



User Guide for the CiscoWorks Wireless LAN Solution Engine

Release 2.5

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

Customer Order Number: DOC-7815902=
Text Part Number: 78-15902-01



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.

Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0304R)

User Guide for the CiscoWorks Wireless LAN Solution Engine
Copyright © 2003 Cisco Systems, Inc. All rights reserved.



Preface xix

Audience xix

Conventions xx

Product Documentation xx

Obtaining Documentation xxii

Cisco.com xxii

Documentation CD-ROM xxiii

Ordering Documentation xxiii

Documentation Feedback xxiv

Obtaining Technical Assistance xxiv

Cisco TAC Website xxiv

Opening a TAC Case xxv

TAC Case Priority Definitions xxv

Obtaining Additional Publications and Information xxvi

CHAPTER 1

Getting Started 1-1

Overview of the Wireless LAN Solution Engine 1-1

WLSE Integration with Network Management Systems 1-2

Understanding the Web Interface 1-3

Supported Browsers 1-3

The WLSE Dashboard 1-5

Device Name and IP Address Display 1-8

Time Display 1-8

Using the Device Selector and Search 1-9

Sorting Table Data	1-11
Logging In and Out	1-11
Customizing the Web Interface	1-12
Setting the Default Tab and Subtab	1-12
Adding a Message to the Splash Screen	1-13
Next Steps	1-13

CHAPTER 2

Fault Monitoring 2-1

Viewing Fault Information	2-1
Understanding Fault and Security Policy Monitoring	2-2
Displaying Faults	2-6
Clearing Summary Table Faults	2-9
Acknowledging Faults	2-10
Viewing Fault Details	2-10
Managing Fault Settings	2-18
Understanding Fault Settings	2-18
Creating a Setting	2-19
Copying a Setting	2-20
Renaming a Setting	2-21
Editing a Setting	2-22
Deleting a Setting	2-22
Viewing a Summary	2-23
Assigning a Setting to a Device	2-23
Setting Security Policies and Thresholds	2-24
Managing Network-Wide Settings	2-49
Setting Rogue AP Detection	2-49
Setting Interference Detection	2-50
Notification Settings	2-51
Setting Trap Notification	2-51

CHAPTER 3**Managing Devices 3-1**

Devices Tab Functions 3-2

Getting Started with Device Management 3-3

Setting Up Devices 3-5

Set Up Non-IOS Access Points and Bridges 3-6

Set Up IOS Access Points 3-8

Set Up Routers and Switches 3-24

Set Up AAA Servers 3-25

Specifying Device Credentials 3-27

Enter SNMP Community Strings for All Devices 3-28

Enter HTTP Usernames and Passwords—Non-IOS Access Points 3-32

Enter Telnet and SSH Usernames and Passwords—IOS Access Points 3-33

Enter HTTP Port Settings—IOS Access Points 3-35

Enter WLCPP Credentials for Wireless Domain Services 3-36

Managing AAA Servers 3-37

About AAA Servers 3-38

Adding an AAA Server 3-39

Removing an AAA Server 3-40

Modifying an AAA Server 3-40

Managing Device Discovery 3-41

About Discovery 3-41

Pre-Discovery Checklist 3-53

About the Discovery Wizard 3-53

Using the Discovery Wizard 3-54

Running CDP Discovery 3-54

Importing Devices from a File 3-59

Importing Devices from a CiscoWorks Server	3-61
Setting Advanced Options	3-63
Using Discovery IP Address Filtering	3-68
Viewing Discovery Logs	3-69
Managing and Unmanaging Devices	3-76
Understanding Device Details	3-79
Limitation on the Number of Managed Devices	3-79
Managing Device Inventories	3-80
About Inventories	3-81
Changing the Polling Intervals for Automatic Inventories	3-82
Running Immediate and Scheduled Inventories	3-84
Managing Polling Parameters	3-87
Viewing Inventory Logs	3-91
Exporting Devices	3-94
Exporting Devices to a CiscoWorks Server	3-94
Exporting Devices to a CSV File	3-96
Managing Groups	3-97
About Groups	3-98
Using the Group Details Window	3-101
Creating a Static Group	3-103
Creating a Rule-Based Group	3-105
Creating a Static Group by Copying a Static or Rule-Based Group	3-107
Copying a Rule-Based Group	3-108
Editing a Static Group	3-110
Editing a Rule-Based Group	3-111
Deleting a Static or Rule-Based Group	3-113

CHAPTER 4

Configuring Devices 4-1

Using the Templates	4-1

What is a Configuration Template?	4-2
Template Choices	4-2
Creating a Template	4-253
Copying a Template	4-254
Editing a Template	4-255
Converting a Template	4-256
Deleting a Template	4-257
Importing a Template	4-257
Exporting a Template	4-261
Managing Configuration Archives	4-261
Viewing Archived Configurations	4-262
Scheduling an Archive Collection	4-263
Viewing Archive Status	4-264
Managing Jobs	4-267
Managing Configuration Jobs	4-267
Managing Archive Jobs	4-285
Automating Configurations	4-300
Assigning a Startup Configuration	4-300
Creating a Startup Configuration Template	4-302
Assigning an Auto-Managed Configuration	4-306

CHAPTER 5

Updating Device Firmware 5-1

About Firmware Upgrades	5-2
How Firmware Upgrades Work	5-2
Recommendations For Running Firmware Upgrades	5-3
Managing Firmware Images	5-5
Viewing Images Downloaded to the WLSE	5-6
Editing Image Details on the WLSE	5-6
Deleting Images from the WLSE	5-8

Importing Images to the WLSE	5-8
Using a Remote TFTP Server for Updating Devices	5-13
Viewing and Updating Firmware Versions that the WLSE Supports	5-14
Managing Firmware Jobs	5-14
Creating and Running a Firmware Job	5-15
Job Creation Tasks	5-16
Using the Functions in the Main Jobs Window	5-27
Converting Access Points to IOS	5-35
About Conversion	5-35
Conversion Procedure	5-37

CHAPTER 6

Using Reports 6-1

Using the Device Center	6-2
Viewing the WDS Summary Report	6-4
Viewing the Fault Status Report	6-6
Viewing Device History	6-6
Viewing Config History	6-7
Viewing Firmware History	6-8
Displaying Radio Manager Reports	6-8
Displaying a Configured Radio Parameters Report (11b)	6-9
Displaying a Path Loss Between Managed APs Report (11b)	6-10
Displaying a Channel Loading Report (11b)	6-11
Displaying Wireless Client Reports	6-13
Displaying a Client Detail Report	6-14
Displaying a Client Statistics Report	6-16
Displaying a Client Historical Association Report	6-18
Displaying Current Reports	6-19
Displaying a Group Client Association Report	6-22
Displaying a Group Security Report	6-26

Displaying a Group SSID Report	6-29
Displaying a Group VLAN Report	6-32
Displaying a Per VLAN Client Report	6-35
Displaying a Group Policy Report	6-38
Displaying an AP Summary Report	6-40
Displaying a Detailed Report	6-43
Displaying an AP Associations Report	6-48
Displaying an EAP Authentication Report	6-50
Displaying an AP Ethertype Protocol Filters Report	6-51
Displaying an AP IP Protocol Filters Report	6-52
Displaying an AP IP Port Filters Report	6-53
Displaying an AP Policy Report	6-55
Displaying an AP QoS Report	6-56
Displaying an AP SSID Report	6-58
Displaying an AP VLAN Report	6-60
Displaying a Per VLAN Client Report	6-62
Displaying an AP Hot Standby Report	6-64
Displaying a Switch Summary Report	6-65
Displaying an AP and Bridge Connected to Switch Report	6-66
Displaying a Router Summary Report	6-67
Displaying an AP and Bridge Connected to Router Report	6-68
Displaying a Server Summary Report	6-69
Displaying an AP Usage Report	6-70
Displaying Trends	6-71
Using Trend Reports For Capacity Planning	6-72
Displaying a Group Performance Report: RF Utilization	6-73
Displaying a Group Performance Report: Ethernet Utilization	6-74
Displaying a Top N Number of Associations Report	6-75
Displaying a Top N Percentage Errors Report	6-77
Displaying an AP and Bridge RF Transmission Statistics Report	6-78

Displaying an AP and Bridge Ethernet Transmission Statistics Report	6-79
Displaying an AP and Bridge Performance Graph	6-80
Displaying an AP and Bridge Performance: Tabular	6-81
Displaying Top N Busiest Clients	6-82
Displaying Top N Client MIC Error Rate	6-84
Displaying Top N Client Bit Error Rate	6-85
Displaying a Server Response Time Graph	6-86
Exporting a Report	6-88
Emailing a Report	6-88
Scheduling Email Jobs	6-90
Viewing Email Job Details	6-91
Editing an Email Job	6-92
Exporting URL-Based Report Data	6-94

CHAPTER 7

Radio Management 7-1

Understanding the Radio Manager	7-2
Understanding the Radio Manager Features	7-2
Collecting Radio Location Measurements	7-4
Radio Monitoring	7-6
Setting Radio Monitoring Options	7-7
AP Radio Scan	7-9
Understanding AP Radio Scans	7-9
Creating a New AP Radio Scan	7-11
Viewing AP Radio Scan Jobs	7-16
Filtering AP Radio Scan Jobs	7-18
Editing AP Radio Scan Jobs	7-19
Stopping AP Radio Scan Jobs	7-20
Deleting AP Radio Scan Jobs	7-20
Copying AP Radio Scan Jobs	7-21

Viewing the AP Radio Scan Job Run Log	7-21
Refreshing the AP Radio Scan Job Summary	7-23
Client Walkabout	7-24
Understanding Client Walkabouts	7-24
Client Walkabout Guidelines	7-25
Creating a New Client Walkabout	7-26
Viewing Client Walkabouts	7-33
Editing Client Walkabouts	7-34
Deleting Client Walkabouts	7-34
Starting Client Walkabouts	7-35
Stopping Client Walkabouts	7-35
Viewing Walkabout Session Details	7-36
Viewing AP Location Details	7-37
Refreshing the Walkabouts Summary	7-38
Location Manager	7-39
Understanding the Location Manager Window	7-39
Obtaining Server Information	7-43
Changing Location Manager Display Options	7-44
Modifying AP Coverage Display Options	7-46
Adding Building Information	7-47
Importing an Image of the Building	7-48
Adding Floor Information	7-49
Adding Devices to the Floor Map	7-51
Moving Devices on Image Map	7-52
Finding Unknown Radios	7-52
Using the Assisted Site Survey Wizard	7-55
Radio Management Assisted Configuration	7-60
Viewing Assisted Configuration Tasks	7-60
Editing Assisted Configuration Tasks	7-61
Copying Assisted Configuration Tasks	7-62

Deleting Assisted Configuration Tasks	7-63
Viewing Details of a Configuration Task	7-63
Refreshing the List of Configuration Tasks	7-64
Creating a New Assisted Configuration Task	7-65
Managing RM Measurements	7-71

CHAPTER 8

Managing the WLSE System 8-1

Managing the Appliance	8-2
Using Log Files	8-3
About Log Files	8-4
Restarting the WLSE	8-5
Managing WLSE Software	8-5
Managing Security	8-15
Backing Up and Restoring Data	8-21
Using WLSE Diagnostics Options	8-28
Specifying a Splash Screen Message	8-32
Setting the Time and Specifying Name Servers	8-33
Configuring the Mail Route	8-35
Using Connectivity Tools	8-35
Firmware Version Support	8-37
Updating Supported Firmware Versions	8-38
Viewing Supported Firmware Versions	8-39
Managing Users	8-39
Managing Roles	8-40
Managing User Accounts	8-42
Modifying Your Profile	8-46
Changing Your Password	8-46
Changing Your Email Address	8-47
Changing the Default Tab and Subtab	8-47

Creating Links	8-48
Running the ACS Failed Login Report	8-49

CHAPTER 9**Managing the WLSE via the CLI 9-1**

Logging In and Out via CLI	9-2
Logging In	9-2
Logging Out	9-2
User Management via CLI	9-3
Managing User Accounts	9-3
Setting Up TACACS+ or RADIUS Authentication for CLI Login	9-4
Backing Up and Restoring via CLI	9-5
Setting Up the Backup Location	9-6
Backing Up the WLSE	9-7
Restoring WLSE Configuration	9-7
Installing a Replacement WLSE	9-8
Removing the Old WLSE	9-8
Installing the Replacement WLSE	9-9
Copying Configuration Data to another WLSE	9-10
Upgrading WLSE Software via CLI	9-10
Rebooting the WLSE via CLI	9-11
Shutting Down and Powering Off the WLSE	9-11
Setting WLSE System Date and Time	9-12
Setting the System Clock Using NTP	9-12
Setting the System Clock Manually	9-13
Configuring Ethernet Interfaces	9-14
Configuring Protocols on Ethernet Interfaces	9-14
Configuring Interface Parameters	9-15
Managing Devices on Both Interfaces	9-15
Configuring the Mail Route via CLI	9-16

Administering Management Services via CLI	9-16
Viewing System Information via CLI	9-17
Recovery Management	9-18
Erasing System Configuration and Resetting to Factory Defaults	9-19
Using the Maintenance Image	9-19
Using the Recovery CD	9-21
Recovering from the Loss of All Administrator Passwords	9-23

CHAPTER 10

FAQs and Troubleshooting 10-1

General FAQs and Troubleshooting	10-2
General FAQs	10-2
General Troubleshooting	10-3
Faults FAQs and Troubleshooting	10-11
Faults FAQs	10-12
Faults Troubleshooting	10-13
Devices FAQs and Troubleshooting	10-14
Devices FAQs	10-14
Devices Troubleshooting	10-15
Configuration FAQs and Troubleshooting	10-19
Configuration FAQs	10-19
Configuration Troubleshooting	10-22
Firmware FAQs and Troubleshooting	10-23
Firmware FAQs	10-23
Firmware Troubleshooting	10-25
Reports FAQs and Troubleshooting	10-30
Reports FAQ	10-30
Reports Troubleshooting	10-30
Radio Manager FAQs and Troubleshooting	10-34
Radio Manager FAQs	10-34

Radio Manager Troubleshooting	10-38
Administration FAQs and Troubleshooting	10-39
Administration FAQs	10-39
Administration Troubleshooting	10-39

APPENDIX A**Naming Guidelines A-1**

APPENDIX B**Using the Command Line Interface (CLI) B-1**

Using the CLI	B-2
CLI Conventions	B-2
Command Privileges	B-2
Checking Command Syntax	B-3
Command History Feature	B-3
Help for CLI Commands	B-3
Command Description Conventions	B-4
Command Summary	B-4
Privilege Level 0 Commands	B-10
exit	B-10
ping	B-10
show clock	B-11
show domain-name	B-12
show interfaces	B-13
show process	B-14
show version	B-15
traceroute	B-15
Privilege Level 15 Commands	B-17
auth	B-17
backup	B-18
backupconfig	B-19

cdp	B-20
clock	B-21
df	B-22
dumptcp	B-23
erase config	B-24
firewall	B-25
gethostbyname	B-26
hostname	B-27
import	B-27
install configure	B-28
install list	B-29
install update	B-30
interface	B-31
ip domain-name	B-33
ip name-server	B-33
listbackup	B-35
mail	B-35
mailcntrl clear	B-36
mailcntrl list	B-37
mailroute	B-37
mkcert	B-38
nslookup	B-40
ntp server	B-40
reload	B-42
reinitdb	B-43
repository add	B-44
repository delete	B-44
repository list	B-45
repository source	B-46
repository server	B-47

restore	B-48
route	B-49
services	B-49
show anilog	B-51
show auth-cli	B-52
show auth-http	B-52
show backupconfig	B-53
show bootlog	B-53
show cdp neighbor	B-55
show cdp run	B-55
show collectorlog	B-56
show config	B-57
show daemonslog	B-58
show dmgtldlog	B-59
show import	B-60
show install logs	B-60
show ipchains	B-61
show hosts	B-61
show maillog	B-62
show proc	B-63
show repository	B-64
show route	B-64
show securitylog	B-65
show snmp-server	B-66
show ssh-version	B-66
show syslog	B-67
show tech	B-68
show telnetenable	B-68
show tomcatlog	B-69
show webaccesslog	B-70

show weberrorlog	B-71
show websslaccesslog	B-72
shutdown	B-72
snmp-server	B-73
ssh	B-74
ssh-version	B-74
telnet	B-75
telnetenable	B-75
username	B-76
webtimeout	B-78
Maintenance Image Commands	B-78
erase config	B-78
fsck	B-79
reload	B-79

GLOSSARY

INDEX



Preface

This guide describes the features of CiscoWorks Wireless LAN Solution Engine (WLSE) Release 2.5 and provides instructions for using Release 2.5 on the CiscoWorks Wireless LAN Solution Engine 1105 and 1130. This guide consists of the following chapters and appendixes and a glossary of terms:

- [Preface](#)
- [Getting Started](#)
- [Fault Monitoring](#)
- [Managing Device Configurations](#)
- [Updating Device Firmware](#)
- [Using Reports](#)
- [Managing the WLSE System](#)
- [FAQs and Troubleshooting](#)
- [Naming Guidelines](#)
- [Using the Command Line Interface \(CLI\)](#)

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 product documentation that is available.

Table 1 Product Documentation

Document Title	Available Formats
<i>Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine</i>	• Printed document included with the product. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com: – Log into Cisco.com. – Select at Products & Services > Network Management CiscoWorks > Wireless LAN Solution Engine > Technical Documentation > Installation and Configuration Guides. • Printed document available by order (part number DOC-7815903=),¹
<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: – Log into Cisco.com. – Select at Products & Services > Network Management CiscoWorks > Wireless LAN Solution Engine > Technical Documentation > User Guides. • Printed document available by order (part number DOC-7815902=),²
<i>Regulatory Compliance and Safety Information for the CiscoWorks 1130 Wireless LAN Solution Engine</i>	• Printed document included with the product. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com: – Log into Cisco.com. – Select Products & Services > Network Management CiscoWorks > Wireless LAN Solution Engine > Technical Documentation > Regulatory Approvals and Compliance.

Table 1 Product Documentation (continued)

Document Title	Available Formats
<i>Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine</i>	1. Log into Cisco.com. 2. Select Products & Services > Network Management CiscoWorks > Wireless LAN Solution Engine > Technical Documentation > Device Support Tables.
Context-sensitive online help	• Select an option from the navigation tree, then click Help. • Click the Help button in the dialog box.
<i>FAQ and Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine</i>	1. Log into Cisco.com. 2. Select Products & Services > Network Management CiscoWorks > Wireless LAN Solution Engine > Alerts and Troubleshooting > Troubleshooting Guides.
<i>Developer Guide for the CiscoWorks Wireless LAN Solution Engine</i>	Development information for the WLSE’s XML application programming interface (API). On Cisco.com at Technical Support > Product Support > Software Support > Network Management CiscoWorks > CiscoWorks Wireless LAN Solution Engine > Implementation and Configuration > Downloads > WLSE20XmlApi.zip.

1. See the “Obtaining Documentation” section on page xxii.
2. See the “Obtaining Documentation” section on page xxii.

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac>) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

The online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—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.

Priority 2 (P2)—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.

Priority 3 (P3)—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.

Priority 4 (P4)—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.

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

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

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- 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/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed 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:

- [Overview of the Wireless LAN Solution Engine, page 1-1](#)
- [WLSE Integration with Network Management Systems, page 1-2](#)
- [Understanding the Web Interface, page 1-3](#)
- [Logging In and Out, page 1-11](#)
- [Customizing the Web Interface, page 1-12](#)
- [Next Steps, page 1-13](#)



Note

Before using the procedures in this guide, you must install and configure the WLSE 1130, as described in the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*

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.

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.

WLSE Integration 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 the document *Integrating CiscoWorks Wireless LAN Solution Engine with a CiscoWorks Server* on Cisco.com.
- Launch a CiscoWorks server's desktop from the WLSE—See [Creating Links, page 8-48](#).
- Use the WLSE's fault notification interface to forward WLSE faults as SNMP traps—See [Notification Settings, page 2-51](#).



Note

WLSE 2.5 supports only SNMP v2c traps. SNMP v1 traps are not supported. Only network management systems that support v2c traps can integrate with the WLSE.

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 8-40](#).

This section describes the following aspects of the UI:

- The supported browsers and versions and browser configuration—See [Supported Browsers, page 1-3](#).
- The dashboard, including the tabs, subtabs, and buttons in the upper right corner—See [The WLSE Dashboard, page 1-5](#).
- How device names and IP addresses are displayed in the WLSE GUI—See [Device Name and IP Address Display, page 1-8](#).
- How the WLSE displays time—See [Time Display, page 1-8](#).
- How to use the device selector and Search—See [Using the Device Selector and Search, page 1-9](#).
- How to sort table data—See [Sorting Table Data, page 1-11](#).

Supported Browsers

The supported browsers and versions are listed in [Table 1-1](#).

**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 Netscape Navigator 7.02
Japanese Windows 2000, Windows NT, and Windows XP	Japanese Microsoft Internet Explorer 6.0 with Service Pack 1 Japanese Netscape Navigator 7.02
Solaris 8 and 9	Netscape Navigator 7.01

For the WLSE's Web interface to function correctly, all browsers require configuration. To configure a browser:

-
- Step 1** Enable JavaScript.
- Step 2** Configure the browser to accept all cookies.
- Step 3** Change the default font to sans serif for improved readability.
- Step 4** 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 Update, page 8-12](#).
 - Using a Windows XP server and Internet Explorer 6.0—See [Creating a Repository on a Windows Server, page 8-10](#).
-

For more detailed information on configuring browsers, see the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5* or the browser's documentation.

The WLSE Dashboard

The WLSE dashboard consists of:

- Tabs and subtabs that provide access to WLSE functions (see [Tabs and Subtabs](#), page 1-5).
- Buttons in the upper right corner that provide general functions (see [Buttons](#), page 1-7).

Tabs and Subtabs

The dashboard contains the following tabs and subtabs:

Table 1-2 *Tabs and Subtabs*

Main Tab	Subtabs	For information, see...
Faults	Display Faults—display device faults. Manage Fault Settings—use profiles to set thresholds and policies. Manage Network-Wide Profiles—assign network wide settings. Notification Settings—send fault information (traps, syslog messages, and emails).	Fault Monitoring , page 2-1.
Devices	Discover—enable discovery options and run discoveries, reset polling intervals, enter device credentials, put devices under management, run inventories, view task history for inventory and discovery, import and export devices, and enter AAA servers (LEAP, RADIUS, EAP-MD5, and PEAP) to be monitored. Group Management—manage device grouping by setting up static and dynamic groups.	Managing Devices , page 3-1
Configure	Templates—create configuration templates. Archives—view and manage the archived configurations. Jobs—apply configuration templates to access points and retrieve configurations for archiving. Auto update—automate initial configuration of access points.	Configuring Devices , page 4-1.

Table 1-2 Tabs and Subtabs (continued)

Main Tab	Subtabs	For information, see...
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.	Updating Device Firmware, page 5-1.
Reports	Device Center—quickly view reports for a particular device. Radio Manager—view reports about radio management information on the access points. Wireless Clients—view reports about client associations with access points. Current—view, export, and email reports about each type of monitored device. Trends—view, export, and email reports about current trends for monitored devices. Scheduled email jobs—manage email jobs.	Using Reports, page 6-1.
Radio Management	Radio Monitoring—monitor the WLAN and collects channel measurements used for radio configuration, rogue AP discovery, and interference detection AP Radio Scan—collect rogue location estimations, radio parameter generation (RPG) data, and coverage display data Client Walkabout—collect radio measurements and report them to the serving AP as you walk a client station throughout the coverage area RM Assisted Configuration—configure your APs using measurement data collected from a Client Walkabout and AP radio scanning Location Manager—display a graphical view of the WLAN environments including AP locations, radio configurations and estimated location of unknown APs	Radio Management, page 7-1

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

Main Tab	Subtabs	For information, see...
Administration	Appliance—manage the WLSE system (view diagnostics, manage WLSE software, manage WLSE security, backup and restore data, configure the login screen, set current time, specify NTP servers and name servers, set up routing for email jobs, use connectivity tools (ping, traceroute, nslookup, TCP port scan, and SNMP reachability), and use the SNMP query tool. System—view information about supported device firmware versions, and import information about newly supported firmware versions. 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), run ACS failed login reports.	Managing the WLSE System, page 8-1.

Buttons

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

- Overview—Displays an overview of the tabs and their functions.
- Help—Displays online help for the subtab or option you are using and a table of contents and index for online help.
- About—Displays information about the WLSE version.
- Logout—Logs you out of the WLSE and displays the login screen.

Device Name and IP Address Display

Many WLSE displays include a field for the device name. The data displayed in this field differs depending upon the following:

- If reverse DNS lookup is enabled on the WLSE, the device name is displayed in this field if the lookup succeeds. If the lookup fails, the device IP address is displayed.
- If you do not enable reverse DNS lookup and the device's sysName is set, the sysName SNMP variable is displayed. If sysName is not set, the device IP address is displayed.

In some displays there are separate fields for device name, sysName, and IP address.

To enable DNS lookup on the WLSE, select **Devices > Discover > DISCOVER > Advanced Options** and select Use reverse DNS lookup.

Time Display

The WLSE uses browser (client) time in most of its displays. The format of timestamps depends on the browser you are using:

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

14:17:16 10/12/2002

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 2002

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

14:17:16 10/12/2002

In some displays the timestamp is the day of the week, time, offset from GMT/UTC, timezone, and year; for example:

Mon Mar 25 13:29:21 GMT-0800 (Pacific Standard Time) 2002

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

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, use the CLI **clock** command to set the UTC date and time correctly. Thereafter, the Web interface will display the correct current local (browser) time.

For more information on the **clock** command and other CLI commands, see the command reference in the *User Guide for the CiscoWorks Wireless LAN Solution Engine*—in the online help, click **View PDF**.

For more information about setting the current local time in the Web interface, see [Set the Current Local and UTC Time, page 8-33](#).

Using the Device Selector and Search

The WLSE contains a device selector and Search that can be used to select a group or devices or an individual device:

- Device Selector—See [Using the Device Selector, page 1-9](#)
- Search—See [Using Search, page 1-10](#)

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 1-10](#).

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.

Procedure

-
Step 1	Click to expand the desired folder.
Step 2	Click to select the 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.

Procedure

- Step 1** From the list, select the method you want to use to search for the device, then enter the search information.



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

- Device Name—The name of the device.
- IP Address—The IP address of the device.
- APs Based on Client MAC—The MAC address of a known client. For both IOS and non-IOS access points.
- 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

The search results, as well as the folders in the device selector, display 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 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.

To set up access for other users, see [Managing User Accounts, page 8-42](#) and [Managing Roles, page 8-40](#). The WLSE supports up to 10 simultaneous users.



Note

The WLSE Web interface times out after 30 minutes of inactivity. You will be logged out after that time. You can use the **webtimeout** command to change the timeout period. for information about the WLSE's command line interface (CLI) see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*. To view this guide from the online help, click **View PDF**.

Procedure

To log into the Web interface:

-
- Step 1** Access the WLSE through a browser by entering the WLSE's IP address, followed by **:1741** (for example: `http://209.165.128:1741`).
 - For information on supported browsers, see [Supported Browsers, page 1-3](#).
 - 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.

Customizing the Web Interface

You can customize the Web interface by:

- [Setting the Default Tab and Subtab, page 1-12](#)
- [Adding a Message to the Splash Screen, page 1-13](#)

Setting the Default Tab and Subtab

By default the overview screen appears when you log in. This screen provides a brief description of each of the main tabs. When you select a tab, the overview describes 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 or overview 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 . The message will be displayed in the splash screen. Users must click Agree in the splash screen before the login prompt will appear.
-

Next Steps

The following list shows the order in which you can access WLSE features:

1. Before you can use WLSE management features, you must configure the WLSE and set up your network devices. These procedures are described in the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*.
2. Initiate discovery and move your network devices to the managed state (see [Managing Devices, page 3-1](#)).
3. Now you can use all of the WLSE features for managing your WLAN.
4. When deploying additional devices, use the device setup procedures in [Setting Up Devices, page 3-5](#).



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 [Viewing Fault Information, page 2-1](#)
- **Manage Fault Settings**—See [Managing Fault Settings, page 2-18](#)
- **Manage Network-Wide Settings**—See [Managing Network-Wide Settings, page 2-49](#)
- **Notification Settings**—See [Notification Settings, page 2-51](#)

Viewing Fault Information



Note

For an explanation of the faults, see the Fault Description Table in the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.5* on Cisco.com.

The topics covered in this section are:

- [Understanding Fault and Security Policy Monitoring, page 2-2](#)
- [Displaying Faults, page 2-6](#)
- [Clearing Summary Table Faults, page 2-9](#)
- [Acknowledging Faults, page 2-10](#)
- [Viewing Fault Details, page 2-10](#)

Related Topics

- [Specifying Fault Thresholds, page 2-37.](#)
- [Specifying Security Policies, page 2-25.](#)

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.



Note

The WLSE does not receive SNMP traps and should not be considered a full featured fault management tool for wireless access points. You can use the notification feature, however, to integrate the WLSE into more advanced fault management applications (see [Setting Trap Notification, page 2-51](#)).

The following topics are included in this section:

- [How Are Faults Generated?, page 2-3](#)
- [Understanding Fault States, page 2-3](#)
- [Understanding Security Policy Monitoring Faults, page 2-4](#)
- [Understanding Threshold-Related Faults, page 2-4](#)

How Are Faults 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 2-3](#)

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 2-10](#)

- **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 2-9](#).
- Fault Details Window—See [Viewing Fault Details, page 2-10](#).
- Thresholds and Policies—See [Viewing Current Faults, page 2-47](#)

Related Topics

- [Managing Fault Settings, page 2-18](#)
- [Understanding Fault and Security Policy Monitoring, page 2-2](#)

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

- [Specifying Security Policies, page 2-25](#)
- [Understanding Fault and Security Policy Monitoring, page 2-2](#)

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 [Specifying Fault Thresholds, page 2-37](#)).

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

- [Understanding Fault and Security Policy Monitoring, page 2-2](#)

Displaying Faults



Note For an explanation of the faults, see the Fault Description Table in the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.5* on Cisco.com.

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 2-1 Display Faults Filter Bar

Field	Description
Devices	From the list, select the device type whose fault summary you want to display.

Table 2-1 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.
State	From the list, select a state to display. See Understanding Fault States, page 2-3 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 60 seconds. 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 2-2 Display Faults Table

Column	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 6-2.
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 6-2.
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 2-10. Note For an explanation of the faults, see the Fault Description Table in the <i>FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.5</i> on Cisco.com.
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 Time Display, page 1-8. Click to see fault details. See Viewing Fault Details, page 2-10.

- 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 2-10](#)
- [Understanding Fault States, page 2-3](#)

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 2-3](#)

Viewing Fault Details

There are two types of fault detail windows:

- [Device Fault Details, page 2-10](#)—Displays details about the device, its fault conditions and history.
- [Rogue Access Point Details, page 2-14](#)—Displays details about the unknown access point, beacon and location information, switch port tracing, reporting access points, and fault history.



Note

For an explanation of the faults, see the Fault Description Table in the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.5* on Cisco.com.

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 for](#)
- [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 for

Table 2-3 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 2-4 *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, see the Fault Description Table in the <i>FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.5</i> on Cisco.com.
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed. See Time Display, page 1-8.
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 2-5 *Fault History Table*

Column	Description
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, see the Fault Description Table in the <i>FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.5</i> on Cisco.com.
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 Time Display, page 1-8.
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.

Rogue Access Point Details

When you click the link in the Description or Timestamp fields in the Fault Summary Table for an unknown access point, the following tables are displayed in the Rogue Access Point Details window:

- [Rogue Access Point Details](#)
- [Beacon Information](#)
- [Location Estimation](#)
- [Switch Port Tracing](#)
- [Reporting APs](#)
- [Fault History](#)

Rogue Access Point Details

A rogue access point is an AP that has not been identified as Friendly. By default, all unknown radios are classified as Rogue until you change them to Friendly.

A Friendly access point is an AP that you know exists, for example, a neighboring network's AP, but that you are not going to modify in any way.

Table 2-6 *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.
Change To Friendly AP	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.
Delete	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**Table 2-7 Beacon Information Table**

Column	Description
SSID	Service set identifier used by client devices to associate with an access point.
Beacon Interval	The beacon interval on which the rogue AP is transmitting.
Channel	The channel on which the rogue AP is transmitting.
Data Rates	The data rates on which the rogue AP is transmitting.

Location Estimation**Table 2-8 Location Estimation Table**

Column	Description
Location	The estimated location of the rogue AP.
Timestamp	Indicates the time, based on the client browser, the rogue was detected. See Time Display , page 1-8.
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 Finding Unknown Radios , page 7-52.

Switch Port Tracing**Table 2-9 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.
Timestamp	Indicates the time, based on the client browser, the rogue AP switch port was detected. See Time Display, page 1-8 .
Re-Trace	Click Re-Trace to locate the switch port again. This is useful if the rogue AP was moved and connected to a different port.

Reporting APs**Table 2-10 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.
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.

Fault History

The following table contains a history of the faults raised against this rogue AP.

Table 2-11 Fault History Table

Column	Description
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, see the Fault Description Table in the <i>FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.5</i> on Cisco.com.
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 Time Display, page 1-8.
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 2-18](#)
- [Creating a Setting, page 2-19](#)
- [Copying a Setting, page 2-20](#)
- [Renaming a Setting, page 2-21](#)
- [Editing a Setting, page 2-22](#)
- [Deleting a Setting, page 2-22](#)
- [Viewing a Summary, page 2-23](#)
- [Assigning a Setting to a Device, page 2-23](#)

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

For example, Site A is connected via high-speed LAN connections, and remote Sites B and 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

- [Specifying Security Policies, page 2-25](#)
- [Specifying Fault Thresholds, page 2-37](#)

Creating a Setting

Use this option to create 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** Enter a unique name. See [Naming Guidelines, page A-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 2-22](#).



Note The new setting is a copy of the Default setting.

Related Topics

[Understanding Fault Settings, page 2-18](#)

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 A-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 2-22](#).

