiting client devices do not need special software; the access point provides proxy Mobile IP services on their behalf.

PSPF Publicly Secure Packet Forwarding. A feature that prevents client devices associated to a bridge or access point from inadvertently sharing files with other client devices on the wireless network.

Q

QoS Quality of Service. Measure of performance for transmission systems that reflects their transmission quality and service availability.

R

radio measurement aggregation WDS service for collecting all of the radio measurements in the layer 2 domain and sending aggregated radio reports to the WLSE.

See also [WDS](#).

RADIUS Remote Authentication Dial-In User Service. Database for authenticating connections and for tracking connection time. The WLSE monitors RADIUS servers. The WLSE also provides a RADIUS module for authenticating users.

See also [AAA](#).

repository The repository stores WLSE images and provides software update services. A repository can be a WLSE (local repository) or another system that functions as an FTP server (remote repository). From a local repository, you can update the WLSE that contains the repository and update other WLSEs.

RPG Radio Parameter Generator, the subsystem of WLSE responsible for determining good frequency and power plans.

RSA Public-key cryptographic system that can be used for encryption and authentication.

RSSI Received signal strength indication.

runstats Database facility that runs (automatically) periodically. Keeps database system tables up-to-date and improves efficiency and performance of the database. Tables are updated as necessary and these changes are logged in the db2runstatat.last.log and db2runstat.times.log.

S

SCP Secure copy protocol. Commonly used to securely copy files between hosts in a network. SCP uses SSH for data transfer and provides the same security and authentication as SSH. Unlike RCP, SCP asks for passwords or pass phrases if they are needed for authentication. SCP is usually available on all UNIX-type systems.

seed A CDP-enabled device used as a starting point for discovery. For example, by adding a seed device (or set of seed devices), the neighbors of the seed device are discovered using CDP.

serving channel The channel on which an AP is transmitting. See [non-serving channel](#).

SMTP Simple Mail Transfer Protocol. Internet protocol providing e-mail services.

SNMP Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SSH Secure Shell. Provides a secure Telnet connection, encrypting all traffic, including passwords

SSID Service Set ID. It is a unique identifier that client devices use to associate with the access point. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity. The SSID can be any alphanumeric entry up to 32 characters long.

SSL	Secure Socket Layer. Provides a secure connection between the WLSE and Web clients.
STA	Station (802.11 radio device).
STP	Spanning-Tree Protocol. Bridge protocol that uses the spanning-tree algorithm, enabling a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. Bridges exchange BPDU messages with other bridges to detect loops, and then remove the loops by shutting down selected bridge interfaces. Refers to both the IEEE 802.1 Spanning-Tree Protocol standard and the earlier Digital Equipment Corporation Spanning-Tree Protocol upon which it is based. The IEEE version supports bridge domains and allows the bridge to construct a loop-free topology across an extended LAN. The IEEE version generally is preferred over the Digital version.
SWAN	Structured Wireless-Aware Network. Comprehensive Cisco framework for deploying, operating, and managing Cisco access points through use of the Cisco infrastructure. Extends to the wireless LAN the same level of security, scalability, and reliability that customers have come to expect in their wired LAN by introducing wireless-aware capabilities into the Cisco infrastructure.
T	
TACACS+	Terminal Access Controller Access Control System Plus. Proprietary Cisco enhancement to Terminal Access Controller Access Control System (TACACS). Provides additional support for authentication, authorization, and accounting.
TCP	Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.
TFTP	Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).
threshold	A range within which you expect your network to perform. If a threshold is exceeded or goes below the expected bounds, you examine the areas for potential problems. You can create thresholds for a specific device.
TKIP	Temporal Key Integrity Protocol, also known as key hashing, is used as part of server-based EAP authentication.
traceroute	This is a diagnostic tool that helps you understand why ping fails or why applications time out. Using it, can view each hop (or gateway) on the route to your device and how long each took.
U	
U-APSD	Unsolicited Automatic Power Save Delivery. A feature that provides a dramatic improvement in talk time for battery-powered handsets.

UDP User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

unmanaged APs APs that do not participate in the SWAN architecture, so that their channel and transmit powers cannot be controlled by WLSE. These might be rogue devices, legitimate devices in adjacent premises, or local devices where SWAN participation is not yet enabled.

uplink Transmissions from client to AP.

UTC Coordinated Universal Time. Time zone at zero degrees longitude. Formerly called Greenwich Mean Time (GMT) and Zulu time.

V

VAD Voice activity detection. This feature detects when the local user is silent and does not transmit any speech frames during those times.

VIP Virtual IP address. Required for each node in a redundant pair of WLSEs. For more information, see [Redundancy Requirements, page 16-29](#).

VLAN Virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VLAN ID Virtual Local Area Network identification used by the standard 802.1Q. Being on 12 bits, it allows the identification of 4096 VLANs.

W

WDC Windows Domain Controller.

WDS Wireless Domain Services. A device providing WDS on the wireless LAN maintains a cache of credentials for clients that are capable of using CCKM (Cisco Centralized Key Management). When a CCKM-capable client roams from one access point to another, WDS forwards the client's credentials to the new access point with the multicast key. *See also* [WLCCP](#).

WDS devices Devices that provides WDS to other access points. *See also* [infrastructure access points, WLSM](#).

WEP keys	Wired equivalent privacy (WEP) keys are the IEEE 802.11b standard that offers a mechanism for securing wireless LAN data streams. The goals of WEP include access control to prevent unauthorized users who lack a correct WEP key from gaining access to the network, and privacy to protect wireless LAN data streams by encrypting them and allowing de-encryption only by users with the correct WEP keys.
WGB	Workgroup bridges connect Ethernet-enabled laptops or other portable computers to a wireless LAN (WLAN), providing the link from these devices to any Cisco access point or wireless bridge.
WINS	Microsoft Windows Internet Naming Service is a name resolution service that resolves computer names to IP addresses.
wireless bridge	Device that connects two or more networks (typically located in different buildings). Bridges connect hard-to-wire sites, non-contiguous floors, satellite offices, school or corporate campus settings, temporary networks, and warehouses. For functional flexibility, the wireless bridge may also be configured as an access point.
WISPr	Wi-Fi Service Provider Roaming.
WLAN	Wireless Local Area Network.
WLCCP	Wireless LAN Context Control Protocol. Protocol used by the WLSE to authenticate with a device that provides WDS to the wireless LAN network. <i>See also</i> WDS .
WLSE 1030	Hardware platform for the WLSE Express .
WLSE 1130 series	WLSE appliances based on the 1130-19, and 1133 hardware platforms.
WLSE Express	WLSE based on the WLSE 1030 hardware platform. The WLSE express manages fewer access points than the WLSE and has the following extra features: internal AAA server, the master configuration file feature (Admin > Appliance > Master Configuration), and the TFTP server feature (Admin > Appliance > TFTP Management).
WLSM	Wireless LAN Services Module. A module for the Cisco Catalyst 6500 series switch that provides WDS to the wireless network. <i>See also</i> WDS .
WNM	Wireless network manager. WNM manages the devices on your wireless LAN.
WPA	Wi-Fi Protected Access. WPA is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP for data protection and 802.1X for authenticated key management.



Symbols

/tftpboot/public directory [16-45](#)

Numerics

802.11a radio

 configuring [5-27](#)

 definition [GL-1](#)

802.11b/g radio

 configuring [5-19](#)

 definition [GL-1](#)

A

AAA, definition [GL-1](#)

AAA-accounting.log file [18-28](#)

AAA-cli.log file [18-28](#)

AAA-daemon-manager.log file [18-28](#)

AAA-database.log file [18-28](#)

AAA server, external

 ACS failed login report [16-57](#)

 AP 1100 or AP 1210 used as AAA server [4-15](#)

 Cisco ACS, ports used by [C-1](#)

 faults [3-1](#)

 monitoring [4-14](#)

 services supported [4-14](#)

 summary report [10-80](#)

 using both interfaces on WLSE [17-14](#)

AAA server, internal

 backup and restore, about [18-5](#)

 certificates, about [18-5](#)

 Cisco-PEAP

 configuring, using CLI [18-32](#)

 configuring, using UI [18-18](#)

clients

 managing, using CLI [18-33](#)

 managing, using UI [18-23](#)

configuring

 overview [18-6](#)

 using CLI commands [18-30](#)

 using UI [18-7](#)

database, reinitializing [18-42](#)

domain authentication

 configuring, using CLI [18-45](#)

 configuring, using UI [18-15](#)

domain authentication, port used for [C-2](#)

EAP-FAST

 configuring, using CLI [18-35](#)

 configuring, using UI [18-21](#)

EAP services supported [18-4](#)

EAP-TLS

 configuring, using CLI [18-21](#)

 configuring, using UI [18-21](#)

fault monitoring [18-5](#)

faults [3-1](#)

groups

 defining [18-26](#)

 mapping, using CLI [18-34](#)

 mapping, using UI [18-15](#)

LDAP central server

 configuring, using CLI [18-37](#)

 configuring, using UI [18-11](#)

LDAP local server

 configuring, using CLI [18-37](#)

 configuring, using UI [18-12](#)

- LDAP parameters, about [18-13](#)
- LEAP
 - configuring, using CLI [18-39](#)
 - configuring, using UI [18-18](#)
- local user database
 - configuring, using CLI [18-45](#)
 - configuring, using UI [18-24](#)
- logging
 - configuring [18-40](#)
 - local [18-40](#)
 - syslog [18-40](#)
- logs [18-28](#)
- monitoring [18-28](#)
- MS-PEAP
 - configuring, using CLI [18-41](#)
 - configuring, using UI [18-19](#)
- naming guidelines [18-6](#)
- overview [18-1](#)
- ports used [18-5](#)
- processes [18-9](#)
- RADIUS attributes of the AAA server [18-46](#)
- reports
 - about [18-5](#)
 - enabling [18-28](#)
- RSA keys, about [18-5](#)
- sessions
 - managing, using CLI [18-43](#)
 - managing, using UI [18-27](#)
- software upgrade, about [18-5](#)
- starting and stopping [18-43](#)
- status
 - displaying, using CLI [18-9](#)
 - displaying, using UI [18-44](#)
- summary report [10-80](#)
- syslog, using [18-40](#)
- trace levels
 - setting, using the CLI [18-44](#)
 - setting, using the UI [18-10](#)
 - trace log [18-28](#)
- tunneling attributes [18-50](#)
- users
 - database, methods for storing [18-3](#)
 - local database, configuring using CLI [18-45](#)
 - local database, configuring using UI [18-24](#)
- AAA-server.log file [18-28](#)
- aaa-server cisco-peap command (WLSE Express) [18-32](#)
- aaa-server client command (WLSE Express) [18-33](#)
- aaa-server domain-auth command (WLSE Express) [18-34](#)
- aaa-server ldap command (WLSE Express) [18-37](#)
- aaa-server leap command (WLSE Express) [18-39](#)
- aaa-server logging command (WLSE Express) [18-40](#)
- aaa-server reinit command (WLSE Express) [18-42](#)
- aaa-server start command (WLSE Express) [18-43](#)
- aaa-server status command (WLSE Express) [18-44](#)
- AAA-server-trace.log file [18-28](#)
- aaa-server trace command (WLSE Express) [18-44](#)
- aaa-server user command (WLSE Express) [18-45](#)
- aaa-server usergroup command (WLSE Express) [18-45](#)
- AAA-status.log file [18-28](#)
- access point
 - category types [14-12](#)
 - configured as an AAA server [4-15](#)
 - configuring
 - ports used for [16-1](#)
 - updating firmware [9-3](#)
 - using Deployment Wizard [2-1](#)
 - using Deployment Wizard templates [7-1](#)
 - using IOS templates [5-1](#)
 - using radio manager assisted configuration [13-71](#)
 - using WLSM templates [6-1](#)
- credentials
 - entering on WLSE [4-5](#)
- definition [GL-1](#)
- duplicate IP addresses, handling [4-61](#)
- faults
 - displaying [3-4](#)
 - notification settings [3-56](#)
 - policy settings [3-10](#)