Related Topics

[Understanding Fault Settings, page 2-18](#)

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 A-1](#) for details.
 - Step 4** Click **OK**. The new name appears in the Existing Fault Settings list.
-

Related Topics

[Understanding Fault Settings, page 2-18](#)

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 Security Policies and Thresholds, page 2-24](#).
-

Related Topics

[Understanding Fault Settings, page 2-18](#)

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 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 and Search, page 1-9](#).
- 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 2-18](#)

Setting Security Policies and Thresholds

When you create or edit a setting, you can also assign security policy settings and fault thresholds. The following choices appear in the left pane of the Editing Settings window:

- Security Policies—See [Specifying Security Policies, page 2-25](#)
- Thresholds—See [Specifying Fault Thresholds, page 2-37](#)

Specifying Security Policies

This option allows you to activate or deactivate a set of predefined policies for access points. The policies you set in this window will determine how some of the faults are displayed in the **Faults > Display Faults** subtab.

**Note**

Security Policies are disabled by default unless otherwise noted.

You can also view the current faults for each setting. See [Viewing Current Faults, page 2-47](#).

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** In the left pane, select the policy you want to apply to the setting:
- SSID—See [Setting the SSID Policy, page 2-26](#).
 - Firmware Version (IOS)—See [Setting the Firmware Version Policy, page 2-27](#).
 - Firmware Version (Non-IOS)—See [Setting the Firmware Version Policy, page 2-27](#).
 - Broadcast SSID Disabled—See [Setting the Broadcast SSID Disabled Policy, page 2-28](#).
 - Key Rotation per VLAN—See [Setting Key Rotation Disabled per VLAN Policy, page 2-28](#).
 - WEP Encryption per VLAN—See [Setting WEP Encryption per VLAN Policy, page 2-29](#).
 - WEP Enforced—See [Setting the WEP Enforced Policy, page 2-30](#).
 - EAP Enforced—See [Setting the EAP Enforced Policy, page 2-31](#).
 - EAP Per SSID Enforced—See [Setting EAP Per SSID Enforced Policy, page 2-32](#).
 - WEP Key Length—See [Setting WEP Key Length Policy, page 2-33](#).
 - HotStandBy Status—See [Setting the HotStandBy Status Policy, page 2-33](#).

- HTTP Disabled (Non-IOS)—See [Setting the HTTP Disabled \(Non-IOS\) Policy, page 2-34](#).
 - Telnet Disabled (Non-IOS)—See [Setting the Telnet Disabled \(Non-IOS\) Policy, page 2-35](#).
 - PSPF Enabled (Non-IOS)—See [Setting the PSPF Enabled \(Non-IOS\) Policy, page 2-35](#).
 - User Manager Enforced (Non-IOS)—See [Setting the User Manager Enforced \(Non-IOS\) Policy, page 2-36](#).
 - HTTP Authentication (Non-IOS)—See [Setting the HTTP Authentication \(Non-IOS\) Policy, page 2-37](#).
-

Related Topics

[Understanding Security Policy Monitoring Faults, page 2-4](#)

Setting the SSID Policy

Procedure

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

Field	Description
Verify	Select if you want to verify that SSID is enabled.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
Enter SSID	Enter the unique identifier used by client devices to associate with the access point. Any alphanumeric character up to 32 characters long. This is for the primary SSID.

- Step 2** Click **Add** to add the SSID to the list.

- Step 3** To remove an SSID from the list, select it, click **Remove**.

- 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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 6** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.
-

Setting the Firmware Version Policy

Procedure

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

Field	Description
Verify	Select if you want to verify that firmware version is enabled.
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 **Add** to add the firmware version to the list.
- Step 3** To remove a firmware version from the list, select it, click **Remove**.
- 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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 6** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.
-

Setting the Broadcast SSID Disabled Policy

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to verify.
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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.

Setting Key Rotation Disabled per VLAN Policy

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select if you want to verify that key rotation is disabled.
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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.

Setting WEP Encryption per VLAN Policy

Procedure

- Step 1** Complete the following:

Field	Description
Verify	Select if you want to verify that key rotation is disabled.
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.

Field	Description
Available Vlans	Lists all the VLAN ID number 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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.

Setting the WEP Enforced Policy

Procedure

- Step 1** Complete the following:

Field	Description
Verify	Select to verify Broadcast SSID is disabled
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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.
-

Setting the EAP Enforced Policy

Procedure

- Step 1** Complete the following:

Field	Description
Verify	Select to verify.
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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.
-

Setting EAP Per SSID Enforced Policy

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select if you want to verify that key rotation is disabled.
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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.

Setting WEP Key Length Policy

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select if you want to verify the WEP key length.
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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.

Setting the HotStandBy Status Policy

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to verify.
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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4

Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.

Setting the HTTP Disabled (Non-IOS) Policy

Procedure

- Step 1

Complete the following:

Field	Description
Verify	Select to verify.
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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4

Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.

Setting the Telnet Disabled (Non-IOS) Policy

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to verify.
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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.

Setting the PSPF Enabled (Non-IOS) Policy

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to verify.
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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.
-

Setting the User Manager Enforced (Non-IOS) Policy

Procedure

- Step 1** Complete the following:

Field	Description
Verify	Select to verify.
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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.
-

Setting the HTTP Authentication (Non-IOS) Policy

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to verify.
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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.

Specifying Fault Thresholds

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

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

You can also view the current faults for each of these thresholds. See [Viewing Current Faults, page 2-47](#).



Note

Your login determines whether you can use this option.

Threshold choices include the following options:

- **Access Point**—See [Setting Access Point Fault Thresholds](#), page 2-38.
- **Switch**—See [Setting Switch Fault Thresholds](#), page 2-41.
- **Router**—See [Setting Router Fault Thresholds](#), page 2-43.
- **LEAP**—See [Setting Server Response Time](#), page 2-44.
- **PEAP**—See [Setting Server Response Time](#), page 2-44.
- **RADIUS**—See [Setting Server Response Time](#), page 2-44.
- **EAP-MD5**—See [Setting Server Response Time](#), page 2-44.
- **WLSE**—See [Setting WLSE Dot11 MIB View](#), page 2-46.
- **WDS**—See [Setting WDS Thresholds](#), page 2-46.

Related Topics

[Understanding Threshold-Related Faults](#), page 2-4

Setting Access Point Fault 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**.



Note

The following thresholds are enabled by default: SNMP Reachable, RF Port Status and Ethernet Port Status.

- See [Setting Up or Down Status](#), page 2-39 to set the fault thresholds for the following access point faults:
 - SNMP Reachable
 - RF Port Status
 - Ethernet Port Status
 - Registration Error

- See [Setting Overloaded, Degraded, and OK Status, page 2-40](#) to set the fault thresholds for the following access point faults:
 - RF Port Utilization
 - RF Port Packet Errors
 - RF Port WEP Errors
 - Ethernet Port Utilization
 - Ethernet Port Packet Errors
 - Max Retry Count
 - Associated Clients
 - Association Rate
 - Authentication Error Rate

Setting Up or Down Status

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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4

Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-47](#) for details.

Setting Overloaded, Degraded, and OK Status

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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-47](#) for details.
-

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**.



Note

The following thresholds are enabled by default: SNMP Reachable and Port Status.

- See [Setting Up or Down Status, page 2-42](#) to set the fault thresholds for the following switch faults:
 - SNMP Reachable
 - Port Status
 - Module Status
- See [Setting Overloaded, Degraded, and OK Status, page 2-43](#) to set the fault thresholds for the following:
 - CPU Utilization
 - Memory Utilization
 - Port Utilization

Setting Up or Down Status

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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-47](#) for details.

Setting Overloaded, Degraded, and OK Status

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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-47](#) 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**.

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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-47](#) for details.

Setting Server Response Time

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

**Note**

This threshold 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	
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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-47](#) for details.

Setting WLSE Dot11 MIB View

Using this option, you can set up a threshold for the dot11 MIB view. When the threshold is exceeded, a fault is generated and can be viewed under **Faults > Display Faults**.

**Note**

This threshold is enabled by default.

For information on the dot11 MIB view fault, see [Faults FAQs, page 10-12](#).

Procedure

Step 1 Complete the following:

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

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 assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-47](#) 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
- WLSE-WDS Link Status

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



Note

These thresholds are enabled by default.

You can set the following WDS thresholds:

- Authentication Failures
- WLSE-WDS Link Status

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 Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-47](#) 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 6-2 .
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 6-2 .
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 2-10 . Note For an explanation of the faults, see the Fault Description Table in the <i>FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.5</i> on Cisco.com.
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 Time Display, page 1-8 . Click to see fault details. See Viewing Fault Details, page 2-10 .

- 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.

Managing Network-Wide Settings

Using this option, you can set the following network-wide policies:

- Rogue AP Detection—See [Setting Rogue AP Detection, page 2-49](#)
- Interference Detection—See [Setting Interference Detection, page 2-50](#)

Setting Rogue AP Detection

Use this option to enable rogue access point detection and to assign a severity level to the fault. When this condition is met, a fault is generated and can be viewed under **Faults > Display Faults**.

Procedure

- Step 1** Select **Faults > Manage Network-Wide Settings > Rogue AP Detection**.
- Step 2** Complete the following:

Field	Description
Enable	Select to enable the setting.
Setting	From the list, select the severity level to assign the fault when a rogue access point is detected.

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

Setting Interference Detection

Use this option to set the threshold condition for interference detection. When the condition is met, a fault is generated and can be viewed under **Faults > Display Faults**.

Procedure

- Step 1** Select **Faults > Manage Network-Wide Settings > Interference Detection**.

- Step 2** Complete the following:

Field	Description
Enable	Select to enable the setting.
Settings	
Degraded	From the list, select the severity level, the interference level, the percentage, and the time interval before the status is Degraded.
OK	From the list, select the interference level, the percentage and the time interval before the status is OK.

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

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

- [Viewing Fault Information, page 2-1](#)
- [Specifying Fault Thresholds, page 2-37](#)

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.

**Note**

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.

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.

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 2-53](#) for an example.
- 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 Row**. 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

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

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

```
Mon Jun 02 18:17:56 2003 192.168.98.44 A tcpConnectionClose trap
received from enterprise cisco with 7 arguments: tslineSesType=48;
tcpConnState=1; loctcpConnElapsed=10.10.10.31;
loctcpConnInBytes=OK; loctcpConnOutBytes=8583602;
cderExcepData = 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 a trap notification message using XML will appear as follows:

```
cderExcepTableIndex = 48
cderExcepId = 1
cderExcepHostAddressType = 1
cderExcepHostAddress = 10.10.10.31
cderExcepPriorityDescription = OK
cderExcepTime = Jun 02 17:47:48 2003
cderExcepData =
<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>SS
ID is
OK</StateChange><AlarmState>Cleared</AlarmState><OverallSeverity
>OK</OverallSeverity></Msg>
cderExcepReportedBy = FaultNotifier@samuraiwhat.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.

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 2-55](#) for an example.
- 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.

- 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>O
K</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 2-56](#).

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.
Priority	From the list, select the priority of the exceptions you want to email.



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 Row** 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.

Attribute	Description
DeviceIp	The IP address of the device with the fault.
DeviceName	The name of the device with the fault.
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 2003 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 tracypv
From:FaultNotifier@samuraiwhat.cisco.com
Date:Tue, 3 Jun 2003 00:57:55 GMT
To:user@cisco.com
<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>O
K</OverallSeverity></Msg>
```



Managing Devices

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

The topics covered in this chapter are:

- [Devices Tab Functions, page 3-2](#)
- [Getting Started with Device Management, page 3-3](#)
- [Setting Up Devices, page 3-5](#)
- [Specifying Device Credentials, page 3-27](#)
- [Managing AAA Servers, page 3-37](#)
- [Managing Device Discovery, page 3-41](#)
- [Managing and Unmanaging Devices, page 3-76](#)
- [Managing Device Inventories, page 3-80](#)
- [Exporting Devices, page 3-94](#)
- [Managing Groups, page 3-97](#)

Devices Tab Functions

The Devices tab provides the facilities for 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 a detailed guide to using these options, see [Getting Started with Device Management, page 3-3](#).

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

**Note**

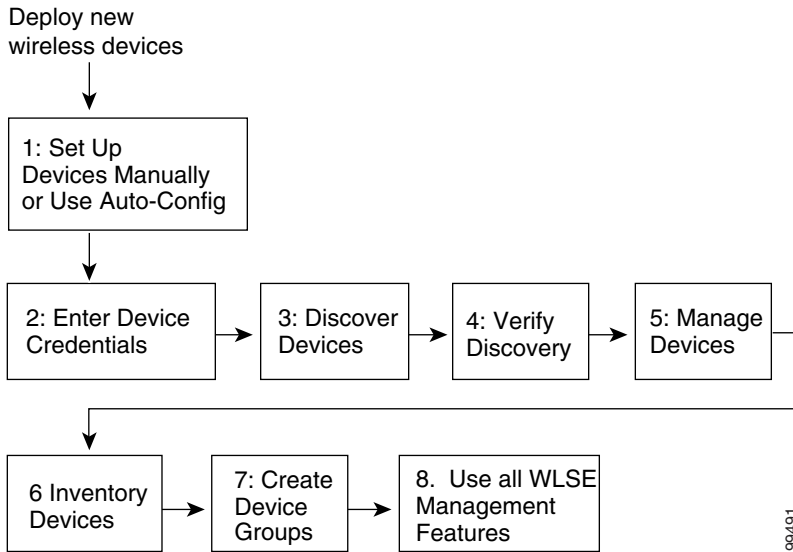
These subtabs may not be visible to some users; what you see under the Devices tab depends on your login.

The options under the Devices tab are:

- Discover subtab:
 - Manage Devices—See [Managing and Unmanaging Devices, page 3-76](#)
 - Discover—See [Managing Device Discovery, page 3-41](#)
 - Device Credentials—See [Specifying Device Credentials, page 3-27](#)
 - Inventory—See [Managing Device Inventories, page 3-80](#)
 - Export Devices—See [Exporting Devices, page 3-94](#)
 - AAA Server—See [Managing AAA Servers, page 3-37](#)
- Group Management subtab—See [Managing Groups, page 3-97](#)

Getting Started with Device Management

Before you can use the WLSE to manage newly added devices, you must set up the devices, configure the WLSE, discover the devices, and move the devices to the managed state. Optionally, you can set up your own device groupings to make management easier. To get started, follow the steps listed in the following illustration and 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.

- The alternatives for setting up access points and bridges are:
 - Configure each device manually—see [Set Up Non-IOS Access Points and Bridges, page 3-6](#) and [Set Up IOS Access Points, page 3-8](#).
 - Use automatic startup configuration—see [Assigning a Startup Configuration, page 4-300](#).
- To set up routers and switches, see [Set Up Routers and Switches, page 3-24](#).
- To set up AAA servers, see [Set Up AAA Servers, page 3-25](#).

Step 2: Enter device credentials

Enter device credentials on the WLSE:

- Enter community strings for all managed devices—see [Enter SNMP Community Strings for All Devices](#), page 3-28.
- Enter HTTP usernames and passwords for non-IOS access points—see [Enter HTTP Usernames and Passwords—Non-IOS Access Points](#), page 3-32.
- Enter Telnet credentials for IOS access points—see [Enter Telnet and SSH Usernames and Passwords—IOS Access Points](#), page 3-33.
- Enter HTTP ports for IOS access points—see [Enter HTTP Port Settings—IOS Access Points](#), page 3-35.
- Enter information about setting up AAA servers—see [Managing AAA Servers](#), page 3-37.

Step 3: Discover Devices

Initiate discovery from the WLSE or import devices:

- Add seed devices and run discovery—see [Managing Device Discovery](#), page 3-41.
- Import devices—see [Importing Devices from a File](#), page 3-59 and [Importing Devices from a CiscoWorks Server](#), page 3-61.

Step 4: Verify discovery

Verify that devices were discovered—see [Viewing Discovery Logs](#), page 3-69.

Step 5: Move devices to managed state

Before you can use configuration, reporting, and monitoring features, you must either move devices to the managed state on the WLSE, or specify that all discovered devices be automatically managed—see [Managing and Unmanaging Devices](#), page 3-76.

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 Inventories](#), page 3-80.

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 the on-demand inventory to populate these reports before the next inventory cycle starts. You can also use on-demand polling 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, upgrade, and view reports for a set of access points as a single operation—see [Managing Groups, page 3-97](#).

Step 8: Use all WLSE features

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

Setting Up Devices

You must set up devices before the WLSE can discover and manage them and before you can use the WLSE for the following tasks: discovery, monitoring, reporting, configuration, and firmware upgrade. In addition, IOS access points must be configured for radio management. This section describes both required and optional setup tasks for the following devices:

- Non-IOS access points—see [Set Up Non-IOS Access Points and Bridges, page 3-6](#)
- IOS access points—See [Set Up IOS Access Points, page 3-8](#)
- Routers and switches—See [Set Up Routers and Switches, page 3-24](#)
- AAA servers—[Set Up AAA Servers, page 3-25](#)

Set Up Non-IOS Access Points and Bridges

You can set up access points and bridges in two ways:

- By using the WLSE's automatic configuration option for first-time device configuration and applying a configuration template to a number of access points. For more information, see [Automating Configurations, page 4-300](#).
- By opening a web browser session on each access point and performing the tasks in the following table. To use this method, you must first configure each access point or bridge for web browsing.

Table 3-1 Set Up Procedures for Non-IOS Access Points and Bridges

Tasks	Procedure	Notes
1. Enable Cisco Discovery Protocol (CDP).	1. In the Summary Status page, click Setup. 2. Under Services: Cisco Services, click Cisco Discovery Protocol. 3. Select Enabled. Click Apply or OK.	Required for the WLSE to use CDP to discover the device.
2. Enable SNMP. (Optional) Set the location. (Optional) Set the system name and system contact.	1. In the Summary Status page, click Setup. 2. Under Services, click SNMP. 3. Select Enabled. 4. Enter a System Name, System Location, and System Contact. 5. Click Apply or OK.	SNMP is required for the WLSE to discover devices, populate reports, transfer configuration information to devices, and upgrade device firmware. Setting the system name, system contact, and system location ensures that this information is included in device detail displays.

Table 3-1 Set Up Procedures for Non-IOS Access Points and Bridges (continued)

Tasks	Procedure	Notes
3. Set the read community string.	1. In the Summary Status page, click Setup. 2. Under Services, click Security. 3. Click User Information; then click Add New User. 4. Create a user with all privileges, including SNMP, Firmware, Write, and Admin privileges. In addition, for access points that are running a firmware version earlier than 12.01(T), assign Ident privileges. 5. Click Apply or OK.	The read community string is required for device discovery and populating reports.
4. Set the read-write community string.	1. In the Summary Status page, click Setup. 2. Under Services, click Security. 3. Click User Information; then click Add New User. 4. To create a user with SNMP read/write privileges, enter a username and password and select the Write, SNMP, Firmware, and Admin privileges. 5. Click Apply or OK.	The read-write community string is required for configuration and firmware jobs.
5. Add an HTTP user with the ability to modify firmware, and enable the User Manager. You can use the same user that you created in Task 4, if the user has firmware privileges.	1. In the Summary Status page, click Setup. 2. Click Security. 3. Click User Information; then click Add New User. 4. Enter a username and password and select Firmware; then click Apply. 5. Navigate back to the Security Setup page and click User Manager. 6. Select Enabled; then click Apply or OK.	This allows configuration uploads from the WLSE to access points. You must also enter HTTP users and passwords on the WLSE (see Enter HTTP Usernames and Passwords—Non-IOS Access Points , page 3-32).

Table 3-1 Set Up Procedures for Non-IOS Access Points and Bridges (continued)

Tasks	Procedure	Notes
6. Set up TFTP as the transfer protocol between the WLSE and access points.	1. In the Summary Status page, click Setup. 2. Under Services, click FTP. 3. Use the pulldown menu to select TFTP as the file transfer protocol. 4. In the Default File Server text box, enter the IP address of the WLSE. 5. Click Apply or OK.	TFTP is used for transferring configuration changes to access points.

Set Up IOS Access Points

This section provides:

- Procedures to prepare IOS access points for basic network management by the WLSE—See [Basic Network Management Setup—IOS Access Points, page 3-8](#).
- Procedures to prepare IOS access points and the WLSE for participation in the Cisco Structured Wireless-Aware Network (SWAN)—See [Radio Management Setup—IOS Devices, page 3-13](#).

Basic Network Management Setup—IOS Access Points

You can set up access points and bridges in the following ways:

- Use the WLSE's automatic configuration option for first-time device configuration and applying a configuration template to a number of access points—See [Automating Configurations, page 4-300](#).
- Log into each device by using Telnet or SSH and use the device's CLI commands—See [Set Up IOS Access Points by Using the Device CLI, page 3-9](#).
- Log into each device's Web interface—See [Set Up IOS Access Points by Using the Device Web Interface, page 3-11](#).

After you set up a device, all of its MIB variables can be accessed and the device can be discovered by the WLSE.

**Note**

VLAN information for IOS access points might not be collected by the WLSE if WEP keys are not configured in each VLAN. This affects VLAN reports, grouping, and faults. VLAN information becomes accessible through SNMP as soon as WEP keys are configured.

**Note**

If you are using Wireless Domain Service (WDS), you must configure both the WLSE and an IOS access point that supports WDS (currently, Cisco Aironet 1100 or 1200). In addition, an AAA server is required. For procedures, see [Enter WLCCP Credentials for Wireless Domain Services, page 3-36](#).

Set Up IOS Access Points by Using the Device CLI

Procedure

- Step 1** Use Telnet or SSH to log into the AP 1100 or AP 1210.
- Step 2** Enter enable mode.
- Step 3** Enter global configuration mode.
- Step 4** Enable CDP by entering the following command:

```
cdp run
```

**Note**

You can find out whether CDP has been enabled by using the **show cdp** command in enable mode.

**Note**

If you do not wish to use CDP, you can add all access points as seeds or import devices. For more information, see [Managing Device Discovery, page 3-41](#).

- Step 5** Enter the following commands in the sequence shown. The first two commands set the read-only SNMP community string and create an ISO view, which enables discovery and the fault and report features on the WLSE. The third command sets a read/write community string, which allows you to use the WLSE to update access point firmware and configuration.

```
snmp-server view iso iso included
snmp-server community community_string view iso RO
snmp-server community community_string RW
```



Note These community strings must be entered on the WLSE. See [Enter SNMP Community Strings for All Devices, page 3-28](#).



Note IOS access points that do not have an ISO view will be placed in the Misconfigured Devices system group after discovery and fault will be generated. The fault refers to a “dot 11 MIB” problem.

- Step 6** You can use either Telnet or SSH to push configuration templates to IOS access points. To use templates to configure IOS access points, you must configure either Telnet or SSH or both. See Steps 7 and 8 to enable and configure SSH and Telnet.

- Step 7** To enable and configure SSH, enter the following commands. In these commands, *hostname* is the hostname of the access point, and *domain_name* is your network’s domain name (for example, cisco.com). At the prompt for the number of bits in the modulus, press **Return** to accept the default or enter a value.

```
hostname hostname
ip domain-name domain_name
crypto key generate rsa
How many bits in the modulus [512]:
```

The following commands are recommended, but optional:

```
ip ssh time-out 120
ip ssh authentication-retries 3
```

- Step 8** To configure Telnet, enter the following commands:

```
line 0 4
no access-class 111 in
```

The following commands are recommended, but optional:

```
width 80
length 24
```

Step 9 Exit global configuration mode, then enter the following command:

```
write memory
```

Set Up IOS Access Points by Using the Device Web Interface

Procedure

Step 1 Log into the Web interface of the AP 1100 or AP 1210 device.

Step 2 Select **SERVICES** from the menu, then click **CDP**:

- a. After Cisco Discovery Protocol (CDP), select **Enabled**.
- b. Click **Apply**.



Note If you do not wish to use CDP, you can add all access points as seeds or import devices. For more information, see [Managing Device Discovery, page 3-41](#).

Step 3 You can use either Telnet or SSH (secure shell protocol) to push configuration templates to IOS access points. To use templates to configure IOS access points, you must configure either Telnet or SSH or both. See Steps 4 and 5 to enable SSH and Telnet.

Step 4 To enable and configure SSH (secure shell protocol), enter the following:

- a. Select **SERVICES > Telnet/SSH**.
- b. Enable **Secure Shell**.
- c. Enter a System Name.
- d. Enter a Domain Name (for example, cisco.com).
- e. (Optional) Enter the RSA key size.
- f. (Optional) Enter the Authentication Timeout.

- g. (Optional) Enter Authentication Retries.
- h. Click **Apply**.

Step 5 To enable and configure Telnet:

- a. Select **SERVICES > Telnet/SSH**.
- b. Enable **Telnet**.
- c. (Optional) Enable **Teletype**.
- d. Enter the number of Columns.
- e. Enter the number of Lines.
- f. Click **Apply**.

Step 6 Select **SNMP** from the menu.

- a. After Simple Network Management Protocol (SNMP), select **Enabled**.
- a. Click **Apply**.

Step 7 In the SNMP Request Communities section, enter a community string for the ISO view. This community string is required for discovery and to enable the fault and report features of the WLSE.

- a. Enter the community string in the SNMP Community field.
- b. Enter **iso** in the Object Identifier field.



Note

IOS access points that do not have an ISO view will be placed in the Misconfigured Devices system group after discovery, and a fault will be generated. The fault message refers to a “dot11 MIB problem.”

- c. Click **Read-Only**.
- d. Click **Apply**.

Step 8 In the SNMP Request Communities section, enter a community string to enable firmware and configuration updates on the access point.

- a. Enter the community string in the SNMP Community field.
- b. Click **Read-Write**.
- c. Click **Apply**.

- Step 9** The community strings created in Steps 7 and 8 must be entered on the WLSE before the device can be discovered and other WLSE features can be used. For more information, see [Enter SNMP Community Strings for All Devices, page 3-28](#).
-

Radio Management Setup—IOS Devices



Note

The basic network configuration must first be done on all of the access points. See [Basic Network Management Setup—IOS Access Points, page 3-8](#).

Setting up access points for radio management involves configuring all access points to register with Wireless Domain Services (WDS). WDS provides wireless client roaming and radio management aggregation.

Only Cisco Aironet 1100 and 1200 access points support WDS. For information about the supported access points and IOS firmware versions, see the WLSE 2.7 Supported Devices Table on cisco.com.

Each WDS access point supports one subnet and up to 30 infrastructure access points. You can add additional WDS access points for redundancy. The priorities you set on the WDS access points determine which one is the primary, and which ones are backups.

The requirements for radio management are:

- Configure the WDS devices that will provide services to the infrastructure access points—See [Configure WDS Access Points, page 3-14](#).
- Configure the infrastructure access points to authenticate to the WDS—See [Configure Infrastructure Access Points, page 3-20](#).
- Configure the WLSE with WLCCP credentials—See [Configuring the WLSE, page 3-21](#).
- Define authentication server(s)—See [Configuring Authentication, page 3-14](#).
- Confirm the configuration—See [Confirming the Configuration, page 3-22](#).

Configuring Authentication

To use WDS, both the infrastructure APs and the WLSE must use LEAP to authenticate to the WDS devices. For this purpose, you can use:

- Local authentication on a WDS device. See [Configure WDS Access Points, page 3-14](#).
- AAA servers that you have already configured, or configure servers as described in [Set Up AAA Servers, page 3-25](#).

Configure WDS Access Points

**Note**

Before making changes to device configuration, you should back up the current configuration, and test the new configuration on non-production devices.

WDS must be active on an access point in each layer-2 domain; backup WDS access point(s) can also be defined in each layer-2 domain.

Configuring WDS involves the following. See the rest of this section for detailed instructions.

- Define the AAA servers and server groups that the WDS will use to LEAP authenticate infrastructure access points and/or wireless clients.
- Enable WDS and set WDS priorities.
- Enter the WMN IP address.

There are three ways to configure WDS access points:

- Using the access point web interface—See [Using the Access Point Web Interface, page 3-15](#).
- Using the access point CLI interface—See [Using the Access Point CLI Interface, page 3-16](#).
- Using a WLSE configuration template—[Using a WLSE Configuration Template, page 3-18](#).

Using the Access Point Web Interface

To configure WDS access points by using the web interface:

-
- Step 1** Log in to an AP that will serve as a WDS device.
- Step 2** Select **Wireless Services > WDS**.
- Step 3** Select the Settings tab.
- Step 4** To enable WDS, select **Use this AP as Wireless Domain Services**.
- Step 5** Enter a value between 1 and 255 in the **Wireless Domain Services** priority field.
The priority value is used to determine which AP will be the active WDS AP when multiple APs are configured to run WDS. The highest priority is 255.
- Step 6** Configure the Wireless Network Manager (WNM) options:
- a. Select **Configure Wireless Network Manager**.
 - b. Enter the IP address of your WLSE in the **Wireless Network Manager IP Address** field.
 - c. Click **Apply**.
- Step 7** Define the AAA server(s) that will be used to LEAP authenticate infrastructure access points participating in SWAN:
- a. Select the Server Groups tab.
 - b. Enter a server group name.
 - c. From the **Priority** lists, select the appropriate AAA servers.
If no AAA servers have been entered into the AP, click **Define Servers** to add the servers, then select the appropriate servers. Consult the AP online help for assistance in entering AAA servers into the AP.
 - d. Under **Use Group For**, select **Infrastructure Authentication**.
- Step 8** The WDS takes over 802.1x authenticator responsibilities for all access points in the subnet that are registered and authenticated with the WDS. If you are using any EAP type for authentication, *you must define a separate server group for client authentication*. The server group for client authentication may contain the same servers defined in the group for infrastructure authentication.
- a. Select the Server Groups tab.
 - b. Enter a server group name.
 - c. From the **Priority** lists, select the appropriate AAA servers.

- d. Under **Use Group For**, select **Client Authentication**.
- e. Select the appropriate **Authentication Settings**.

See the access point documentation for more details on wireless client authentication through WDS.

Step 9 Configure the WDS AP to authenticate itself to the WDS so that it can participate in the SWAN hierarchy:

- a. Select **Wireless Services > AP**.
- b. Select **Enable**.
- c. Enter a username and password that can be LEAP authenticated by the AAA servers in the infrastructure server group.

Step 10 To commit the configuration, click **Apply**.

Using the Access Point CLI Interface



Tip

Consult the IOS and access point documentation for details on the subtleties of IOS commands.

The key steps in configuring the WDS are:

- Configure AAA servers to authenticate SWAN infrastructure access points and/or wireless clients.
- Configure WDS.
- Configure the WNM.

To configure the WDS access points using the IOS command line interface:

Step 1 Log in to an access point that will be a WDS device.

Step 2 Turn on AAA services:

```
aaa new-model
```

Step 3 Define the RADIUS servers that you will use for infrastructure authentication and/or client authentication. Consult your RADIUS server documentation for the correct port numbers. CiscoSecure ACS uses port 1645 for authorization and port 1646 for accounting.