- thresholds settings [3-10](#)
- firmware
 - updating [9-3](#)
- friendly to rogue reclassification [14-12](#)
- infrastructure AP, definition [GL-6](#)
- replacing [4-61](#)
- reports [10-47](#)
- rogue AP detection [14-12](#)
- scanning-only APs [12-19](#)
- specific settings
 - configuring [5-98](#)
 - exporting [8-50](#)
 - importing [8-48](#)
 - managing [8-47](#)
 - report [8-52](#)
 - viewing [8-51](#)
- SSH passwords, entering on WLSE [4-10](#)
- system-defined groups for [4-74](#)
- Telnet passwords, entering on WLSE [4-10](#)
- user-defined groups for [4-77](#)
- viewing in Location Manager [13-2](#)
- WDS access point [11-8](#)
- access point reports
 - AP and bridge connected to router report [10-80](#)
 - AP and bridge connected to switch report [10-78](#)
 - associated client statistics real-time report [10-101](#)
 - associations report [10-69](#)
 - auto config retry report [10-63](#)
 - CPU utilization real-time report [10-99](#)
 - detailed report [10-67](#)
 - EAP and MAC failed authentications report [10-75](#)
 - Ethernet transmission statistics report [10-91](#)
 - failed authentication and login attempt per AP report [10-76](#)
 - group CDP inline power report [10-59](#)
 - group client association report [10-48](#)
 - group client port [10-56](#)
 - group identity report [10-57](#)
 - group inventory [10-60](#)
 - group MBSSID report [10-53](#)
 - group performance report
 - Ethernet utilization [10-86](#)
 - RF utilization [10-85](#)
 - group security report [10-50](#)
 - group security violation report [10-59](#)
 - group serial number report [10-58](#)
 - group SSID report [10-52](#)
 - group VLAN report [10-54](#)
 - hot standby report [10-74](#)
 - LBS [10-61](#)
 - MBSSID report [10-72](#)
 - memory utilization real-time report [10-98](#)
 - packet errors real-time report [10-100](#)
 - packet statistics real-time report [10-99](#)
 - per VLAN client (group) report [10-55](#)
 - per VLAN client (individual) report [10-73](#)
 - QoS report [10-70](#)
 - radio utilization real-time report [10-101](#)
 - RF and Ethernet utilization graph [10-92](#)
 - RF and Ethernet utilization tabular report [10-92](#)
 - RF transmission statistics report [10-89](#)
 - SSID report [10-71](#)
 - summary report [10-65](#)
 - top n busiest clients report [10-93](#)
 - top n client MIC error rate report [10-94](#)
 - top n number of associations graph report [10-88](#)
 - top n number of associations tabular report [10-87](#)
 - top n percentage errors report [10-88](#)
 - version summary report [10-62](#)
 - VLAN report [10-73](#)
- ACS Failed Login report
 - running [16-60](#)
- ad-hoc network detection [14-37](#)
 - disabled faults [11-4](#)
 - faults [14-46](#)
 - guidelines [14-37](#)
 - managing faults [14-39](#)
 - understanding [14-37](#)

- admin access
 - setting [5-34](#)
- advanced
 - security, configuring [5-59](#)
- aggregation data for reports, intervals
 - about [4-69](#)
 - resetting [4-66](#)
 - understanding [4-69](#)
- apptyp command [A-7](#)
- AP radio scans [13-43](#)
- AP summary report [10-65](#)
- AP usage report, displaying [10-81](#)
- archives
 - managing, configuration [8-1](#)
- ARP, definition [GL-1](#)
- ARP cache, configuring [5-87](#)
- assisted configuration, radio manager
 - guidelines [13-72](#)
 - jobs [13-73](#)
 - calculating parameters [13-79](#)
 - copying [13-75](#)
 - deleting [13-75](#)
 - editing [13-74](#)
 - filtering [13-74](#)
 - refreshing job list [13-75](#)
 - viewing details [13-75](#)
 - viewing run log [13-75](#)
- assisted site survey
 - client walkabout [13-19](#)
 - performing radio scan [13-17](#)
 - radio parameters, generating [13-19](#)
 - selecting APs [13-17](#)
- audience for this document [xxiv](#)
- auth command [A-7](#)
- authentication (WLSE)
 - CLI
 - displaying [A-44](#)
 - enabling [A-7](#)
 - external authentication of WLSE users [16-15](#)
 - HTTPS
 - displaying [A-44](#)
 - enabling [A-7](#)
 - modules supported [16-15](#)
 - overview [16-15](#)
 - setting up
 - using CLI command [17-4](#)
 - using Web interface [16-16](#)
- authentication, access point
 - failed and login attempt per AP report [10-76](#)
 - failed for EAP and MAC report, displaying [10-75](#)
- authentication/protection attack detection [14-63](#)
 - enabling, disabling [14-65](#)
 - faults [14-79](#)
 - guidelines [14-64](#)
 - policies and thresholds [14-65](#)
 - understanding [14-63](#)
- auto config retry group report [10-63](#)
- auto-managed configuration [8-43](#)
 - assigning [8-43](#)
 - options for email [8-47](#)
- automatic configurations, creating [8-39](#)
- auto re-site survey [12-6](#)
 - checking for performance degradations [12-10](#)
 - collecting baseline data [12-8](#)
 - disabled faults [11-4](#)
 - enabling, disabling [12-8](#)
 - guidelines for running [12-7](#)
 - monitoring AP performance [12-10](#)
 - reviewing run log [12-8](#)
 - running [12-8](#)
 - selecting floors [12-8](#)
 - understanding [12-6](#)
- AVVID, definition [GL-1](#)

B

- backing up and restoring WLSE configuration
 - backing up

- using CLI commands [17-6](#)
 - using SCP (secure copy) [16-22](#)
 - using Web interface [16-23](#)
- backup and restore log
 - clearing [16-21](#)
 - displaying [16-5](#)
- backup CLI command [A-8](#)
- backupconfig CLI command [A-9](#)
- backup location, configuring
 - on Windows server [16-22](#)
 - using the CLI [17-5](#)
 - using the Web interface [16-21](#)
- files in /tftpboot/public directory [16-46](#)
- listbackup CLI command [A-28](#)
- pre-released to released software not allowed [16-20](#)
- redundant nodes, backup and restore on [16-37](#)
- restore CLI command [A-41](#)
- restoring
 - from one WLSE to another [17-9](#)
 - using the CLI [17-7](#)
 - using Web interface [16-24](#)
- secure copy (SCP) [16-22](#)
- show backupconfig CLI command [A-44](#)
- backup command [A-8](#)
- backupconfig command [A-9](#)
- basic security template, configuring
 - IOS template [5-12](#)
- basic template, configuring
 - IOS template [5-8](#)
- BDPU, definition [GL-10](#)
- beta software, on WLSE
 - upgrade not allowed [16-7](#)
- black hole mitigation
 - definition [GL-2](#)
 - enabling [13-79](#)
- booting, WLSE
 - boot messages, displaying [A-45](#)
 - from the maintenance image [17-18](#)
 - from Web interface [16-7](#)
- reload command [A-38](#)
- BOOTP
 - definition [GL-2](#)
- bridge
 - definition [GL-2](#)
 - firmware, updating [9-3](#)
 - IOS, configuring [5-1](#)
- bridge reports
 - AP and bridge connected to router report [10-80](#)
 - AP and bridge connected to switch report [10-78](#)
 - associations report [10-69](#)
 - detailed report [10-67](#)
 - Ethernet transmission statistics report [10-91](#)
 - group auto config retry report [10-63](#)
 - group client association report [10-48](#)
 - group client report [10-56](#)
 - group identity report [10-57](#)
 - group inventory report [10-60](#)
 - group LBS report [10-61](#)
 - group MBSSID report [10-53](#)
 - group performance report
 - Ethernet utilization [10-86](#)
 - RF utilization [10-85](#)
 - group security report [10-50](#)
 - group serial number report [10-58](#)
 - group SSID report [10-52](#)
 - group version summary report [10-62](#)
 - group VLAN report [10-54](#)
 - per VLAN client (group) report [10-55](#)
 - per VLAN client (individual) report [10-73](#)
 - RF and Ethernet utilization graph [10-92](#)
 - RF transmission statistics report [10-89](#)
 - top n number associations graph report [10-88](#)
 - top n number associations tabular report [10-87](#)
 - top n percentage errors report [10-88](#)
- browser
 - configuring [1-4](#)
 - date and time display [1-10](#)
 - supported browsers [1-4](#)

BSS, definition [GL-2](#)

BSSID

definition [GL-2](#)

multiple [11-14](#)

C

cautions

backup from pre-released to released software on WLSE
not allowed [16-20](#)

configuring for redundancy [16-33](#)

erase config command [A-18](#)

losing data

jobs, configuration [8-11](#)

jobs, firmware [9-12](#)

NAT, not supported on WLSE [1-1](#)

radiomanager command [A-35](#)

reload command [A-38](#)

shutdown command, failure to run [A-66](#)

significance of [xxiv](#)

upgrading from pre-release software not allowed [16-7](#)

CCK, definition [GL-2](#)

CCKM, definition [GL-2](#)

CCMP, definition [GL-2](#)

CDP (Cisco Discovery Protocol)

alternatives to [4-28](#)

configuring [5-68](#)

definition [GL-2](#)

individual device seeding [4-28](#)

neighbors of WLSE, displaying [A-46](#)

status on WLSE, displaying [A-47](#)

understanding [4-26](#)

CDPbrdcast process (on WLSE) [16-42](#)

cdp command [A-10](#)

CDP distance

definition [GL-3](#)

specifying [4-36](#)

channel load data

determining [10-19](#)

historical [10-21](#)

reviewing [10-19](#)

channels, monitoring [12-4](#)

character set, allowable (in WLSE UI) [B-1](#)

ciscoinstall.log [16-5](#)

CiscoWorks server

adding links to a WLSE [1-3](#)

exporting devices to [4-71](#)

importing devices from

procedure for [4-39](#)

understanding [4-31](#)

linking to CiscoWorks server [16-57](#)

CKIP, definition [GL-2](#)

clearbackuphosts command [A-11](#)

clear command [A-11](#)

CLI

access to, configuring [16-51](#)

command history feature [A-2](#)

command privileges [A-2](#)

commands [A-1](#)

command summary (table) [A-3](#)

conventions [A-2](#)

definition [GL-3](#)

help for commands [A-2](#)

logging into [17-2](#)

maintenance image commands [A-73](#)

erase config [A-73](#)

fsck [A-73](#)

reload [A-73](#)

Privilege Level 0 commands [A-7](#)

apptyp [A-7](#)

exit [A-18](#)

ping [A-34](#)

show clock [A-47](#)

show domain-name [A-50](#)

show interfaces [A-53](#)

show version [A-63](#)

traceroute [A-70](#)

Privilege Level 15 commands [A-7](#)

aaa-server cisco-peap (WLSE Express) [18-32](#)
aaa-server client (WLSE Express) [18-33](#)
aaa-server domain-auth (WLSE Express) [18-34](#)
aaa-server ldap (WLSE Express) [18-37](#)
aaa-server leap (WLSE Express) [18-39](#)
aaa-server logging (WLSE Express) [18-40](#)
aaa-server reinit (WLSE Express) [18-42](#)
aaa-server session (WLSE Express) [18-43](#)
aaa-server start (WLSE Express) [18-43](#)
aaa-server status (WLSE Express) [18-44](#)
aaa-server trace (WLSE Express) [18-44](#)
aaa-server user (WLSE Express) [18-45](#)
aaa-server usergroup (WLSE Express) [18-45](#)
auth [A-7](#)
backup [A-8](#)
backupconfig [A-9](#)
cdp [A-10](#)
clear [A-11](#)
clearbackuphosts [A-11](#)
clock [A-12](#)
debug [A-13](#)
diagnostic-info [A-15](#)
dumpcores [A-15](#)
dumptcp [A-16](#)
dumptech [A-17](#)
erase config [A-17](#)
firewall [A-19](#)
gethostbyname [A-20](#)
hostname [A-21](#)
http-server [A-21](#)
import [A-22](#)
interface [A-25](#)
ip domain-name [A-26](#)
ip name-server [A-27](#)
listbackup [A-28](#)
mail [A-28](#)
mailcntrl clear [A-30](#)
mailroute [A-30](#)
mkcert [A-31](#)
nslookup [A-32](#)
ntp server [A-32](#)
ps [A-35](#)
radiomanager [A-35](#)
redundancy [A-36](#)
reload [A-38](#)
repository [A-38](#)
reset device-snmp [A-40](#)
restore [A-41](#)
route [A-42](#)
services [A-42](#)
setup [A-43](#)
show auth-cli [A-44](#)
show auth-http [A-44](#)
show backupconfig [A-44](#)
show backuplog [A-45](#)
show bootlog [A-45](#)
show cdp-neighbor [A-46](#)
show cdp-run [A-47](#)
show config [A-48](#)
show import [A-51](#)
show process [A-55](#)
show redundancy [A-56](#)
show route [A-57](#)
show ssh-server [A-59](#)
show ssh-version [A-59](#)
show syslog [A-60](#)
show tech [A-61](#)
show time [A-62](#)
shutdown [A-65](#)
snmp-server [A-66](#)
ssh host [A-67](#)
ssh-server accept [A-67](#)
ssh-version [A-68](#)
tarlog [A-68](#)
telnetenable [A-69](#)
tftpserver [A-70](#)
username [A-71](#)
webtimeout [A-72](#)

- wlseconfig (do not use this command) [A-6](#)
- syntax, checking [A-2](#)
- timeout period [17-2](#)
- typographical conventions [A-3](#)
- use of quotes in commands [A-2](#)
- using [A-1](#)
- client
 - inventory of associations [4-63](#)
 - of internal AAA server [18-23](#)
 - tracking, through WDS [4-18](#)
 - unregistered clients, detecting [14-58](#)
- client polling interval, setting [4-68](#)
- client reports
 - access failure report, displaying [10-42](#)
 - associated clients statistics real-time report, displaying [10-101](#)
 - detail report, displaying [10-37](#)
 - enhanced (WDS) client tracking [4-18](#)
 - group association report, displaying [10-48](#)
 - group report [10-56](#)
 - historical association report [10-40](#)
 - per VLAN (group) report, displaying [10-55](#)
 - per VLAN (individual) report, displaying [10-73](#)
 - RADIUS username in [4-22](#)
 - statistics report [10-39](#)
 - top n busiest clients [10-93](#)
 - top n busiest report, displaying [10-93](#)
 - top n client MIC error rate report [10-94](#)
 - top n MIC error rate report, displaying [10-94](#)
 - voice client detail report, displaying [10-43](#)
- client tracking, WDS
 - about [4-20](#)
 - configuring [4-19](#)
- client walkabout
 - AP locations, viewing [13-60](#)
 - AP power setting, choosing [13-63](#)
 - client MAC addresses, entering [13-63](#)
 - guidelines for running [13-55](#)
 - jobs
 - checking status [13-57](#)
 - creating [13-61](#)
 - deleting [13-59](#)
 - details, viewing [13-59](#)
 - managing [13-59](#)
 - refreshing job list [13-60](#)
 - run logs [13-65](#)
 - running [13-64](#)
 - starting and stopping [13-59](#)
 - viewing [13-60](#)
 - radio location data, collecting [13-54](#)
 - results
 - viewing [13-59](#)
 - understanding [13-54](#)
- clock set command [A-12](#)
- CMIC, definition [GL-3](#)
- collector log, displaying [A-48](#)
- command reference, WLSE CLI [A-1](#)
- community strings
 - definition [GL-3](#)
 - guidelines [4-8](#)
 - recommendations [4-8](#)
 - requirement for [4-6](#)
 - specifying [4-6](#)
- community strings, WLSE
 - configuring [A-66](#)
 - displaying [A-59](#)
 - resetting [A-40](#)
- configbackup.log [16-5](#)
- configexport.log [16-5](#)
- configuration, access points
 - configuration history, viewing device's [10-7](#)
 - configuration history report [10-14](#)
 - radio manager assisted configuration [13-71](#)
- configuration, WLSE
 - backing up
 - by using the CLI [17-5](#)
 - using Web interface [16-20](#)
 - copying to another WLSE [17-9](#)

- Ethernet interfaces [17-12](#)
- high availability [16-32](#)
- master configuration file (WLSE Express) [16-26](#)
- redundancy [16-32](#)
- restoring
 - by using the CLI [17-7](#)
 - using Web interface [16-20](#)
 - using DHCP for [16-26](#)
- configuration archives
 - recommendations for using [8-27](#)
- configured radio parameters report [10-16](#)
- connectivity (WLSE), testing [16-47](#)
- console, using with WLSE [17-2](#)
- conventions
 - CLI [A-2](#)
 - in command descriptions [A-3](#)
- core files, command for saving [A-15](#)
- CoS (class of service)
 - definition [GL-3](#)
- CPU (WLSE), displaying [A-63](#)
- credentials, devices
 - configuring
 - Deployment Wizard [2-4](#)
 - entering on WLSE
 - manually [4-5](#)
 - entering on WLSE, using Deployment Wizard [2-4](#)
 - HTTP port [4-13](#)
 - SNMP [4-6](#)
 - Telnet/SSH [4-10](#)
 - WLCCP [4-13](#)
- CSR, definition [GL-3](#)
- CSV
 - definition [GL-3](#)
 - files, about
 - device [4-30](#)
- CSV files, about
 - device specific settings [8-48](#)
- current reports [10-45](#)
 - AP and bridge connected to router report [10-80](#)
 - AP and bridge connected to switch report [10-78](#)
 - AP summary [10-65](#)
 - AP usage report [10-81](#)
 - associations [10-69](#)
 - detailed [10-67](#)
 - EAP and MAC failed authentications report [10-75](#)
 - failed authentications and login attempt per AP report [10-76](#)
 - group auto config retry report [10-63](#)
 - group CDP inline power report [10-59](#)
 - group client association [10-48](#)
 - group client report [10-56](#)
 - group identity report [10-57](#)
 - group inventory report [10-60](#)
 - group LBS report [10-61](#)
 - group MBSSID [10-53](#)
 - group mobility ID report [10-62](#)
 - group security [10-50](#)
 - group security violation report [10-59](#)
 - group serial number report [10-58](#)
 - group SSID [10-52](#)
 - group version summary report [10-62](#)
 - group VLAN [10-54](#)
 - hot standby report [10-74](#)
 - MBSSID report [10-72](#)
 - per VLAN (group) client report [10-55](#)
 - per VLAN client (individual) report [10-73](#)
 - QoS report [10-70](#)
 - RADIUS authentication [10-69](#)
 - router summary [10-79](#)
 - server summary report [10-80](#)
 - SSID report [10-71](#)
 - switch summary [10-77](#)
 - VLAN report [10-73](#)
 - WLSM modules [10-78](#)
- current users of WLSE, listing [16-19](#)
- custom values, configuring
 - IOS template [5-98](#)
 - WLSM template [6-10](#)

cxexport.log [16-5](#)

D

daemon log, displaying

- using CLI command [A-48](#)
- using Web interface [16-5](#)

daemon manager log, displaying

- using CLI command [A-49](#)
- using Web interface [16-5](#)

daemons.log file [16-5](#)

database

- backing up [16-20](#)
- purging [17-18](#)
- reinitializing [A-37](#)
- restoring [16-20](#)

dataUpdate.log [16-5](#)

date and time

- in WLSE displays [1-10](#)
- setting
 - browser time [16-43](#)
 - by using CLI command [A-12](#)
 - by using NTP [17-11](#)
 - current local time [16-43](#)
- synchronizing to a time server
 - using CLI command [A-32](#)
 - using Web interface [16-44](#)

db2runstatlast.log [16-5](#)

db2runstattimes.log [16-5](#)

db2uext2.log file [16-5](#)

debug command [A-13](#)

Deployment Wizard

- about [2-1](#)
- deploying devices [2-9](#)
- launch at login, enable or disable [2-3](#)
- requirements [2-4](#)
- templates, creating [2-4](#)
- templates, managing [7-1](#)
- wlsestartup.ini file [2-3](#)

detailed report [10-67](#)

device_events.log [16-5](#)

device center [10-7](#)

Device Credentials option [4-5](#)

device name

- characters allowed in [B-2](#)
- display of, configuring [4-41](#)
- display of, effects of reverse DNS lookup [4-44](#)
- format of [4-41](#)

devices

- adding to location manager [13-14](#)
- auto-management [4-45](#)
- configuring
 - archive jobs [8-33](#)
 - configuration jobs [8-10](#)
 - Deployment Wizard [2-1](#)
 - Deployment Wizard templates, managing [7-1](#)
 - firmware, updating [9-1](#)
 - IOS templates, using [5-1](#)
 - managing configuration jobs [8-7](#)
 - managing Deployment Wizard templates [7-1](#)
 - using IOS templates [5-1](#)
 - using WLSM templates [6-1](#)

connectivity, testing [16-47](#)

credentials, setting manually [4-5](#)

deleting [4-60](#)

device history report, displaying [10-13](#)

device identifier, selecting the type [4-41](#)

device name, display of [1-10](#)

- specifying the format [4-41](#)

exporting

- to a file [4-73](#)
- to CiscoWorks server [4-71](#)

fault summary, viewing [10-7](#)

firmware, updating [9-1](#)

grouping [4-74](#)

history viewing [10-7](#)

how WLSE communicates with devices [4-3](#)

managing

- auto-management [4-45](#)
 - device detail display [4-57](#)
 - limitation on number of [4-60](#)
 - limitations, displaying [A-63](#)
 - management state, changing [4-54](#)
 - understanding [4-24](#)
 - unmanaged [4-54](#)
- DFS, definition [GL-3](#)
- DHCP
 - definition [GL-3](#)
 - used with Deployment Wizard [2-1](#)
 - using for initial configuration of WLSE Express [16-26](#)
- dhcp.log [16-5](#)
- diagnostic-info.log [16-5](#)
- diagnostic-info command [A-15](#)
- diagnostics, WLSE
 - log files [16-4](#)
 - processes, viewing [16-42](#)
 - self-test [16-40](#)
 - status reports [16-39](#)
- discovery
 - advanced options [4-41](#)
 - after WLSE restarts [16-7](#)
 - CDP discovery, running [4-34](#)
 - device import
 - running [4-38](#)
 - understanding [4-29](#)
- Discovery Run Details window [4-48](#)
- filtering
 - by IP address [4-47](#)
 - by MAC address (access points) [4-45](#)
- history [4-69](#)
- individual device seeding [4-28](#)
- logs
 - deleting [4-65](#)
 - viewing [4-48](#)
- messages [4-50](#)
- port used for [C-1](#)
- troubleshooting, common problems [4-52](#)
- understanding [4-24](#)
- wizard [4-33](#)
- Discovery Run Details window [4-48](#)
- disk
 - capacity, displaying [A-63](#)
 - checking and repairing [A-73](#)
 - usage, viewing [A-13](#)
- dmgttd.log file [16-6](#)
- DNS
 - configuring [5-69](#)
 - definition [GL-4](#)
 - name servers, specifying
 - using CLI command [A-27](#)
 - using Web interface [16-44](#)
 - port for IOS AP configuration [C-1](#)
 - reverse lookup
 - effect on device name display [4-44](#)
 - enabling [4-44](#)
- documentation [xxiv](#)
 - audience for this [xxiv](#)
 - locating on Cisco.com [xxiv](#)
 - typographical conventions in [xxiv](#)
- domain name
 - default, defining [A-26](#)
 - displaying [A-50](#)
- DSCP, definition [GL-4](#)
- DTIM, definition [GL-4](#)
- dumpcores
 - command description [A-15](#)
- dumptcp
 - command description [A-16](#)
 - log file [16-6](#)
- dumptech.tgz [16-6](#)
- dumptech command [A-17](#)
- Duplicate IP folder (Managed Devices)
 - contents of [4-61](#)
 - description [4-56](#)
 - duplicate IP detection, fault policy for [3-49](#)