```
radius-server host [ ip_address | hostname ] auth-port port
acct-port port key shared_secret_key
```

Step 4 Define a server group for infrastructure authentication:

```
aaa group server radius server_group_name server radius_server
```

Step 5 Define at least one additional server group for wireless client authentication.

Step 6 Configure the AP to run WDS:

```
wlccp wds priority priority interface BVI1
```

where *priority* is a value from 1 to 255. Priority determines which AP will be the active WDS AP when multiple APs are configured to run WDS. The highest priority is 255.

Step 7 Configure the Wireless Network Manager (WNM) component:

```
wlccp wnm ip address wlse_ip_address
```

where *wlse_ip_address* is the address of the WLSE.

Step 8 Configure the server group the WDS will use to LEAP authenticate SWAN infrastructure access points:

```
aaa authentication login named_authentication_list group
infrastructure_authentication_server_group_name
```

```
wlccp authentication-server infrastructure named_authentication_list
```

Step 9 The WDS takes over 802.1x authenticator responsibilities for all access points in the subnet that are registered and authenticated with the WDS. If you are using any EAP type for authentication, *you must configure another server group for client authentication*. The server group for client authentication may contain the same servers defined in the group for infrastructure authentication.

Use the following commands:

```
aaa authentication login named_authentication_list group
client_authentication_server_group_name
```

```
wlccp authentication-server client [ any | eap | leap | mac ]
named_authentication_list
```

Step 10 The WDS access point must also register and authenticate itself to the WDS to participate in the SWAN hierarchy, so the WDS AP is also an infrastructure AP. Configure the WDS access point as an infrastructure access point:

```
wlccp ap username username password password
```

Using a WLSE Configuration Template

You can use the WLSE to configure one or more WDS access points.

The major configuration steps are:

- Create a configuration template to set up AAA servers and the WDS.
- Apply the configuration template to the appropriate access points by running a configuration job.



Note

Your login determines whether you can use this option.

To configure WDS access points by using a WLSE configuration template:

- Step 1** Log in to the WLSE web interface.
- Step 2** Select **Configure > Templates**.
 - a. Enter a template name, selecting IOS as the template type.
 - b. Click **Create New**.
- Step 3** Enter the AAA servers that will be used to LEAP authenticate the infrastructure access points and the WLSE to the WDS, and the AAA servers that will be used to authenticate wireless client devices:
 - a. Select **Security > Server Manager**.
 - b. In the Corporate Servers section, for each server, enter the IP address, select RADIUS, and enter the shared secret.
 - c. Click **Save**.
- Step 4** Select **Wireless Services > WDS** to configure the WDS parameters.
In the Global Properties section:
 - a. Select **Enable**.
 - b. Enter the Wireless Domain Services priority. This value determines which access point will serve as the active WDS when multiple access points are configured to run WDS on the same subnet. Valid priority values are 1-255, with 255 being the highest.

- c. Enter the WLSE's IP address in the WNM IP Address field.

Step 5 Configure a server group for authenticating the SWAN infrastructure components.

In the Server Groups section:

- a. Enter one or more server names or server IP addresses.
- b. Under Use Group For, select Infrastructure Authentication.
- c. Click **Save**.

Step 6 The WDS takes over 802.1x authenticator responsibilities for all access points in the subnet that are registered and authenticated with the WDS. This means that if you are using any EAP type for authentication, *you must also define a separate server group for client authentication*.

The server group for client authentication may contain the same servers defined in the group for infrastructure authentication.

In the Server Groups section:

- a. Enter one or more server names or server IP addresses.
- b. Under Use Group For, select Client Authentication.
- c. Select the appropriate client Authentication Settings.
- d. Click **Save**.

Step 7 The WDS access point must also register and authenticate itself to the WDS to participate in the SWAN hierarchy, so the WDS AP is also an infrastructure AP. To authenticate and register the WDS AP as an infrastructure AP:

- a. Select **Wireless Services > AP Configuration**.
- b. Select **Enabled** as the Wireless Services option.
- c. Enter a username and password that can be LEAP authenticated by the AAA servers in the infrastructure server group.

Step 8 (Optional) Select **Preview** to see a preview of the configuration template.

Step 9 Select **Save**, then click the **Save** button.

Step 10 Select **Yes** to apply the template immediately or select **No** to save the template. For information on configuration jobs, see [Managing Jobs, page 4-267](#).

Configure Infrastructure Access Points

The infrastructure access points initiate participation in SWAN by registering and LEAP authenticating with the WDS.

The only required configuration for infrastructure access points is the username and password used to register with the WDS.

There are three ways to configure infrastructure access points:

- Using the access point web interface—See [Using the Web Interface to Configure Infrastructure APs](#), page 3-20.
- Using the access point CLI interface—See [Using the Command Line Interface to Configure Infrastructure APs](#), page 3-20.
- Using a WLSE configuration template—See [Using a WLSE Configuration Job to Configure Infrastructure APs](#), page 3-21.

Using the Web Interface to Configure Infrastructure APs

To use the web-based interface to configure infrastructure APs:

-
Step 1	Log in to the AP's web interface.
Step 2	Select Wireless Services > AP .
Step 3	Select Enabled .
Step 4	Enter the username and password for authenticating the infrastructure AP to the WDS.
Step 5	Click Apply .
-

Using the Command Line Interface to Configure Infrastructure APs

To use the command line interface to configure infrastructure APs:

-
Step 1	Log in to the AP's CLI.
Step 2	Enter the following command:
- ```
wlccp ap username username password password
```



where *username* and *password* are the credentials for authenticating the infrastructure access point to the WDS.

---

### Using a WLSE Configuration Job to Configure Infrastructure APs

The WLSE can be used to configure multiple infrastructure APs in a single job. To configure infrastructure APs using the WLSE, create a configuration template using the template creation wizard, then apply the template in a configuration job. For more information about using the template creation wizard and the configuration job interface, see [Chapter 5, “Using IOS Templates.”](#)



#### Note

Your login determines whether you can use this option.

---

To configure the username and password used to authenticate the AP to the WDS:

---

- Step 1** Log in to the WLSE web interface.
  - Step 2** Select **Configure > Templates**.
  - Step 3** Select **Wireless Services > AP Configuration**.
  - Step 4** Select **Enabled**.
  - Step 5** Enter the username and password for LEAP authenticating infrastructure APs to the WDS.
  - Step 6** Create a configuration job to apply the template to the appropriate devices. For information on configuration jobs, see [Managing Jobs, page 4-267](#).
- 

## Configuring the WLSE

The WLSE is the Wireless Network Manager (WNM) component of SWAN. The WLSE polls and aggregates radio management data from WDS devices and processes this data. The following configuration is required on the WLSE for radio management:

- SWAN components communicate via a Cisco proprietary technology called [WLCCP](#). You must enter the WLCCP username and password in the WLSE. This username and password is used to LEAP authenticate the WLSE to the WDS APs in the network. See [Enter WLCCP Credentials for Wireless Domain Services](#), page 3-36.
- Enter the SNMP read-only and read/write communities for all managed IOS access points. See [Enter SNMP Community Strings for All Devices](#), page 3-28.
- Enter Telnet/SSH credentials for IOS access points. See [Enter Telnet and SSH Usernames and Passwords—IOS Access Points](#), page 3-33.

## Confirming the Configuration

After the configuration is complete, there are two ways to confirm that they are correct and that the SWAN components are properly communicating:

- Using the Web interface—See [Using the Web-based Interface to Validate the Configuration](#), page 3-22.
- Using the command-line interface—See [Using the Command-Line Interface to Validate the Configuration](#), page 3-23.

## Using the Web-based Interface to Validate the Configuration

To confirm the configurations using the web-based interface on WDS APs:

**Step 1** Log in to the web interface on each WDS AP.

**Step 2** Select **Wireless Services > WDS > WDS Status**.

Check for the following:

- The WDS Information section should display the device WDS state as ACTIVE.
- The WDS Registration and AP Information sections should show the correct number of APs (all of the infrastructure APs and the WDS AP).
- The Mobile Node Information section should display the wireless clients participating in SWAN.

- The Wireless Network Manager section should contain the WLSE IP address. If the WLSE authentication status is SECURITY KEYS SETUP, the WLSE is properly registered.
- 

## Using the Command-Line Interface to Validate the Configuration

To use the CLI on the WDS APs to validate the configuration:

---

**Step 1** Log in to the CLI on each WDS AP.

**Step 2** To validate the WDS configuration, enter:

```
show wlcgp wds ap
```

This command lists all of the infrastructure APs and the WDS AP.

**Step 3** To verify that the WLSE is correctly registered, enter:

```
show wlcgp wnm status
```

This command should display the WLSE IP address. If the WLSE authentication status is SECURITY KEYS SETUP, the WLSE is properly registered.

---

## Set Up Routers and Switches


**Note**

Only routers and switches that have properly configured access points or bridges attached to them will be discovered.

On each router and switch, configure the following:

**Table 3-2 Setup Procedures for Routers and Switches**

| Task                                                                                           | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Notes                                                            |
|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| 1. Enable CDP and verify that access points and bridges are visible from the router or switch. | <ol style="list-style-type: none"> <li>1. In enable mode, verify that CDP is running on the device by using one of the following commands: <ul style="list-style-type: none"> <li>• On IOS-based devices—<b>show cdp run</b>.</li> <li>• On Hybrid OS-based Catalyst switches—<b>show cdp</b>.</li> </ul> </li> <li>2. If CDP is not running, in global configuration mode, enter <b>cdp run</b> to enable CDP.</li> <li>3. To verify that access points or bridges are visible in the device's CDP table, enter <b>show cdp neighbors</b>.</li> </ol> | CDP is required for the WLSE to discover the device.             |
| 2. Enable SNMP and set up community strings.                                                   | <p>On IOS-based devices, enter configuration mode and use the <b>snmp community community_string ro</b> command.</p> <p>On Hybrid OS-based Catalyst devices, enter enable mode and use the <b>set snmp community read-only community_string</b> command.</p>                                                                                                                                                                                                                                                                                           | SNMP is required for the WLSE to discover and manage the device. |

**Table 3-2 Setup Procedures for Routers and Switches (continued)**

| Task                                                                | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Notes                                                                                                                                                   |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3. (Optional) Set the system name, contact, and location variables. | <p>On IOS-based devices, enter configuration mode and use the following commands.</p> <ul style="list-style-type: none"> <li>Set system name—<b>hostname</b> <i>name</i></li> <li>Set system contact—<b>snmp contact</b> <i>contact</i></li> <li>Set location—<b>snmp location</b> <i>location</i></li> </ul> <p>On Hybrid OS-based Catalyst switches, enter enable mode and use the following commands:</p> <ul style="list-style-type: none"> <li>Set system name—<b>set system name</b> <i>name</i> command.</li> <li>Set system contact—<b>set system contact</b> <i>contact</i></li> <li>Set location—<b>set system location</b> <i>location</i></li> </ul> | <p>These variables make the device more manageable.</p> <p>The system name, system contact, and location will appear in the device detail displays.</p> |

## Set Up AAA Servers

The WLSE can monitor the performance of [AAA](#) (Authentication, Authorization, and Accounting) services provided by CiscoSecure ACS server. The WLSE can also monitor a Cisco Access Registrar (CAR) RADIUS server. The services supported are LEAP, RADIUS, EAP-MD5, and PEAP (EAP-GTC only).

To enable monitoring, you must:

- Configure CiscoSecure ACS server to recognize the WLSE as a client. Follow the procedure in this section on each server.



### Note

For PEAP, besides the procedure in this section, you must set up a certificate and private key on the ACS server and then enable PEAP. For more information, see the CiscoSecure ACS documentation.

- Configure the WLSE to add information about servers. For more information, see [Managing AAA Servers, page 3-37](#).

In addition to monitoring AAA servers, the WLSE uses an AAA server to authenticate to a Wireless Domain Services (WDS) access point. To enable this authentication, make sure an AAA server is configured as described in this section. You must also configure the WDS access point and the WLSE. For more information, see [Enter WLCCP Credentials for Wireless Domain Services, page 3-36](#).

### Procedure

**Step 1** Log into the CiscoSecure ACS Server that will provide authentication services to the wireless network.



**Note** You will need the IP address or name of the system on which CiscoSecure ACS Server is running when you configure the WLSE.

**Step 2** Click **User Setup** on the left side of the initial page.

**Step 3** Enter a username for the user the WLSE will use for synthetic transactions and click **Add/Edit**.

**Step 4** Enter a password in the first set of Password and Confirm Password fields. Click **Submit**.



**Note** You will need this name and password when configuring the WLSE.

**Step 5** Click **Network Configuration** on the left side of the page.

**Step 6** Click **Add Entry**. In the Add AAA Client area, enter the WLSE information in the following text boxes:

- Client Hostname—enter the WLSE hostname (or IP address)
- Client IP—enter the WLSE IP address
- Key—enter a secret key



**Note** You will need this key when configuring the WLSE.

**Step 7** Select RADIUS (Cisco Aironet) from the Authenticate Using list.

- Step 8** Click **Submit** or **Submit+Restart**. A restart is required for the changes to take effect.
- 

## Specifying Device Credentials

Before the WLSE device discovery or device polling can successfully communicate with the network devices, the WLSE must be aware of the appropriate device SNMP credentials to use.

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

- For all managed devices, you must enter SNMP credentials.
- For access points, the following additional credentials are required:
  - For IOS-based access points, you must enter Telnet or SSH credentials and IOS HTTP port settings.
  - For non-IOS access points, you must enter HTTP credentials.
- If you are using Wireless Domain Services (WDS), you must enter RADIUS credentials and configure the WDS access point.

The Device Credentials options are:

- **SNMP Communities**—Specify community strings for managed devices. Using this option, you can specify device [community strings](#), other required device credentials, and ports. Community strings are required for discovery, and community strings and other credentials are required for other WLSE functions. See [Enter SNMP Community Strings for All Devices](#), page 3-28.
- **HTTP User/Password**—Specify the HTTP usernames and passwords for configuring non-IOS access points. See [Enter HTTP Usernames and Passwords—Non-IOS Access Points](#), page 3-32.
- **Telnet/SSH User/Password**—Specify the Telnet usernames and passwords for IOS access points. See [Enter Telnet and SSH Usernames and Passwords—IOS Access Points](#), page 3-33.
- **IOS HTTP Port Settings**—Specify the HTTP ports for IOS access points. See [Enter HTTP Port Settings—IOS Access Points](#), page 3-35.

- **WLCCP Credentials**—Specify the RADIUS credentials for Wireless Domain Service (WDS). See [Enter WLCCP Credentials for Wireless Domain Services](#), page 3-36.

## Enter SNMP Community Strings for All Devices

The Wireless LAN Solution Engine uses a device's read-only [SNMP](#) community string to discover the device and populate reports and uses the read/write community string to configure the device and update firmware. 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 is *public* for both the read-only string and the read-write string. If the community strings on your devices differ from the defaults, you must specify the community strings on the WLSE before the discovery process can begin and before you can configure the devices.

If you are importing devices from a file or CiscoWorks, 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 3-59 and [Importing Devices from a CiscoWorks Server](#), page 3-61.

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 3-54.



### Note

---

Your login determines whether you can use this option.

---

### Procedure

- 
- Step 1** Select **Devices > Discover > Device Credentials > SNMP Communities**. The SNMP Communities dialog box contains a default entry that covers all devices, provided device community strings are set to the default (*public*).



**Step 2** To add community strings, use either of the following methods to enter the community strings you created during initial device setup. For more information, see [Setting Up Devices, page 3-5](#).

- Use the individual text boxes and list for the variables: Hostname (IP address), Read Community, SNMP Timeout, SNMP Retries, and Write Community. Then click **Add**. The community string appears in the large text box.
- Enter the data directly in the large text box. Use the following syntax:

```
target:read_community::timeout:retries:::write_community
```

**Note**

You must enter the correct number of colons between variables. Otherwise, the community strings cannot be read.

[Table 3-3](#) describes the community string variables.

**Table 3-3 Community String Variables**

| Variable       | Description                                                                                                     | Notes                                                                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| target         | The IP address of a device or range of devices that use these community strings.                                | If you do not specify a target, the default community strings apply to all devices in the network.                                                                          |
| read_community | A password allowing read-only access to the target devices.                                                     | You must specify the read community string. Otherwise, the default value of <i>public</i> is used.                                                                          |
| timeout        | The 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 value is one and the maximum value is 60. |

**Table 3-3 Community String Variables (continued)**

| Variable        | Description                                                                                                        | Notes                                                                                                                                                                                     |
|-----------------|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 | The password that allows write access to the target devices.                                                       | You must specify the write community string. Otherwise, the default value of <i>public</i> is used.                                                                                       |

**Step 3** To modify a community string, make your changes directly in the large text box.

**Step 4** Click **Save** to apply your changes.

---

#### Related Topics

- [Community String Guidelines, page 3-30](#)
- [Recommendations For Configuring SNMP Credentials, page 3-31](#)

## Community String Guidelines

Use these guidelines when adding or modifying community strings:

- You can assign community strings to any of the following:
  - Complete IP address; for example, 172.20.4.9
  - Any wild cards (based on IP addresses); for example:  
 \*.\*.\*.\*.  
 172.\*.\*.\*
  - Address ranges, which can include wild cards; for example:  
 27.20.[4-55].\*  
 172.[21-30].[44-88].\*  
 172.\*.\*.[121-255]

- You can add a combination of general and specific entries, but the WLSE reads the community strings from most specific to least specific.
- If you enter duplicate community strings for a device, the most specific community string is used.
- All printable characters, except for colons (:), are allowed in community strings.
- Spaces are not allowed in community strings.
- Comments are not allowed.

## Recommendations For Configuring SNMP Credentials

This section contains information about setting the SNMP credentials on the WLSE.

### Community Strings

When there are multiple potential entries, the WLSE will use the most specific SNMP community entry for a device IP. In the case of equally specific entries, the WLSE will select the first entry in the list, which may not be the correct community.

### SNMP Timeouts and Retries

Exercise 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. To do this:

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 8-36](#)) 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 Guidelines, page 3-30](#)

## Enter HTTP Usernames and Passwords—Non-IOS Access Points

[HTTP](#) usernames and passwords are required for downloading configuration files to non-[IOS](#) access points. The password must be set on each access point, and you can enter as many usernames and passwords as necessary on the WLSE. For more information about setting passwords on access points, see [Setting Up Devices, page 3-5](#).



#### Note

---

Your login determines whether you can use this option.

---

#### Procedure

---

- Step 1** Select **Devices > Discover > Device Credentials > HTTP User/Password**.
- Step 2** To add a username and password:
- a. Enter the access point IP address or range of IP addresses that will use this username and password.

For information on using ranges and wildcards in IP addresses, click **Learn More** or see [Entering IP Addresses, page 3-35](#).

- b. Enter the username.
- c. Enter the password.
- d. Click **Save**. The IP address and username are added to the Current Entries text box.

**Step 3** To modify an entry:

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

**Step 4** To delete an entry, select it from the Current Entries text box and click **Delete**.

---

#### Related Topics

[Chapter 4, “Configuring Devices”](#)

## Enter Telnet and SSH Usernames and Passwords—IOS Access Points

Telnet or SSH (SSH1 only) usernames and passwords are required for applying configuration templates to IOS access points and for upgrading firmware on IOS 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 [Setting Up Devices, page 3-5](#).

The Telnet/SSH credentials you enter in this dialog must match the login sequence on the IOS access points. For example, if the device prompts for an enable password only, enter the Enable Password only. Do not enter a User Name or User Password. Otherwise the WLSE will not be able to open a login session on the device.



#### Note

Your login determines whether you can use this option.

### Procedure

**Step 1** Select **Devices > Discover > Device Credentials > Telnet/SSH User/Password**.

**Step 2** 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 <a href="#">Entering IP Addresses, page 3-35</a> . |
| Username                | Telnet username.<br><br><b>Note</b> If the device is configured for a Telnet password only, enter a user password but leave the Username field blank.                                                      |
| User Password           | Telnet password.                                                                                                                                                                                           |
| Confirm Password        |                                                                                                                                                                                                            |
| Enable Password         | Telnet 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**.

### Related Topics

[Chapter 4, “Configuring Devices”](#)

## 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 Port Settings—IOS Access Points

HTTP port settings are required for reports on IOS 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.



#### Note

For non-IOS access points, there is no need to specify HTTP ports. Port information is collected during inventory.

### Procedure

- Step 1** Select **Devices > Discover > Device Credentials > IOS HTTP Port Settings**.

- Step 2** To add a port:
- 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 3-35](#).
  - Enter the port number.
  - 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 configure an AAA server, enter [WLCCP](#) credentials on the WLSE, and configure the WDS access point. The steps in setting up WDS on the network are:

- [1. Configure an AAA Server, page 3-36](#)
- [2. Configure the WLSE, page 3-36](#)
- [3. Configure the WDS Access Points, page 3-37](#)

### 1. Configure an AAA Server

Use an AAA server that you have already configured, or configure a server as described in [Set Up AAA Servers, page 3-25](#).

### 2. Configure the WLSE

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 that you set for the WLSE on the AAA server.
- Step 3** To modify the WLCCP credentials, modify the fields as needed.
- Step 4** To save the credentials, click **Save**.



To clear all fields and remove the WLCCP credentials, click **Clear Fields**.

---

### 3. Configure the WDS Access Points

WDS is currently supported on two types of IOS-based access points: Cisco Aironet 1100 and Cisco Aironet 1200. The WDS access points must be managed by the WLSE.

To configure an access point to provide WDS:

---

**Step 1** Log in to the access point's CLI interface.

**Step 2** In configure mode, enter the following command:

```
wlccp wnm ip address x.x.x.x
```

where *x.x.x.x* is the WLSE's IP address.

**Step 3** In enable mode, verify that authentication is working by entering the following command:

```
show wlccp wnm status
```

If the command returns a status of SECURITY KEYS SETUP, the WLSE has authenticated successfully with the WDS.

---

#### Related Topics

[Viewing the WDS Summary Report, page 6-4](#)

## Managing AAA Servers

The options in this screen allow you to:

- Add AAA servers—See [Adding an AAA Server, page 3-39](#).
- Remove AAA servers—See [Removing an AAA Server, page 3-40](#).
- Edit AAA server entries—See [Modifying an AAA Server, page 3-40](#).

**Note**

Before the WLSE can monitor your AAA servers, you must configure the servers to add the WLSE as a client. For information on adding the WLSE as a client on AAA servers, see [Set Up AAA Servers, page 3-25](#).

**Related Topics**

- [About AAA Servers, page 3-38](#)
- [Set Up AAA Servers, page 3-25](#)

## About AAA Servers

Before adding Authentication, Authorization, and Accounting (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 AAA servers, see [Set Up AAA Servers, page 3-25](#).

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**. The WLSE can monitor AAA services provided by Cisco Secure ACS.

If you are using Wireless Domain Services (WDS), you will also use an AAA server to allow the WLSE to authenticate with the WDS access point. For more information, see [Enter WLCCP Credentials for Wireless Domain Services, page 3-36](#).

- The services supported by the WLSE are
- EAP-MD5
- LEAP
- PEAP (EAP-GTC only)
- RADIUS

For information about changing the polling interval and response time fault thresholds for AAA server monitoring, see [Specifying Fault Thresholds, page 2-37](#).

## Adding an AAA Server

**Note**

Before the WLSE can monitor your AAA servers, you must configure the servers to add the WLSE as a client. For information on adding the WLSE as a client on AAA servers, see [Set Up AAA Servers, page 3-25](#).

**Procedure**

**Step 1** Select **Devices > Discover > AAA Server**.

**Step 2** Enter the following data:

| Field       | Description                                                                                                                                                        |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Show List   | Select server type from the pulldown list: <ul style="list-style-type: none"><li>• EAP-MD5</li><li>• LEAP</li><li>• PEAP (EAP-GTC only)</li><li>• RADIUS</li></ul> |
| Server Name | Hostname or IP address of the AAA server.                                                                                                                          |
| Server Port | Port on the server that is used for authentication; this should always be 1645.                                                                                    |
| Username    | Client username that you entered on the LEAP server.                                                                                                               |
| Password    | Client password that you entered on the LEAP server.                                                                                                               |
| Secret      | Shared secret key that you entered on the LEAP server.                                                                                                             |

**Step 3** Click **Save**.

**Step 4** To discard your entries, click **Cancel**.

## Removing an AAA Server

### Procedure

- 
- Step 1** Select **Devices > Discover > AAA Server**.
- Step 2** Select the server type from Show List; all servers of that type are displayed.
- Step 3** Select the server to be removed.
- Step 4** Click **Remove**.
- 

## Modifying an AAA Server

### Procedure

- 
- Step 1** Select **Devices > Discover > AAA Server**.
- Step 2** Select the server type from Show List; all servers of that type are displayed.
- Step 3** Select the server to be modified.
- Step 4** Modify any of the following characteristics of the server:

| Field       | 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 LEAP server.                            |
| Password    | Client password that you entered on the LEAP server.                            |
| Secret      | Shared secret key that you entered on the LEAP server.                          |

- Step 5** Click **Save**.
- Step 6** To discard your entries, click **Cancel**.
-

# Managing Device Discovery

By default, the WLSE runs Cisco Discovery Protocol (CDP) discovery every 24 hours. You can use the options under **Devices > Discover > DISCOVER** to:

- Run additional CDP discoveries and modify the default schedule.
  - For more information, see [About Discovery, page 3-41](#).
  - To run CDP discoveries, see [Using the Discovery Wizard, page 3-54](#).
- Discover devices by importing them from a file or from a CiscoWorks server.
  - For more information, see [About Discovery, page 3-41](#).
  - To run device imports, see [Using the Discovery Wizard, page 3-54](#).

**Note**

After devices are discovered, they must be put under management—see [Managing and Unmanaging Devices, page 3-76](#). Unmanaged devices do not appear in WLSE displays.

- Set advanced options that modify the behavior of discovery and device management—See [Setting Advanced Options, page 3-63](#).
- Set up IP address filtering for discovery—See [Using Discovery IP Address Filtering, page 3-68](#).
- View discovery job details—See [Viewing Discovery Logs, page 3-69](#).

## About Discovery

The topics covered in this section are:

- [Understanding Discovery and Management, page 3-42](#)
- [Understanding WLSE Discovery Methods, page 3-43](#)
- [About CDP-Based Discovery, page 3-44](#)
- [About Individual Device Seeding, page 3-46](#)
- [About Device Import From a File, page 3-47](#)
- [About Device Import From CiscoWorks, page 3-51](#)
- [About CSV Files, page 3-49](#)

## Understanding Discovery and Management

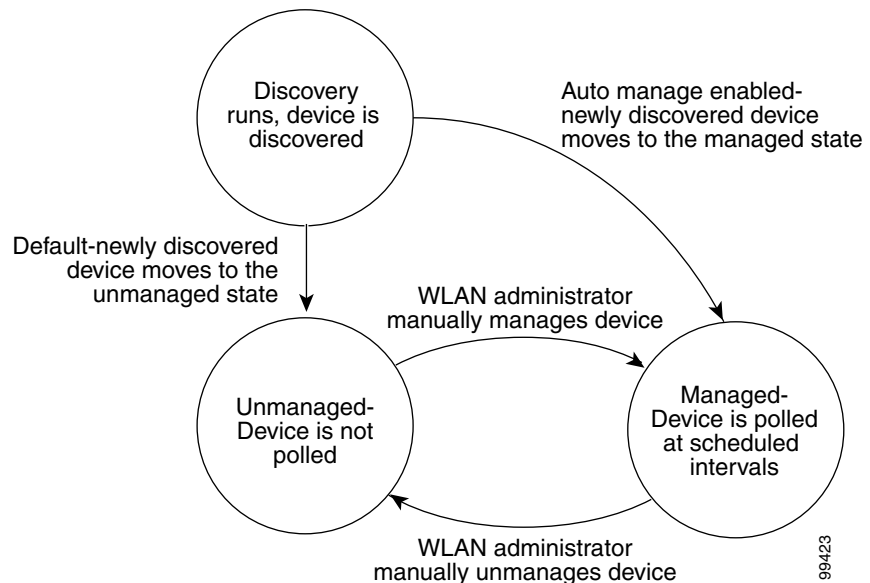
Network devices are interrogated by the WLSE by multiple processes: discovery and inventory polling.

Device discovery is a periodic process that finds new devices and possibly topology and network changes. The WLSE can discover Cisco wireless access points and bridges, and Cisco switches or routers that have Cisco wireless devices attached to them. The discovery process can be run at scheduled intervals or on-demand.

Discovered devices can exist in one of two states: managed and unmanaged. By default, newly-discovered devices are in the unmanaged state and will not be polled until manually moved 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 3-1](#) illustrates the managed/unmanaged state machine.

**Figure 3-1 Device Management 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.

## Understanding WLSE Discovery Methods

Before the WLSE can manage devices, it must discover them. There are several discovery techniques:

- CDP-based discovery
- Individual device seeding
- Device import from a file
- Device import from CiscoWorks Resource Manager Essentials (RME)

Use the following table to help you decide which technique to use:



**Note** AAA servers must be input individually regardless of discovery method. See [About AAA Servers, page 3-38](#).

**Table 3-4** *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 <a href="#">About CDP-Based Discovery, page 3-44</a> . |

**Table 3-4** *Discovery Options (continued)*

| Discovery Method                                                | Use This Method When...                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Individual device seeding                                       | <p>If the wireless devices are connected to switches or routers that don't run CDP (for example, non-Cisco switches), this is one option.</p> <p><b>Note</b> This method forces the user to input each device IP address, so it may not scale.</p> <p>For more information, see <a href="#">About Individual Device Seeding, page 3-46</a>.</p>                                                                   |
| Device import from a file                                       | <p>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.</p> <p><b>Note</b> Using this method, you might need to create a large CSV file listing each device.</p> <p>For more information, see <a href="#">About Device Import From a File, page 3-47</a>.</p> |
| Device import from CiscoWorks Resource Manager Essentials (RME) | <p>Use this technique if you have already inventoried the wireless devices using RME. This technique adds an entry for each device for SNMP credentials.</p> <p>For more information, see <a href="#">About Device Import From CiscoWorks, page 3-51</a>.</p>                                                                                                                                                     |

## 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.

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.



---

**Note** To configure a scheduled or recurring CDP-based discovery process, or to run a CDP-based discovery on-demand, see [Using the Discovery Wizard, page 3-54](#).

---

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
- Change the default CDP schedule

Devices must be properly configured for access by the WLSE before they can be discovered and managed (see [Setting Up Devices, page 3-5](#)).

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 3-46](#).

## 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 3-46](#)
- [About Device Import From a File, page 3-47](#)
- [About Device Import From CiscoWorks, page 3-51](#)

## 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 or the scheduled discovery options 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 Options, page 3-63](#).
- IP Filter Rules—See [Using Discovery IP Address Filtering, page 3-68](#).

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.

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 3-56](#)) for each device during the import process. The WLSE will do this even if there are already entries that qualify for the devices configured.

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 3-69](#)), the name of the import from file is shown as CDPDiscovery\_Import\_Devices\_ *number*.

### 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 also 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.
;
```