E

EAP and MAC failed authentications

report, displaying [10-75](#)

EAP-FAST

definition [GL-4](#)

server

adding to WLSE [4-16](#)

prerequisites for adding to WLSE [4-15](#)

EAP-MD5 server

AP usage report, displaying [10-81](#)

definition [GL-4](#)

summary report, displaying [10-80](#)

EAPOL, definition [GL-4](#)

EAPOL flooding

understanding [14-64](#)

EAPOL flooding thresholds

EAPOL detection (IOS) policy [14-72](#)

EAPOL settings (IOS) policy [14-71](#)

EAP-TLS

configuring [18-21](#)

definition [GL-4](#)

email

automatic configuration results [8-47](#)

fault notifications [3-61](#)

logs and queues

managing [A-30](#)

viewing, using CLI command [A-54](#)

viewing, using Web interface [16-4](#)

mail server

specifying by using the CLI [17-15](#)

mail server, specifying

by using Web interface [16-45](#)

redundancy messages [16-31](#)

report [10-3](#)

scheduling [10-5](#)

testing and debugging [A-28](#)

EMF (excessive management frame transmissions),

detecting [14-47](#)

EMF detection [14-47](#)

displaying faults [14-49](#)

enabling, disabling [14-48](#), [15-6](#)

guidelines [14-48](#)

reports [14-50](#)

understanding [14-47](#)

viewing EMF statistics [14-50](#)

encryption failures

understanding [14-63](#)

erase config command [A-17](#)

erasing system configuration

CLI command for [A-17](#)

procedure for [17-18](#)

error.log file [16-6](#)

Ethernet, configuring fast [5-18](#)

Ethernet, WLSE

firewall CLI command [A-19](#)

interface CLI command [A-25](#)

ports, configuring [17-12](#)

Ethertype filters, configuring [5-75](#)

event

log, configuring [5-94](#)

ExcepReporter process (on WLSE) [16-42](#)

excessive management frame transmissions (EMF) [14-47](#)

exit command [A-18](#)

exporting

Deployment Wizard templates [7-4](#)

devices [4-71](#)

IOS templates [5-5](#)

reports

GUI-based, using [10-2](#)

URL-based, using [10-2](#)

WLSM templates [6-5](#)

F

failed authentication and login attempt per AP

report, displaying [10-76](#)

fastEthernet, configuring [5-18](#)

- fast secure roaming, definition [GL-5](#)
- faults
 - access/point bridge thresholds
 - CPU utilization [3-31](#)
 - Ethernet port packet errors [3-33](#)
 - Ethernet port status [3-32](#)
 - Ethernet port utilization [3-33](#)
 - memory utilization [3-31](#)
 - SNMP reachable [3-30](#)
 - access point/bridge policies [3-15](#)
 - disabled [11-4](#)
 - EAP per SSID, Enforced for Cisco-Supplicant [3-18](#)
 - EAP per SSID Enforced, for Mixed-Cisco-Supplicant [3-20](#)
 - EAP per SSID Enforced, for Non-Cisco-Supplicant [3-19](#)
 - firmware version [3-17](#)
 - hotstandby status [3-17](#)
 - HTTP disabled [3-15](#)
 - Key Rotation per VLAN [3-22](#)
 - MIC per VLAN [3-20](#)
 - PSPF per Vlan [3-23](#)
 - registration error [3-18](#)
 - Telnet disabled [3-16](#)
 - WEP Encryption per VLAN [3-23](#)
 - WEP per VLAN [3-21](#)
 - acknowledging [3-7](#)
 - ad hoc network detection [14-41](#)
 - ad hoc network faults [14-39](#)
 - authentication and protection attack [14-79](#)
 - clearing [3-6](#)
 - current [3-51](#)
 - defined [3-2](#)
 - displaying [3-4](#)
 - displaying details [3-7](#)
 - Duplicate IP fault [4-61](#)
 - emailing [3-61](#)
 - EMF detection [14-49](#)
 - exception, definition of [GL-4](#)
 - faults log (WLSE), displaying [16-5](#)
 - fault status report, displaying [10-13](#)
 - IDS [14-4](#)
 - assigning devices to profile [14-9](#)
 - copying profiles [14-7](#)
 - creating profiles [14-6](#)
 - deleting profiles [14-8](#)
 - disabled [11-4](#)
 - displaying [14-4](#)
 - editing profiles [14-8](#)
 - renaming profiles [14-7](#)
 - viewing fault profile summary [14-9](#)
 - interference detection [14-43](#)
 - MFP detection [14-54](#)
 - notification, ports used for [16-1](#)
 - notification settings
 - email [3-61](#)
 - syslog [3-60](#)
 - trap notification [3-56](#)
 - types of [3-56](#)
 - policies
 - radio-802.11x policies [3-24](#)
 - WLSE [3-49](#)
 - policy profiles [3-10](#)
 - process for [16-42](#)
 - radio-801.11x thresholds [3-34](#)
 - associated clients [3-40](#)
 - association rate [3-40](#)
 - max retry count [3-39](#)
 - RF port AdminStatus [3-35](#)
 - RF port packet errors [3-37](#)
 - RF port status [3-34](#)
 - RF port utilization [3-36](#)
 - RF port WEP errors [3-38](#)
 - voice bandwidth [3-41](#)
 - voice QoS status [3-42](#)
 - radio-811x policies
 - Broadcast Disabled [3-26](#)
 - Broadcast SSID [3-24](#)

- disabled [11-4](#)
- Dynamic Frequency Selection [3-29](#)
- EAP Enforced-Cisco Supplicant [3-27](#)
- EAP Enforced-Mixed Supplicant [3-28](#)
- EAP Enforced-Other Supplicant [3-28](#)
- Infrastructure SSID [3-25](#)
- PSPF Enabled [3-26](#)
- WEP Key Length [3-27](#)
- rogue AP detection [14-19](#)
- rogue AP faults [14-19](#)
- router thresholds
 - SNMP reachable [3-48](#)
- security policy, specifying [3-10](#)
- security policy monitoring, understanding [3-2](#)
- settings
 - assigning to devices [3-14](#)
 - copying [3-11](#)
 - creating [3-11](#)
 - deleting [3-13](#)
 - editing [3-12](#)
 - notifications [3-56](#)
 - policies and thresholds [3-14](#)
 - renaming [3-12](#)
 - understanding [3-10](#)
 - viewing [3-13](#)
- states, understanding [3-2](#)
- switch thresholds
 - CPU utilization [3-43](#)
 - memory utilization [3-44](#)
 - module status threshold [3-46](#)
 - port status [3-45](#)
 - port utilization [3-45](#)
 - SNMP reachable [3-43](#)
- threshold-related, understanding [3-3](#)
- thresholds [3-50](#)
 - AAA server response time [3-49](#)
 - access point/bridge [3-30](#)
 - radio-802.11x thresholds [3-34](#)
 - router [3-48](#)
 - specifying [3-10](#)
 - switch [3-42](#)
 - WLSM [3-46](#)
- trap notification settings [3-56](#)
- understanding [3-2](#)
- unregistered clients [14-58](#)
- WDS
 - disabled [11-4](#)
- WDS policies
 - authentication failures [3-50](#)
 - WLSE-WDS link status [3-51](#)
- WLSE policies
 - duplicate IP detection [3-49](#)
- faults.log file [16-6](#)
- files
 - managing with WLSE TFTP server [16-45](#)
 - master configuration file (WLSE Express) [16-26](#)
 - WLSE log files [16-4](#)
- filters
 - discovery
 - by IP Address [4-47](#)
 - by MAC address (access points) [4-45](#)
 - Ethertype, configuring [5-75](#)
 - IP, configuring [5-72](#)
 - MAC address, configuring [5-70](#)
- firewall
 - firewall CLI command [A-19](#)
 - ports on WLSE [16-1](#)
- firmware
 - "not verified" status [9-25](#)
 - estimating change window [9-2](#)
 - firmware history report, displaying [10-14](#)
 - history, viewing device's [10-7](#)
 - how firmware upgrades work [9-1](#)
- images
 - deleting [9-5](#)
 - editing on WLSE [9-4](#)
 - importing [9-6](#)
 - storing on remote TFTP server [9-9](#)

- transfer, ports used for [C-1](#)
- viewing [9-3](#)
- jobs
 - copying [9-23](#)
 - creating [9-12](#)
 - deleting [9-23](#)
 - details, displaying [9-24](#)
 - displaying [9-22](#)
 - editing [9-22](#)
 - failures [9-25](#)
 - job choices [9-12](#)
 - parameters for [9-9](#)
 - protocol, changing [9-23](#)
 - scheduling [9-14](#)
 - status, checking [9-20](#)
 - status, details [9-25](#)
 - validating [9-14](#)
- supported versions, displaying [16-49](#)
- upgrading
 - about [9-1](#)
 - procedures [9-3](#)
- frame monitoring [12-19](#)
 - configuring [12-20](#)
 - displaying APs [12-23](#)
 - enabling, disabling [12-20](#)
 - guidelines for running [12-19](#)
 - scanning-only APs [12-19](#)
 - selecting APs [12-20](#)
 - selecting radio types [12-20](#)
 - understanding [12-19](#)
- frame transmissions (EMF), detecting [14-47](#)
- friendly AP
 - reclassifying to rogue [14-18](#)
 - reports, viewing [14-28](#)
- fsck command [A-73](#)
- FTP
 - port for IOS AP configuration [C-1](#)

G

- gethostbyname command [A-20](#)
- getting started
 - with device management [4-1](#)
 - with WLSE [1-1](#)
- GRE, definition [GL-5](#)
- group reports [10-45](#)
 - auto config retry report, displaying [10-63](#)
 - CDP inline power report, displaying [10-59](#)
 - client association report, displaying [10-48](#)
 - client report, displaying [10-56](#)
 - group client association report, displaying [10-48](#)
 - identity report, displaying [10-57](#)
 - inventory report, displaying [10-60](#)
 - LBS report, displaying [10-61](#)
 - MBSSID report, displaying [10-53](#)
 - mobility ID report, displaying [10-62](#)
 - performance report for Ethernet utilization, displaying [10-86](#)
 - performance report for RF utilization, displaying [10-85](#)
 - per VLAN client report, displaying [10-55](#)
 - security report, displaying [10-50](#)
 - security violation report, displaying [10-59](#)
 - serial number report, displaying [10-58](#)
 - SSID report, displaying [10-52](#)
 - top number of associations graph report, displaying [10-88](#)
 - top number of associations tabular report, displaying [10-87](#)
 - top percentage errors report, displaying [10-88](#)
 - version summary report, displaying [10-62](#)
 - VLAN report, displaying [10-54](#)
- groups
 - copying
 - rule-based [4-83](#)
 - static [4-82](#)
 - creating
 - rules-based [4-81](#)
 - static [4-80](#)

- deleting [4-86](#)
- editing
 - rule-based [4-85](#)
 - static [4-84](#)
- overview [4-74](#)
- rule-based
 - copying [4-83](#)
 - creating [4-81](#)
 - deleting [4-86](#)
 - editing [4-85](#)
- static
 - creating [4-80](#)
 - creating by copying [4-82](#)
 - deleting [4-86](#)
 - editing [4-84](#)
- system-defined [4-74](#)
- understanding [4-74](#)
- user-defined [4-77](#)
- GUI, WLSE
 - About button [1-9](#)
 - dashboard [1-7](#)
 - device name display [1-10](#)
 - Help button [1-9](#)
 - Logout button [1-9](#)
 - Overview button [1-9](#)
 - tabs and subtabs [1-7](#)
 - time display [1-10](#)
 - timeout period
 - default [1-13](#)
 - resetting [16-44](#)
 - Wizard button [1-9](#)
- high availability, WLSE [16-28](#)
- host file
 - displaying, show hosts command [A-50](#)
 - displaying, show import command [A-51](#)
 - importing [A-22](#)
- hostname (WLSE)
 - characters allowed [A-21](#)
- hostname command [A-21](#)
- hostnames (in WLSE dialogs), characters allowed in [B-2](#)
- hostnames, translating to IP addresses [A-32](#)
- hot standby
 - configuring [5-67](#)
 - report, displaying [10-74](#)
- HTTP
 - access to WLSE, configuring [A-21](#)
 - configuring [5-77](#)
 - definition [GL-5](#)
 - http-server command [A-21](#)
 - port for VxWorks access point configuration [C-1](#)
 - WLSE HTTP port, configuring [A-21](#)
 - WLSE Web port for [C-2](#)
- HTTPS
 - access to WLSE, configuring [A-21](#)
 - certificate signed request, obtaining [16-18, A-31](#)
 - definition [GL-6](#)
 - http-server command [A-21](#)
 - log, viewing [16-4](#)
 - port used for [C-2](#)
 - using to export devices [4-73](#)
- http-server command
 - description of [A-21](#)
 - on redundant WLSEs [16-38](#)

H

- HaMibDaemon process (on WLSE) [16-42](#)
- hardware type (WLSE), displaying [A-7](#)
- help
 - CLI, displaying [A-2](#)
 - Web interface [1-9](#)

-
- IBSS, definition [GL-6](#)
 - ICMP, definition [GL-6](#)
 - IDS (Intrusion Detection System)
 - ad-hoc networks, detecting [14-37](#)

- authentication attacks, detecting [14-63](#)
- EMF, detecting [14-47](#)
- enable/disable [A-35](#)
- fault profiles [14-6](#)
- interference, detecting [14-43](#)
- MIC failure
 - definition [GL-7](#)
- network-wide settings [14-11](#)
- policies and thresholds [14-10](#)
- protection attacks, detecting [14-63](#)
- reports [14-5](#)
- rogue AP detection [14-12](#)
- settings [14-6](#)
- settings, remaining [14-11](#)
- summary of intrusions [14-2](#)
- switch ports, detecting and suppressing [14-30](#)
- understanding [14-2](#)
- unregistered clients, detecting [14-58](#)
- IGMP, definition [GL-6](#)
- images
 - access point firmware [9-1](#)
 - using WLSE TFTP server to download [16-45](#)
 - WLSE software [16-7](#)
- import command [A-22](#)
- importing
 - device firmware [9-6](#)
 - devices
 - about CSV files [4-30](#)
 - from CiscoWorks server [4-39](#)
 - from file [4-38](#)
 - understanding [4-29](#)
 - templates
 - IOS [5-4](#)
 - WLSM [6-4](#)
- infrastructure access point, definition [GL-6](#)
- installation (WLSE)
 - configuring the web browser [1-4](#)
 - installing a replacement WLSE [17-8](#)
- interface command [A-25](#)
- interference detection [14-43](#)
 - disabled faults [11-4](#)
 - understanding [14-43](#)
 - viewing faults [14-46](#)
- intrusion detection
 - enable/disable [A-35](#)
 - using [14-1](#)
- inventory
 - after WLSE restarts [16-7](#)
 - automatic
 - polling interval [4-64](#)
 - understanding [4-63](#)
 - client associations inventory [4-63](#)
 - group report, displaying [10-60](#)
 - history [4-69](#)
 - immediate [4-65](#)
 - logs
 - deleting [4-65](#)
 - viewing [4-69](#)
 - performance inventory [4-63](#)
 - polling intervals
 - guidelines for [4-65](#)
 - setting [4-66](#)
 - port used for [C-1](#)
 - run by Radio Manager [4-70](#)
 - running [4-65](#)
 - scheduled [4-63](#)
 - troubleshooting
 - common problems [4-71](#)
- IOS
 - access point reports [10-47](#)
 - templates, using [5-1](#)
- IP address (WLSE), changing [17-14](#)
- IP addresses
 - in UI, display of [1-10](#)
 - of devices
 - displaying [4-44](#)
 - display of [4-41](#)
 - translating to hostnames [A-32](#)

IP chains, displaying [A-50](#)
 ip domain-name command [A-26](#)
 IP filters, configuring [5-72](#)
 ip name-server command [A-27](#)

J

Java Plugin

general requirement [1-5](#)
 requirement for Windows XP repository [16-11](#)

job history truncation interval, setting [4-68](#)

jobs, AP radio scan [13-48](#)

jobs, archive

copying [8-37](#)
 creating [8-33](#)
 deleting [8-37](#)
 editing [8-36](#)
 filtering [8-35](#)
 job run details, viewing [8-37](#)
 managing [8-1](#)
 overview [8-26](#)
 recommendations [8-27](#)
 running again [8-37](#)
 viewing status [8-33](#)

jobs, client walkabout [13-59](#)

jobs, configuration

copying [8-24](#)
 creating [8-18](#)
 deleting [8-24](#)
 editing [8-23](#)
 filtering [8-22](#)
 managing [8-7](#)
 naming guidelines [B-1](#)
 overview [8-8](#)
 recommendations [8-9](#)
 running again [8-23](#)
 undoing [8-24](#)
 viewing status [8-18](#)

jobs, discovery

CDP discovery, running [4-33](#)

import from CiscoWorks server [4-39](#)

job run log [4-48](#)

server time discrepancy message [1-11](#)

jobs, email [10-5](#)

jobs, firmware

copying [9-23](#)
 creating [9-11](#)
 deleting [9-23](#)
 duration [9-18](#)
 editing [9-22](#)
 filtering [9-22](#)
 job run details [9-24](#)
 managing [9-11](#)
 naming guidelines [B-1](#)
 parameters for [9-9](#)
 server time discrepancy message [1-11](#)
 viewing [9-20](#)

jobs, radio manager assisted configuration [13-74](#)

jobs log (jobvm.log), displaying [16-6](#)

L

LBS

group report, displaying [10-61](#)

LDAP

definition [GL-6](#)
 in built-in AAA server (WLSE Express) [18-3](#)

LEAP server

AP usage report, displaying [10-81](#)
 definition [GL-6](#)
 monitoring [3-10](#)
 summary report, displaying [10-80](#)

Links subtab [16-57](#)

listbackup command [A-28](#)

location manager

editing antenna placement [13-28](#)
 enabling/disabling [A-35](#)
 interference reports [13-34](#)

- locating devices [13-27](#)
- measuring tool [13-35](#)
- prerequisites for using [13-2](#)
- server information, obtaining [13-34](#)
- setting up [13-3](#)
- system-defined groups for [4-76](#)
- viewing [13-1](#)
- view modes [13-29](#)
- window
 - tools [13-34](#)
 - understanding [13-36](#)
- logging in (to the WLSE)
 - from Web interface [1-13](#)
 - splash screen, adding a message [16-43](#)
 - via the CLI [17-2](#)
- logging out (from the WLSE)
 - from the CLI [17-3](#)
 - from the Web interface [1-13](#)
- logs, WLSE
 - AAA server logs (WLSE Express) [18-28](#)
 - archiving [A-68](#)
 - ciscoinstall.log [16-5](#)
 - collector log [A-48](#)
 - configbackup.log [16-5](#)
 - configexport.log [16-5](#)
 - cwexport.log [16-5](#)
 - daemon manager log, viewing
 - from Web interface [16-4](#)
 - show dmgtldlog command [A-49](#)
 - daemons log, viewing
 - from the Web interface [16-4](#)
 - show daemonslog command [A-48](#)
 - database logs [16-5](#)
 - dataUpdate.log [16-5](#)
 - db2runstatlast.log [16-5](#)
 - db2runstattimes.log [16-5](#)
 - device_events.log [16-5](#)
 - dhcp.log [16-5](#)
 - diagnostic-info.log [16-5](#)
 - discovery logs
 - deleting [4-65](#)
 - viewing [4-48](#)
 - displaying, using the CLI [17-15](#)
 - displaying, using Web interface [16-4](#)
 - downloading [16-4](#)
 - dumptcp log [16-6](#)
 - dumptechn.tgz [16-6](#)
 - emailing [16-4](#)
 - faults [16-6](#)
 - HTTPS events [16-6](#)
 - install logs [A-51](#)
 - inventory logs
 - deleting [4-65](#)
 - viewing [4-69](#)
 - jobvm log [16-6](#)
 - logs_tgz.log [16-6](#)
 - procps_last.log [16-6](#)
 - radio management [16-6](#)
 - redundancy.log [16-6](#)
 - redundancy logs
 - redundancy.log [16-6](#)
 - systemCheck.log [16-6](#)
 - redundancy events [16-36](#)
 - Repository.log [16-5](#)
 - runstats.log [16-6](#)
 - searching [16-4](#)
 - SNMP agent [16-6](#)
 - software installation [16-6](#)
 - syslog [A-60](#)
 - systemCheck.log [16-6](#)
 - system log [16-42](#)
 - tftp.log [16-6](#)
 - Tomcat log [16-4, A-62](#)
 - trace logging, enabling (WLSE Express) [18-10](#)
 - var_logs_tgz.log [16-6](#)
 - View Log File option [16-4](#)
 - web access log
 - viewing from CLI [A-63](#)

viewing from UI [16-5](#)

Web error log

viewing from CLI [A-64](#)

viewing from Web interface [16-4](#)

web SSL access log

viewing, from CLI [A-65](#)

viewing, from Web interface [16-5](#)

M

MAC address

filters (discovery) [4-45](#)

filters, configuring [5-70](#)

WLSE MAC address, displaying [A-53](#)

MAC spoofing

policy [14-70](#)

understanding [14-63](#)

mailcntrl clear command [A-30](#)

mail command [A-28](#)

mailroute command [A-30](#)

mail server

specifying by using the CLI [17-15](#)

specifying by using Web interface [16-45](#)

maintenance image, WLSE

booting from [17-18](#)

CLI commands for [A-73](#)

using [17-18](#)

Managed folder (Managed Devices) [4-55](#)

management frame protection

displaying faults [14-54](#)

enabling/disabling [14-53](#)

understanding [14-52](#)

viewing MFP events [14-56](#)

management services (WLSE), stopping/starting [17-15](#)

Manage Roles option [16-49](#)

Manage Users option [16-51](#)

managing devices

auto-manage options [4-45](#)

changing device state [4-56](#)

deleting devices [4-60](#)

device descriptions, entering [4-59](#)

device details

understanding [4-57](#)

viewing [4-57](#)

Managed Devices folders [4-55](#)

using the Deployment Wizard [2-1](#)

MBSSID

report, displaying [10-72](#)

understanding [11-14](#)

memory (WLSE), displaying [A-63](#)

mfgtest.log file [16-6](#)

MFP

capabilities, reports [14-55](#)

events, reports [14-56](#)

MHAE, definition [GL-7](#)

MIC/encryption failure thresholds

CcmpDecryptErrorsClient policy [14-69](#)

CcmpReplaysClient policy [14-68](#)

TkipLocalMicFailureClient policy [14-66, 14-70](#)

TkipRemoteMicFailureClient policy [14-67](#)

TkipReplayClient Policy [14-65](#)

MIC failures

understanding [14-63](#)

mkcert command [A-31](#)

mobility groups report, displaying [10-82](#)

mobility ID report, displaying [10-82](#)

mod_jk.log file [16-6](#)

MOK, definition [GL-7](#)