## Managing Device Discovery

```

; 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 > 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 Options, page 3-63](#).
- IP Filter Rules—See [Using Discovery IP Address Filtering, page 3-68](#).

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:
  - **RMEDiscovery**—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\_***number*—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.



## Pre-Discovery Checklist

The following checklist will help you confirm that the prerequisites for successful discovery have been met.



**Note** This list is only the requirements for successful device discovery. To use other WLSE features, other configuration requirements exist. For details about how to configure the specific device parameters, see [Chapter 4, Configuring Devices](#).

- CDP enabled on network devices (for CDP-based discovery).
- SNMP communities configured on network devices.
  - Read-only SNMP community on switches and routers.
  - Correct access capabilities for SNMP communities on non-IOS-based wireless access points and bridges.
  - Read-only SNMP community strings configured for IOS-based wireless access points.
- SNMP communities entered into WLSE device credentials fields.
- WLSE configured as network access server (NAS) for CiscoSecure Access Control Server (ACS) (for RADIUS, LEAP, EAP-MD5 server monitoring) or equivalent in other AAA servers.
- WLSE synthetic transaction user created on AAA server.

## 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 3-54](#). The discovery methods are:

- CDP discovery—see [Running CDP Discovery, page 3-54](#)
- Device import from a file—see [Importing Devices from a File, page 3-59](#)
- Device import from a CiscoWorks server [Importing Devices from a CiscoWorks Server, page 3-61](#)

## Using the Discovery Wizard

The discovery wizard provides the following choices for discovering devices.

### Procedure

**Step 1** Select a discovery option:

| Option                        | Description                                                                                      | Reference Information                      |
|-------------------------------|--------------------------------------------------------------------------------------------------|--------------------------------------------|
| <b>CDP Discovery</b>          | Runs immediate or scheduled discovery by using Cisco Discovery Protocol (CDP).                   | <a href="#">About Discovery, page 3-41</a> |
| <b>Import from File</b>       | Imports devices from a file.                                                                     |                                            |
| <b>Import from CiscoWorks</b> | Runs immediate or scheduled imports from a CiscoWorks server (uses Resource Manager Essentials). |                                            |

**Step 2** 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 > CDP Discovery**.

The tasks for running CDP discovery are:

**Table 3-5 Tasks for CDP Discovery**

| Type Discovery  | Task                                    | Reference                                                  |
|-----------------|-----------------------------------------|------------------------------------------------------------|
| Run Now         | Select Run Now.                         | Select the Type of CDP Discovery, page 3-55                |
|                 | Specify SNMP communities                | Enter SNMP Communities, page 3-56                          |
|                 | Specify initiating IP addresses (seeds) | Enter Initiating IP Addresses, page 3-57                   |
|                 | Verify your settings and finish         | Verify Your Settings and Finish—Run Now, page 3-58         |
|                 | View discovery run details              |                                                            |
| Modify Schedule | Select Modify Schedule                  | Select the Type of CDP Discovery, page 3-55                |
|                 | Modify the schedule                     | Specify the Schedule, page 3-56                            |
|                 | Specify SNMP communities                | Enter SNMP Communities, page 3-56                          |
|                 | Specify initiating IP addresses (seeds) | Enter Initiating IP Addresses, page 3-57                   |
|                 | Verify your settings and finish         | Verify Your Settings and Finish—Modify Schedule, page 3-58 |
|                 | 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 3-44](#)

## 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**.

You can also find details on entering community strings and the community string requirements for discovery in [Enter SNMP Community Strings for All Devices, page 3-28](#).

**Step 4** Click **Next**.

## Enter Initiating IP Addresses

You must enter at least one initiating IP address (seed device).

### Procedure

**Step 1** Add seed devices by entering comma-separated IP addresses or device names 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.

Device names must resolve to your local [DNS](#) in order to translate device names to IP addresses during discovery. The requirements for entering 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 (-), and the period (.).
- The last character cannot be a minus or a period.

- 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**.
- 

## Verify Your Settings and Finish—Run Now

### 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 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 3-69](#).
- 

### Related Topics

[Viewing Discovery Logs, page 3-69](#)

## 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.
- 

### Related Topics

[Viewing Discovery Logs, page 3-69](#)

## 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**.

The tasks for importing devices from a file are:

**Table 3-6** *Tasks for Import from File*

| Task                                                           | Reference                                                          |
|----------------------------------------------------------------|--------------------------------------------------------------------|
| Specify the file and set the SNMP retry and timeout (optional) | <a href="#">Select the File and Set SNMP Parameters, page 3-59</a> |
| Verify your settings and finish                                | <a href="#">Finish the Import, page 3-60</a>                       |
| 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 3-49](#).

### 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 3-69](#)



## 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 3-7** *Tasks for Import from CiscoWorks*

| Task                          | Description                                               |
|-------------------------------|-----------------------------------------------------------|
| Specify the CiscoWorks server | <a href="#">Schedule the Import and Finish, page 3-61</a> |
| 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. For more information about importing devices from a CiscoWorks server, see [About Device Import From CiscoWorks, page 3-51](#).

#### 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             | The CiscoWorks server IP address.                                                                                                                                        |
| Port             | The 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             | The username and password of any user who has the authority to export and import device credentials on the CiscoWorks server.                                            |
| Password         |                                                                                                                                                                          |
| Confirm Password |                                                                                                                                                                          |

**Step 2** To run a one-time import:

- a. Select **Run Now**.
- b. Click **Finish**. The import will begin immediately.

**Step 3** To schedule a one-time import or repeated imports:

- a. Select the start date from the Start Date pulldown lists.
- b. Enter the start time from the Start Time pulldown lists.
- c. If you want 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.
- d. Click **Finish**. A one-time import will begin immediately.

**Step 4** To view the status of the last import from CiscoWorks, click **Check Last Status**. Details on the latest import (if any) are shown. Click **Refresh** to update the display. You might see the following error messages:

**Table 3-8 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 3-69](#)

## Setting Advanced Options

This window provides the following options for discovery and device management:

- Reverse DNS lookup—See [Enable Reverse DNS Lookup, page 3-64](#).
- Automatic management of newly discovered devices—See [Enable Auto-Management, page 3-65](#).
- Filtering for time-based access point management—See [Enable MAC Address Auto-Manage Filtering for Access Points, page 3-65](#).

**Note**

Your login determines whether you can use these options.

## Enable Reverse DNS Lookup

Enabling reverse DNS lookup affects hostname (device name) display on the WLSE as follows:

| 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. |
|                             | If the sysName is not set, the device IP address is displayed. |



### 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

[Understanding WLSE Discovery Methods, page 3-43](#)

## Enable Auto-Management

Enabling this option causes all discovered devices to be automatically managed.

### 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 4-300](#).

---

**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 3-65](#).

**Step 4** Click **Save** to save all of your settings in the Advanced Options screen.

---

### Related Topics

- [Understanding WLSE Discovery Methods, page 3-43](#)
- [Managing and Unmanaging Devices, page 3-76](#)

## 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.

Auto-management affects all discovered devices. Access point filtering affects only access points. See the following table for details on how these two options affect each other.

**Table 3-9 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                     | <p>Only access points listed in <b>Access Points to Auto-Manage</b> will be auto-managed and they will be auto-managed only during the specified interval.</p> <p><b>Note</b> If the time interval expires, newly discovered access points will not be auto-managed. Any access points that you have manually placed in the Managed folder will still be managed.</p> |

You can specify the access points to 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 3-67.

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.

- b. 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.
    - c. Repeat Step b to add more addresses.
  - Step 6** To import a list of Ethernet MAC addresses from a file:
    - a. Create an ASCII file consisting of one address per line or a comma-separated list (.txt file). For sample files, see [Example MAC Address Files, page 3-67](#).
    - b. Enter the path to the file in the **Import From File** text box or click **Browse** to find the file.
    - c. 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.


**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 the following table.


**Note**

Exclude rules take precedence over include rules.

**Table 3-10 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. |



**Table 3-10 Effects of Include and Exclude Rules in Discovery Filters**

| Include Rules Defined? | Exclude Rules Defined? | Result                                                                                                        |
|------------------------|------------------------|---------------------------------------------------------------------------------------------------------------|
| 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 3-43](#)

## Viewing Discovery Logs

This option displays details on the results of discoveries and imports.

### Procedure

**Step 1** Select **Devices > Discover > DISCOVER > Logs**.

A list of the last 15 jobs is displayed.

**Step 2** To filter the list of jobs, select All, Running, or Scheduled from the Discovery Job State list.

**Step 3** The names of the jobs indicate the type of discovery that was run, as explained in the following table:

**Table 3-11 Discovery Job Names**

| Folder Name | Discovery Name                             | Discovery Type                                   |
|-------------|--------------------------------------------|--------------------------------------------------|
| Scheduled   | CDPDiscovery                               | Scheduled discoveries                            |
| Run Now     | CDPDiscovery_Run_Now_ <i>number</i>        | On-demand discoveries                            |
| Import      | CDPDiscovery_Import_Devices_ <i>number</i> | Imported from a file or from a CiscoWorks server |
|             | RMEDiscovery                               | Imported from a CiscoWorks server <sup>1</sup>   |

1. Two items are listed in the discovery log for each import from a CiscoWorks server: CDPDiscovery\_Import\_Devices\_*number* and RMEDiscovery.

**Step 4** 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 3-71](#).

If the log files show that problems occurred while running discovery, see [Diagnosing Common Discovery Problems, page 3-74](#).

**Step 5** To refresh the display, click **Refresh**.

## Discovery Run Details Display

A typical, healthy discovery process 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 Inventories, page 3-80](#).

The following messages may appear in the Discovery Run Details display.

**Table 3-12 Error Messages—Discovery Run Log**

| Message                                                                                                 | Meaning                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No seeds defined.                                                                                       | Although discovery is initially enabled and runs every 24 hours, it will not run unless you add seed devices. See <a href="#">Using the Discovery Wizard, page 3-54</a> .                                                                                                                                                                                                                                 |
| Device being updated                                                                                    | The device was previously discovered and information is being updated.                                                                                                                                                                                                                                                                                                                                    |
| Inventory collection does not run for updated devices, run on-demand or wait for the next polling cycle | 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.                                                                                                                                                                                                                                      |
| New device discovered.                                                                                  | The device was discovered for the first time.                                                                                                                                                                                                                                                                                                                                                             |
| Inventory collection will run immediately for auto-managed devices.                                     | Auto-management is enabled; therefore, inventory collection will run immediately for the auto-managed devices.                                                                                                                                                                                                                                                                                            |
| x.x.x.x is SNMP unreachable, unable to read CDP cache.                                                  | <p>The community strings may be set up incorrectly. See <a href="#">Setting Up Devices, page 3-5</a>.</p> <p>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.</p> <p>For more information on troubleshooting SNMP problems, see <a href="#">Diagnosing Common Discovery Problems, page 3-74</a>.</p> |
| 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.                                                                                                                                                                                                                                                                             |

**Table 3-12 Error Messages—Discovery Run Log (continued)**

| Message                                                                                                                                                                                                                                                                                    | Meaning                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>x.x.x.x</code> does not respond to <code>ieee802.11</code> attributes.                                                                                                                                                                                                               | Make sure the SNMP community has a proper view associated.<br><br>The IOS access point has not been configured with an IOS view. To correct this, you can configure the device manually (see <a href="#">Set Up IOS Access Points, page 3-8</a> ) or create a configuration job to correct it (see <a href="#">Managing Configuration Jobs, page 4-267</a> ). Affected devices are placed in the Misconfigured Devices system group. After the device is properly configured, you can run discovery or wait for the next scheduled discovery. After discovery, the device will be placed in the proper group(s). See <a href="#">Managing Device Discovery, page 3-41</a> . |
| IP conflict for <code>ip_address</code> ( <code>hostname</code> ). Identifier or ethernet MAC is <code>identifier</code> or <code>MAC address</code> . 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.<br><br>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 <a href="#">Managing Device Discovery, page 3-41</a> .         |
| Unable to auto-manage device: <code>x.x.x.x</code> 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 <a href="#">Enable MAC Address Auto-Manage Filtering for Access Points, page 3-65</a> .                                                                                                                                                                                                                                                                                                                                                                                                    |
| <code>172.19.12.39,public,private,14,1.3.6.1.4.1.9.1.507,!{[NOVALUE]}</code> ,...                                                                                                                                                                                                          | Messages similar to this are informational and show data obtained during device import from CiscoWorks:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

**Related Topics**

- [Running CDP Discovery, page 3-54](#)
- [Diagnosing Common Discovery Problems, page 3-74](#)

## Diagnosing Common Discovery Problems

This section contains information on:

- [Troubleshooting SNMP Connectivity Problems, page 3-74](#)
- [Obtaining Detailed Discovery Logs, page 3-76](#)

### 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 8-36](#)). 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 a -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 TAC web-site at <http://www.cisco.com/tac> for more information.

---

2. After IP connectivity has been confirmed, use the SNMP Connectivity Tool (see [Using Network Tools, page 8-36](#)) 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 3-31](#).

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 8-37](#)) 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](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](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 and Unmanaging Devices

Discovered devices can exist in one of two states: managed and unmanaged. By default, newly-discovered devices are in the unmanaged state and will not be polled until manually moved to the managed state.

The Manage/Unmanage window provides a view of newly discovered devices, managed devices, and unmanaged devices, allows you to manually change the management status of devices, and provides details about all devices. You can also delete devices from this window. Devices must be placed under management before you can use the WLSE to monitor and configure them.





**Note** There is a limitation on the number of access points and bridges that can be managed by a single Wireless LAN Solution Engine. For more information, see [Limitation on the Number of Managed Devices, page 3-79](#).

- To manually place devices under management or unmanage them, use the following procedure.
- To delete devices, see the following procedure.
- To arrange for devices to be automatically managed, see [Setting Advanced Options, page 3-63](#).
- To filter access point auto-management, see [Setting Advanced Options, page 3-63](#).



**Note** Your login determines whether you can use this option.

### Procedure

- Step 1** Select **Devices > Discover > Managed Devices > Manage/Unmanage**. The following folders are displayed:
- Newly discovered devices (New folder).
  - Managed devices (Managed folder)
  - Unmanaged devices (Unmanaged folder).
- Step 2** To modify the status of devices in a folder:
- a. Click the folder name. You can search for devices; for information on how to search, see [Using the Device Selector and Search, page 1-9](#).
  - b. Select the devices you want to change.
  - c. To manage devices, click **Manage**. Devices will be moved into the Managed folders.
    - Only managed devices appear in WLSE displays.

- After you move devices to the managed state, an immediate inventory is run for those devices. This ensures that device attributes appear in displays, such as reports and system-defined groups without waiting for the next scheduled inventory.
- d. To unmanage devices, click **Unmanage**. Devices will be moved into the Unmanaged folder.
- e. To delete devices, click **Delete**.

**Step 3** To view details about an individual device or modify its status, select the device from the device selector. You can search for devices; for information about searching, see [Using the Device Selector and Search, page 1-9](#).

- For information on the device details displayed, see [Understanding Device Details, page 3-79](#).



**Note**

---

Some details are not displayed unless the corresponding parameters are set on the device; for example, location and contact information.

---

- To change a device's status:
    - To manage a device, click **Manage**.
    - To unmanage, click **Unmanage**.
    - To delete a device, click **Delete**.
- 

### Related Topics

- [Managing Device Discovery, page 3-41](#)
- [Device Name and IP Address Display, page 1-8](#)

## Understanding Device Details

The details shown in the Device Details panel are:

**Table 3-13 Device Details Pane**

| Field           | Description                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------|
| Device Name     | Hostname, IP address, or SNMP sysname.                                                       |
| State           | Whether the device is new, managed, or unmanaged.                                            |
| Description     | Detailed device description.                                                                 |
| Version         | Software version installed on the device.                                                    |
| Device Family   | Device type.                                                                                 |
| SysName         | The system name.                                                                             |
| SysObjectId     | Unique identifier that identifies the device type.                                           |
| Location        | Where the device is located.                                                                 |
| 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.                                                       |
| Profile         | Name of the profile that contains threshold values and policy settings for fault management. |

## Limitation on the Number of Managed Devices

Limits on the number of managed devices are enforced according to the type of WLSE hardware you have.

**Note**

The following numbers are based on the number of radios in a device. Therefore, the number of managed devices must be reduced for dual-radio devices.

- The WLSE 1130 can manage 2500 access points and wireless bridges. After you have placed 2500 of these devices under management, warning messages are displayed each time you place more devices in the folder. After 2550 devices are under management, no additional devices can be placed in the Managed folder.
- The WLSE 1105 can manage 500 access points and wireless bridges. After you have placed 500 of these devices under management, warning messages are displayed each time you place more devices in the folder. After 525 devices are under management, no more devices can be placed in the Managed folder. Installing WLSE 2.0 software on a WLSE 1105 does not increase the number of devices you can manage.

**Note**

---

Device discovery continues after the absolute limit is reached, but no additional devices can be placed under management.

---

## Managing Device Inventories

During inventory, the WLSE retrieves device attributes in order 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 3-81](#).

You can use the inventory options to:

- Run immediate or scheduled inventories of specified devices—See [Running Immediate and Scheduled Inventories, page 3-84](#).
- Reset the polling intervals for automatic inventories, job retention, and report data retention—See [Changing the Polling Intervals for Automatic Inventories, page 3-82](#).
- View details on all types of inventory jobs—See [Viewing Inventory Logs, page 3-91](#).

### Related Topics

[About Inventories, page 3-81](#)

## 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 populate WLSE trending reports.
- Inventory polling is typically run at regular intervals, but can also be run on-demand. You can also run on-demand polling per device or per device group.
- Other polled data are processed and compared against fault, performance, and configuration policy thresholds.
- Device polling and data aggregation intervals are configurable.

The WLSE runs 3 types of automatic inventories on a regularly scheduled basis:

- **Basic** inventories of all devices that 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 appear in the Scheduled folder.



---

**Note**

An automatic basic inventory runs immediately after a device is discovered for the first time if the device is auto-managed. Inventory does not run automatically after a device is rediscovered.

---

- **Client** inventories that only collect information about associations of clients to access points.

In the inventory log, these inventories appear in the Periodic - All Devices folder under the name *ClientInventory*.

- **Performance** inventories that only collect the performance attributes used in trend reports for access points, bridges, and AAA servers.

In the inventory log, these inventories appear in the Periodic - All Devices folder under the name *PerformanceInventory*.

You can reset the polling intervals for automatic inventories. See [Changing the Polling Intervals for Automatic Inventories, page 3-82](#). You can run immediate or scheduled inventories. See [Running Immediate and Scheduled Inventories, page 3-84](#).

You can run immediate and schedule inventories to run one time or at a specified interval. You select the devices for these inventories.

**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 3-83](#).

### Procedure

- 
- Step 1** Select **Devices > Discover > Inventory > Polling** option.
- 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 3-87](#)
- [Guidelines For Choosing Inventory Intervals, page 3-83](#)

## Guidelines For Choosing Inventory Intervals

Following are some suggestions for deciding how to set the polling intervals.

### Setting Different Intervals For Different Device Groups

The scheduled inventory feature (see [Running Immediate and Scheduled Inventories, page 3-84](#)) lets you define more frequent inventory polling for a set of devices. This feature allows you to set general polling system parameters at a less frequent interval than the scheduled inventory parameters.

For example, you might decide to set the inventory intervals based on connection speeds. Suppose Site B and Site C are connected via 256 KB frame relay links back to the Site A corporate headquarters network. Assuming the headquarters network is minimally a high-speed Ethernet network, there is obviously a higher tolerance for inventory polling for Site A than for Sites B and C. So in this case, you might want to set the global inventory intervals for Sites B and C to less frequent values than those of Site A.

### Setting the Recurring Interval Size

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.

## Running Immediate and Scheduled Inventories

This section provides procedures for running immediate and scheduled 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.

To get started, select **Devices > Discover > Inventory**. Then refer to [Table 3-14 on page 3-84](#).


**Note**

Your login determines whether you can use this option.

The tasks for running inventories are:

**Table 3-14 Tasks for Running Inventories**

| Type of Inventory | Task                                               | Reference                                                           |
|-------------------|----------------------------------------------------|---------------------------------------------------------------------|
| All               | Select inventory type.                             | <a href="#">Select Inventory Type, page 3-84</a>                    |
| Run Now           | Select devices, run inventory, and verify results. | <a href="#">Run Now—Select Devices and Run Inventory, page 3-85</a> |
| Scheduled         | Select devices.                                    | <a href="#">Scheduled Inventory—Select Devices, page 3-86</a>       |
|                   | Schedule and run inventory and verify results.     | <a href="#">Scheduled Inventory—Specify the Schedule, page 3-86</a> |

## Select Inventory Type


**Note**

Your login determines whether you can use this option.

### Procedure

- Step 1** Select the inventory type:
- Run Now allows you to run an immediate inventory. You can only select one group or the individual devices in one group.



- Scheduled allows you to schedule inventory. There is also an option for scheduling repeated inventories. You can select multiple groups and individual devices from multiple groups.

Use this option to run scheduled inventories of selected devices. You can use this option when you need to inventory certain devices more frequently than the inventories provided by the automatic inventory feature.

**Step 2** Click **Next**.

---

#### Related Topics

- [Managing Device Inventories, page 3-80](#)
- [Guidelines For Choosing Inventory Intervals, page 3-83](#)

## Run Now—Select Devices and Run Inventory

You can 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 the on-demand inventory 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 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 and Search, page 1-9](#).
- Step 2** 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 3** Click **Run Inventory**. The inventory job starts immediately. Managed devices are polled and information is collected. WLSE displays are updated accordingly.

- Step 4** In the Tasks list, expand the Inventory folder and the Run Now folder to see the results of the inventory collection.
- Immediate inventories of selected devices are named `InventoryRunNow_number`. The *number* increments each time you run an inventory.
- Step 5** To view details on an inventory, click the inventory name. The Run Log shows the start and end times of the inventory and the type of data that was collected for the devices you selected. For more information on inventory logs, see [Viewing Inventory Logs, page 3-91](#).
- 

## Scheduled Inventory—Select Devices

### Procedure

---

- Step 1** 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 and Search, page 1-9](#).
- Step 2** Select the entire group or individual devices and click >>. The devices are moved to the Selected Devices list.
- Step 3** Repeat Steps 1 and 2 to select more devices.
- Step 4** Click **Next**.
- 

## Scheduled Inventory—Specify the Schedule

### Procedure

---

- Step 1** Select a Start Date and Time. Do not schedule an inventory within 5 minutes of the current time; the first inventory might not run. Use the Run Now option instead.
- Step 2** If you want the job to repeat at regular intervals, select **Enable Repeat**. Enter an interval and select Minutes, Hours, Days, Weeks or Months.



---

**Note** The minimum interval is 30 minutes.

---

- Step 3** Click **Finish** to schedule the inventory.  
To return to the previous screen, click **Back**.  
To cancel the inventory, click **Cancel**.
- Step 4** In the Tasks list, expand the Inventory folder and the Scheduled folder to see the results of the inventory collection.
- Step 5** To view details on an inventory, click the inventory name. The Run Log shows the start and end times of the inventory and the type of data that was collected for the devices you selected. For more information on inventory logs, see [Viewing Inventory Logs, page 3-91](#).
- 

#### Related Topics

- [Guidelines For Choosing Inventory Intervals, page 3-83](#)

## 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.



---

**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 3-88](#) are displayed.
- Step 2** To change parameter values, select new values from the pulldown lists.
- Step 3** To reset parameters to their previous values, click **Reset** *before* clicking **Apply**.

- Step 4** To save your changes, click **Apply**. To return to the System Parameters window, click **Back**.

### Related Topics

[About Trending and Aggregation Data, page 3-90](#)

## 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 3-15 on page 3-88](#)).
- [Fault and Job Truncation Parameters](#)—Control the amount of data displayed in fault history tables and job history tables (see [Table 3-16 on page 3-89](#)).
- [Data Retention Parameters](#)—Control how long to retain the raw and aggregated data used in trend reports (see [Table 3-17 on page 3-90](#)).

For general information about polling intervals and data retention parameters and guidelines for choosing the appropriate settings, see [About Inventories, page 3-81](#).

**Table 3-15 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.<br><br><b>Tip</b> For more accurate trending, set this parameter at a lower interval than the <a href="#">Performance Attributes Poll Interval</a> . | Default: 12 hours<br>Minimum: 1 hour<br>Maximum: 7 days |

**Table 3-15 Polling Interval Parameters (continued)**

| Parameter                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Values                                                                       |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Wireless Client Poll Interval        | <p>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.</p> <p><b>Tip</b> 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 <a href="#">Running Immediate and Scheduled Inventories</a>, page 3-84.</p> | <p>Default: 51 minutes</p> <p>Minimum: 17 minutes</p> <p>Maximum: 7 days</p> |
| Performance Attributes Poll Interval | <p>Interval during which performance and utilization data are collected from the devices for the performance inventory.</p> <p>To set the aggregation period of this data, change the <a href="#">Raw Trend Data</a> parameter.</p>                                                                                                                                                                                                                                                                                                                                                                                         | <p>Default: 13 minutes</p> <p>Minimum: 13 minutes</p> <p>Maximum: 7 days</p> |

**Table 3-16 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.                                                                                                                                                                          | <p>Default: 30 days</p> <p>Minimum: 15 days</p> <p>Maximum: 60 days</p> |
| Job History Truncation Interval   | <p>How long displayed job data is retained. This is the data shown in <b>Configure &gt; Jobs, Firmware &gt; Jobs</b>, and <b>Reports &gt; Scheduled Email Jobs</b>.</p> <p><b>Note</b> Recurring jobs are truncated every day to retain the last 30 runs.</p> | <p>Default: 30 days</p> <p>Minimum: 15 days</p> <p>Maximum: 60 days</p> |

**Table 3-17 Data Retention Parameters**

| Parameter               | Description                                                     | Values                                                       |
|-------------------------|-----------------------------------------------------------------|--------------------------------------------------------------|
| Raw Trend Data          | How long the raw (unaggregated) trend data is retained.         | Default: 2 days<br>Minimum: 1 day<br>Maximum: 5 days         |
| Hourly Aggregated Data  | How long to retain the reports data that is aggregated hourly.  | Default: 7 days<br>Minimum: 1 day<br>Maximum: 15 days        |
| Daily Aggregated Data   | How long to retain the reports data that is aggregated daily.   | Default: 30 days<br>Minimum: 8 days<br>Maximum: 30 days      |
| Weekly Aggregated Data  | How long to retain the reports data that is aggregated weekly.  | Default: 6 months<br>Minimum: 1 month<br>Maximum: 12 months  |
| Monthly Aggregated Data | How long to retain the reports data that is aggregated monthly. | Default: 12 months<br>Minimum: 1 month<br>Maximum: 48 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 3-88](#).

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** To view a list of jobs, expand the Inventory folder. Then expand the folder that contains the type of inventory you want to see:

- The Scheduled folder contains the last 15 scheduled inventories.
- The Periodic- All Devices folder contains the last 15 performance and client inventories.
- The Run Now folder contains the last 15 immediate inventories.

In each subfolder, the latest job is listed first and earliest is listed last.

**Step 3** The names of inventory jobs indicate the type of inventory that was run, as explained in the following table.

**Table 3-18 Inventory Folders and Job Names**

| Folder Name          | Inventory Name                 | Inventory Type                                                                                        |
|----------------------|--------------------------------|-------------------------------------------------------------------------------------------------------|
| Periodic—All Devices | Inventory                      | Automatic inventories of all devices                                                                  |
|                      | ClientInventory                | Automatic inventories of client associations with access points                                       |
|                      | PerformanceInventory           | Automatic inventories of performance attributes for trend reports                                     |
| Run Now              | InventoryRunNow_ <i>number</i> | On-demand inventories of selected devices, run by users and generated by the radio management module. |
| Scheduled            | ScheduledInventory             | Inventories of all devices, scheduled by users                                                        |

- Step 4** 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 3-92](#).

### Related Topics

[Diagnosing Common Inventory Problems, page 3-93](#)

## Run Log Details—Inventory

Most inventory run log messages show the type of data collected and the devices you selected for inventory.

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 3-93](#)

## 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 **Administration > 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](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](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.

---

# 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 3-94.
- A comma-separated values (CSV) file—see [Exporting Devices to a CSV File](#), page 3-96.

**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 > 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 3-19 Messages—Export Status Log**

| Type of Information or Message                                                                                                                 | Description                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device information                                                                                                                             | Name of the device, device status, and device status details.<br><br>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** 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 3-49](#).

### Procedure

- 
- Step 1** Select **Devices > Discover > Export Devices > To CSV File**.
- Step 2** Device credentials are exported to the file in plain text. For added security during the transmission of credentials, you can switch your browser to HTTPS so that HTTPS is used for the downloading the file. To switch to HTTPS, enter the following URL in the browser:
- `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 a message appears about the HTTPS certificate, follow the directions for installing the certificate.
- Step 3** Click **Download CSV File**, then click **Save**. Specify the filename and location.




---

**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 3-98](#).

The group management window allows you to:

- Select a group and view details about it—See [Using the Group Details Window, page 3-101](#).
- Create a new static or rule-based group:
  - [Creating a Static Group, page 3-103](#)
  - [Creating a Rule-Based Group, page 3-105](#)
- Create a new group by copying an existing group:
  - [Creating a Static Group by Copying a Static or Rule-Based Group, page 3-107](#)
  - [Copying a Rule-Based Group, page 3-108](#)
- Edit a group:
  - [Editing a Static Group, page 3-110](#)
  - [Editing a Rule-Based Group, page 3-111](#)
- Delete a group—See [Deleting a Static or Rule-Based Group, page 3-113](#).

## Related Topics

- [Managing Device Discovery, page 3-41](#)
- [Managing Device Inventories, page 3-80](#)

## 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 3-98](#).
- User-defined groups—See [User-Defined Groups, page 3-100](#).

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.

**Tip**

A complete listing of supported devices can be found on [Cisco.com](http://Cisco.com).

[Table 3-20](#) lists the system-defined groups, dynamic groups and subgroups.

**Table 3-20 System-Defined Groups**

| System-Defined Groups | Contained in Folder | Subgroups                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device Type           | Device Type         | <ul style="list-style-type: none"> <li>• AAA servers—LEAP, RADIUS, EAP-MD5, and PEAP groups. Groups appear and servers are added to groups after you add the servers to the WLSE (see <a href="#">Managing AAA Servers, page 3-37</a>).</li> <li>• AP 1100, AP 1200, AP 1210</li> <li>• AP 340, AP 350, AP 350-IOS</li> </ul> <p><b>Note</b> Cisco Aironet 4800 access points being managed by the WLSE will appear in the AP350 group.</p> <ul style="list-style-type: none"> <li>• Bridge 350</li> <li>• Routers</li> <li>• Switches</li> </ul> |
| SSID                  | More System Groups  | Contains a group for each radio service set ID ( <b>SSID</b> ) that is configured on access points. For information about configuring SSIDs on access points, see <a href="#">Setting Up Devices, page 3-5</a> .                                                                                                                                                                                                                                                                                                                                  |
| Software Version      | More System Groups  | Contains a group for each software version that is installed on the devices.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Subnet                | More System Groups  | Contains a group for each subnet that is configured in the network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

Table 3-20 System-Defined Groups (continued)

| System-Defined Groups          | Contained in Folder   | Subgroups                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLAN                           | More System Groups    | <p>Contains a group for each <a href="#">VLAN</a> that is configured on the access points.</p> <p><b>Note</b> VLAN groups for IOS access points might not be populated if the WEP keys are not configured in each VLAN. VLAN information becomes accessible through SNMP as soon as WEP keys are configured.</p>                                                                                                                                                                   |
| Wireless Domain Services (WDS) | WDS                   | <p>Contains WDS access points:</p> <ul style="list-style-type: none"> <li>• Active WDS—Contains the access point that is actively providing WDS services.</li> <li>• Backup WDS—Contains the backup WDS access points.</li> </ul>                                                                                                                                                                                                                                                  |
| Misconfigured Devices          | Misconfigured Devices | <p>Contains IOS access points that do not have an ISO view configured.</p> <ul style="list-style-type: none"> <li>• To manually correct this problem on an access point, see <a href="#">Set Up IOS Access Points, page 3-8</a>.</li> <li>• To correct the problem by creating a configuration job, see <a href="#">Managing Configuration Jobs, page 4-267</a>.</li> </ul> <p><b>Note</b> Devices that receive a dot11 mib view fault are automatically placed in this group.</p> |

## User-Defined Groups

You can define any number of groups, and set up hierarchies of groups which can contain subgroups and devices.



### Tip

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.



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.
- 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.

Useful user-created groups in a WLAN greatly depend on the structure of the network and the application demands. [Table 3-21](#) contains examples of groups that might be worthwhile in a typical wireless LAN environment.

**Table 3-21 Sample Useful 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 |
| Operating System   | non-IOS, IOS                                |
| Special Features   | Proxy Mobile IP, Wireless Domain Services   |
| 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 3-22 Group Details Window Fields**

| Field         |                  | Description                                                                                                                                                                                                                                                                                   |
|---------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description   |                  | Description entered when the group was created or edited (if any)                                                                                                                                                                                                                             |
| 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.<br>Subgroup—A subgroup of the group you selected.                                                                                                                                                                                            |
|               | Name             | Hostname of a member device or name of a subgroup. <ul style="list-style-type: none"> <li>Click a device name to display a summary report and links to the device's fault status and history.</li> <li>Click a subgroup name to see details for the subgroup in a separate window.</li> </ul> |
|               | 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 3-23 Group Details Window Buttons**

| Button Name             | Function                                  | Reference                                                                                                                                             |
|-------------------------|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create Static Group     | Create a static group.                    | <a href="#">Creating a Static Group, page 3-103.</a>                                                                                                  |
| Create Rule-Based Group | Create a rule-based group.                | <a href="#">Creating a Rule-Based Group, page 3-105.</a>                                                                                              |
| Copy                    | Copy a static or rule-based group.        | <a href="#">Creating a Static Group by Copying a Static or Rule-Based Group, page 3-107</a><br><a href="#">Copying a Rule-Based Group, page 3-108</a> |
| Copy Static             | Make a static copy of a rule-based group. | <a href="#">Copying a Rule-Based Group, page 3-108</a>                                                                                                |
| Edit                    | Edit a static or rule-based group.        | <a href="#">Editing a Static Group, page 3-110</a> or <a href="#">Editing a Rule-Based Group, page 3-111</a>                                          |
| Delete                  | Delete a static or rule-based group.      | Click <b>Delete</b> to delete the group.                                                                                                              |

## 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** and enter the following information:
  - Enter a name in the Name text box.

- Enter a description in the Description text box (optional).

Group names can be up to 64 characters in length. For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page A-1](#).

**Step 3** The new group is placed at the top (root) level or becomes a subgroup of another static group as follows:

- If another static group was selected when you created the new group, the new group becomes a subgroup of that group.
- If no static group was selected, the new group becomes a subgroup of root.

To change the subgroup designation:

- To make your new group a subgroup of any existing static group, select 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 and Search, page 1-9](#).

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 3-107](#)

[Copying a Rule-Based Group, page 3-108](#)

## Creating a Rule-Based Group

To create a new rule-based group:

### 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.
- (Optional) enter a description in the Description text box.



---

**Note** New groups are always added at the top level ([root]).

---

Group names can be up to 64 characters in length. For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page A-1](#).

**Step 3** 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. The sysLocation <i>null</i> matches all devices that do not have this variable set.                                                                                                                                               |
| WDS State                   | The WDS state of the access points in the group: <ul style="list-style-type: none"> <li>• Active WDS—the active WDS access point.</li> <li>• Backup WDS—the backup WDS access point.</li> <li>• Candidate WDS—any other access points that are configured for WDS.</li> </ul> |
| Registration State with WDS | Whether the access points in the group are registered with a WDS access point.                                                                                                                                                                                                |
| Device Type                 | Select an access point type from the list, if this group contains access points. If you select AP350, BR 350 devices will be included in the group as well.                                                                                                                   |
| 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 4** To preview the group, click **Preview**. The rule(s) you defined and any currently managed devices that match the rule(s) are displayed.
- Step 5** To reset the window to its contents before this session, click **Reset**.
- Step 6** 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 3-108](#)

## 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.
- Group names can be up to 64 characters in length. For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page A-1](#).
- Step 4** The devices in the group you copied appear in the Devices in Group list.
- Step 5** 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 and Search, page 1-9](#).
- 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 6** To remove devices from the group, select them from the Devices in Group list and click <<.

**Step 7** 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 3-110](#)
- [Deleting a Static or Rule-Based Group, page 3-113](#)
- [About Groups, page 3-98](#)

## 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 Static** to create a static group.

- If you selected **Copy Static** to create a new static group, see [Creating a Static Group by Copying a Static or Rule-Based Group, page 3-107](#).



- 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.

Group names can be up to 64 characters in length. For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page A-1](#).

**Step 4** 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. The sysLocation <i>null</i> 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. If you select AP350, BR 350 devices will be included in the group as well.                                                                                                                    |
| Subnet                      | A subnet, in decimal-dot format; for example 172.10.10.10, or 172.*.                                                                                                                                                                                                           |
| WDS State                   | The WDS state of the access points in the group: <ul style="list-style-type: none"> <li>• Active WDS—the currently active WDS access point.</li> <li>• Backup WDS—the backup WDS access point.</li> <li>• Candidate WDS—any other access points configured for WDS.</li> </ul> |
| Registration State with WDS | Whether the access points in the group are registered with a WDS access point.                                                                                                                                                                                                 |
| SSID                        | An SSID defined on devices.                                                                                                                                                                                                                                                    |
| VLAN ID                     | An existing VLAN configured on managed access points.                                                                                                                                                                                                                          |

**Step 5** 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.  
Group names can be up to 64 characters in length. For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page A-1](#).
  - Step 4** To make the group a subgroup of another group, select a group from the Subgroup Of list. The group you are editing will become a subgroup of the group you select.
  - 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 and Search, page 1-9](#).
    - a. Select the group or individual devices from the list and click >>. Devices are placed in the Devices in Group list.
    - b. 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 3-103](#)
- [Deleting a Static or Rule-Based Group, page 3-113](#)
- [About Groups, page 3-98](#)

## 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.
- Group names can be up to 64 characters in length. For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page A-1](#).
- Step 4** 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. The sysLocation <i>null</i> 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. If you select AP350, BR 350 devices will be included in the group as well. |

| Rule Name                   | Data to Select or Enter                                                                                                                                                                                                                                          |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Subnet                      | A subnet, in decimal-dot format; for example, 172.10.10.10, or 172.*.                                                                                                                                                                                            |
| WDS State                   | The WDS state of the access points in the group: <ul style="list-style-type: none"> <li>• Active WDS—the active WDS access point.</li> <li>• Backup WDS—the backup WDS access point.</li> <li>• Candidate WDS—other access points configured for WDS.</li> </ul> |
| Registration State with WDS | Whether the access points in the group are registered with a WDS access point.                                                                                                                                                                                   |
| SSID                        | An SSID defined on devices.                                                                                                                                                                                                                                      |
| VLAN ID                     | The existing VLANs configured on managed access points.                                                                                                                                                                                                          |

- Step 5** 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 3-98](#)
- [Editing a Static Group, page 3-110](#)
- [Creating a Static Group, page 3-103](#)





## Configuring Devices

---

The Configure tab allows you to view, create, copy, edit, and delete configuration templates and apply them to large numbers of devices at a time. It also allows you to schedule a configuration job and to check on the job's status.

Following are the subtabs under Configure:



### Note

---

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

---

- **Templates**—See [Using the Templates, page 4-1](#).
- **Archives**—See [Managing Configuration Archives, page 4-261](#).
- **Jobs**—See [Managing Jobs, page 4-267](#).
- **Auto Update**—See [Automating Configurations, page 4-300](#).

## Using the Templates

This window allows you to create, modify, and delete configuration templates.

The topics covered in this section are:

- [What is a Configuration Template?, page 4-2](#)
- [Template Choices, page 4-2](#)
- [Creating a Template, page 4-253](#)
- [Copying a Template, page 4-254](#)

- [Editing a Template, page 4-255](#)
- [Converting a Template, page 4-256](#)
- [Deleting a Template, page 4-257](#)
- [Importing a Template, page 4-257](#)
- [Exporting a Template, page 4-261](#)

**Related Topics**

[Managing Jobs, page 4-267](#)

## What is a Configuration Template?

You can think of a configuration template as a configuration update file for an access point. This file might contain the update for only one parameter or a complete access point configuration.

Templates for non-IOS access points are stored internally as files in the `.ini` format that is understood by the access points. IOS-based templates are stored as text files containing IOS commands.

You can use the **Configure > Templates** option to:

- Create a configuration template (see [Creating a Template, page 4-253](#)).
- Import templates directly from devices and export them to files (see [Exporting a Template, page 4-261](#)).
- Convert non-IOS templates to IOS-based templates (see [Converting a Template, page 4-256](#)).

## Template Choices

The template choices vary depending upon the type of template you are creating:

- [IOS Templates, page 4-3](#)
- [Non-IOS Templates, page 4-100](#)



## IOS Templates

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 4-101.
2. **Template Categories**



---

**Note** Any or all of the template categories can be completed in any order.

---

- **Basic Settings**—See [Using Basic Settings](#), page 4-4.
  - **Network Interfaces**—See [Setting Up Network Interfaces](#), page 4-9.
  - **Security**—See [Defining Security Settings](#), page 4-26.
  - **Services**—See [Defining Services](#), page 4-55.
  - **Event Log**—See [Configuring the Event Log](#), page 4-91.
  - **Wireless Services**—See [Configuring Wireless Services](#), page 4-95.
  - **Custom Values**—See [Configuring Custom Values](#), page 4-99.
3. **Preview**—See [Previewing the Template](#), page 4-252.
  4. **Save**—See [Saving the Template](#), page 4-253.

## Naming the Template

This option enables to you to name the template.

### Procedure



**Note** Clicking **Clear** removes all the entries you have made.

**Step 1** Select **Template Name**. The Template Name dialog box appears:

| Field       | Description                                                                                                                                                                                      |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name        | Enter a name for the template.<br>See <a href="#">Naming Guidelines, page A-1</a> .                                                                                                              |
| Description | Enter a description of the purpose of the template.<br>See <a href="#">Naming Guidelines, page A-1</a> .<br>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 [Template Categories, page 4-3](#).

## 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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-1 Basic Settings**

| Field                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuration Server Protocol | <p>Set this entry to match the network's method of IP address assignment.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"><li>• DHCP—Use this setting if your network uses Dynamic Host Configuration Protocol, in which IP addresses are “leased” for predetermined periods of time.</li><li>• Static IP—Use this setting if your network does has an automatic system for IP address assignment.</li></ul> |
| Default Gateway               | <p>Enter the IP address of your default Internet gateway.</p> <p>The entry 255.255.255.255 indicates no gateway.</p>                                                                                                                                                                                                                                                                                                                           |
| SNMP Community                | <p>Enter the SNMP community name.</p> <p>Select one of the following: Read-Only, Read-Write</p>                                                                                                                                                                                                                                                                                                                                                |
| Radio0-802.11b                |                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| SSID                          | <p>Enter any alphanumeric, case-sensitive string, from 1 to 32 characters long.</p> <p>The SSID is a unique identifier that clients use to associate with the radio.</p>                                                                                                                                                                                                                                                                       |

**Table 4-1 Basic Settings (continued)**

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Role in Radio Network      | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul> |
| Broadcast SSID in Beacon   | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this setting to allow devices that do not specify an SSID to associate with the access point.</li> <li>• No—Use this setting require that the SSID used by the client devices must match exactly the access point's SSID.</li> </ul>                                                                                                                   |
| Optimize Radio Network for | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• Throughput—Use this setting to maximize the data volume handled by the access point; however, it might reduce the access point's range.</li> <li>• Range—Use this setting to maximize the access point's range; however, it might reduce throughput.</li> </ul>                                                                                                |
| Aironet Extensions         | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• Enable—Use this setting to enable load balancing, Message Integrity Check (MIC), and WEP key hashing.</li> <li>• Disable—Use this setting to disables load balancing, Message Integrity Check (MIC), and WEP key hashing.</li> </ul>                                                                                                                           |

**Table 4-1 Basic Settings (continued)**

| Field                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Radio0-802.11a            |                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SSID                      | <p>Enter any alphanumeric, case-sensitive string, from 1 to 32 characters long.</p> <p>The SSID is a unique identifier that clients use to associate with the radio.</p>                                                                                                                                                                                                                                                                 |
| Role in Radio Network     | <p>Select one of the following:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li></ul> |
| Broadcast SSID in Beacon: | <p>Select one of the following:</p> <ul style="list-style-type: none"><li>• Yes—Use this setting to allow devices that do not specify an SSID to associate with the access point.</li><li>• No—Use this setting require that the SSID used by the client devices must match exactly the access point's SSID.</li></ul>                                                                                                                   |

**Table 4-1 Basic Settings (continued)**

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Optimize Radio Network for | <p>Select one of the following:</p> <ul style="list-style-type: none"><li>• <b>Throughput</b>—Use this setting to maximize the data volume handled by the access point; however, it might reduce the access point's range.</li><li>• <b>Range</b>—Use this setting to maximize the access point's range; however, it might reduce throughput.</li><li>• <b>Default</b>—Use this setting to specify the that the access point use settings entered for the Network Interfaces Settings.</li></ul> |
| Aironet Extensions         | <p>Select one of the following:</p> <ul style="list-style-type: none"><li>• <b>Enable</b>—Use this setting to enable load balancing, Message Integrity Check (MIC), and WEP key hashing.</li><li>• <b>Disable</b>—Use this setting to disables load balancing, Message Integrity Check (MIC), and WEP key hashing.</li></ul>                                                                                                                                                                     |

**Step 2** Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-3](#).
- 

## 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 4-9](#).
  - Radio-802.11b—See [Configuring Radio-802.11b Settings, page 4-11](#).
  - Radio-802.11a—See [Configuring Radio-802.11a Settings, page 4-19](#)
- 

## 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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-2 Fast Ethernet Settings**

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Ethernet  | Select one of the following: <ul style="list-style-type: none"> <li>• Enable—Use this setting to enable Ethernet.</li> <li>• Disable—Use this setting to disable Ethernet.</li> </ul>                                                                                                                                                                                                                                             |