N

name servers, specifying

ip name-server command [A-27](#)

using Web interface [16-44](#)

names of devices

display of [4-41](#)

rules for [B-2](#)

naming guidelines [B-1](#)

- built-in AAA server (WLSE Express) [B-3](#)
- descriptions [B-2](#)
- device names [B-2](#)
- hostnames [B-2](#)
- other names [B-2](#)
- roles [B-1](#)
- users [B-1](#)
- NAT, not supported by WLSE [1-1](#)
- neighbors (of WLSE), displaying [A-46](#)
- Network Address Translation (NAT), not supported by WLSE [1-1](#)
- network connectivity, testing [16-47](#)
- network interfaces
 - configuring
 - fastEthernet [5-18](#)
 - radio-802.11a [5-27](#)
 - radio-802.11b/g [5-19](#)
 - on WLSE
 - configuring, interface CLI command [A-25](#)
 - configuring, procedures for [17-12](#)
 - information about, displaying [A-53](#)
 - IP chains, displaying [A-50](#)
 - using both interfaces [17-14](#)
 - template [5-18](#)
- network management systems, integrating with WLSE [1-3](#)
- New folder (Managed Devices) [4-55](#)
- non-serving channels
 - definition [GL-7](#)
 - monitoring [12-4](#)
- notification settings, faults [3-56](#)
- notification settings, IDS faults [14-12](#)
- nslookup
 - definition [GL-7](#)
 - from CLI [A-32](#)
 - from Web interface [16-47](#)
- NTP (Network Time Protocol)
 - configuring time servers on WLSE
 - ntp server CLI command [A-32](#)
 - using Web interface [16-44](#)
 - definition [GL-7](#)
 - setting current date and time [16-44](#)
 - setting system date and time [17-11](#)
- ntp server command [A-32](#)

O

- OFDM, definition [GL-7](#)

P

PAC

- definition [GL-8](#)
- provisioning, on internal AAA server [4-17](#)
- packet content, command for displaying [A-16](#)
- packet handling template, configuring [5-90](#)
- passwords (WLSE)
 - changing your password [16-55](#)
 - loss of, recovering from [17-21](#)
 - WLSE users [16-51](#)
- passwords, devices
 - SSH password, entering on WLSE [2-1, 4-10](#)
 - Telnet password, entering on WLSE [2-1, 4-10](#)

path loss data

- collecting [11-15](#)
- historical [10-19](#)
- reviewing [10-17](#)

PEAP server, external

- definition [GL-8](#)
- monitoring [4-14](#)

performance

- inventory [4-63](#)
- polling interval, setting [4-68](#)

- per VLAN client (group) report, displaying [10-55](#)

ping

- definition [GL-8](#)
- from CLI [A-34](#)

from Web interface [16-47](#)

polling

- aggregation parameters [4-68](#)
- fault and job data truncation parameters [4-68](#)
- inventory parameters [4-67](#)

pop-up blocker software [1-4](#)

ports, on the WLSE

- HTTP access port, configuring [A-21](#)
- port filtering, configuring [A-19](#)
- ports hosted by WLSE [C-2](#)
- ports used by WLSE [16-1](#)

processes

- failure of [16-40](#)

processes, WLSE

- AAA server processes (WLSE express [18-9](#)
- active statistics, displaying [A-55](#)
- displaying
 - using CLI [A-35](#)
 - using Web interface [16-40](#)
- starting and stopping
 - from the CLI [A-42](#)
 - from the UI [16-40, A-42](#)

procs_last.log [16-6](#)

protection attacks, detecting [14-63](#)

protocols, on WLSE

- configuring Ethernet interface [17-13](#)
- ports used for [16-1](#)

proxy mobile IP

- definition [GL-8](#)

proxy server, for firmware import [9-7](#)

ps CLI command [A-35](#)

PSPF, definition [GL-8](#)

Q

quality of service (QoS)

- configuring
 - 802.11b/g [5-81](#)
 - policies [5-77](#)

definition [GL-8](#)

report, displaying [10-70](#)

R

radio

- 802.11a, configuring [5-27](#)
- 802.11b/g, configuring [5-19](#)
- AP/client relationships [11-10](#)
- coverage and capacity [11-10](#)
- performance regions [11-11](#)
- reports, displaying [10-15](#)
- uplink contention regions [11-12](#)

radio interference thresholds

- authentication error rate policy [14-73](#)
- CCMP replays discarded policy [14-78](#)
- TKIP counter measure invoked policy [14-76](#)
- TKIP local MIC failures policy [14-74](#)
- TKIP remote MIC failures policy [14-75](#)
- TKIP replays detected policy [14-77](#)

radio location data

- AP radio scans, collecting [11-15](#)
- collecting [11-14](#)
- radio monitoring data, collecting [12-1](#)

Radio Management

- CLI command [11-4](#)
- disabled faults [11-4](#)
- disabled fault settings [14-11](#)
- enabling/disabling [11-4](#)

radio management

- network, configuring for [11-5](#)
- overview [11-1](#)
- radio management capability, verifying [13-27](#)
- understanding [11-7](#)

radio manager

- assisted configuration [13-71](#)
- auto re-site survey [12-6](#)
- client walkabout [13-54](#)
- enable/disable [A-35](#)

- frame monitoring [12-19](#)
- getting started [12-1](#), [13-2](#)
- location manager [13-2](#)
- log file for [16-6](#)
- managing data [13-81](#)
- processes for [16-42](#)
- radio monitoring [12-1](#)
- radio performance [12-6](#)
- reports, displaying [12-25](#)
- self healing [12-11](#)
- understanding [11-7](#)
- WLSE, configuring for [4-13](#)
- radiomanager command [A-35](#)
- radio measurement aggregation, definition [GL-8](#)
- radio monitoring [12-1](#)
 - enabling, disabling [12-4](#)
 - guidelines for running [12-3](#)
 - selecting APs [12-4](#)
 - understanding [12-2](#)
- radio parameters, generating [13-66](#)
- radio performance
 - evaluating [12-6](#)
 - understanding [11-10](#)
- radio scans
 - filtering [13-49](#)
 - guidelines for running [13-45](#)
 - jobs
 - copying [13-49](#)
 - creating [13-50](#)
 - deleting [13-49](#)
 - editing [13-49](#)
 - job run logs [13-53](#)
 - managing [13-48](#)
 - naming [13-51](#)
 - run logs, viewing [13-53](#)
 - running [13-49](#)
 - scheduling [13-52](#)
 - stopping [13-49](#)
 - selecting devices [13-51](#)
 - selecting radio types [13-51](#)
 - understanding [13-44](#)
 - viewing results [13-48](#)
- RADIUS
 - attributes for internal AAA server (WLSE Express) [18-46](#)
 - authentication module [16-16](#)
 - definition [GL-9](#)
 - port for WLCCP authentication [C-2](#)
- RADIUS server
 - AP usage report, displaying [10-81](#)
 - authentication report, displaying [10-69](#)
 - built-in (on WLSE Express) [18-1](#)
 - monitoring [3-10](#)
 - ports for [C-1](#)
 - summary report, displaying [10-80](#)
- RAM (WLSE), displaying [A-63](#)
- real-time reports
 - AP CPU utilization [10-99](#)
 - AP memory utilization [10-98](#)
 - AP packet errors [10-100](#)
 - AP packet statistics [10-99](#)
 - AP radio utilization [10-101](#)
 - associated client statistics [10-101](#)
 - WLSM roaming statistics [10-102](#)
- rebooting, WLSE
 - using the CLI [A-38](#)
 - using Web interface [16-7](#)
- recovery (WLSE)
 - maintenance image [17-18](#)
 - recovery CD
 - creating [17-19](#)
 - using [17-19](#)
 - reimaging the WLSE [17-19](#)
 - rescue image, using [17-21](#)
 - resetting WLSE to factory defaults [17-18](#)
- redundancy, WLSE
 - backup and restore on redundant nodes [16-37](#)
 - checking settings [16-35](#)

- configuring [16-32](#)
- email messages [16-31](#)
- event log [16-36](#)
- files in /tftpboot/public directory [16-46](#)
- hardware requirements [16-29](#)
- http-server accept command, using [16-38](#)
- manual failover [16-36](#)
- message log [16-6](#)
- nodes, replacing [16-37](#)
- prerequisites for [16-29](#)
- redundancy CLI command [A-36](#)
- show redundancy CLI command [A-56](#)
- software, upgrading [16-37](#)
- system check log [16-6](#)
- system check timeout period [16-34](#)
- web timeout period, resetting [16-38](#)
- redundancy.log [16-6](#)
- redundancy command [A-36](#)
- reimaging the WLSE [17-19](#)
- reload, configuring [5-96](#)
- reload command [A-38](#)
- replacement WLSE, installing [17-8](#)
- reports
 - ACS failed login report [16-60](#)
 - ad-hoc network [14-41](#)
 - AP and bridge connected to router [10-80](#)
 - AP and bridge connected to switch [10-78](#)
 - AP CPU utilization, real-time [10-99](#)
 - AP memory utilization, real-time [10-98](#)
 - AP packet errors, real-time [10-100](#)
 - AP packet statistics, real-time [10-99](#)
 - AP radio scan results, viewing [13-48](#)
 - AP radio utilization, real-time [10-101](#)
 - APs registered with WDS [10-12](#)
 - AP summary [10-65](#)
 - AP usage, displaying [10-81](#)
 - associated client statistics, real-time [10-101](#)
 - associations [10-69](#)
 - auto config retry [10-15](#)
 - channel loading [10-19](#)
 - channel loading, historical [10-21](#)
 - client access failure [10-42](#)
 - client detail [10-37](#)
 - client historical association [10-40](#)
 - client roaming statistics [10-96](#)
 - client statistics [10-39](#)
 - configuration history [10-14](#)
 - configured radio parameters [10-16](#)
 - current [10-45](#)
 - detailed [10-67](#)
 - device center, using [10-7](#)
 - device fault status [10-13](#)
 - device history [10-13](#)
 - device specific [8-52](#)
 - EAP and MAC failed authentication [10-75](#)
 - emailing [10-3](#)
 - EMF detection [14-50](#)
 - Ethernet transmission statistics [10-91](#)
 - exporting [10-2](#)
 - failed authentication and login attempt per AP [10-76](#)
 - firmware history [10-14](#)
 - friendly AP reports [14-28](#)
 - group auto config retry [10-63](#)
 - group CDP inline power [10-59](#)
 - group client [10-56](#)
 - group client association [10-48](#)
 - group identity [10-57](#)
 - group inventory [10-60](#)
 - group LBS [10-61](#)
 - group MBSSID [10-53](#)
 - group mobility ID [10-62](#)
 - group performance, Ethernet utilization [10-86](#)
 - group performance, RF utilization [10-85](#)
 - group security [10-50](#)
 - group security violation [10-59](#)
 - group serial number [10-58](#)
 - group SSID [10-52](#)
 - group version summary [10-62](#)

- group VLAN [10-54](#)
- hot standby [10-74](#)
- IDS
 - viewing [14-5](#)
- interference reports (Location Manager) [13-34](#)
- links to from Group Details display [4-79](#)
- MBSSID [10-72](#)
- MFP capabilities [14-55](#)
- MFP events [14-56](#)
- mobility groups, displaying [10-82](#)
- mobility ID, displaying [10-82](#)
- path loss between managed APs [10-17](#)
- path loss between managed APs, historical [10-19](#)
- per VLAN client [10-55](#), [10-73](#)
- QoS [10-70](#)
- radio manager reports [10-15](#)
- RADIUS authentication [10-69](#)
- real-time, displaying [10-97](#)
- RF and Ethernet utilization, tabular [10-92](#)
- RF and utilization, graph [10-92](#)
- RF transmission statistics [10-89](#)
- router summary [10-79](#)
- scheduling email [10-5](#)
- server response time, graph [10-95](#)
- server summary [10-80](#)
- SSID [10-71](#)
- switch summary [10-77](#)
- top n busiest clients [10-93](#)
- top n client MIC error rate [10-94](#)
- top n number of associations graph [10-88](#)
- top n number of associations tabular [10-87](#)
- top n percentage errors [10-88](#)
- trend, using for capacity planning [10-85](#)
- trends, displaying [10-83](#)
- unregistered clients [14-61](#)
- VLAN [10-73](#)
- voice client detail [10-43](#)
- WDS summary [10-10](#)
- wireless client
 - WLSM modules [10-78](#)
- repository
 - browsing [16-13](#)
 - defining
 - using CLI [A-38](#)
 - using Web interface [16-11](#)
 - definition [GL-9](#)
 - install configure CLI command [A-23](#)
 - install list CLI command [A-24](#)
 - port for [C-1](#)
 - repository CLI command [A-38](#)
 - show repository CLI command [A-57](#)
- Repository.log [16-5](#)
- rescue image, WLSE [17-21](#)
- reset device-snmp command [A-40](#)
- resetting WLSE to factory defaults [17-18](#)
- restarting (rebooting) WLSE
 - bootlog, displaying [A-45](#)
 - from Web interface [16-7](#)
 - reload command [A-38](#)
- restore command [A-41](#)
- restoring data from backups
 - from pre-released to released not allowed [16-20](#)
 - restoring from one WLSE to another [17-9](#)
 - using the CLI
 - procedure for [17-7](#)
 - restore command reference [A-41](#)
 - using Web interface [16-24](#)
- reverse DNS lookup [4-44](#)
- roaming, client statistics report [10-96](#)
- rogue AP
 - automatic suppression [14-30](#)
 - changing to friendly [14-24](#)
 - detection, enabling/disabling [14-16](#)
 - detection guidelines [14-14](#)
 - disabled faults [11-4](#)
 - displaying information about [13-22](#)
 - displaying location of [13-22](#)
 - fault history [14-23](#)

- managing [14-24](#)
- maximum limit [14-14](#)
- reclassification, enabling/disabling [14-18](#)
- reports [14-26](#)
- rogue APs
 - detecting [14-12](#)
- roles
 - creating and modifying [16-51](#)
 - debug tools privilege [16-50](#)
 - deleting [16-49](#)
 - for users created by using the CLI [17-3](#)
 - naming guidelines [B-1](#)
 - predefined [16-50](#)
 - XML API privileges [16-49](#)
- route command [A-42](#)
- router
 - AP and Bridge connected to, displaying [10-80](#)
 - fault monitoring [3-1](#)
 - fault thresholds, setting [3-10](#)
 - summary report, displaying [10-79](#)
 - system-defined group for [4-74](#)
- routes (WLSE)
 - adding or deleting [A-42](#)
 - displaying
 - show route CLI command [A-57](#)
- RSA, definition [GL-9](#)
- RSSI, definition [GL-9](#)
- runstats.log [16-6](#)

S

- scanning AP
 - system group for [4-76](#)
 - using [14-47](#)
- scheduling
 - archive jobs [8-31](#)
 - backups [16-23](#)
 - configuration jobs [8-15](#)
 - discovery [4-33](#)
- email [10-5](#)
- firmware jobs [9-11](#)
- SCP
 - definition [GL-9](#)
 - using for backups [16-22](#)
- searching for devices [1-12](#)
- security
 - last 10 logged in users, viewing [16-19](#)
 - SSL
 - certificate signed request, obtaining [16-18](#)
 - Telnet, enabling or disabling [16-19](#)
- security (devices)
 - advanced, configuring [5-59](#)
 - templates [5-33](#)
 - admin access [5-34](#)
 - advanced [5-59](#)
 - local RADIUS server [5-62](#)
 - server manager [5-55](#)
 - SSID 802.11b/g [5-36](#)
 - WEP 802.11a [5-51](#)
 - WEP 802.11b/g [5-49](#)
- security, WLSE
 - authentication
 - enabling [A-7](#)
 - modules [16-15](#)
 - HTTP access to WLSE, controlling [A-21](#)
 - HTTPS [16-18](#)
 - log, displaying [A-58](#)
 - SSH [16-19](#)
 - access to WLSE, controlling [A-68](#)
 - access to WLSE, enabling [A-68](#)
- seed
 - CDP-based discovery [4-26](#)
 - definition [GL-9](#)
 - individual device seeding [4-28](#)
- self healing
 - assigning severity level [12-15](#)
 - clearing faults [12-17](#)
 - enabling, disabling [12-15](#)

- guidelines for running [12-14](#)
- reviewing history [12-17](#)
- running [12-17](#)
- selecting floors [12-15](#)
- tracking progress [12-17](#)
- understanding [12-11](#)
- server
 - AAA server, internal [18-1](#)
 - local RADIUS server, configuring [5-62](#)
 - manager, configuring [5-55](#)
 - SMTP server [17-15](#)
- server, AAA
 - response time graph report, displaying [10-95](#)
- server manager, configuring
 - WLSM template [6-7](#)
- services (WLSE)
 - managing
 - procedure for [17-15](#)
 - using CLI services command [A-42](#)
 - ports used for [16-1](#)
 - reintdb command, effect on [A-37](#)
 - stopping and starting [17-15](#)
 - time reset, requirement for stopping services [A-12](#)
- services, configuring [5-65](#)
 - ARP cache [5-87](#)
 - CDP [5-68](#)
 - DNS [5-69](#)
 - Ethertype filters [5-75](#)
 - hot standby [5-67](#)
 - HTTP [5-77](#)
 - IP filters [5-72](#)
 - MAC address filters [5-70](#)
 - packet handling [5-90](#)
 - QoS 802.11b/g [5-81](#)
 - QoS policies [5-77](#)
 - SNMP [5-82](#)
 - SNTP [5-84](#)
 - STP [5-88](#)
 - Telnet/SSH [5-65](#)
 - VLAN [5-85](#)
- services command [A-42](#)
- serving channels
 - definition [GL-9](#)
 - monitoring [12-4](#)
- setting system date and time
 - using the CLI [17-11](#)
 - using the Web interface [16-43](#)
- setup command [A-43](#)
- show auth-cli command [A-44](#)
- show auth-http [A-44](#)
- show backupconfig command [A-44](#)
- show backuplog command [A-45](#)
- show bootlog command [A-45](#)
- show cdp-neighbor [A-46](#)
- show cdp-run command [A-47](#)
- show clock command [A-47](#)
- show config command [A-48](#)
- show domain-name command [A-50](#)
- show import command [A-51](#)
- show interfaces command [A-53](#)
- show process command [A-55](#)
- show redundancy CLI command [A-56](#)
- show route command [A-57](#)
- show ssh-server command [A-59](#)
- show ssh-version command [A-59](#)
- show syslog command [A-60](#)
- show tech command [A-61](#)
- show time command [A-62](#)
- show version command [A-63](#)
- shutdown command [A-65](#)
- shutting down (WLSE)
 - from the CLI [17-10](#)
 - using CLI [A-65](#)
- Sites tab options
 - AP radio scan, using [13-43](#)
 - assisted configuration, using [13-66](#)
 - client walkabouts, using [13-54](#)
 - enabling/disabling [A-35](#)

- location manager, using [13-2](#)
- radio manager data, managing [13-81](#)
- SMTP
 - definition [GL-9](#)
 - port for fault notification [C-1](#)
 - server, specifying by using the CLI [17-15](#)
 - server, specifying by using the Web interface [16-45](#)
- SNMP
 - agent, configuring [A-66](#)
 - agent log, displaying [16-5](#)
 - community strings
 - for WLSE server, displaying [A-59](#)
 - for WLSE server, resetting [A-40](#)
 - for WLSE server, setting [A-66](#)
 - community strings, for devices
 - entering on WLSE [4-6](#)
 - guidelines for [4-8](#)
 - recommendations [4-8](#)
 - configuring [5-82](#)
 - definition [GL-9](#)
 - faults
 - trap notification settings [3-56](#)
 - trap version supported [3-56](#)
 - port for for discovery, inventory, and AP configuration [C-1](#)
 - port for SNMPTRAP [C-1](#)
 - port on trap receiver for traps from APs [C-1](#)
 - port on WLSE for traps from APs [C-2](#)
 - reachability, testing [16-47](#)
 - retries, recommendations for [4-9](#)
 - timeouts, recommendations for [4-9](#)
 - traps, version supported [3-56](#)
 - traps supported [1-3](#)
 - variables, querying [16-48](#)
- snmp-server command [A-66](#)
- SNTP (Simple Network Time Protocol)
 - configuring [5-85](#)
- software, on devices
 - firmware, managing [9-1](#)
 - groups for [4-74](#)
- software, on WLSE
 - installation logs, displaying [16-5](#)
 - maintenance image [A-73](#)
 - overview [16-7](#)
 - recovery CD
 - creating [17-19](#)
 - using to reimage [17-19](#)
 - reimaging the WLSE
 - locally [17-19](#)
 - remotely [17-20](#)
- repository
 - browsing [16-13](#)
 - port for [C-1](#)
- status, viewing [16-8](#)
- updates
 - data preserved [16-15](#)
 - history, viewing [16-14](#)
 - installing, by using Web interface [16-12](#)
 - not allowed from pre-released version [16-7](#)
 - transferring to WLSE [A-38](#)
- upgrading on a redundancy (high availability) cluster [16-37](#)
- version, viewing
 - from Web interface [1-10](#)
 - using the CLI [A-63](#)
- spanning tree protocol
 - configuring [5-88](#)
 - definition [GL-10](#)
- specific settings, device
 - configuring [5-98](#)
 - exporting [8-50](#)
 - importing [8-48](#)
 - managing [8-47](#)
 - report [8-52](#)
 - viewing [8-51](#)
- splash screen, adding a message [16-43](#)
- SSH, definition [GL-9](#)
- SSH access to WLSE

- access control
 - displaying [A-59](#)
- controlling [A-67](#)
- enabling [A-68](#)
- show ssh-server command [A-59](#)
- show ssh-version command [A-59](#)
- ssh-server accept command [A-67](#)
- ssh-version command [A-68](#)
- type, displaying [A-59](#)
- version, displaying [A-59](#)
- version, setting
 - using CLI [A-68](#)
 - using Web interface [16-19](#)
- ssh host command [A-67](#)
- SSH on access points
 - credentials, entering on WLSE [4-10](#)
 - port for IOS AP configuration [C-1](#)
- ssh-server accept command [A-67](#)
- ssh-version command [A-68](#)
- SSID
 - 802.11b/g, configuring [5-36](#)
 - definition [GL-9](#)
 - report, displaying [10-71](#)
 - system-defined groups for [4-74](#)
- SSL
 - definition [GL-10](#)
 - log, displaying [16-5](#)
 - web SSL access log, displaying [A-65](#)
- SSL certificate
 - certificate signed request, viewing [16-18](#)
 - for built-in AAA server [18-5](#)
 - mkcert CLI command [A-31](#)
 - signed, obtaining [16-18](#)
 - unsigned certificate, obtaining [A-31](#)
- STA, definition [GL-10](#)
- startup configuration
 - assigning [8-41](#)
 - creating a template for [8-39](#)
- startup configuration, WLSE
 - configbackup.log file [16-5](#)
- STP
 - configuring [5-88](#)
 - definition [GL-10](#)
- subnet, system-defined group for [4-74](#)
- summary report
 - access point, displaying [10-65](#)
 - router [10-79](#)
 - server [10-80](#)
 - switch [10-77](#)
- SWAN
 - configuring, using Deployment Wizard [2-1](#)
 - definition [GL-10](#)
- switch
 - AP and bridge connected to report, displaying [10-78](#)
 - fault monitoring [3-1](#)
 - fault thresholds, setting [3-10](#)
 - summary report, displaying [10-77](#)
 - system-defined group for [4-74](#)
 - WLSM modules report, displaying [10-78](#)
- switch port
 - guidelines for detecting and suppressing [14-31](#)
 - locating and detecting [14-30](#)
 - viewing suppressed ports [14-32](#)
- syntax of commands, checking [A-2](#)
- syslog
 - displaying [A-60](#)
- faults
 - notification settings [3-60](#)
- port for [C-1](#)
- using for AAA server logging (WLSE express) [18-40](#)
- sysName
 - display of [1-10](#)
 - effect of single quote on display [1-10](#)
 - reverse DNS lookup, effect on display [4-44](#)
- system (WLSE)
 - configuration
 - displaying [A-48](#)
 - erasing [A-17](#)

date and time [A-12, A-32](#)
 information, viewing [17-15](#)
 logs, displaying [17-15](#)
 processes, managing [16-40](#)
 rebooting
 from the Web interface [16-7](#)
 using the CLI [17-10](#)
 shutting down
 procedure for [17-10](#)
 shutdown CLI command [A-65](#)
 status, displaying [16-40](#)
 storage usage, displaying [A-14](#)
 system log, using [16-42](#)
 systemCheck.log [16-6](#)
 system time, setting
 using CLI [A-12](#)
 using Web interface [16-43](#)