| Requested Duplex | Select one of the following: <ul style="list-style-type: none"> <li>• 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.</li> <li>• Half—Use this setting to allow operation in half-duplex mode.</li> <li>• Full—Use this setting to allow operation in full-duplex mode.</li> </ul>               |
| Requested Speed  | Select one of the following: <ul style="list-style-type: none"> <li>• 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.</li> <li>• 100Mbps—Use this setting to allow a transmission speed of 100 Mbps.</li> <li>• 10Mbps—Use this setting to allow a transmission speed of 10 Mbps.</li> </ul> |



- Step 3** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-3](#).
- 

## Configuring Radio-802.11b Settings

Use this option to configure the device's 802.11b radio.

### Procedure

---

**Step 1** Select **Network Interfaces > Radio-802.11b**. The Network Interfaces: Radio-802.11b 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 Template windows up until that point.

---

**Table 4-3** *Radio-802.11b Settings*

| Field        | Description                                                                                                                                                                                                                                                                                                                                                                            |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Radio | Select one of the following: <ul style="list-style-type: none"><li>• <b>Enable</b>—Use this setting to allow the access point to send packets through its 802.11b radio interface and monitor when other devices use the 802.11b radio interface to send packets.</li><li>• <b>Disable</b>—Use this setting to change the administrative state of the radio from up to down.</li></ul> |

**Table 4-3 Radio-802.11b Settings (continued)**

| Field                                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Role in Radio Network<br>(Fallback mode upon loss of Ethernet connection) | <p>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.</p> <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> </ul> |

**Table 4-3 Radio-802.11b Settings (continued)**

| Field      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Rates | <ul style="list-style-type: none"><li>Click one of the following to automatically set the data transmission rates:<ul style="list-style-type: none"><li>Best Range—Use this setting to maximize the access point's range; however, it might reduce throughput.</li><li>Best Throughput—Use this setting to maximize the data volume handled by the access point; however, it might reduce the access point's range.</li></ul></li></ul> <p>Or</p> <ul style="list-style-type: none"><li>Select one of the following to manually set the data transmission rates:<ul style="list-style-type: none"><li>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.</li><li>Enable—Use this setting to enable transmission at this rate for unicast packets only.</li><li>Disable—Use this setting to not allow transmission at this rate.</li></ul></li></ul> |

**Table 4-3 Radio-802.11b Settings (continued)**

| Field                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Transmitter Power (mW)  | <p>Select the power level of the radio transmission.</p> <p><b>Note</b> 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.</p> <p>To reduce interference, limit the range of your access point, or conserve power, select a lower power setting.</p> <p></p> <p><b>Caution</b> Do not use the 50mW or 10mW setting for Japanese channels.</p> <p>For a list of maximum power levels allowed in each regulatory domain refer to one of the following:</p> <ul style="list-style-type: none"> <li>• URL:<br/> <a href="http://www.cisco.com/en/US/products/hw/wireless/ps430/products_command_reference_chapter09186a0080147d8b.html#87443">http://www.cisco.com/en/US/products/hw/wireless/ps430/products_command_reference_chapter09186a0080147d8b.html#87443</a></li> <li>• Cisco IOS Commands for Access in the <i>Cisco Aironet 1200 Series Access Point Command Reference</i>.</li> </ul> |
| 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

**Table 4-3 Radio-802.11b Settings (continued)**

| Field                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default Radio Channel             | <p>From the list, select the radio channel you want for a default.</p> <p>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.</p>                                                                                                                                                                                                             |
| Least Congested Channel Search    | <p>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.</p>                                                                                                                                                                                                                                                                                                                            |
| World Mode Multi-Domain Operation | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Enable</b>—Use this setting to enable the access point to add channel carrier set information to its beacon.</li> </ul> <p>Client devices with world-mode enabled receive the carrier set information and adjust their settings automatically.</p> <ul style="list-style-type: none"> <li>• <b>Disable</b>—Use this setting to not allow the access point to add channel carrier set information to its beacon.</li> </ul> |
| Radio Preamble                    | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Short</b>—Use this setting to improves throughput performance; Cisco Aironet's Wireless LAN Adapter supports short preambles.</li> <li>• <b>Long</b>—Use this setting to ensure compatibility between the access point and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A).</li> </ul>                                                                                                        |

**Table 4-3 Radio-802.11b Settings (continued)**

| Field                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Receive Antenna                  | From the list, select one of the following:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Transmit Antenna                 | <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.)</li> <li>• 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.)</li> </ul> |
| Aironet Extensions               | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• Enable—Use this setting to enable load balancing, Message Integrity Check (MIC), and WEP key hashing.</li> <li>• Disable—Use this setting to disable load balancing, Message Integrity Check (MIC), and WEP key hashing.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                |
| Ethernet Encapsulation Transform | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• RFC1042—Use this setting to ensure interoperability with non-Cisco Aironet wireless equipment.</li> <li>• 802.1H—Use this setting to provide optimum performance for Cisco Aironet wireless products.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                   |

**Table 4-3 Radio-802.11b Settings (continued)**

| Field                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reliable Multicast to WGB       | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• Disable—Use this setting to not allow reliable multicast to workgroup bridges.</li> <li>• Enable—Use this setting to allow reliable multicast to workgroup bridges.</li> </ul>                                                                                                                                                                                                                                                                                     |
| Public Secure Packet Forwarding | <p><b>Note</b> Use this setting only if no VLAN is configured. If a VLAN is configured, then enable and disable PSPF by selecting <b>Services &gt; VLAN</b>.</p> <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• 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.)</li> <li>• Disable—Use this setting to disable the use of the port for secure mode configuration.</li> </ul> |
| Beacon Period                   | Enter the amount of time between beacons in kilomicroseconds. (One kilomicrosecond equals 1,024 microseconds.)                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Data Beacon Rate (DTIM)         | <p>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).</p> <p>The DTIM tells power-save client devices that a packet is waiting for them.</p> <p>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.</p>                                                                               |
| Max. Data Retries               | Enter the maximum number of attempts the access point makes to send a packet before giving up and dropping the packet.                                                                                                                                                                                                                                                                                                                                                                                                                          |

**Table 4-3 Radio-802.11b Settings (continued)**

| Field                                 | Description                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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               | <p>Enter a setting to determine the size at which packets are fragmented (sent as several pieces instead of as one block).</p> <p>Use a low setting in areas where communication is poor or where there is a great deal of radio interference.</p>                                                                                                                      |
| RTS Threshold                         | <p>Enter a setting to determine the packet size at which the access point issues a request to send (RTS) before sending the packet.</p> <p>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.</p> |
| 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 | <p>Enter the MAC address for the access point to which the repeater should associate.</p> <p>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.</p>                                        |



- Step 3** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-3](#).
- 

## 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 current entries in the window and any entries you have made in other Template windows up until that point.

---

**Table 4-4** *Radio-802.11a Settings*

| Field        | Description                                                                                                                                                                                                                                                                                                                                                                            |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Radio | Select one of the following: <ul style="list-style-type: none"><li>• <b>Enable</b>—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.</li><li>• <b>Disable</b>—Use this setting to change the administrative state of the radio from up to down.</li></ul> |

**Table 4-4 Radio-802.11a Settings (continued)**

| Field                                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Role in Radio Network<br>(Fallback mode upon loss of Ethernet connection) | <p>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.</p> <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> </ul> |

**Table 4-4 Radio-802.11a Settings (continued)**

| Field      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Rates | <ul style="list-style-type: none"><li>• Click one of the following to automatically set the data transmission rates:<ul style="list-style-type: none"><li>– Best Range—Use this setting to maximize the access point's range; however, it might reduce throughput.</li><li>– Best Throughput—Use this setting to maximize the data volume handled by the access point; however, it might reduce the access point's range.</li><li>– Default—Use this setting to compromise between range and throughput, providing good range and good throughput.</li></ul></li></ul> <p>Or</p> <ul style="list-style-type: none"><li>• Select one of the following to manually set the data transmission rates:<ul style="list-style-type: none"><li>– 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.</li><li>– Enable—Use this setting to enable transmission at this rate for unicast packets only.</li><li>– Disable—Use this setting to not allow transmission at this rate.</li></ul></li></ul> |

**Table 4-4 Radio-802.11a Settings (continued)**

| Field                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Transmitter Power (mW)         | <p>Select the power level of the radio transmission.</p> <p><b>Note</b> 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.</p> <p>To reduce interference, limit the range of your access point, or conserve power, select a lower power setting.</p> <p>For a list of maximum power levels allowed in each regulatory domain refer to one of the following:</p> <ul style="list-style-type: none"> <li>URL:<br/><a href="http://www.cisco.com/en/US/products/hw/wireless/ps430/products_command_reference_chapter09186a0080147d8b.html#87443">http://www.cisco.com/en/US/products/hw/wireless/ps430/products_command_reference_chapter09186a0080147d8b.html#87443</a></li> <li>Cisco IOS Commands for Access in the <i>Cisco Aironet 1200 Series Access Point Command Reference</i>.</li> </ul> |
| 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Default Radio Channel          | <p>From the list, select the radio channel you want for a default.</p> <p>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.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Table 4-4 Radio-802.11a Settings (continued)**

| Field                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Receive Antenna                  | From the list, select one of the following:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Transmit Antenna                 | <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.)</li> <li>• 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.)</li> </ul> |
| Aironet Extensions               | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• Enable—Use this setting to enable load balancing, Message Integrity Check (MIC), and WEP key hashing.</li> <li>• Disable—Use this setting to disable load balancing, Message Integrity Check (MIC), and WEP key hashing.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                |
| Ethernet Encapsulation Transform | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• RFC1042—Use this setting to ensure interoperability with non-Cisco Aironet wireless equipment.</li> <li>• 802.1H—Use this setting to provide optimum performance for Cisco Aironet wireless products.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                   |

**Table 4-4 Radio-802.11a Settings (continued)**

| Field                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reliable Multicast to WGB       | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• Disable—Use this setting to not allow reliable multicast to workgroup bridges.</li> <li>• Enable—Use this setting to allow reliable multicast to workgroup bridges.</li> </ul>                                                                                                                                                                                                                                                                                     |
| Public Secure Packet Forwarding | <p><b>Note</b> Use this setting only if no VLAN is configured. If a VLAN is configured, then enable and disable PSPF by selecting <b>Services &gt; VLAN</b>.</p> <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• 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.)</li> <li>• Disable—Use this setting to disable the use of the port for secure mode configuration.</li> </ul> |
| Beacon Period                   | Enter the amount of time between beacons in kilomicroseconds. (One kilomicrosecond equals 1,024 microseconds.)                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Data Beacon Rate (DTIM)         | <p>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).</p> <p>The DTIM tells power-save client devices that a packet is waiting for them.</p> <p>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.</p>                                                                               |
| Max. Data Retries               | Enter the maximum number of attempts the access point makes to send a packet before giving up and dropping the packet.                                                                                                                                                                                                                                                                                                                                                                                                                          |

**Table 4-4 Radio-802.11a Settings (continued)**

| Field                                 | Description                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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               | <p>Enter a setting to determine the size at which packets are fragmented (sent as several pieces instead of as one block).</p> <p>Use a low setting in areas where communication is poor or where there is a great deal of radio interference.</p>                                                                                                                      |
| RTS Threshold                         | <p>Enter a setting to determine the packet size at which the access point issues a request to send (RTS) before sending the packet.</p> <p>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.</p> |
| 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 | <p>Enter the MAC address for the access point to which the repeater should associate.</p> <p>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.</p>                                        |

**Step 3** Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-3](#).
- 

## 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 4-26](#).
  - SSID 802.11x—See [Configuring SSID 802.11x Settings, page 4-29](#).
  - WEP 802.11x—See [Configuring WEP 802.11x Settings, page 4-37](#).
  - Server Manager—See [Configuring Server Manager Settings, page 4-41](#).
  - Advanced Security—See [Configuring Advanced Security, page 4-46](#).
  - Local Radius Server—See [Setting Up the Local RADIUS Server, page 4-51](#).
- 

## 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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-5 Admin Access Settings**

| Field                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrator<br>Authenticated by | <p>Select one of the following:</p> <ul style="list-style-type: none"><li>• <b>Default Authentication (Global Password)</b>—Use this setting to skip the username and enter only a password.<br/><br/>You will need to enter the password in the Default Authentication (Global Password field below).</li><li>• <b>Local User List Only (Individual Password)</b>—Use this setting to designate the local user list for authentication.<br/><br/>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.</li><li>• <b>Authentication Server Only</b>—Use this setting to designate the server for authentication.</li><li>• <b>Authentication Server if not found in Local List</b>—Use this setting to designate the server for authentication if not in the local list.<br/><br/>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.</li></ul> |

**Table 4-5 Admin Access Settings (continued)**

| Field                                    | Description                                                                                                |
|------------------------------------------|------------------------------------------------------------------------------------------------------------|
| 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.<br><br>To delete a username from the list, select it, then click <b>Delete</b> . |
| Username                                 | Enter the username.                                                                                        |
| Password                                 | Enter the password                                                                                         |
| Confirm Password                         | Reenter the password                                                                                       |
| Capability Settings                      | Select one of the settings, then click <b>Add</b> .                                                        |
| Delete Users                             |                                                                                                            |
| User ID                                  | Enter the user identification, then click >>.                                                              |
| Users to Delete                          | Lists the users to be deleted.<br><br>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 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).

## Configuring SSID 802.11x Settings

Use this option to configure SSID 802.11b and 802.11a settings.

### Procedure

**Step 1** Select **Security > SSID Manager**. The Security: SSID Manager 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 Template windows up until that point.

**Table 4-6** *SSID 802.11x Settings*

| Field     | Description                                                                                                                                                   |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSID List | Lists the currently configured SSIDs.<br>To delete an SSID from the list, select it, then click <b>Delete</b> .                                               |
| SSID      | Enter any alphanumeric, case-sensitive string, from 1 to 32 characters long.<br>The SSID is a unique identifier that clients use to associate with the radio. |
| VLAN      | Enter the identification number of the VLAN.                                                                                                                  |

**Table 4-6 SSID 802.11x Settings (continued)**

| Field                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication Methods Accepted |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Open Authentication             | <p>Select one of the following from the list:</p> <ul style="list-style-type: none"> <li>• <b>MAC Authentication</b>—Use this setting to specify that client devices that associate to the access point with open authentication, use MAC authentication.</li> <li>• <b>EAP</b>—Use this setting to specify that client devices that associate to the access point with open authentication, use EAP authentication.</li> <li>• <b>MAC Authentication and EAP</b>—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.</li> <li>• <b>MAC Authentication or EAP</b>—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.</li> </ul> |

**Table 4-6 SSID 802.11x Settings (continued)**

| Field                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Shared Authentication | <p>Select one of the following from the list:</p> <ul style="list-style-type: none"><li>• MAC Authentication—Use this setting to specify that client devices that associate to the access point with shared authentication, use MAC authentication.</li><li>• EAP—Use this setting to specify that client devices that associate to the access point with shared authentication, use EAP authentication.</li><li>• 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.</li></ul> |
| Network EAP           | <p>Select the following from the list:</p> <p>MAC Authentication—Use this setting to specify that client devices that associate to the access point with network EAP authentication, use MAC authentication.</p>                                                                                                                                                                                                                                                                                                                                                                                       |

**Table 4-6 SSID 802.11x Settings (continued)**

| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Priorities            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| EAP Authentication Servers   | Select one of the following: <ul style="list-style-type: none"> <li>• Use Defaults—Use this setting to use the defaults.</li> <li>• Use Server Group—Use this setting to specify a server group then enter the group name.</li> <li>• Customize—Use this setting to create a new server group.</li> <li>• New Group Name—Enter a name for the new group.</li> <li>• Priority—Enter the server IP address or hostname.               <ul style="list-style-type: none"> <li>– Auth Port—Enter the authentication port.</li> <li>– Acct Port—Enter the accounting port.</li> </ul> </li> </ul> or <ul style="list-style-type: none"> <li>– Select a name from the list.</li> </ul> |
| MAC Authentication Servers   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Authenticated Key Management | From the list, select one of the following: <p><b>Note</b> For 802.11a you select either CCKM or WPA; for 802.11b, you can select both.</p> <ul style="list-style-type: none"> <li>• None—Use this setting to indicate you do not want to use authenticated key management.</li> <li>• Mandatory—Use this setting to indicate authenticated key management is mandatory.</li> <li>• Optional—Use this setting to indicate authenticated key management is optional.</li> </ul>                                                                                                                                                                                                   |

**Table 4-6 SSID 802.11x Settings (continued)**

| Field | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CCKM  | <p>Select this option to use Cisco Centralized Key Management (CCKM).</p> <p>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.</p> <p><b>Note</b> To enable CCKM for an SSID, you must configure network-EAP authentication.</p> |
| WPA   | <p>Select this option to use Wi-Fi Protected Access (WPA).</p> <p>The WPA key management uses a combination of encryption methods to protect communication between client devices and the access point.</p> <p>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.</p> <p><b>Note</b> To enable WPA for an SSID, you must also enable Open authentication and/or Network EAP.</p>                                                                                                       |

**Table 4-6 SSID 802.11x Settings (continued)**

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WPA Pre-shared Key  | <p>Enter a key for the access point to support client devices using WPA key management.</p> <p>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.</p> <p>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.</p> |
| 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.                                                                                                                                                                                                                                                                                                                                                                                  |
| Proxy Mobile IP     | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Enable</b>—Use this setting to use this server for storing security association (SA) bindings for mobile agents. The access point uses this server to retrieve the SPI and key associated with the IP address of the client to which it is trying to roam. The SPI and key is then sent to the home agent to validate the client before allowing it to roam.</li> <li>• <b>Disable</b>—Use this setting if you do not want the server used for storing SA bindings for mobile agents.</li> </ul>                 |



**Table 4-6 SSID 802.11x Settings (continued)**

| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Accounting                   | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"><li>• Enable—Use this setting to indicate whether you want this server to record usage data of clients associating with the access point.</li><li>• Disable—Use this setting to turn off accounting for your wireless network</li></ul>                                                                                                                                                                                                                                                                                                                   |
| Accounting Server Priorities | <p>Select one of the following:</p> <ul style="list-style-type: none"><li>• Use Defaults—Use this setting to select the defaults.</li><li>• Use Server Group—Use this setting to specify a server group, then enter the name of the group.</li><li>• Customize—Use this setting to create a new server group, then enter the name of the group.</li><li>• Priority—Enter the server IP address or hostname.</li><li>• Auth Port—Enter the authentication port.<ul style="list-style-type: none"><li>– Acct Port—Enter the accounting port.</li></ul>or<ul style="list-style-type: none"><li>– Select a name from the list.</li></ul></li></ul> |

**Step 3** Click **Save**.

**Step 4** To delete an entry from the listbox, select it, then click **Delete**.

**Step 5** Complete the following to set global SSID properties:

**Table 4-7 Setting SSID 802.11x Global Properties**

| Field                                                      | Description                                                                                                                                                                                                                               |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Set Guest Mode SSID                                        | Enter the your access point's guest-mode SSID. The access point includes the SSID in its beacon and allows associations from client devices that do not specify an SSID.                                                                  |
| 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. |
| Force infrastructure device to associate only to this SSID | Select this option to force infrastructure devices to associate to the access point using the specified SSID.                                                                                                                             |

**Step 6** Complete the following to delete an SSID:

**Table 4-8 Setting SSID 802.11x Global Properties**

| Field          | Description                                                                                     |
|----------------|-------------------------------------------------------------------------------------------------|
| SSID           | Enter the SSID you want to delete, then click >>. The SSID is added to the SSID to Delete list. |
| 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 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).

## Configuring WEP 802.11x 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 802.11x**. The Security: WEP Key Manager 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 Template windows up until that point.

**Table 4-9** *WEP 802.11x Settings*

| Field                                 | Description                                                                                                                   |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Set Encryption Mode and Keys for VLAN | Enter the VLAN for which you want to set the encryption mode and keys.<br>If you enter None, properties are applied globally. |
| VLAN List                             | Lists the currently configured VLANs.<br>To remove a VLAN from the list, select it, then click <b>Delete</b> .                |

**Table 4-9 WEP 802.11x Settings (continued)**

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Encryption Modes |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| None             | Select this option if the device communicates only with client devices that are not using WEP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| WEP Encryption   | <p>Select this option if you want to use WEP key encryption.</p> <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Optional—Use this option to allow client devices to communicate with the access point either with or without WEP.</li> <li>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.</li> </ul> <p>Check one of the following:</p> <ul style="list-style-type: none"> <li>Cisco Compliant TKIP Features—Use this option to enable Temporal Key Integrity Protocol (TKIP).<br/>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.</li> <li>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.</li> <li>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.</li> </ul> |

**Table 4-9 WEP 802.11x Settings (continued)**

| Field                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cipher                      | <p>Select this option to enable Wi-Fi Protected Access (WPA) or Cisco Centralized Key Management (CKKM).</p> <p>Cipher suites are sets of encryption and integrity algorithms designed to protect radio communication on your wireless LAN.</p> <p>From the list, select the one of the cipher suites.</p> <ul style="list-style-type: none"> <li>• WEP—Wired equivalent privacy is the least secured cipher suite.</li> <li>• TKIP—Temporal key integrity protocol is the most secured cipher suite.</li> <li>• CKIP—Cisco Key Integrity Protocol is Cisco's WEP key permutation technique based on an early algorithm.</li> <li>• CMIC—Cisco Message Integrity Check) is Cisco's message integrity check mechanism designed to detect forgeries attracts.</li> </ul> |
| 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              | <p>Enter the type of encryption key used:</p> <ul style="list-style-type: none"> <li>• For 40-bit WEP keys, enter as 10 hexadecimal digits (0-9, a-f, or A-F).</li> <li>• For 128-bit WEP keys, enter as 26 hexadecimal digits (0-9, a-f, or A-F).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Key Size                    | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• 40 bit</li> <li>• 128 bit</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

**Table 4-9 WEP 802.11x Settings (continued)**

| Field                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Broadcast Key Rotation Interval | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Disable Rotation</b>—Use this setting to disable broadcast key rotation.</li> <li>• <b>Enable Rotation with Interval</b>—Use this setting for the access point to provide a dynamic broadcast WEP key and to change it at the selected interval.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| WPA Group Key Update            | <p>Select the appropriate checkbox to determine how frequently the access point changes and distributes the group key to WPA-enabled client devices.</p> <ul style="list-style-type: none"> <li>• <b>Enable Group Key Update on Membership Termination</b>—Select this setting if clients do not roam frequently among access points.<br/><br/>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.</li> <li>• <b>Enable Group Key Update on Member's Capability Change</b>—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.<br/><br/>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.</li> </ul> |

**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 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-3](#).
- 

## 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 current entries in the window and any entries you have made in other Template windows up until that point.

---

**Table 4-10 Backup Radius Server**

| Field                | Description                                                                                                                                                                                                  |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup Radius Server | Select one of the following: <ul style="list-style-type: none"><li>• Create—Use this setting to create a backup RADIUS server.</li><li>• Delete—Use this setting to delete a backup RADIUS server.</li></ul> |
| 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.                                                                                                                                                                            |

**Table 4-10 Backup Radius Server (continued)**

| Field               | Description                                                                                                                 |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Corporate Servers   |                                                                                                                             |
| Current Server List | Lists the servers that are currently configured.<br>To remove a server from the list, select it, then click <b>Delete</b> . |
| 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, select it from the list, then click **Delete**.



**Step 5** Complete the following to set default server priorities:

**Table 4-11 Default Server Priority Settings**

| Field                          | Description                                                                                                                                                                                                                                 |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EAP Authentication             | <ul style="list-style-type: none"><li>• Priority—Enter the server IP address or hostname.</li><li>• Auth Port—Enter the authentication port used by the server.</li><li>• Acct Port—Enter the accounting port used by the server.</li></ul> |
| MAC Authentication             |                                                                                                                                                                                                                                             |
| Accounting                     |                                                                                                                                                                                                                                             |
| Admin Authentication (RADIUS)  |                                                                                                                                                                                                                                             |
| Admin Authentication (TACACS+) |                                                                                                                                                                                                                                             |
| Proxy Mobile IP Authentication |                                                                                                                                                                                                                                             |

**Step 6** Complete the following to set global server properties:

**Table 4-12 Global Server Properties**

| Field                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Accounting Update Interval        | Enter the interval at which the accounting updates should be performed.<br><br>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 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.<br><br>Select one of the following: <ul style="list-style-type: none"> <li>• Disable—Use this setting to disable the feature.</li> <li>• 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).</li> </ul> |
| 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.                                                                                                                                                                                                                                                                                                      |

**Table 4-12 Global Server Properties (continued)**

| Field              | Description                                                                                                                                                                                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ISO Country Code   | Enter a unique two-letter code.<br><br>Information about the ISO 3166 country codes can be found at the following URL:<br><a href="http://www.iso.ch/iso/en/prods-services/iso3166ma/index.html">http://www.iso.ch/iso/en/prods-services/iso3166ma/index.html</a>                       |
| E.164 Country Code | Enter a three-digit code for special uses.<br><br>Information about the ISO 3166 country codes can be found at the following URL:<br><a href="http://www.iso.ch/iso/en/prods-services/iso3166ma/index.html">http://www.iso.ch/iso/en/prods-services/iso3166ma/index.html</a> .          |
| E.164 Area Code    | Enter a three-digit code based on the International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T) recommendations.<br><br>Information about ITU-T can be found at the following URL: <a href="http://www.itu.int/ITU-T/">http://www.itu.int/ITU-T/</a> |

**Step 7** Complete the following to delete RADIUS servers:

**Table 4-13 Deleting Servers and Server Groups**

| Field               | Description                                                                                                                                                                                                                                    |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Servers to Delete   | Lists the servers to delete.<br><br>To delete a server from the list, select it, then click <b>Delete</b> .                                                                                                                                    |
| 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.                                                                                                                                                                      |
| 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, select, then click >>. The group name is added to the list.<br><br>Click <b>Add Server to Delete List</b> 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 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).

## 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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-14** *Advanced Security*

| Field                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MAC Address Authentication     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MAC Addresses Authenticated by | <p>Select one of the following:</p> <ul style="list-style-type: none"><li>• <b>Local List Only</b>—Use this setting if you want the authentication to be stored on the access point, and enter MAC addresses.</li><li>• <b>Authentication Server Only</b>—Use this setting if you want the authentication to be stored on the server.</li><li>• <b>Authentication Server if not found in Local List</b>—Use this setting if you want to try MAC authentication list first and then automatically try the Authentication server list.</li></ul> |

**Table 4-14 Advanced Security (continued)**

| Field                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Holdoff Time                                   |                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Client Holdoff Time                            | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Disable Holdoff</b>—Use this setting to disable the client holdoff feature.</li> <li>• <b>Enable Holdoff with Interval</b>—Use this setting to specify the number of seconds a client device must wait before it can reattempt to authenticate following a failed authentication.</li> </ul>                                       |
| TKIP MIC Failure Holdoff Time (Radio0-802.11X) | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Disable Holdoff</b>—Use this setting to disable the TKIP MIC failure holdoff feature.</li> <li>• <b>Enable Holdoff with Interval</b>—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.</li> </ul> |
| Local MAC Address List                         |                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Local List                                     | <p>The local MAC address list is displayed in this listbox.</p> <p>To delete an entry, select it, then click <b>Delete</b>.</p>                                                                                                                                                                                                                                                                                    |
| New MAC Address                                | Enter the MAC address, then click <b>Add</b> .                                                                                                                                                                                                                                                                                                                                                                     |

**Table 4-14 Advanced Security (continued)**

| Field                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Radio0-802.11b EAP Authentication |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| EAP Reauthentication Interval     | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• Disable Reauthentication—Use this setting to disable reauthentication.</li> <li>• 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.</li> <li>• Enable Reauthentication with Interval given by Authentication Server—Use this setting to use the reauthentication period specified by the authentication server.</li> </ul> |
| 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.                                                                                                                                                                                                                                                                                                                                                                                      |
| Radio1-802.11a EAP Authentication |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| EAP Reauthentication Interval     | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• Disable Reauthentication—Use this setting to disable reauthentication.</li> <li>• 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.</li> <li>• Enable Reauthentication with Interval given by Authentication Server—Use this setting to use the reauthentication period specified by the authentication server.</li> </ul> |
| 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.                                                                                                                                                                                                                                                                                                                                                                                      |

**Table 4-14 Advanced Security (continued)**

| Field                                                  | Description                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Association Access List                                |                                                                                                                                                                                                                                                                                                                             |
| Filter client association with MAC address access list | Select one of the following: <ul style="list-style-type: none"> <li>• <b>Enable</b>— Use this setting to enable a MAC address filter for clients who are trying to associate with the access point.</li> <li>• <b>Disable</b>—Use this setting to prevent clients from associating based on their MAC addresses.</li> </ul> |
| Filter                                                 | Enter the MAC address filter or select one from the list.                                                                                                                                                                                                                                                                   |

**Step 3** Complete the following to delete local MAC addresses:

**Table 4-15 Deleting Local MAC Addresses**

| Field                   | Description                                                                                                    |
|-------------------------|----------------------------------------------------------------------------------------------------------------|
| 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.<br><br>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 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).



## 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.

Using this option you can do the following:

- Set up the network access server—See [Setting Up Network Access Servers, page 4-51](#).
- Set up user groups—[Setting Up User Groups, page 4-52](#).
- Set up individual users—[Setting Up Individual Users, page 4-54](#).
- Delete servers, groups, and users—[Deleting Servers, Groups, and Users, page 4-55](#).



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

### Setting Up Network Access Servers

#### Procedure

- Step 1** Complete the following:

**Table 4-16 Local Radius Server - Network Access Server**

| Field                          | Description                                                                                                  |
|--------------------------------|--------------------------------------------------------------------------------------------------------------|
| Current Network Access Servers | Lists the network access servers.<br>To remove a server from the list, select it, then click <b>Delete</b> . |
| 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.                     |

**Step 2** Click **Save**. The server appears in the Current Network Access Servers list.

**Step 3** Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).

## Setting Up User Groups

### Procedure

**Step 1** Complete the following:

**Table 4-17 Local Radius Server - User Groups**

| Field                            | Description                                                                                                                                                                                                                                                    |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Current User Group               | Lists the user groups.<br><br>To remove a group from the list, select it, then click <b>Delete</b> .                                                                                                                                                           |
| 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 4-17 Local Radius Server - User Groups (continued)**

| Field     | Description                                                                                                                                                                                                                                                                                              |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Lockout   | Select one of the following: <ul style="list-style-type: none"><li>• Infinite—Use this setting to manually unlock any locked-out users.</li><li>• Interval—Use this setting to specify the length of time that the access point locks out a user before the user can reattempt authentication.</li></ul> |
| 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 <b>Add</b> .                                                                                                                                                                                          |
| SSID List | Lists all the SSIDs.<br><br>To delete an SSID from the list, select it, then click <b>Delete</b> .                                                                                                                                                                                                       |

**Step 2** Click **Save**. The Group name is added to the Current User Group List.

**Step 3** Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).

## Setting Up Individual Users

### Procedure

**Step 1** Complete the following:

**Table 4-18 Local Radius Server - Individual Users**

| Field             | Description                                                                            |
|-------------------|----------------------------------------------------------------------------------------|
| Current User List | Lists the current usernames.                                                           |
| 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. |

**Step 2** Click **Save**. The user name is added to the Current User List.

**Step 3** Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).

## Deleting Servers, Groups, and Users

### Procedure

**Step 1** Complete the following:

**Table 4-19** *Deleting Servers, Groups, and Users*

| Field             | Description                                                                                                          |
|-------------------|----------------------------------------------------------------------------------------------------------------------|
| Server            | Enter the server you want to delete, then click <b>Add</b> . The server name is added to the Servers to Delete list. |
| Servers to Delete | Select the server to delete, then click <b>Delete</b> .                                                              |
| Group             | Enter the group you want to delete, then click <b>Add</b> . The group name is added to the Groups to Delete list.    |
| Groups to Delete  | Select the group to delete, then click <b>Delete</b> .                                                               |
| User              | Enter the user you want to delete, then click <b>Add</b> . The user name is added to the Servers to Delete list.     |
| Users to Delete   | Select the user to delete, then click <b>Delete</b> .                                                                |

**Step 2** Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).

## 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 4-56](#).
  - Hot Standby—See [Configuring Hot Standby, page 4-58](#).
  - CDP—See [Configuring CDP, page 4-60](#).
  - DNS—See [Configuring DNS, page 4-62](#).
  - MAC address filters—See [Configuring MAC Address Filters, page 4-63](#).
  - IP filters—See [Configuring IP Filters, page 4-66](#).
  - Ethertype filters—See [Configuring Ethertype Filters, page 4-72](#).
  - HTTP—See [Configuring HTTP, page 4-74](#).
  - Proxy Mobile IP—See [Configuring Proxy Mobile IP, page 4-75](#).
  - QoS policies—See [Configuring QoS Policies, page 4-78](#).
  - QoS radio 802.11x—See [Configuring QoS Radio 802.11x, page 4-82](#).
  - SNMP—See [Configuring SNMP, page 4-83](#).
  - NTP—See [Configuring NTP, page 4-87](#).
  - VLAN—See [Configuring VLAN, page 4-88](#).
  - ARP Cache—See [Configuring ARP Cache, page 4-90](#).

## 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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-20 Telnet/SSH**

| Field                      | Description                                                                                                                                                                                                                                                             |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Telnet                     | Select one of the following: <ul style="list-style-type: none"><li>• Enabled—Use this setting to enable Telnet access to the management system.</li><li>• Disabled—Use this setting to disable Telnet access to the management system.</li></ul>                        |
| Terminal Type              | Select one of the following: <ul style="list-style-type: none"><li>• Teletype—Use this setting if your terminal emulator does not support ANSI.</li><li>• ANSI—Use this setting to offer graphic features such as reverse video buttons and underlined links.</li></ul> |
| 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.                                                                                                                                                |
| Secure Shell Configuration |                                                                                                                                                                                                                                                                         |
| Secure Shell               | Select one of the following: <ul style="list-style-type: none"><li>• Enabled—Use this setting to enable secure shell.</li><li>• Disabled—Use this setting to disable secure shell.</li></ul>                                                                            |
| System Name                | Enter a system name for your access point.                                                                                                                                                                                                                              |
| Domain Name                | Enter a domain name for your access point.                                                                                                                                                                                                                              |

**Table 4-20 Telnet/SSH (continued)**

| Field                             | Description                                                                                                                          |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| RSA Key Size                      | Enter the additional bits used for authentication.<br><br><b>Note</b> For SSH, you must enter a key size or it will remain disabled. |
| Authentication Timeout (optional) | Enter the timeout in seconds, not to exceed 120 seconds for the length of time for authentication to take place.                     |
| Authentication Retries (optional) | 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 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).

## 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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-21 Hot Standby**

| Field                                       | Description                                                                                                                                                                                                                                  |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hot Standby Mode                            | Select one of the following: <ul style="list-style-type: none"><li>• Enabled—Use this setting to enable hot standby mode on the access point.</li><li>• Disabled—Use this setting to disable hot standby mode on the access point.</li></ul> |
| MAC Address for the Monitored 802.11bRadio  | 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.                                                                                                            |
| 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.                                                                       |

- Step 3** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-3](#).
- 

## 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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-22 CDP Settings**

| Field                          | Description                                                                                                                                                                                                                         |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco Discovery Protocol (CDP) | Select one of the following: <ul style="list-style-type: none"> <li>• <b>Enabled</b>—Use this setting to enable CDP on the access point.</li> <li>• <b>Disabled</b>—Use this setting to disable CDP on the access point.</li> </ul> |

**Table 4-22 CDP Settings (continued)**

| Field                         | Description                                                                                                                                                                                                       |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Packet Hold Time (optional)   | Enter the number of seconds other CDP-enabled devices should consider the access point's CDP information valid.                                                                                                   |
| Packets Sent Every (optional) | Enter the number of seconds between each CDP packet the access point sends.<br><br>This value should always be less than the packet hold time.                                                                    |
| Individual Port Enable        |                                                                                                                                                                                                                   |
| Ethernet                      | Select one of the following: <ul style="list-style-type: none"> <li>Enabled—Use this option to enable CDP on the Ethernet port.</li> <li>Disabled—Use this option to disable CDP on the Ethernet port.</li> </ul> |
| Radio0-802.11b                | Select one of the following: <ul style="list-style-type: none"> <li>Enabled—Use this option to enable CDP on the radio port.</li> <li>Disabled—Use this option to disable CDP on the radio port.</li> </ul>       |
| Radio0-802.11a                | Select one of the following: <ul style="list-style-type: none"> <li>Enabled—Use this option to enable CDP on the radio port.</li> <li>Disabled—Use this option to disable CDP on the radio port.</li> </ul>       |

- Step 3** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-3](#).
- 

## 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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-23 DNS Settings**

| Field                    | Description                                                                                                                                                                                                             |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Domain Name System (DNS) | Select one of the following: <ul style="list-style-type: none"> <li>• <b>Enabled</b>—Use this setting if your network uses DNS.</li> <li>• <b>Disabled</b>—Use this setting if you network does not use DNS.</li> </ul> |
| Domain Name (optional)   | Enter the domain name.                                                                                                                                                                                                  |

**Table 4-23 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 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).

## 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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-24 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.<br>To delete a filter from the list, select it, then click <b>Delete Filter</b> .                                                                                                |
| Filter Index     | Enter a number from 700 to 799. The number you assign creates an access control list (ACL) for the filter.                                                                                                               |
| Add MAC Address  | Enter the MAC address.                                                                                                                                                                                                   |
| Mask             | Enter the subnet mask.                                                                                                                                                                                                   |
| Action           | From the list, select one of the following actions: <ul style="list-style-type: none"> <li>Forward—Use this setting to forward the MAC addresses.</li> <li>Block—Use this setting to block the MAC addresses.</li> </ul> |
| VLAN ID          | Enter the VLAN identification number then click >>.<br>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.                                                                                                                  |

**Table 4-24 MAC Address Filters (continued)**

| Field           | Description                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Apply Filter to |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| FastEthernet    | Select one of the following: <ul style="list-style-type: none"> <li>• Incoming—Use this option to apply the filter to the incoming packets.</li> <li>• Outgoing—Use this option to apply the filter to the outgoing packets.</li> </ul> Click <b>AddFilter</b> .                                                                                                                                                                |
| Radio0-802.11b  |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Radio0-802.11a  |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Default Action  | Select one of the following: <ul style="list-style-type: none"> <li>• Block All</li> <li>• Forward All</li> </ul> then click <b>Update</b> .<br><br>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.<br><br>To remove the MAC address from the Filters Classes list, select it, then click <b>Delete</b> .                                                                                                                                                                                                                                                                                                      |
| Delete Filters  |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Filters         | To delete a filter, select it from the list, then click <b>Delete</b> .                                                                                                                                                                                                                                                                                                                                                         |
| Filter Index    | Enter the filter index number.                                                                                                                                                                                                                                                                                                                                                                                                  |
| VLAN ID         | Enter the VLAN identification number, then click >> to add it to the list.<br><br>To delete a VLAN ID from the list, click <<.                                                                                                                                                                                                                                                                                                  |
| Bridge-Group    | Enter a valid bridge group number.                                                                                                                                                                                                                                                                                                                                                                                              |

**Table 4-24 MAC Address Filters (continued)**

| Field              | Description                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remove Filter from |                                                                                                                                                                                                                  |
| FastEthernet       | Select one of the following:                                                                                                                                                                                     |
| Radio0-802.11b     | <ul style="list-style-type: none"> <li>• Incoming—Use this option to remove the filter from the incoming packets.</li> <li>• Outgoing—Use this option to remove the filter from the outgoing packets.</li> </ul> |
| Radio0-802.11a     |                                                                                                                                                                                                                  |
|                    | Click <b>AddFilter</b> .                                                                                                                                                                                         |

**Step 3** Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).

## 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.

If you use this template to apply IP filters to access points with versions 12.2(4)JA, 12.2(4)JA1, or 12.2(8)JA, the configuration commands generated through the template may not display correctly on the access point's UI.

To work around this problem, do the following:

1. Use this template to create the IP filters and select **Create Only**.
2. Click Preview.
3. Copy and paste the commands in the Preview window into a custom template (see [Configuring Custom Values, page 4-99](#)).



4. Note the following WLSE-generated commands:

```
permit/deny ip source-ip source-mask dest-ip dest-mask
permit/deny tcp/udp any any eq port-number
```

5. Change the commands as follows:

- For versions 12.2(4)JA or 12.2(4)JA1, enter the following custom values:

```
permit/deny ip source-ip source-mask any
permit/deny tcp/udp any eq port-number any
```

- For version 12.2(8)JA, enter the following custom values:

```
permit/deny tcp/udp any eq port-number any
```

### 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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-25 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.<br><br>To delete a filter from the list, select it, then click <b>Delete Filter</b> . |

**Table 4-25 IP Filters (continued)**

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Filter Name         | Enter a name for the filter.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Default Action      | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Block All—Use this setting to block all IP addresses.</li> <li>Forward All—Use this setting to forward all IP addresses.</li> </ul> <p>then click <b>Update</b>.</p>                                                                                                                                                                                                                    |
| IP Address          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Destination Address | <p>Enter the IP address that you want to filter.</p> <p><b>Note</b> This is not valid for versions 12.2(4) or 12.2(4)JA1.</p>                                                                                                                                                                                                                                                                                                                                                     |
| Mask                | <p>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).</p> <p>If you enter 255.255.255.255 as the mask, the access point accepts any IP address.</p> <p>If you enter 0.0.0.0, the access point looks for an exact match with the IP address you entered.</p> <p>The mask you enter in this field behaves the same way that a mask behaves when you enter it in the CLI.</p> |
| Source Address      | Enter the IP address you want to filter.                                                                                                                                                                                                                                                                                                                                                                                                                                          |

**Table 4-25 IP Filters (continued)**

| Field       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mask        | <p>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.</p> <p>If you are using the 12.2(4)JA release, entering 0.0.0.0 as the mask causes the access point to accept any IP address.</p> <p>If you enter 255.255.255.255, the access point looks for an exact match with the IP address you entered in the IP Address field.</p> <p>If you are using the 12.2(8)JA or later release, entering 255.255.255.255 as the mask causes the access point to accept any IP address.</p> <p>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.</p> |
| Action      | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"><li>• Forward —Use this setting to forward the IP address.</li><li>• Block —Use this setting to block the IP address.</li></ul> <p>Click <b>Add</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| IP Protocol |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| IP Protocol | <p>Do one of the following:</p> <ul style="list-style-type: none"><li>• From the list, select a protocol.</li><li>• Enter a custom protocol.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Table 4-25 IP Filters (continued)**

| Field        | Description                                                                                                                                                                                                                                    |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action       | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Forward —Use this setting to forward the IP protocol.</li> <li>Block —Use this setting to block the IP protocol.</li> </ul> <p>Click <b>Add</b>.</p> |
| UDP/TCP Port |                                                                                                                                                                                                                                                |
| TCP Port     | <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>From the list, select a TCP port.</li> <li>Enter a custom port.</li> </ul>                                                                                              |
| Action       | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Forward —Use this setting to forward the TCP port.</li> <li>Block —Use this setting to block the IP TCP port.</li> </ul> <p>Click <b>Add</b>.</p>    |
| UDP Port     | <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>From the list, select a TCP port.</li> <li>Enter a custom port.</li> </ul>                                                                                              |
| Action       | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Forward —Use this setting to forward the UDP port.</li> <li>Block —Use this setting to block the IP UDP port.</li> </ul> <p>Click <b>Add</b>.</p>    |
| VLAN ID      | <p>Enter the VLAN identification number then click &gt;&gt;.</p> <p>To remove a VLAN ID from the list, select it, then click &lt;&lt;.</p>                                                                                                     |

**Table 4-25 IP Filters (continued)**

| Field              | Description                                                                                                                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Apply Filter to    |                                                                                                                                                                                                                                                                        |
| FastEthernet       | Select one of the following: <ul style="list-style-type: none"> <li>• Incoming—Use this option to apply the filter to the incoming packets.</li> <li>• Outgoing—Use this option to apply the filter to the outgoing packets.</li> </ul> Click <b>Apply</b> .           |
| Radio0-802.11b     |                                                                                                                                                                                                                                                                        |
| Radio0-802.11a     |                                                                                                                                                                                                                                                                        |
| Filters Classes    | Lists the currently configured filters.<br>To delete a filter, select it, then click <b>Delete</b> .                                                                                                                                                                   |
| Delete Filters     |                                                                                                                                                                                                                                                                        |
| Filters            | To delete a filter, select it from the list, then click <b>Delete</b> .                                                                                                                                                                                                |
| Filter Name        | Enter the filter name.                                                                                                                                                                                                                                                 |
| VLAN ID            | Enter the VLAN identification number, then click >> to add it to the list.<br>To remove a VLAN ID from the list, click <<.                                                                                                                                             |
| Remove Filter from |                                                                                                                                                                                                                                                                        |
| FastEthernet       | Select one of the following: <ul style="list-style-type: none"> <li>• Incoming—Use this option to remove the filter from the incoming packets.</li> <li>• Outgoing—Use this option to remove the filter from the outgoing packets.</li> </ul> Click <b>AddFilter</b> . |
| Radio0-802.11b     |                                                                                                                                                                                                                                                                        |

- Step 3** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-3](#).

## 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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-26 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.<br><br>To remove a filter from the list, select it, then click <b>Delete Filter</b> . |

**Table 4-26** *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: <ul style="list-style-type: none"> <li>Forward —Use this setting to forward the traffic.</li> <li>Block —Use this setting to block the traffic.</li> </ul>                                                   |
| VLAN ID         | Enter the VLAN identification number then click >>. <p>To remove a VLAN ID from the list, select it, then click &lt;&lt;.</p>                                                                                                                            |
| 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: <ul style="list-style-type: none"> <li>Incoming—Use this option to apply the filter to the incoming packets.</li> <li>Outgoing—Use this option to apply the filter to the outgoing packets.</li> </ul> Click <b>Apply</b> . |
| Radio0-802.11b  |                                                                                                                                                                                                                                                          |
| Radio0-802.11a  |                                                                                                                                                                                                                                                          |
| Default Action  | From the list, select one of the following: <ul style="list-style-type: none"> <li>Block All—Use this setting to block all.</li> <li>Forward All—Use this setting to forward all.</li> </ul> then click <b>Update</b> .                                  |
| Filters Classes | Lists the currently configured filters. <p>To delete a filter, select it, then click <b>Delete</b>.</p>                                                                                                                                                  |

**Table 4-26** *Ethertype Filters (continued)*

| Field              | Description                                                                                                                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Delete Filters     |                                                                                                                                                                                                                                                                        |
| Filters            | To delete a filter, select it from the list, then click <b>Delete</b> .                                                                                                                                                                                                |
| Filter Index       | Enter the filter index.                                                                                                                                                                                                                                                |
| VLAN ID            | Enter the VLAN identification number, then click <b>Add</b> to add it to the list.<br><br>To delete a VLAN ID from the list, click <b>Delete</b> .                                                                                                                     |
| Bridge-Group       | Enter a valid bridge group number.                                                                                                                                                                                                                                     |
| Remove Filter from |                                                                                                                                                                                                                                                                        |
| FastEthernet       | Select one of the following: <ul style="list-style-type: none"> <li>• Incoming—Use this option to remove the filter from the incoming packets.</li> <li>• Outgoing—Use this option to remove the filter from the outgoing packets.</li> </ul> Click <b>AddFilter</b> . |

**Step 3** Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).

## 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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-27 HTTP**

| Field                                    | Description                                                                                                                                                                                                                                                              |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Allow Web-based Configuration Management | Select one of the following: <ul style="list-style-type: none"><li>• <b>Enabled</b>—Use this setting to allow web-based browsing to the management system.</li><li>• <b>Disabled</b>—Use this setting to disallow web-based browsing to the management system.</li></ul> |
| HTTP Port                                | Enter the port through which the access point provides 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 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).

## Configuring Proxy Mobile IP

Use this option to allow access points to help 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 for the client.

**Procedure**

**Step 1** Select **Services > Proxy Mobile IP**. The Services: Proxy Mobile IP 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 Template windows up until that point.

**Table 4-28 Proxy Mobile IP**

| Field                                         | Description                                                                                                                                                                                                                                                                             |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Proxy Mobile IP                               | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>Enabled—Use this setting to enable the proxy mobile IP feature on the access point.</li> <li>Disabled—Use this setting to disable the proxy mobile IP features.</li> </ul>                                   |
|                                               | Select either Radio 802-11b or Radio 802.11a                                                                                                                                                                                                                                            |
| GRE encapsulation in the Registration Request | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>Enabled—Use this setting to enable the access point to request the encapsulation type in all mobile node registration requests.</li> <li>Disabled—Use this setting to disable this feature.</li> </ul>       |
| Reverse Tunnel in the Registration Request    | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>Enabled—Use this setting to enable the access point to request reverse tunnel encapsulation in all mobile mode registration requests.</li> <li>Disabled—Use this setting to disable this feature.</li> </ul> |

**Table 4-28 Proxy Mobile IP (continued)**

| Field                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authoritative Access Points (Hostname or IP Address) | Enter the hostname or IP address of up to three authoritative access points (AAPs) on the wireless network. At least one AAP is required for the proxy mobile IP feature to work.                                                                                                                                                                                                                                                                                                     |
| Current SA Bindings List                             | Lists the clients that are able to establish contact with a foreign agent in another network segment or network other than the client's home network.                                                                                                                                                                                                                                                                                                                                 |
| New/Edit SA Binding                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| IP Address Range                                     | Enter the range IP addresses within which client devices must reside in order to be valid.                                                                                                                                                                                                                                                                                                                                                                                            |
| Security Parameter Index                             | <p>Enter an index for the IP address range.</p> <p>The index is a 32-bit number (8 hexadecimal digits) assigned to the initiator of the security association request by the receiving IPSec endpoint. On receiving a packet, the destination address, protocol, and SPI are used to determine the security association. The security association allows the node to authenticate or decrypt the packet according to the security policy configured for that security association.</p> |
| Key                                                  | <ol style="list-style-type: none"><li>1. Enter a key (ASCII or Hexadecimal) used to access a foreign agent.</li><li>2. Select ASCII or Hexadecimal to indicate the type of key entered.</li></ol>                                                                                                                                                                                                                                                                                     |

- Step 3** Click **Add**. The entry is added to the Current SA Bindings list.
- Step 4** To Delete and entry, select it from the Current SA Bindings list, then click **Delete**.
- Step 5** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-3](#).

## 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** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-29 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.                   |

**Table 4-29 QoS Policies (continued)**

| Field                                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| QoS Element for Wireless Phones                                   | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• Enable—Use this setting to specify that wireless phone clients' traffic has a higher priority than the rest of the clients.</li> <li>• Disable—Use this setting to disable this feature.</li> </ul>                                                                                                                                                                                                                                             |
| IGMP Snooping Helper                                              | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Disable—Use this setting to disable this feature.</li> </ul> |
| AVVID Priority Mapping - Map Ethernet Packets with CoS 5 to CoS 6 | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• 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).</li> <li>• No—Use this setting if your network is not based on the Cisco AVVID specification.</li> </ul>                                                                                                                                                                             |
| Policy List                                                       | <p>Lists the names of the existing policies.</p> <p>To remove a name from the list, select it, then click <b>Delete Policy</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                          |
| Policy Name                                                       | Enter a name for the policy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Classifications                                                   | <p>Lists the classifications assigned to that policy.</p> <p>To delete a classification, select it, then click <b>Delete</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                            |

**Table 4-29 QoS Policies (continued)**

| Field                                          | Description                                                                                                                                                                        |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 <b>Add</b> .             |
| 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 <b>Add</b> .                |
| 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 <b>Add</b> . |
| Apply Class of Service                         |                                                                                                                                                                                    |
| 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 <b>Add</b> .                 |
| 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 <b>Add</b> .  |
| 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 <<.                                                                                                                                       |

**Table 4-29 QoS Policies (continued)**

| Field                              | Description                                                                                                                                                                                                                                                         |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Apply Policy to                    |                                                                                                                                                                                                                                                                     |
| FastEthernet                       | Select one of the following: <ul style="list-style-type: none"><li>• Incoming—Use this option to apply the filter to the incoming packets.</li><li>• Outgoing—Use this option to apply the filter to the outgoing packets.</li></ul> Click <b>ApplyPolicy</b> .     |
| Radio0-802.11b                     |                                                                                                                                                                                                                                                                     |
| Radio0-802.11a                     |                                                                                                                                                                                                                                                                     |
| Remove Policy from Interface/VLANs |                                                                                                                                                                                                                                                                     |
| Policy List                        | To delete a policy, select it from the list, then click <b>Delete</b> .                                                                                                                                                                                             |
| 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: <ul style="list-style-type: none"><li>• Incoming—Use this option to remove the filter from the incoming packets.</li><li>• Outgoing—Use this option to remove the filter from the outgoing packets.</li></ul> Click <b>AddPolicy</b> . |
| Radio0-802.11B                     |                                                                                                                                                                                                                                                                     |
| Radio0-802.11A                     |                                                                                                                                                                                                                                                                     |
| Remove Policy Map and Class Map    |                                                                                                                                                                                                                                                                     |
| Policy List                        | Lists the policies. Select the policy to remove, then click <b>Delete</b> .                                                                                                                                                                                         |
| Policy Name                        | Enter the policy name, then click <b>Add Policy</b> . 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 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).

## Configuring QoS Radio 802.11x

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 802.11x**. The Services: QoS Policies - Traffic Class Definition 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 Template windows up until that point.

**Table 4-30 QoS Radio 802.11x Traffic Class Definition**

| Field               | Description                              |
|---------------------|------------------------------------------|
| 802.11e 4 Level Qos | Select for version 12.2(13)JA and above. |
| 802.1D 8 Level Qos  | Select for versions below 12.2(13)JA.    |



**Table 4-30 QoS Radio 802.11x Traffic Class Definition (continued)**

| Field                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Background           | <ul style="list-style-type: none"> <li>Min Contention Window—Enter the minimum contention window value. The access point computes Contention Window values.</li> <li>Max Contention Window—Enter the maximum contention window value. The access point computes Contention Window values.</li> <li>Fixed Slot Time—Enter a value for a fixed slot time.</li> </ul>                                                                               |
| Best Effort          |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Video                |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Voice                |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 802.1D 8 Level QoS   | Select if you are setting 8 QoS levels.                                                                                                                                                                                                                                                                                                                                                                                                          |
| Best Effort          | <ul style="list-style-type: none"> <li>Min Contention Window—Enter the minimum contention window value. The value listed is to the power of 2. The access point computes Contention Window values.</li> <li>Max Contention Window—Enter the maximum contention window value. The value listed is to the power of 2. The access point computes Contention Window values.</li> <li>Fixed Slot Time—Enter a value for a fixed slot time.</li> </ul> |
| Background           |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Spare                |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Excellent Effort     |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Controlled Load      | <ul style="list-style-type: none"> <li>Fixed Slot Time—Enter a value for a fixed slot time.</li> </ul>                                                                                                                                                                                                                                                                                                                                           |
| Video <100ms Latency |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Voice <100ms Latency |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Network Control      |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

**Step 3** Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).

## Configuring SNMP

Use this option to configure settings for notifications to be sent to an SNMP server.

**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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-31 SNMP**

| Field                                     | Description                                                                                                                                                                                                                                                             |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Simple Network Management Protocol (SNMP) | Select one of the following: <ul style="list-style-type: none"> <li>• Enabled—Use this setting to allow event notifications to be sent to an SNMP server.</li> <li>• Disabled—Use this setting to disallow event notifications to be sent to an SNMP server.</li> </ul> |
| System Name (optional)                    | Enter the name of the access point.<br><br>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 (optional)                | Enter a description of the access point's physical location, such as the building or room in which it is installed.                                                                                                                                                     |
| System Contact (optional)                 | Enter the name the system administrator responsible for the access point.                                                                                                                                                                                               |

**Table 4-31 SNMP (continued)**

| Field                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNMP Request Communities  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Current Community Strings | <p>Lists the current community strings.</p> <p>To delete an entry, select it, then click <b>Delete</b>.</p> <p>To edit an entry, select it.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Edit Community Strings    | <ul style="list-style-type: none"><li>• <b>SNMP Community</b>—The SNMP Community value for the selected community string displays. SNMP community strings authenticate access to MIB objects and function as embedded passwords.</li><li>• <b>Object Identifier (Optional)</b>—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.<p>For for example, if you enter <b>iso</b> 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.)</p></li><li>• Select one of the following one of the following: Read-Only or Read-Write.</li></ul> |

**Table 4-31 SNMP (continued)**

| Field                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNMP Trap Destination                         | <ol style="list-style-type: none"> <li>1. Enter the IP address or the host name of the server running the SNMP Management software.</li> <li>2. Select one of the following: <ul style="list-style-type: none"> <li>– Enable All Trap Notifications—Use this setting to enable all traps.</li> <li>– Enable Specific Traps—Use this setting to select one or more of trap types.</li> </ul> </li> <li>3. Click <b>Save</b>.</li> </ol> |
| Delete Communities and SNMP Trap Destinations |                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Community                                     | Enter the community to delete, then click >>.                                                                                                                                                                                                                                                                                                                                                                                          |
| Communities to Delete                         | <p>Lists the communities to be deleted.</p> <p>To delete a community, select it, then click &lt;&lt;.</p>                                                                                                                                                                                                                                                                                                                              |
| 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                        | <p>Lists the SNMP trap destinations to be deleted.</p> <p>To delete a destination, select it, then click &lt;&lt;.</p>                                                                                                                                                                                                                                                                                                                 |

**Step 3** Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).

## Configuring NTP

This option allows you to configure the date and time on using NTP (Network Time Protocol) servers.

### Procedure

**Step 1** Select **Services > NTP**. The Services: NTP - Network Time Protocol 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 Template windows up until that point.

**Table 4-32 NTP**

| Field                             | Description                                                                                                                                                                                                        |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NTP Server                        |                                                                                                                                                                                                                    |
| Network Time Protocol (NTP)       | Select one of the following: <ul style="list-style-type: none"><li>• Enabled—Use this setting to use of NTP.</li><li>• Disabled—Use this setting to disallow the use NTP.</li></ul>                                |
| Time Server IP Address (optional) | 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: <ul style="list-style-type: none"><li>• Yes—Use this setting to use daylight savings time.</li><li>• No—Use this setting if you are not going to use daylight savings time.</li></ul> |
| 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 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-3](#).
- 

## 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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-33 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.<br><br>To delete a VLAN from the list, select it, then click <b>Delete</b> . |
| Create VLAN            |                                                                                                       |
| VLAN ID                | Enter a VLAN ID.                                                                                      |

**Table 4-33 VLAN (continued)**

| Field                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bridge-Group                           | <p>Enter the bridge group number.</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul> <p>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.</p> <p>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.</p> |
| Enable Public Secure Packet Forwarding | <p>Select to enable public secure packet forwarding (PSPF).</p> <p>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.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Radio0-802.11B<br>Radio1-802.11A       | Select the radio.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SSID                                   | Enter an SSID, then click <b>Add</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

**Table 4-33 VLAN (continued)**

| Field                            | Description                                                                                       |
|----------------------------------|---------------------------------------------------------------------------------------------------|
| Delete VLANs                     |                                                                                                   |
| VLANs to Delete                  | Lists the VLANs to delete.<br>To delete VLAN from the list, select it, then click <b>Delete</b> . |
| VLAN ID                          | Enter the identification number of the VLAN you want to add to the VLANs to Delete list.          |
| Radio0-802.11B<br>Radio1-802.11A | Select the radio to delete.                                                                       |
| SSID                             | Enter the SSID, then click <b>Add</b> . 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 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).

## 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: ARP Caching 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 Template windows up until that point.

**Table 4-34 ARP Cache**

| Field                                                                               | Description                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Client ARP Caching                                                                  | Select one of the following: <ul style="list-style-type: none"> <li>• <b>Enable</b>—Use this setting to allow ARP caching.</li> <li>• <b>Disable</b>—Use this setting to disable the feature.</li> </ul> |
| 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 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-3](#).

## 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 4-92](#).
  - Notification Options—See [Setting Notification Options, page 4-94](#).
- 

**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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-35 Configuration Options**

| Field                                     | Description                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disposition of Events (by Severity Level) |                                                                                                                                                                                                                                                                                                                                                     |
| Emergency                                 | <div>Check one or more of the following for each of the events:</div> <ul style="list-style-type: none"><li>• Display on Event Log</li><li>• Notify via SNMP/Syslog Trap</li><li>• Record for SNMP/Syslog History Table</li><li>• Display on Telnet/SSH Monitor</li></ul>                                                                           |
| Alert                                     |                                                                                                                                                                                                                                                                                                                                                     |
| Critical                                  |                                                                                                                                                                                                                                                                                                                                                     |
| Error                                     |                                                                                                                                                                                                                                                                                                                                                     |
| Warning                                   |                                                                                                                                                                                                                                                                                                                                                     |
| Notification                              |                                                                                                                                                                                                                                                                                                                                                     |
| Information                               |                                                                                                                                                                                                                                                                                                                                                     |
| Debugging                                 |                                                                                                                                                                                                                                                                                                                                                     |
| Time Stamp Format for Future Events       | <div>Select one of the following:</div> <ul style="list-style-type: none"><li>• System Uptime—Use this setting to use the system uptime in the timestamp.</li><li>• Global Standard Time—Use this setting to use the global standard time in the timestamp.</li><li>• Local Time—Use this setting to use the local time in the timestamp.</li></ul> |
| 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 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-3](#).

## 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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-36 Notification Options**

| Field                                   | Description                                                                                                                                                                                                                     |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Events Generate Syslog Messages         | Select one of the following: <ul style="list-style-type: none"> <li>• <b>Enable</b>—Use this setting to allow events to generate syslog messages.</li> <li>• <b>Disable</b>—Use this setting to disable the feature.</li> </ul> |
| 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 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-3](#).
- 

## 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 4-95](#).
  - WDS—See [Configuring WDS, page 4-96](#).
- 

## 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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-37 AP Configuration**

| Field             | Description                                                                                                                                                                             |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Wireless Services | Select one of the following: <ul style="list-style-type: none"> <li>• Enabled—Use this setting to enable services.</li> <li>• Disabled—Use this setting to disable services.</li> </ul> |
| 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 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).

## 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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-38 WDS Settings**

| Field                                   | Description                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Global Properties                       |                                                                                                                                                                                                                                                                                                                                   |
| Use this AP as Wireless Domain Services | Select to enable the access point to provide Wireless Domain Services.                                                                                                                                                                                                                                                            |
| Wireless Domain Services Priority       | Enter a number between 1 and 255 to indicate the priority.<br><br>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.                                                                                                                             |
| WNM IP Address                          | Enter the access point's IP address.                                                                                                                                                                                                                                                                                              |
| Server Groups                           |                                                                                                                                                                                                                                                                                                                                   |
| Server Group List                       | Lists the configured servers.<br><br>To delete a server, select it, then click <b>Delete</b> .                                                                                                                                                                                                                                    |
| Server Group Name                       | Enter the name of the server group. <ul style="list-style-type: none"> <li>• Priority—Enter the server IP address or hostname.</li> <li>• Auth Port—Enter the authentication port.</li> <li>• Acct Port—Enter the accounting port.</li> </ul> or <ul style="list-style-type: none"> <li>• Select a name from the list.</li> </ul> |

**Table 4-38 WDS Settings (continued)**

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Use Group for       | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>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.</li> <li>Client Authentication—Use this setting to provide client authentication services.</li> </ul> <p>Select the type of client authentication.</p>                                                                       |
| SSID                | <p>Enter the SSID or leave blank to apply to all SSIDs, then click &gt;&gt; to add to the SSID List.</p> <p>The click <b>Save</b>.</p>                                                                                                                                                                                                                                                                                                                                                            |
| Delete Server Group |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Server Group Name   | Enter the server group to delete.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Use Group For       | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>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.</li> <li>Client Authentication—Use this setting to provide client authentication services.</li> </ul> <p>Select the type of client authentication.</p> <p>Then click &gt;&gt; to add to the Server Group List to Delete.</p> |

**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 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-3](#).
- 

## Configuring Custom Values

This option enables to 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**

This option should be used only by advanced users.

---

Templates with custom values are not validated.

### Procedure

---

**Step 1** Select **Configure > Templates > Custom Values**. The Custom IOS Values dialog box appears.



**Note**

Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

---



**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 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-3](#).
- 

## Non-IOS Templates

When you create or edit a non-IOS configuration template, the following choices appear in the left pane of the Templates window:



### Note

Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

---

When you create or edit a configuration template, the following choices appear in the left pane of the Templates window:

1. **Template Name**—See [Naming the Template, page 4-101](#).
2. **Template Categories**



### Note

Any or all of the template categories can be completed in any order.

---

- **Basic Settings**—See [Using Basic Settings, page 4-102](#).
- **Association**—See [Setting Up Association, page 4-107](#).
- **Ethernet**—See [Configuring the Ethernet Port, page 4-149](#).
- **11b Radio**—See [Configuring the 11b Radio, page 4-157](#).
- **11a Radio**—See [Configuring the 11a Radio, page 4-175](#).
- **Security**—See [Defining the Security Settings, page 4-208](#).
- **Services**—See [Configuring Services, page 4-221](#).

- **Events**—See [Configuring Events](#), page 4-245.
  - **Custom Values**—See [Configuring Custom Values](#), page 4-251.
3. **Preview**—See [Previewing the Template](#), page 4-252.
  4. **Save**—See [Saving the Template](#), page 4-253.

## Naming the Template

This option enables to you to name the template.

### Procedure



**Note** Clicking **Clear** removes all the entries you have made.

- Step 1** Select **Template Name**. The Template Name dialog box appears:

| Field       | Description                                                                                                                                                                                      |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name        | Enter a name for the template.<br>See <a href="#">Naming Guidelines</a> , page A-1.                                                                                                              |
| Description | Enter a description of the purpose of the template.<br>See <a href="#">Naming Guidelines</a> , page A-1.<br>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 [Template Categories](#), page 4-100.

## 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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-39 Basic Settings**

| Field         | Description                                                                                                                                                                                                                                                |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reboot Device | From the list, select Yes if you want to allow device reboots.                                                                                                                                                                                             |