T

TAC (Technical Assistance Center), obtaining information for [A-61](#)
 TACACS+ (for WLSE login)
 authentication module [16-15](#)
 definition [GL-10](#)
 tarlog command [A-68](#)
 TCP/IP packet content, displaying [A-16](#)
 TCP Port Scan tool [16-47](#)
 TCP ports used by WLSE [C-1](#)
 Telnet
 credentials for IOS access points, entering [4-10](#)
 port for IOS AP configuration [C-1](#)
 Telnet/SSH services, configuring [5-65](#)
 Telnet access to WLSE
 access from selected IP addresses, specifying [A-69](#)
 enabling/disabling
 using CLI [A-69](#)
 using Web interface [16-19](#)
 status, displaying [A-61](#)

telnetenable command [A-69](#)
 templates
 automatic configurations [8-39](#)
 copying
 Deployment Wizard [7-2](#)
 IOS [5-3](#)
 WLSM [6-2](#)
 creating
 Deployment Wizard [2-4, 7-2](#)
 IOS [5-2](#)
 WLSM [6-2](#)
 deleting
 Deployment Wizard [7-3](#)
 IOS [5-4](#)
 WLSM [6-3](#)
 editing
 IOS [5-3](#)
 WLSM [6-3](#)
 exporting
 Deployment Wizard [7-4](#)
 IOS [5-5](#)
 WLSM [6-5](#)
 for Deployment Wizard, defined [7-1](#)
 for IOS configuration, defined [5-1](#)
 for WLSM configuration, defined [6-1](#)
 importing
 IOS [5-4](#)
 WLSM [6-4](#)
 using
 [5-1](#)
 TFTP
 definition [GL-10](#)
 ports used for firmware upgrade [C-2](#)
 tftp.log [16-6](#)
 TFTP process (on WLSE) [16-42](#)
 TFTP server, on WLSE Express
 managing from Web interface [16-45](#)
 tftpserver CLI command [A-70](#)
 tftpserver command [A-70](#)

- threshold, definition [GL-10](#)
 - time
 - browser time, setting [16-43](#)
 - display of, on WLSE [1-10](#)
 - server time discrepancy when scheduling jobs [1-11](#)
 - synchronizing to an NTP server [16-44](#)
 - UTC
 - definition [GL-11](#)
 - display of [1-10](#)
 - timeout period
 - WLSE CLI [17-2](#)
 - WLSE web interface
 - default [1-13](#)
 - resetting, from Web interface [16-44](#)
 - resetting, using CLI [A-72](#)
 - TKIP
 - counter measure invoked policy [14-76](#)
 - definition [GL-10](#)
 - local MIC failures policy [14-74](#)
 - remote MIC failures policy [14-75](#)
 - replays detected policy [14-77](#)
 - tomcat.log file [16-6](#)
 - tomcat log, displaying
 - from Web interface [16-5](#)
 - using CLI [A-62](#)
 - Tomcat process [16-42](#)
 - tomcat process, failure of [A-40](#)
 - traceroute
 - definition [GL-10](#)
 - from CLI [A-70](#)
 - from Web interface [16-47](#)
 - transmission statistics
 - displaying Ethernet report [10-91](#)
 - displaying RF [10-89](#)
 - traps
 - notification settings [3-56](#)
 - received from APs, port for [C-2](#)
 - version supported [3-56](#)
 - trending data
 - aggregation parameters [4-68](#)
 - data retention parameters [4-68](#)
 - trend reports, using for capacity planning [10-85](#)
 - trends, displaying [10-83](#)
 - client roaming statistics report [10-96](#)
 - Ethernet transmission statistics report [10-91](#)
 - group performance report, Ethernet utilization [10-86](#)
 - group performance report, RF utilization [10-85](#)
 - RF and Ethernet tabular report [10-92](#)
 - RF and Ethernet utilization graph [10-92](#)
 - RF transmission statistics report [10-89](#)
 - server response time graph report [10-95](#)
 - top n busiest clients report [10-93](#)
 - top n client MIC error rate report [10-94](#)
 - top n number of associations graph report [10-88](#)
 - top n number of associations tabular report [10-87](#)
 - top n percentage errors report [10-88](#)
 - troubleshooting (WLSE)
 - diagnostics tools [16-39](#)
 - passwords, loss of [17-21](#)
 - process management [16-40](#)
 - recovery procedures [17-17](#)
 - troubleshooting guide
 - displaying from online help [1-9](#)
 - locating on Cisco.com [1-15](#)
 - typographical conventions
 - in command descriptions [A-3](#)
 - in this document [xxiv](#)
-
- ## U
- UDP ports used by WLSE [C-1](#)
 - undoing a job [8-24](#)
 - unknown radio, displaying [13-22](#)
 - Unmanaged folder (Managed Devices) [4-55](#)
 - unregistered client detection [14-58](#)
 - displaying faults [14-60](#)
 - enabling, disabling [14-59](#)
 - guidelines [14-53, 14-59](#)

- reports [14-61](#)
- understanding [14-58](#)
- updateWLSE-x.x.x.log file [16-6](#)
- upgrade
 - access point firmware [9-1](#)
 - WLSE software (by using the CLI) [17-10](#)
 - WLSE software (by using Web interface) [16-7](#)
 - WLSE software, data preserved [16-15](#)
- usage report, AP [10-81](#)
- user-defined
 - groups [4-77](#)
 - roles [16-49](#)
- user guide
 - displaying from online help [1-9](#)
 - locating on Cisco.com [1-15](#)
- username command [A-71](#)
- users (WLSE)
 - authentication servers [16-16](#)
 - CLI access [16-51](#)
 - creating
 - using the CLI [17-3, A-71](#)
 - using Web interface [16-51](#)
 - current users, listing [16-19](#)
 - deleting
 - from Web interface [16-55](#)
 - using the CLI [A-71](#)
 - home page, modifying [16-56](#)
 - last 10 logged in users. viewing [16-19](#)
 - modifying
 - using the CLI [A-71](#)
 - using the Web interface [16-51](#)
 - naming guidelines [B-1](#)
 - of internal AAA server (WLSE Express) [18-24](#)
 - roles
 - assigning to users [16-52](#)
 - managing [16-49](#)
 - username CLI command [A-71](#)
- UTC
 - definition [GL-11](#)

- displayed on WLSE [1-10](#)
- utilization
 - RF and Ethernet graph, displaying [10-92](#)
 - RF and Ethernet tabular report, displaying [10-92](#)

V

- version summary
 - group report, displaying [10-62](#)
- VLAN
 - configuring [5-85](#)
 - definition [GL-11](#)
 - group report, displaying [10-54](#)
 - per client report (group), displaying [10-55](#)
 - per client report (individual), displaying [10-55](#)
 - report, displaying [10-73](#)
 - VLAN ID, definition [GL-11](#)
- voice
 - bandwidth in use threshold, enabling [3-41](#)
 - QoS status [3-53](#)
 - status, viewing [3-53](#)
 - voice QoS status threshold, enabling [3-42](#)

W

- WDC, definition [GL-11](#)
- WDS
 - access points [2-7, 11-8](#)
 - and radio manager [11-8](#)
 - configuring
 - using a template [5-92](#)
 - using Deployment Wizard [2-1](#)
 - definition [GL-11](#)
 - discovery through [4-27](#)
 - enhanced client tracking [4-18](#)
 - fault thresholds for [3-50](#)
 - infrastructure access point, definition [GL-6](#)
 - registered APs report [10-12](#)

- summary report [10-10](#)
- system-defined groups for [4-76](#)
- understanding [11-8](#)
- WDS access points
 - understanding [11-8](#)
- WDS device, definition [GL-11](#)
- WLCCP
 - credentials, configuring manually [4-13](#)
 - port for [C-2](#)
- WLSM
 - understanding [11-8](#)
- Web access log, displaying
 - from CLI (show webaccesslog command) [A-63](#)
 - from Web interface [16-5](#)
- Web error log, displaying
 - from CLI (show weberrorlog command) [A-64](#)
 - from Web interface [16-5](#)
- Web interface (WLSE)
 - browsers, configuring [1-4](#)
 - browsers, supported [1-4](#)
 - overview [1-4](#)
- Web session timeout (WLSE)
 - default [1-13](#)
 - resetting from Web interface [16-44](#)
- Web session timeout, WLSE
 - resetting, using the CLI [A-72](#)
- Web SSL log, displaying [A-65](#)
- webtimeout command [A-72](#)
- WEP 802.11a, configuring [5-51](#)
- WEP 802.11b/g, configuring [5-49](#)
- WEP keys, definition [GL-12](#)
- WGB, definition [GL-12](#)
- WHISK port [C-1](#)
- Windows server
 - as backup location [16-22](#)
 - as repository [16-11](#)
- WINS, definition [GL-12](#)
- wireless client reports
 - access failure, displaying [10-42](#)
 - client detail, displaying [10-37](#)
 - client historical association, displaying [10-40](#)
 - client statistics, displaying [10-39](#)
 - displaying [10-37](#)
 - polling interval, setting [4-68](#)
 - voice client detail, displaying [10-43](#)
- WirelessSvcMgr process [16-42](#)
- WISPr, definition [GL-12](#)
- wizard
 - assisted site survey [13-17](#)
 - Deployment Wizard [2-2](#)
 - Discovery wizard [4-33](#)
- WLCCP
 - credentials, adding from Deployment Wizard [2-6](#)
 - credentials, entering on WLSE [4-13](#)
 - definition [GL-12](#)
 - discovery through [4-27](#)
- WLSE
 - device limit, displaying [A-63](#)
 - memory
 - amount of displaying [A-63](#)
- WLSE 1030 Express
 - built-in AAA server on [18-1](#)
 - documentation for [xxiv](#)
 - number of devices managed [4-61](#)
 - redundancy, hardware requirements [16-29](#)
- WLSE 1130
 - redundancy, hardware requirements [16-29](#)
- WLSE 1130 series
 - Ethernet port labelling [17-13](#)
- wlseconfig command (do not use this command) [A-6](#)
- WLSEFaults process [16-42](#)
- WLSEIdleServer process (on WLSE) [16-42](#)
- WLSEjobvm process [16-42](#)
- WLSERepository process (on WLSE) [16-42](#)
- wlsestartup.ini file [2-3](#)
- WLSM
 - configuring
 - using Deployment Wizard [2-1](#)

- using templates [6-1](#)
- definition [GL-12](#)
- fault thresholds, setting [3-46](#)
- group report, mobility ID [10-62](#)
- mobility groups report, displaying [10-82](#)
- mobility ID report, displaying [10-82](#)
- modules report [10-78](#)
- WNM, definition [GL-12](#)
- workgroup bridge, definition [GL-12](#)
- WPA, definition [GL-12](#)

X

- XML API, privileges in roles [16-49](#)