| SysName       | <p>Enter a system name.</p> <p>The system name appears in the titles of the management system pages and in the access point's Association Table page.</p> <p>This is not an essential setting, but it helps identify the access point on your network.</p> |
| SysLocation   | <p>Enter the system's location.</p> <p>This is not an essential setting, but it helps identify the access point on your network.</p>                                                                                                                       |
| SysContact    | <p>Enter a contact name.</p> <p>This is not an essential setting but it helps identify the person responsible for the access point on your network.</p>                                                                                                    |

**Table 4-39 Basic Settings (continued)**

| Field                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuration Server Protocol | <p>Set this entry to match the network's method of IP address assignment.</p> <p>From the list, select one of the following options:</p> <ul style="list-style-type: none"><li>• None-Static IP—Use this if your network does not have an automatic system for IP address assignment.</li><li>• BOOTP—Use this if your network uses Bootstrap Protocol, in which IP addresses are hard-coded based on MAC addresses.</li><li>• DHCP—Use this if your network uses Dynamic Host Configuration Protocol, in which IP addresses are “leased” for predetermined periods of time.</li></ul> |
| Default Subnet Mask           | <p>Enter an IP subnet mask to identify the subnetwork so the IP address can be recognized on the LAN.</p> <p>If DHCP or BOOTP is not enabled, this field is the subnet mask.</p> <p>If DHCP or BOOTP is enabled, this field provides the subnet mask only if no server responds to the access point's DHCP or BOOTP request.</p>                                                                                                                                                                                                                                                       |
| Default Gateway               | <p>Enter the IP address of your default Internet gateway.</p> <p>The entry 255.255.255.255 indicates no gateway.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

**Table 4-39 Basic Settings (continued)**

| Field                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Radio Service Set ID (SSID) | <p>Enter any alphanumeric, case-sensitive string, from 1 to 32 characters long.</p> <p>The SSID 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 and provides access to VLANs by wireless client devices.</p> <p>Several access points on a network or subnetwork can share an SSID.</p> |

**Table 4-39 Basic Settings (continued)**

| Field           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Role in Network | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"><li>• Access Point—Use this setting if the access point is connected to the wired LAN.</li><li>• Repeater—Use this setting for access points not connected to the wired LAN.</li><li>• Survey Client—Use this setting when performing a site survey for a repeater access point. When you select this setting, clients are not allowed to associate and the bridge's STP function is disabled.</li><li>• Root Bridge—Use this setting to set a bridge as the root bridge. (One bridge in each group of bridges must be set as the root bridge.) The root bridge cannot associate with another root bridge.</li><li>• Non-Root Bridge w/ Client—Use this setting for non-root bridges that accept associations from client devices and for bridges acting as repeaters. A non-root bridge will only associate to another bridge (root or non-root).</li><li>• Non-Root Bridge w/o Client—Use this setting for non-root bridges that should not accept associations from client devices. A non-root bridge (without clients) can connect to a wired LAN and only associates to another bridge (root or non-root).</li></ul> |

**Table 4-39 Basic Settings (continued)**

| Field                                        | Description                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ensure Compatibility with 1MB/sec Clients    | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Enable</b>— Use this setting to operate at a maximum speed of one megabit per second.</li> <li>• <b>Disable</b>—Use this setting if you do not want devices to operate at a maximum speed of one megabit per second.</li> </ul>                                                                   |
| Ensure Compatibility with 2MB/sec Clients    | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Enable</b>— Use this setting to operate at a maximum speed of two megabits per second.</li> <li>• <b>Disable</b>—Use this setting if you do not want devices to operate at a maximum speed of two megabits per second.</li> </ul>                                                                 |
| Ensure Compatibility with non-Aironet 802.11 | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Enable</b>—Use this setting to automatically configure the device to be compatible with other Cisco devices on your wireless LAN.</li> <li>• <b>Disable</b>—Use this setting to not automatically configure the device to be compatible with other Cisco devices on your wireless LAN.</li> </ul> |

**Step 2** Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).



## Setting Up Association

Use this option to set up spanning tree protocol (STP) on bridges and to set up filtering to control the flow of data through the access point.

### Procedure

- 
- Step 1** Select **Association**. The menu expands and the Association dialog box displays in the right pane.
- Step 2** Select one of the following from the Association menu:
- Spanning Tree—See [Defining Spanning Tree Protocol, page 4-108](#).
  - Address Filters—See [Defining Address Filters, page 4-110](#).
  - Ethertype Filters—See [Defining Ethertype Filters, page 4-112](#).
  - IP Protocol Filters—See [Defining IP Protocol Filters, page 4-116](#).
  - IP Port Filters—See [Defining IP Port Filters, page 4-120](#).
  - Policy Groups—See [Configuring Policy Groups, page 4-124](#).
  - VLANs—See [Configuring VLANs, page 4-126](#).
  - Quality of Service—See [Configuring Quality of Service, page 4-133](#).
  - Service Sets—See [Configuring Service Sets, page 4-134](#).
  - Primary Service Set—See [Configuring Primary Service Set, page 4-139](#).
  - Advanced—See [Defining Advanced Associations, page 4-142](#).
  - Port Assignments—See [Configuring Port Assignments, page 4-147](#).
  - DSCP to CoS—See [Configuring DSCP to CoS, page 4-148](#).
-

## Defining Spanning Tree Protocol

This option is used for only bridges.

### Procedure

- 
- Step 1** Select **Association > Spanning Tree**. The Association: Spanning Tree Protocol dialog box appears.
- Step 2** Click **See detail** for information on which bridges this configuration is valid.
- Step 3** Complete the following:




---

**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

---

**Table 4-40 Spanning Tree Protocol Settings**

| Field                                        | Description                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Spanning Tree Protocol (STP)                 | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Enable—Use this setting to enable STP on the bridge.</li> <li>• Disable—If you do not want STP enabled the bridge.</li> </ul>                                                                                                                      |
| Always Unblock Ethernet when STP is disabled | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this setting to maintain a bridge link when STP is disabled.</li> <li>• No—Use this setting to not maintain a bridge link when STP is disabled.</li> </ul> <p>Click <b>See detail</b> to see for which versions this setting is valid.</p> |

**Table 4-40 Spanning Tree Protocol Settings (continued)**

| Field                        | Description                                                                                                                                                                                                                                                                                                                                             |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Root Configuration           |                                                                                                                                                                                                                                                                                                                                                         |
| Priority (0-65535)           | <p>Enter a number to influence which bridge is designated the root bridge in the spanning tree.</p> <p>When bridges have the same priority setting, STP uses the MAC addresses as a tiebreaker.</p> <p>The bridge with the lowest priority setting is likely to be designated the root bridge in the tree.</p>                                          |
| Max Age (6-40 Seconds)       | <p>Enter the number of seconds to define how long the bridge waits before deciding the network has changed and the spanning tree needs to be rebuilt.</p> <p>For example, with Max Age set to 20, the bridge attempts to rebuild the spanning tree if it does not receive a hello BPDU from the root bridge in the spanning tree within 20 seconds.</p> |
| Hello Time (1-10 Seconds)    | <p>Enter the number of seconds to define how often the root bridge in the spanning tree sends out a hello BPDU telling the other bridges that the network topology has not changed and that the spanning tree should remain the same.</p>                                                                                                               |
| Forward Delay (4-30 Seconds) | <p>Enter the number of seconds to define how long the bridge's ports should stay in the listening and learning transition states if there is a change in the spanning tree.</p>                                                                                                                                                                         |
| Port Configuration           |                                                                                                                                                                                                                                                                                                                                                         |
| Path Cost (1-65535)          | <p>Enter a number to indicates the relative efficiency of a port's network link.</p> <p>A port with a high path cost is less likely to become a bridge's root port.</p>                                                                                                                                                                                 |

**Table 4-40 Spanning Tree Protocol Settings (continued)**

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Priority (0-255) | Enter a number to influence whether STP designates a port as a bridge's root port.<br><br>A port with a low priority setting is more likely to become a bridge's root port.                                                                                                                                                                                                |
| Enable           | From the list, select one of the following for each port configured: <ul style="list-style-type: none"> <li>• <b>Enable</b>—Use this setting to indicate whether the port participates in STP. (This determines whether the port blocks or forwards traffic.)</li> <li>• <b>Disable</b>—Use this setting to indicate that the port does not participate in STP.</li> </ul> |

**Step 4** Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Defining Address Filters

Using this option, you can:

- Create a MAC address filter
- Remove a MAC address filter

### Procedure

**Step 1** Select **Association > Address Filters**. The Association: Address Filters dialog box appears.

**Step 2** To add or delete a new MAC address filter complete the following fields:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-41 Address Filters Settings**

| Field                                                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| New Destination MAC Address                                                    | Enter a destination MAC address by entering the address in one of the following ways: <ul style="list-style-type: none"> <li>With colons separating the character pairs (00:40:96:12:34:56, for example).</li> <li>Without any intervening characters (004096123456, for example).</li> </ul>                                                                                                                              |
| Allowed                                                                        | Click to pass traffic to the MAC address.                                                                                                                                                                                                                                                                                                                                                                                  |
| Disallowed                                                                     | Click to discard traffic to the MAC address.                                                                                                                                                                                                                                                                                                                                                                               |
| Delete MAC Address                                                             | Enter the MAC address to delete                                                                                                                                                                                                                                                                                                                                                                                            |
| Lookup MAC address on Authentication Server if not in an Existing Filter List? | Click one of the following: <ul style="list-style-type: none"> <li>Yes—Use this setting to allow looking up a MAC address on the authentication server.</li> <li>No—Use this setting to disallow looking up a MAC address.</li> </ul>                                                                                                                                                                                      |
| Is MAC Authentication alone sufficient for a client to be fully authenticated? | From the list, select one of the following: <ul style="list-style-type: none"> <li>Yes—Use this setting to specify that client devices that associate to the access point using 802.11 open authentication, first attempt MAC authentication.</li> <li>No—Use this setting to specify that MAC authentication alone is not sufficient.</li> </ul> Click <b>See detail</b> to see for which versions this setting is valid. |

- Step 3** To add a MAC address to the enter the MAC address, then click >> to add it to the Current MAC Address Filters list.
- Step 4** To delete a MAC address, enter the MAC address to delete in the Delete MAC address field, then click >>.
- Step 5** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Defining Ethertype Filters

### Procedure

---

- Step 1** Select **Association > Ethertype Filters**. The Association: Ethertype Filters dialog box appears.
- Step 2** Using this option:
- Create new filters—See [Creating New Ethertype Filters, page 4-113](#).
  - Create Special Cases—See [Creating Special Cases, page 4-114](#).
-

## Creating New Ethertype Filters

### Procedure

- Step 1** To create and enable protocol filters for the access point's Ethernet port, enter the following:



**Note** For a list of protocols, refer to Appendix B, Protocol Filter Lists in the *Cisco Aironet Access Point Software Configuration Guide*. The guide can be found on Cisco.com by selecting **Products and Services > Wireless LAN Products > Cisco Aironet 350 Series > Configuration Guides Books**.

**Table 4-42** *Creating New Ethertype Filters Settings*

| Field                       | Description                                                                                                                                                                                                     |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| New Ethertype Filter        |                                                                                                                                                                                                                 |
| Set ID                      | Enter an identification number for the filter set.                                                                                                                                                              |
| Set Name                    | Enter a descriptive filter set name.<br>See <a href="#">Naming Guidelines, page A-1</a> .                                                                                                                       |
| Default Disposition         | From the list, select one of the following: <ul style="list-style-type: none"><li>• Forward—Use this setting to forward protocol traffic.</li><li>• Block—Use this setting to block protocol traffic.</li></ul> |
| Default Time to Live (msec) |                                                                                                                                                                                                                 |
| Unicast                     | Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.                                                                                            |
| Multicast                   | Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.                                                                                          |

- Step 2** Click >>. The new name is added to the Ethertype Filters list.

- Step 3** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Creating Special Cases

### Procedure

**Step 1** Select the default filter for which you want to define a special case.

**Step 2** Enter the following:

**Table 4-43 Ethertype Filter Special Cases Settings**

| Field             | Description                                                                                                                                                                                                                                                                                 |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| New Special Cases |                                                                                                                                                                                                                                                                                             |
| Ethertype         | Enter the Ethertype filter name.                                                                                                                                                                                                                                                            |
| Disposition       | From the list, select one of the following: <ul style="list-style-type: none"> <li>• Default—Use the disposition you set for the Ethertype filter.</li> <li>• Forward—Use this setting to forward protocol traffic.</li> <li>• Block—Use this setting to block protocol traffic.</li> </ul> |



**Table 4-43 Ethertype Filter Special Cases Settings (continued)**

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Priority            | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Default</b>—This setting is the same as best effort, which applies to normal LAN traffic.</li> <li>• <b>Background</b>—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications.</li> <li>• <b>Excellent Effort</b>—Use this setting for a network's most important users.</li> <li>• <b>Controlled Load</b>—Use this setting for important business applications that are subject to some form of admission control.</li> <li>• <b>Interactive Video</b>—Use this setting for traffic with less than 100 ms delay.</li> <li>• <b>Interactive Voice</b>—Use this setting for traffic with less than 10 ms delay.</li> <li>• <b>Network Control</b>—Use this setting for traffic that must get through to maintain and support the network infrastructure.</li> </ul> |
| Time to Live (msec) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Unicast             | Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Multicast           | Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Alert               | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b>—Use this setting to send an alert to the event log when a user transmits or receives the protocol through the access point.</li> <li>• <b>No</b>—Use this setting to not send an alert to the event log.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

**Step 3** Click >>. The new name 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 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Defining IP Protocol Filters

### Procedure

---

- Step 1** Select **Association > IP Protocol Filters**. The Association: IP Protocol Filters dialog box appears.
- Step 2** With this option you can:
- Create new filters—See [Creating New IP Protocol Filters, page 4-116](#).
  - Create Special Cases—See [Creating Special Cases, page 4-118](#).
- 

### Creating New IP Protocol Filters

#### Procedure

---

- Step 1** To create and enable IP protocol filters, enter the following:



**Note** For a list of protocols, refer to Appendix B, Protocol Filter Lists in the *Cisco Aironet Access Point Software Configuration Guide*. The guide can be found on Cisco.com by selecting **Products and Services > Wireless LAN Products > Cisco Aironet 350 Series > Configuration Guides Books**.

---

**Table 4-44 IP Protocol Filter Settings**

| Field                       | Description                                                                                                                                                                                                     |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| New Protocol Filter         |                                                                                                                                                                                                                 |
| Set ID                      | Enter an identification number for the filter set.                                                                                                                                                              |
| Set Name                    | Enter a descriptive filter set name.<br>See <a href="#">Naming Guidelines, page A-1</a> .                                                                                                                       |
| Default Disposition         | From the list, select one of the following: <ul style="list-style-type: none"><li>• Forward—Use this setting to forward protocol traffic.</li><li>• Block—Use this setting to block protocol traffic.</li></ul> |
| Default Time to Live (msec) |                                                                                                                                                                                                                 |
| Unicast                     | Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.                                                                                            |
| Multicast                   | Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.                                                                                          |

**Step 2** Click >>. The new name is added to the Current Protocol Filters list.

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Creating Special Cases

### Procedure

- Step 1** Select the default filter for which you want to define a special case.
- Step 2** Enter the following:

**Table 4-45** *IP Protocol Filters Special Cases Settings*

| Field             | Description                                                                                                                                                                                                                                                          |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| New Special Cases |                                                                                                                                                                                                                                                                      |
| Protocol          | Enter the IP protocol name.                                                                                                                                                                                                                                          |
| Disposition       | From the list, select one of the following: <ul style="list-style-type: none"><li>• Default—Use the disposition you set for the protocol filter.</li><li>• Forward—Use this setting to forward traffic.</li><li>• Block—Use this setting to block traffic.</li></ul> |

**Table 4-45 IP Protocol Filters Special Cases Settings (continued)**

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Priority            | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Default</b>—This setting is the same as best effort, which applies to normal LAN traffic.</li> <li>• <b>Background</b>—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications.</li> <li>• <b>Excellent Effort</b>—Use this setting for a network's most important users.</li> <li>• <b>Controlled Load</b>—Use this setting for important business applications that are subject to some form of admission control.</li> <li>• <b>Interactive Video</b>—Use this setting for traffic with less than 100 ms delay.</li> <li>• <b>Interactive Voice</b>—Use this setting for traffic with less than 10 ms delay.</li> <li>• <b>Network Control</b>—Use this setting for traffic that must get through to maintain and support the network infrastructure.</li> </ul> |
| Time to Live (msec) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Unicast             | Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Multicast           | Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Alert               | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b>—Use this setting to send an alert to the event log when a user transmits or receives the protocol through the access point.</li> <li>• <b>No</b>—Use this setting to not send an alert to the event log.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

- Step 3** Click >>. The new name is added to the list box.
- Step 4** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Defining IP Port Filters

### Procedure

---

- Step 1** Select **Association > IP Port Filters**. The Association: IP Port Filters dialog box appears.
- Step 2** With this option you can:
- Create new filters—See [Creating New Port Filters, page 4-121](#).
  - Create Special Cases—See [Creating Special Cases, page 4-122](#).
-

## Creating New Port Filters



**Note** For a list of protocols, refer to Appendix B, Protocol Filter Lists in the *Cisco Aironet Access Point Software Configuration Guide*. The guide can be found on Cisco.com by selecting **Products and Services > Wireless LAN Products > Cisco Aironet 350 Series > Configuration Guides Books**.

### Procedure

**Step 1** To create and enable port filters, enter the following:

**Table 4-46 IP Port Filter Settings**

| Field                       | Description                                                                                                                                                                                   |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| New Port Filter             |                                                                                                                                                                                               |
| Set ID                      | Enter an identification number for the filter set.                                                                                                                                            |
| Set Name                    | Enter a descriptive filter set name.<br>See <a href="#">Naming Guidelines, page A-1</a> .                                                                                                     |
| Default Disposition         | From the list, select one of the following: <ul style="list-style-type: none"><li>• Forward—Use this setting to forward traffic.</li><li>• Block—Use this setting to block traffic.</li></ul> |
| Default Time to Live (msec) |                                                                                                                                                                                               |
| Unicast                     | Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.                                                                          |
| Multicast                   | Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.                                                                        |

**Step 2** Click >>. The new name is added to the Current Port Filters list.

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Creating Special Cases

### Procedure

---

**Step 1** Select the default filter for which you want to define a special case.

**Step 2** Enter the following:

**Table 4-47 IP Port Filters Special Cases Settings**

| Field             | Description                                                                                                                                                                                                                                                                            |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| New Special Cases |                                                                                                                                                                                                                                                                                        |
| Port              | Enter the IP Port filter name.                                                                                                                                                                                                                                                         |
| Disposition       | From the list, select one of the following: <ul style="list-style-type: none"> <li>• Default—Use the disposition you set for the port filter.</li> <li>• Forward—Use this setting to forward protocol traffic.</li> <li>• Block—Use this setting to block protocol traffic.</li> </ul> |



**Table 4-47 IP Port Filters Special Cases Settings (continued)**

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Priority            | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Default</b>—This setting is the same as best effort, which applies to normal LAN traffic.</li> <li>• <b>Background</b>—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications.</li> <li>• <b>Excellent Effort</b>—Use this setting for a network's most important users.</li> <li>• <b>Controlled Load</b>—Use this setting for important business applications that are subject to some form of admission control.</li> <li>• <b>Interactive Video</b>—Use this setting for traffic with less than 100 ms delay.</li> <li>• <b>Interactive Voice</b>—Use this setting for traffic with less than 10 ms delay.</li> <li>• <b>Network Control</b>—Use this setting for traffic that must get through to maintain and support the network infrastructure.</li> </ul> |
| Time to Live (msec) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Unicast             | Enter the number of milliseconds unicast packets should stay in the buffer before they are discarded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Multicast           | Enter the number of milliseconds multicast packets should stay in the buffer before they are discarded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Alert               | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b>—Use this setting to send an alert to the event log when a user transmits or receives the protocol through the access point.</li> <li>• <b>No</b>—Use this setting to not send an alert to the event log.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

- Step 3** Click >>. The new name is added to the Special Cases list.
- Step 4** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Configuring Policy Groups

Policy groups are used to configure access parameters to a logical group of stations in a consistent manner from a single place. For example, protocol filters can be applied to frames for a selected group of stations.

### Procedure

---

- Step 1** Select **Association > Policy Group**. The Association: Policy Group dialog box appears.

Click **See detail** to see for which versions this setting is valid.



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

---

- Step 2** Using this option you can:
- Add a policy group—See [Adding a New Policy Group, page 4-125](#).
  - Delete an exiting Policy Group From a Device—See [Deleting an Existing Policy Group from a Device, page 4-126](#).
-

## Adding a New Policy Group

### Procedure

**Step 1** To add a new policy group, enter the following:

**Table 4-48 New Policy Group Settings**

| Field                 | Description                                                                                                                                |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Group ID              | Enter an identification number for the policy group.                                                                                       |
| Group Name            | Enter a name for the policy group, then click >>.                                                                                          |
| Policy Groups to Add. | Lists the policy groups to be added.<br>To remove a group from the list, click <<.                                                         |
| Ethertype             |                                                                                                                                            |
| Receive               | Enter the ID of a defined Ethertype filter, or select one of the filters you created using <b>Association &gt; Ethertype Filters</b> .     |
| Transmit              | Enter the ID of a defined Ethertype filter, or select one of the filters you created using <b>Association &gt; Ethertype Filters</b> .     |
| IP Protocol           |                                                                                                                                            |
| Receive               | Enter the ID of a defined IP protocol filter, or select one of the filters you created using <b>Association &gt; IP Protocol Filters</b> . |
| Transmit              | Enter the ID of a defined IP protocol filter, or select one of the filters you created using <b>Association &gt; IP Protocol Filters</b> . |
| IP Port               |                                                                                                                                            |
| Receive               | Enter the ID of a defined IP port filter, or select one of the filters you created using <b>Association &gt; IP Port Filters</b> .         |
| Transmit              | Enter the ID of a defined IP port filter, or select one of the filters you created using <b>Association &gt; IP Port Filters</b> .         |

- Step 2** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

### Deleting an Existing Policy Group from a Device

#### Procedure

- 
- Step 1** Enter the group identification number in the **Group ID** text box, then click >> to add it to the Policy Groups to Delete list.
- To remove a group from the list, click <<.
- Step 2** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Configuring VLANs

Access points and bridges in a VLAN network, which are running specific software versions, can provide a wireless VLAN trunk link between two wired segments of the network.

Using this option, you can configure VLANs on the access point.

## Procedure

**Step 1** Select **Association > VLANs**. The Association: VLAN dialog box appears.



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

**Step 2** Click **See detail** to see for which versions this option is valid.

**Step 3** Enter the following information:

**Table 4-49 VLAN Configuration**

| Field                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLAN (802.1Q) Tagging                                  | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Enabled—Use this setting to allow IEEE 802.1Q protocol tagging on VLAN packets.</li> </ul> <p>The IEEE 802.1Q protocol is used to interconnect multiple switches and routers, and for defining VLAN topologies.</p> <ul style="list-style-type: none"> <li>Disabled—Use this setting to not allow tagging.</li> </ul> |
| Native VLAN ID                                         | <p>Enter identification number of the access point's native VLAN.</p> <p><b>Note</b> This setting must agree with the native VLAN ID setting on the switch.</p>                                                                                                                                                                                                                                                 |
| Single VLAN ID which allows unencrypted packets        | <p>Enter an identification number to allow unencrypted packets. An entry with a value of 0 (zero requires the use of encryption.)</p>                                                                                                                                                                                                                                                                           |
| Optionally allow Encrypted Packets on unencrypted VLAN | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Yes—Use this setting to allow point-to-point encryption.</li> <li>No—Use this setting to not allow point-to-point encryption.</li> </ul>                                                                                                                                                                              |

**Step 4** Using this option you can:

- Add a new VLAN—See [Adding a New VLAN](#), page 4-128.
  - Delete an exiting VLAN from a Device—See [Deleting an Existing VLAN](#), page 4-132.
- 

## Adding a New VLAN

### Procedure

---

**Step 1** To add a new VLAN, enter the following:

**Table 4-50 New VLAN Settings**

| Field       | Description                                                                                                                                                                                         |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLAN ID     | Enter the identification number of the VLAN.<br><b>Note</b> This setting must match the setting on the switch.                                                                                      |
| VLAN Name   | Enter the a unique name for the VLAN configured on the access point.                                                                                                                                |
| VLAN Enable | From the list, select one of the following: <ul style="list-style-type: none"><li>• Enabled—Use this setting to enable the VLAN.</li><li>• Disabled—Use this setting to disable the VLAN.</li></ul> |

**Table 4-50 New VLAN Settings (continued)**

| Field                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default Priority        | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Background—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications.</li> <li>Default—Use this setting for normal LAN traffic.</li> <li>Excellent Effort—Use this setting for the network's most important users.</li> <li>Controlled Load—Use this setting for important business applications that are subject to some form of admission control.</li> <li>Interactive Video—Use this setting for traffic with less than 100 ms delay.</li> <li>Interactive Voice—Use this setting for traffic with less than 10ms delay.</li> <li>Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.</li> </ul> |
| Default Policy Group    | Enter the default policy group number, or select one you created using <b>Association &gt; Policy Groups</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Enhanced MIC verify WEP | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>None—Use this setting if you do not want Message Integrity Check (MIC) enabled.</li> <li>MMH—Use this setting if you want MIC enabled to protect WEP keys.</li> </ul> <p><b>Note</b> When you enable MIC, only MIC-capable client devices can communicate with the access point.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

**Table 4-50 New VLAN Settings (continued)**

| Field                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default Priority        | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Background—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications.</li> <li>Default—Use this setting for normal LAN traffic.</li> <li>Excellent Effort—Use this setting for the network's most important users.</li> <li>Controlled Load—Use this setting for important business applications that are subject to some form of admission control.</li> <li>Interactive Video—Use this setting for traffic with less than 100 ms delay.</li> <li>Interactive Voice—Use this setting for traffic with less than 10ms delay.</li> <li>Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.</li> </ul> |
| Default Policy Group    | Enter the default policy group number, or select one you created using <b>Association &gt; Policy Groups</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Enhanced MIC verify WEP | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>None—Use this setting if you do not want Message Integrity Check (MIC) enabled.</li> <li>MMH—Use this setting if you want MIC enabled to protect WEP keys.</li> </ul> <p><b>Note</b> When you enable MIC, only MIC-capable client devices can communicate with the access point.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |



**Table 4-50 New VLAN Settings (continued)**

| Field                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Temp Key Integrity Protocol | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>None—Use this setting if you do not want to enable the temporal key integrity protocol (TKIP), or WEP key hashing.</li> <li>Cisco—Use this setting to enable TKIP.</li> </ul> <p><b>Note</b> 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.</p>                                                                                                                                                                                                                          |
| WEP Key Rotation Interval   | <p>Use this setting to enable or disable broadcast key rotation.</p> <ul style="list-style-type: none"> <li>To enable it, enter the rotation interval in seconds.</li> </ul> <p>If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes.</p> <p><b>Note</b> When you enable broadcast key rotation, only wireless client devices using LEAP or EAP-TLS authentication can use the access point. Client devices using static WEP (with open, shared key, or EAP-MD5) cannot use the access point when you enable broadcast key rotation.</p> <ul style="list-style-type: none"> <li>To disable it, enter 0 (zero).</li> </ul> |
| Alert?                      | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Yes—Use this setting if you are not adding an encrypted VLAN.</li> <li>No—Use this setting if you are adding an encrypted VLAN.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| WEP Keys 1 through 4        | Enter the encryption keys used: 40 bit or 128 bit hexadecimal digits.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Size                        | For each WEP key, select one of the following: Not set, 40 bit, or 128 bit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

- Step 2** Click >> to add the VLAN to the VLANs to Add list.
- Step 3** To make sure the VLAN ID you want to create does not already exist, click **Update**.
- Step 4** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Deleting an Existing VLAN

### Procedure

- Step 1** Enter the VLAN identification number in the **VLAN ID** text box, then click >> to add it to the VLANs to Delete list.
- Step 2** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
-

## Configuring Quality of Service

This option is used to configure the access point's Quality of Service feature.

### Procedure

- Step 1** Select **Association > Quality of Service**. The Association: Quality of Service dialog box appears.



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

- Step 2** Click **See detail** to see for which versions this option is valid.

- Step 3** Enter the following information:

**Table 4-51** *Quality of Service Settings*

| Field                   | Description                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Generate QBBS Element   | From the list, select one of the following: <ul style="list-style-type: none"><li>• Yes—Use this setting to enable support for basic 802.11 Quality of Service.</li><li>• No—Use this setting to disable support for basic 802.11 Quality of Service.</li></ul>                                                                                             |
| User Symbol Extensions  | From the list, select one of the following: <ul style="list-style-type: none"><li>• Yes—Use this setting enables support for Symbol Voice over IP (VoIP phones).</li><li>• No—Use this setting to disable support for Symbol VoIP phones.</li></ul>                                                                                                         |
| Send IGMP General Query | From the list, select one of the following: <ul style="list-style-type: none"><li>• Yes—Use this setting to allow the access point to send an IGMP General Query to all associated stations when they complete all required high-level authentication.</li><li>• No—Use this setting to not allow the access point to send an IGMP General Query.</li></ul> |

**Table 4-51 Quality of Service Settings (continued)**

| Field                    | Description                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Background<br>(spare)    | From the <b>CWmin</b> and <b>CWmax</b> lists, select the minimum and maximum contention window values for each traffic category. |
| Best Effort<br>(default) |                                                                                                                                  |
| Excellent Effort         |                                                                                                                                  |
| Controlled Load          |                                                                                                                                  |
| Interactive Video        |                                                                                                                                  |
| Interactive Voice        |                                                                                                                                  |
| Network Control          |                                                                                                                                  |

**Step 4** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Configuring Service Sets

This option allows you to define service sets.

## Procedure

- Step 1** Select **Association > Service Sets**. The Association: Service Sets dialog box appears.



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

- Step 2** Click **See detail** to see for which versions this option is valid.

- Step 3** Enter the following information:

**Table 4-52** *Service Set Settings*

| Field                                                       | Description                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device                                                      |                                                                                                                                                                                                                                                                                                                                                              |
| SSID for use by Infrastructure Stations (such as Repeaters) | Enter the SSID to be used by repeaters and workgroup bridges to associate to the access point.<br><br>This SSID should be mapped to the native VLAN ID in order to facilitate communications between infrastructure devices and a non-root access point or bridge.                                                                                           |
| Disallow Infrastructure Stations on any other SSID          | From the list, select one of the following: <ul style="list-style-type: none"><li>• Yes—This setting prevents repeaters or workgroup bridges from associating to SSIDs other than the infrastructure SSID.</li><li>• No—This setting does not prevent repeaters or workgroup bridges from associating to SSIDs other than the infrastructure SSID.</li></ul> |

- Step 4** Using this option you can:

- Add a new Service Set—See [Adding a New Service Set, page 4-136](#).
- Delete an exiting Service Set from a device—See [Deleting an Existing Service Set, page 4-138](#).

## Adding a New Service Set

### Procedure

**Step 1** To add a new Service set, enter the following:

**Table 4-53 New Service Set Settings**

| Field                          | Description                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service Set ID (1-24)          | Enter an identification for the SSID.                                                                                                                                                                                                                                                                                                        |
| Service Set Name               | Enter the SSID, then click >>.                                                                                                                                                                                                                                                                                                               |
| Service Sets To Add            | Lists the added service sets.<br>To remove a service set from the list, click <<.                                                                                                                                                                                                                                                            |
| Maximum Number of Associations | Enter a number to limit the maximum number of wireless clients per SSID.                                                                                                                                                                                                                                                                     |
| Proxy Mobile IP Enabled        | From the list, select one of the following: <ul style="list-style-type: none"> <li>• Yes—This setting allows proxy mobile IP use by all stations associated to this access point.</li> <li>• No—This setting does not allow proxy mobile IP use.</li> </ul>                                                                                  |
| Default VLAN ID                | Enter the identification number for a defined VLAN, or select one of the VLAN IDs you created using <b>Association &gt; VLANs</b> .                                                                                                                                                                                                          |
| Default Policy Group           | Enter the identification number of a defined policy group, or select one of the policy groups you created using <b>Association &gt; Policy Groups</b> .                                                                                                                                                                                      |
| Accept Authentication Type     |                                                                                                                                                                                                                                                                                                                                              |
| Open                           | From the list, select one of the following: <ul style="list-style-type: none"> <li>• Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting.</li> <li>• No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.</li> </ul> |

**Table 4-53 New Service Set Settings (continued)**

| Field       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Shared      | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Tells the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting.</li> <li>• No—Does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.</li> </ul> |
| Network-EAP | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Allows EAP-enabled client devices to authenticate through the access point.</li> <li>• No—Does not allow EAP-enabled client devices to authenticate through the access point.</li> </ul>                                                                                                                                                                                                                             |
| Require EAP |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Open        | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point.</li> <li>• No—Use this option if you do not use open and EAP authentication.</li> </ul>                                                                                                                                                                          |
| Shared      | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point.</li> <li>• No—Use this option if you do not use shared and EAP authentication.</li> </ul>                                                                                                                                                                      |

**Table 4-53 New Service Set Settings (continued)**

| Field                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default Unicast Address Filter |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Open                           | From the list, select one of the following: <ul style="list-style-type: none"> <li>Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters.</li> <li>Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed with the Address Filters or on your authentication server.</li> </ul> Select Disallowed for each authentication type that also uses MAC-based authentication. |
| Shared                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Network-EAP                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

**Step 2** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Deleting an Existing Service Set

### Procedure

**Step 1** Enter the Service Set number in the **Service Set ID** text box, then click >> to add it to the Service Sets to Delete list.



- Step 2** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Configuring Primary Service Set

This option allows you to set a default VLAN for the primary SSID on an access point.

### Procedure

---

- Step 1** Select **Association > Primary Service Set**. The Association: Primary Service Set dialog box appears.
- Step 2** Complete the following:

**Table 4-54 Primary Service Set**

| Field                          | Description                                                                                                                                                                                                                                              |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service Set Name               | Enter the SSID.                                                                                                                                                                                                                                          |
| Maximum Number of Associations | Enter a number to limit the maximum number of wireless clients per SSID.                                                                                                                                                                                 |
| Proxy Mobile IP Enabled        | From the list, select one of the following: <ul style="list-style-type: none"><li>• Yes—This setting allows proxy mobile IP use by all stations associated to this access point.</li><li>• No—This setting does not allow proxy mobile IP use.</li></ul> |
| Default VLAN ID                | Enter the identification number for a defined VLAN, or select one of the VLAN IDs you created using <b>Association &gt; VLANs</b> .                                                                                                                      |

**Table 4-54 Primary Service Set (continued)**

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default Policy Group       | Enter the identification number of a defined policy group, or select one of the policy groups you created using <b>Association &gt; Policy Groups</b> .                                                                                                                                                                                                                                                                                                                                                              |
| Accept Authentication Type |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Open                       | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting.</li> <li>• No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.</li> </ul>                                                                                                                                                                  |
| Shared                     | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Tells the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting.</li> <li>• No—Does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.</li> </ul> |
| Network-EAP                | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Allows EAP-enabled client devices to authenticate through the access point.</li> <li>• No—Does not allow EAP-enabled client devices to authenticate through the access point.</li> </ul>                                                                                                                                                                                                                             |

**Table 4-54 Primary Service Set (continued)**

| Field                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Require EAP                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Open                           | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point.</li> <li>• No—Use this option if you do not use open and EAP authentication.</li> </ul>                                                                                                                                                                             |
| Shared                         | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point.</li> <li>• No—Use this option if you do not use shared and EAP authentication.</li> </ul>                                                                                                                                                                         |
| Default Unicast Address Filter |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Open                           | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters.</li> <li>• Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed with the Address Filters or on your authentication server.</li> </ul> <p>Select Disallowed for each authentication type that also uses MAC-based authentication.</p> |
| Shared                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Network-EAP                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Defining Advanced Associations

Use this option to control the total number of devices an access point can list in the Association Table and the amount of time the access point continues to track each device class when a device is inactive.

### Procedure

---

- Step 1** Select **Association > Advanced**. The Association: Advanced dialog box appears.
- Step 2** To define advanced associations, enter the following:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

---

**Table 4-55 Advanced Association Settings**

| Field                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alert Severity Level | <p>From the list select one of the following:</p> <ul style="list-style-type: none"><li>• systemFatal—Indicates an event that prevents operation of the port or device.</li><li>• protocolFatal—Indicates an event that prevents operation of the port or device</li><li>• portFatal—Indicates an event that prevents operation of the port or device</li><li>• systemAlert—Indicates that you need to take action to correct the condition.</li><li>• protocolAlert—Indicates that you need to take action to correct the condition.</li><li>• portAlert—Indicates that you need to take action to correct the condition.</li><li>• externalAlert—Indicates that you need to take action to correct the condition.</li></ul> |

**Table 4-55 Advanced Association Settings (continued)**

| Field                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                   | <ul style="list-style-type: none"> <li>• systemWarning—Indicates that an error or failure may have occurred.</li> <li>• protocolWarning—Indicates that an error or failure may have occurred.</li> <li>• portWarning—Indicates that an error or failure may have occurred.</li> <li>• externalWarning—Indicates that an error or failure may have occurred.</li> <li>• systemInfo—Notification that some sort of event has occurred.</li> <li>• protocolInfo—Notification that some sort of event has occurred.</li> <li>• portInfo—Notification that some sort of event has occurred.</li> <li>• externalInfo—Notification that some sort of event has occurred.</li> </ul> |
| Max Bytes Stored Per Alert Packet | <p>Enter the maximum number of bytes the access point stores for each Station Alert packet when packet tracing is enabled.</p> <p>If you use 0, the access point does not store bytes for Station Alert packets; it only logs the event.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Max Fwd Table Entries             | <p><b>Note</b> Changing this setting may cause the access point to reboot.</p> <p>From the list, select one of the settings to designate the maximum number of devices that can appear in the Association Table.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

**Table 4-55 Advanced Association Settings (continued)**

| Field                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rogue AP alert timeout (minutes)    | <p>Enter the amount of time in minutes the access point transmits an alert message. (When an access point detects a rogue access point, it sends an alert message to the system log.) When the timeout is reached, the access point stops sending the alert message.</p> <p>Click <b>See detail</b> to see for which versions this option is valid.</p>                                                                                                                                                                                                                   |
| Enable RFC 1493 802.1D Stats In MIB | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"><li>• <b>Enable</b>—Use this setting to enable the storage of detailed RFC 1493 802.1D statistics in access point memory.</li><li>• <b>Disable</b>—Use this setting to disable the storage of detailed RFC 1493 802.1D statistics in access point memory. When you disable extended statistics you conserve memory, and the access point can include more devices in the Association Table.</li></ul> <p>Click <b>See detail</b> to see for which versions this option is valid.</p> |
| Enable Extended Stats in MIB        | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"><li>• <b>Enable</b>—Use this setting to enable the storage of detailed statistics in the device's memory.</li><li>• <b>Disable</b>—Use this setting to disable the storage of detailed statistics in the device's memory.</li></ul> <p>When you disable extended statistics you conserve memory, and the device can include more devices in the Association Table.</p>                                                                                                               |

**Table 4-55 Advanced Association Settings (continued)**

| Field                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Map Multicast Entries to Broadcast Entry | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Enable</b>—Use this setting to make the access point more virus-resistant by mapping all multicast MAC addresses into the Broadcast address.</li> <li>• <b>Disable</b>—Use this setting to disable this feature.</li> </ul> <p>Click <b>See detail</b> to see for which versions this setting is valid.</p>                                                                                                                                                                      |
| Enable PSPF                              | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Enable</b>—Use this setting to enable Publicly Secure Packet Forwarding, which ensures that 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.</li> <li>• <b>Disable</b>—Use this setting to disable Publicly Secure Packet Forwarding.</li> </ul> <p>Click <b>See detail</b> to see for which versions this option is valid.</p> |



**Table 4-55 Advanced Association Settings (continued)**

| Field                        | Description                                                                                                                                                                                                                                                                                                          |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unknown Class Timeout        | Enter the number of seconds the access point continues to track an inactive device depending on its class.<br><br>A setting of zero tells the access point to track a device indefinitely no matter how long it is inactive.<br><br>A setting of 300 equals 5 minutes; 1800 equals 30 minutes; 28800 equals 8 hours. |
| Multicast Addresses Timeout  |                                                                                                                                                                                                                                                                                                                      |
| Infrastructure Hosts Timeout |                                                                                                                                                                                                                                                                                                                      |
| Client Stations Timeout      |                                                                                                                                                                                                                                                                                                                      |
| Repeaters Timeout            |                                                                                                                                                                                                                                                                                                                      |
| Access Points Timeout        |                                                                                                                                                                                                                                                                                                                      |
| Across Bridge Hosts Timeout  |                                                                                                                                                                                                                                                                                                                      |
| Non-Root Bridges Timeout     |                                                                                                                                                                                                                                                                                                                      |
| Root Bridges Timeout         |                                                                                                                                                                                                                                                                                                                      |

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Configuring Port Assignments

When you assign specific ports, your network topology remains constant even when devices reboot.

## Procedure

- Step 1** Select **Association > Port Assignments**. The Association: Port Assignments dialog box appears.
- Step 2** To define port assignments, enter the following:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-56 Port Assignments Settings**

| Field         | Description                                                                             |
|---------------|-----------------------------------------------------------------------------------------|
| ifIndex       | Lists the port's designator in the Standard MIB-II (RFC1213)-MIB.my interface index.    |
| dot1dBasePort | Lists the port's designator in the Bridge MIB (RFC1493); BRIDGE-MIB.my interface index. |
| AID           | Lists the port's 802.11 radio drivers association identifier.                           |
| Station       | Enter the MAC address of the device to which you want to assign the port.               |

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).

## Configuring DSCP to CoS

This option is use to statically map Differentiated Services Code-Point (DSCP) values to corresponding Class of Service (CoS) values.

### Procedure

**Step 1** Select **Association > DSCP to CoS**. The Association: DSCP to CoS Conversion dialog box appears.



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

**Step 2** Click **See detail** to see for which versions this option is valid.

**Step 3** For each DSCP, enter the CoS conversion. Select one of the following:

- No Change
- Background
- Spare
- Best Effort
- Excellent Effort
- Controlled Load
- Interactive Video
- Interactive Voice
- Network Control

**Step 4** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Configuring the Ethernet Port

Use this option to configure the device's Ethernet port.

### Procedure

---

**Step 1** Select **Ethernet**. The menu expands and the Ethernet dialog box displays in the right pane.

**Step 2** Select one of the following from the Ethernet menu:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

---

- Identification—See [Identifying the Ethernet Port, page 4-150](#).
  - Filters—See [Setting Up Ethernet Filters, page 4-152](#).
  - Hardware—See [Setting Up Hardware, page 4-153](#).
  - Advanced—See [Defining the Ethernet Advanced Settings, page 4-154](#).
- 

## Identifying the Ethernet Port

Use this option to define basic identity information for the Ethernet port.

### Procedure

---

**Step 1** Select **Ethernet > Identification**. The Ethernet: Identification dialog box displays in the right pane.

**Step 2** Enter the following information to identify the port:

**Table 4-57 Ethernet Port Settings**

| Field                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Primary Port                | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"><li>• Ethernet—Sets the Ethernet port for all access points other than AP1200's as the primary port.</li><li>• Ethernet AP 1200—Sets the Ethernet port for AP1200 access points as the primary port.</li><li>• Radio 11b—Sets the 11b radio port as the primary port.</li><li>• Radio 11a—Sets the 11a radio port as the primary port.</li></ul> |
| Adopt Primary Port Identity | <p><b>Note</b> Changing this setting may cause the access point to reboot.</p> <p>From the list, select one of the following:</p> <ul style="list-style-type: none"><li>• yes—This adopts the primary port settings (MAC and IP addresses for the Ethernet port).</li><li>• no—This uses different MAC and IP addresses for the Ethernet port.</li></ul>                                                                              |

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Setting Up Ethernet Filters

Use this option to define filters for the Ethernet port, the IP Protocol, and the IP Port.

### Procedure

- Step 1** Select **Ethernet > Filters**. The Ethernet: Filters dialog box displays in the right pane.
- Step 2** Complete the following:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-58 Ethernet Filters Settings**

| Field       | Description                                                                                                                                |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Ethertype   |                                                                                                                                            |
| Receive     | Enter the ID of a defined Ethertype filter, or select one of the filters you created using <b>Association &gt; Ethertype Filters</b> .     |
| Transmit    | Enter the ID of a defined Ethertype filter, or select one of the filters you created using <b>Association &gt; Ethertype Filters</b> .     |
| IP Protocol |                                                                                                                                            |
| Receive     | Enter the ID of a defined IP protocol filter, or select one of the filters you created using <b>Association &gt; IP Protocol Filters</b> . |
| Transmit    | Enter the ID of a defined IP protocol filter, or select one of the filters you created using <b>Association &gt; IP Protocol Filters</b> . |
| IP Port     |                                                                                                                                            |
| Receive     | Enter the ID of a defined IP port filter, or select one of the filters you created using <b>Association &gt; IP Port Filters</b> .         |
| Transmit    | Enter the ID of a defined IP port filter, or select one of the filters you created using <b>Association &gt; IP Port Filters</b> .         |

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Setting Up Hardware

This option allows you to select the hardware settings used by the access point's Ethernet port.

### Procedure

---

- Step 1** Select **Ethernet > Hardware**. The Ethernet: Hardware dialog box displays in the right pane.



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

---

- Step 2** Click **See detail** to see for which versions this option is valid.

- Step 3** Complete the following:

**Table 4-59 Ethernet Hardware Settings**

| Field                                            | Description                                                                                                                                                                                                                           |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Loss of Backbone Connectivity # of Secs (1-1000) | Enter the number of seconds the system must detect loss of backbone connectivity (i.e. loss of Ethernet link and no active trunk available on any of the radios) before taking the specified by Loss of Backbone Connectivity Action. |

**Table 4-59 Ethernet Hardware Settings (continued)**

| Field                                | Description                                                                                                                                                                                            |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Loss of Backbone Connectivity Action | From the list, select one of the following: <ul style="list-style-type: none"> <li>• No action</li> <li>• Switch to repeater mode</li> <li>• Shut the radio off</li> <li>• Restrict to SSID</li> </ul> |
| Loss of Backbone Connectivity SSID   | Enter an SSID index required if the Loss of Backbone Connectivity Action is set to Restrict to SSID, or select the SSID from the list.                                                                 |

**Step 4** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Defining the Ethernet Advanced Settings

Use this option to define the settings and operational status of the Ethernet port.

### Procedure

**Step 1** Select **Ethernet > Advanced**. The Ethernet: Advanced dialog box displays in the right pane.



**Step 2** Complete the following:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-60 Ethernet Advanced Settings**

| Field                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status                           | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>up—Enables the Ethernet port for normal operation.</li> <li>down—Disables the device’s Ethernet port.</li> </ul>                                                                                                                                                                                                                    |
| Packet Forwarding                | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>enabled—Allows normal operation.</li> <li>disabled—Prevents data from moving between the Ethernet and the radio, which is useful in troubleshooting.</li> </ul>                                                                                                                                                                     |
| Default Multicast Address Filter | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed under <b>Association &gt; Address Filters</b>.</li> <li>disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed under <b>Association &gt; Address Filters</b>.</li> </ul> |
| Maximum Multicast Packets/Second | <p>Use this setting to control the number of multicast packets that can pass through the Ethernet port each second.</p> <p>If you enter 0, the access point passes an unlimited number of multicast packets.</p> <p>If you enter a number other than 0, the device passes only that number of multicast packets per second.</p>                                                                                               |

**Table 4-60 Ethernet Advanced Settings (continued)**

| Field                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default Unicast Address Filter               | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>allowed—The access point forwards all traffic except packets sent to MAC addresses that have been set as disallowed under <b>Association &gt; Address Filters</b>.</li> <li>disallowed—The access point discards all traffic except packets sent to the MAC addresses that have been set as allowed under <b>Association &gt; Address Filters</b>.</li> </ul> |
| Always Unblock Ethernet when STP is disabled | <p>From the list, select one of the following:</p> <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Yes—Use this setting to maintain a bridge link when STP is disabled</li> <li>No—Use this setting to not maintain a bridge link when STP is disabled.</li> </ul> <p>Click <b>See detail</b> to see for which versions this option is valid.</p>                                                             |
| Optimize Ethernet for                        | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Performance—Allows faster packet forwarding.</li> <li>Statistics Collection—Allows better statistics collection.</li> </ul> <p>Click <b>See detail</b> to see for which versions this option is valid.</p>                                                                                                                                                    |

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Configuring the 11b Radio

Use this option to configure the device's 11b radio.

### Procedure

---

- Step 1** Select **11b Radio**. The menu expands and the Radio dialog box displays in the right pane.
- Step 2** Select one of the following from the Radio menu:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

---

- Identification—See [Identifying the 11b Radio Port, page 4-158](#).
  - Filters—See [Setting Up 11b Radio Filters, page 4-160](#).
  - Hardware—See [Defining the 11b Radio Hardware Settings, page 4-161](#).
  - Advanced—See [Defining the 11b Radio Advanced Settings, page 4-167](#).
  - Searched Channels—See [Defining the 11b Radio Searched Channels Settings, page 4-173](#).
-

## Identifying the 11b Radio Port

Use this option to define basic identity information for the port.


**Note**

Changing this setting may cause the access point to reboot.

### Procedure

- Step 1** Select **11b Radio > Identification**. The 11b Radio: Identification dialog box displays in the right pane.
- Step 2** Enter the following information to identify the port:


**Note**

Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-61 11b Radio Identification Settings**

| Field        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Primary Port | <p>From the list, select one of the following:</p> <p><b>Note</b> If the primary port was set using <b>Ethernet &gt; Identification</b>, the selected value is displayed.</p> <ul style="list-style-type: none"> <li>• Ethernet—Sets the Ethernet port for all access points other than AP1200's as the primary port.</li> <li>• Ethernet AP 1200—Sets the Ethernet port for AP1200 access points as the primary port.</li> <li>• Radio 11b—Sets the 11b radio port as the primary port.</li> <li>• Radio 11a—Sets the 11a radio port as the primary port.</li> </ul> |

**Table 4-61 11b Radio Identification Settings (continued)**

| Field                       | Description                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Adopt Primary Port Identity | <p><b>Note</b> Changing this setting may cause the access point to reboot.</p> <p>From the list, select one of the following:</p> <ul style="list-style-type: none"><li>• yes—This adopts the primary port settings (MAC and IP addresses) for the Ethernet port.</li><li>• no—This uses different MAC and IP addresses for the Ethernet port.</li></ul> |
| LEAP User Name              | <p>Use this field if the radio is set up as a repeater and authenticates to the network using LEAP. When the radio authenticates using LEAP, the access point sends this user name to the authentication server.</p> <p>Click <b>See detail</b> to see for which versions this option is valid.</p>                                                      |
| LEAP Password               | <p>Enter the LEAP password.</p> <p>Click <b>See detail</b> to see for which versions this option is valid.</p>                                                                                                                                                                                                                                           |

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Setting Up 11b Radio Filters

### Procedure

**Step 1** Select **11b Radio > Filters**. The 11b Radio Filters dialog box displays in the right pane.

**Step 2** Complete the following:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-62 11b Radio Filters Settings**

| Field       | Description                                                                                                                                |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Ethernet    |                                                                                                                                            |
| Receive     | Enter the ID of a defined Ethernet filter, or select one of the filters you created using <b>Association &gt; Ethernet Filters</b> .       |
| Transmit    | Enter the ID of a defined Ethernet filter, or select one of the filters you created using <b>Association &gt; Ethernet Filters</b> .       |
| IP Protocol |                                                                                                                                            |
| Receive     | Enter the ID of a defined IP protocol filter, or select one of the filters you created using <b>Association &gt; IP Protocol Filters</b> . |
| Transmit    | Enter the ID of a defined IP protocol filter, or select one of the filters you created using <b>Association &gt; IP Protocol Filters</b> . |

**Table 4-62 11b Radio Filters Settings (continued)**

| Field    | Description                                                                                                                                 |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------|
| IP Port  |                                                                                                                                             |
| Receive  | Enter the ID of a defined IP port protocol filter, or select one of the filters you created using <b>Association &gt; IP Port Filters</b> . |
| Transmit | Enter the ID of a defined IP port protocol filter, or select one of the filters you created using <b>Association &gt; IP Port Filters</b> . |

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Defining the 11b Radio Hardware Settings

### Procedure

- Step 1** Select **11b Radio > Hardware**. The 11b Radio: Hardware dialog box displays in the right pane.

**Step 2** Complete the following:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-63 11b Radio Hardware Settings**

| Field                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service Set ID (SSID)               | <p>Enter a unique identifier client devices use to associate with the access point. It can be any alphanumeric, case-sensitive string, from 1 to 32 characters long.</p> <p>Several access points on a network or sub-network can share an SSID.</p>                                                                                                                                                                                                                                                                                                                     |
| Allow “Broadcast” SSID to Associate | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• yes—Allows devices that do not specify an SSID (devices that are “broadcasting” in search of an access point) to associate with to associate with the access point.</li> <li>• no—Does not allow devices that do not specify an SSID (devices that are “broadcasting” in search of an access point) to associate with to associate with the access point.</li> </ul> <p>With no selected, the SSID used by the client device must match exactly the access point’s SSID.</p> |



**Table 4-63 11b Radio Hardware Settings (continued)**

| Field                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable “World Mode” multi-domain operation? | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"><li>• yes—Allows the access point to add channel carrier set information to its beacon.</li></ul> <p>Client devices with world-mode enabled receive the carrier set information and adjust their settings automatically.</p> <ul style="list-style-type: none"><li>• no—Does not allow the access point to add channel carrier set information to its beacon.</li></ul> |
| Data Rates (Mb/sec)                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 1.0                                         | <p>From the list, select one of the following for each of the four rates in megabits per second:</p> <ul style="list-style-type: none"><li>• basic—Allows transmission at this rate for all packets, both unicast and multicast. At least one data rate must be set to basic.</li><li>• yes—Allows transmission at this rate for unicast packets only.</li><li>• no—Does not allow transmission at this rate.</li></ul>                                      |
| 2.0                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 5.5                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 11.0                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Transmit Power                              | <p>From the list, select one of the following milliwatt settings: 1, 5, 20, 30, 50, 100.</p> <p>To reduce interference or to conserve power, select a lower power setting.</p> <p>Click <b>See detail</b> to see for which versions this option is valid.</p>                                                                                                                                                                                                |

**Table 4-63 11b Radio Hardware Settings (continued)**

| Field                              | Description                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fragmentation Threshold (256-2338) | <p>Enter a setting to determine the size at which packets are fragmented (sent as several pieces instead of as one block).</p> <p>Use a low setting in areas where communication is poor or where there is a great deal of radio interference.</p>                                                                                                                      |
| RTS Threshold (0-2339)             | <p>Enter a setting to determine the packet size at which the access point issues a request to send (RTS) before sending the packet.</p> <p>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.</p> |
| Maximum RTS Retries (1-128)        | Enter the maximum number of times the access point issues an RTS before stopping the attempt to send the packet through the radio.                                                                                                                                                                                                                                      |
| Max. Data Retries (1-128)          | Enter the maximum number of attempts the access point makes to send a packet before giving up and dropping the packet.                                                                                                                                                                                                                                                  |
| Beacon Period (Kusec)              | Enter the amount of time between beacons in kilomicroseconds. (One kilomicrosecond equals 1,024 microseconds.)                                                                                                                                                                                                                                                          |

**Table 4-63 11b Radio Hardware Settings (continued)**

| Field                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Beacon Rate (DTIM)                  | <p>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).</p> <p>The DTIM tells power-save client devices that a packet is waiting for them.</p> <p>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.</p> |
| Default Radio Channel                    | <p>From the list, select the radio channel you want for a default. Each channel covers 22 MHz.</p> <p>The factory setting for Cisco wireless LAN systems is Radio Channel 6 transmitting at 2437 MHz.</p>                                                                                                                                                                                                                                                         |
| Search for less-congested Radio Channel? | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• yes—Allows the access point to scan for the radio channel that is least busy and selects that channel for use.</li> <li>• no—Will not allow the access point to scan for a radio channel that is least busy.</li> </ul>                                                                                                                                               |

**Table 4-63 11b Radio Hardware Settings (continued)**

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Receive Antenna  | From the list, select one of the following:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Transmit Antenna | <ul style="list-style-type: none"> <li>• <b>Right</b>—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.)<br/><br/>Use this setting for both receive and transmit.</li> <li>• <b>Left</b>—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's left connector. (When you look at the access point's back panel, the left antenna is on the left.)<br/><br/>Use this setting for both receive and transmit.</li> <li>• <b>Diversity</b>—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.<br/><br/>Use this setting for both receive and transmit.</li> </ul> |

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Defining the 11b Radio Advanced Settings

Use this option to define the settings and operational status of the Ethernet port.

### Procedure

---

- Step 1** Select **11b Radio > Advanced**. The 11b Radio: Advanced dialog box displays in the right pane.
- Step 2** Complete the following:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

---

**Table 4-64 11b Radio Advance Settings**

| Field             | Description                                                                                                                                                                                                                                         |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status            | From the list, select one of the following: <ul style="list-style-type: none"><li>• up— Enables the Radio port for normal operation.</li><li>• down—Disables the device’s Radio port.</li></ul>                                                     |
| Packet Forwarding | From the list, select one of the following: <ul style="list-style-type: none"><li>• enabled—Allows normal operation.</li><li>• disabled—Prevents data from moving between the Ethernet and the radio, which is useful in troubleshooting.</li></ul> |

**Table 4-64 11b Radio Advance Settings (continued)**

| Field                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default Multicast Address Filter | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed under <b>Association &gt; Address Filters</b>.</li> <li>Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed under <b>Association &gt; Address Filters</b>.</li> </ul> |
| Maximum Multicast Packets/Second | <p>Use this setting to control the number of multicast packets that can pass through the Ethernet port each second.</p> <p>If you enter 0, the access point passes an unlimited number of multicast packets.</p> <p>If you enter a number other than 0, the device passes only that number of multicast packets per second.</p>                                                                                               |
| Maximum Number of Associations   | <p>Enter the maximum number of wireless networking devices that are allowed to associate to the access point.</p> <p>If you enter 0 it means that the maximum possible number of associations is allowed.</p> <p>Click <b>See detail</b> to see for which versions this option is valid.</p>                                                                                                                                  |
| Use Aironet Extensions           | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>yes—Enable load balancing, Message Integrity Check (MIC), and WEP key hashing.</li> <li>no—Does not enable the features listed above.</li> </ul>                                                                                                                                                                                    |

**Table 4-64 11b Radio Advance Settings (continued)**

| Field                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Classify Workgroup Bridges as network infrastructure | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• yes—Use this setting to limit the number of workgroup bridges that can associate to the access point to 20 or less.</li> <li>• no—Use this setting to allow more than 20 workgroup bridges to associate to the access point.</li> </ul> <p>Click <b>See detail</b> to see for which versions this option is valid.</p>    |
| User Symbol Extensions                               | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• yes—Use this setting to enable the following features: load balancing, message integrity check (MIC), temporal key integrity protocol (TKIP).</li> <li>• no—Use this setting to disable use of Cisco Aironet 802.11 extensions.</li> </ul> <p>Click <b>See detail</b> to see for which versions this option is valid.</p> |
| Ethernet encapsulation transform                     | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• 802.1H—Provides optimum performance for Cisco Aironet wireless products.</li> <li>• RFC1042—Ensures interoperability with non-Cisco Aironet wireless equipment.</li> </ul>                                                                                                                                                |

**Table 4-64 11b Radio Advance Settings (continued)**

| Field                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enhanced MIC verification for WEP         | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>None—Does not enable MIC.</li> <li>NMH—Enables MIC (Message Integrity Check), a security feature that protects your WEP keys by preventing attacks on encrypted packets called bit-flip attacks.</li> </ul> <p>Click <b>See detail</b> to see for which versions this setting is valid.</p>                                |
| Temporal Key Integrity Protocol           | <p>From the list, select the following:</p> <ul style="list-style-type: none"> <li>None—Does not enable WEP key hashing.</li> <li>Cisco—Enables WEP key hashing that defends against an attack on WEP in which the intruder uses the unencrypted initialization vector (IV) in encrypted packets to calculate the WEP key.</li> </ul> <p>Click <b>See detail</b> to see for which versions this option is valid.</p> |
| Broadcast WEP Key rotation interval (sec) | <p>Enter a rotation interval in seconds.</p> <ul style="list-style-type: none"> <li>If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes.</li> <li>If you enter 0, you disable broadcast WEP key rotation.</li> </ul> <p>Click <b>See detail</b> to see for which versions this option is valid.</p>                                      |



**Table 4-64 11b Radio Advance Settings (continued)**

| Field                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default Unicast Address Filter |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Open                           | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters.</li> <li>Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed with the Address Filters or on your authentication server.</li> </ul> <p>Select Disallowed for each authentication type that also uses MAC-based authentication.</p> |
| Shared                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Network-EAP                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Specified Access Point 1       | <p>If this access point is a repeater, enter the MAC address of one or more root-unit access points with which you want this access point to associate.</p> <p>With MAC addresses in these fields, the repeater access point always tries to associate with the specified access points instead of with other less-efficient access points.</p>                                                                                                                                                                     |
| Specified Access Point 2       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Specified Access Point 3       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Specified Access Point 4       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Radio Modulation               | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Standard—This setting is the modulation type specified in IEEE 802.11, the wireless standard published by the Institute of Electrical and Electronics Engineers (IEEE) Standards Association.</li> <li>MOK—This modulation was used before the IEEE finished the high-speed 802.11 standard and may still be in use in older wireless networks.</li> </ul>                                                                |

**Table 4-64 11b Radio Advance Settings (continued)**

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Radio Preamble      | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Long—Ensures compatibility between the access point and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A).</li> <li>• Short—Cisco Aironet's Wireless LAN Adapter supports short preambles; it improves throughput performance.</li> </ul>                                                                                                                                                                                                                                                 |
| Bridge Spacing (km) | <p>Enter a value from 0 to 40 kilometers to specify the distance from a root bridge to non-root bridges with which it communicates. Note that you do not need to adjust this setting on non-root bridges.</p> <p>The Bridge Spacing setting adjusts the bridge's timeout values to account for the time required for radio signals to travel from bridge to bridge. If more than one non-root bridge communicates with the root bridge, enter the distance from the root bridge to the non-root bridge that is farthest away.</p> <p>Click <b>See detail</b> to see for which versions this option is valid.</p> |

**Table 4-64 11b Radio Advance Settings (continued)**

| Field             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Non-Root Mobility | <p>This setting applies mainly to repeater access points that you intend to use in a roaming environment.</p> <p>From the list, select one of the following:</p> <ul style="list-style-type: none"><li>• <b>Stationary</b>—Use this setting to specify that the radio firmware not aggressively scan for a better root association, which makes the association more stable but does not allow the access point to roam.</li><li>• <b>Mobile</b>—Use this setting to specify that the radio firmware aggressively scan for a better root association, which allows the access point to roam throughout the wireless network.</li></ul> <p>Click <b>See detail</b> to see for which versions this setting is valid.</p> |

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Defining the 11b Radio Searched Channels Settings

Use this option to limit the channels that the access point scans when Search for less-congested radio channel is enabled.

The access point uses this setting to scan for the radio channel that is least busy and selects that channel for use.



**Note** Not all channels are available for all geographic domains.

### Procedure

- Step 1** Select **11b Radio > Searched Channels**. The 11b Radio: Searched Channels dialog box displays in the right pane.
- Step 2** Click **See details** to see for which versions this option is valid.
- Step 3** Complete the following:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-65 11b Radio Searched Channels Settings**

| Field          | Description                             |
|----------------|-----------------------------------------|
| Channel Number | Lists the available channels by number. |

**Table 4-65 11b Radio Searched Channels Settings (continued)**

| Field           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Frequency (mHz) | <p>Lists the channel frequency.</p> <p>For a list of channel frequency, refer to one of the following:</p> <ul style="list-style-type: none"><li>• URL:<br/><a href="http://www.cisco.com/en/US/products/hw/wireless/ps430/products_command_reference_chapter09186a0080147d8b.html#2450296">http://www.cisco.com/en/US/products/hw/wireless/ps430/products_command_reference_chapter09186a0080147d8b.html#2450296</a></li><li>• Cisco IOS Commands for Access in the <i>Cisco Aironet 1200 Series Access Point Command Reference</i>.</li></ul> |
| Search?         | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"><li>• Yes—Use this option to include the channel in the scan for less-congested channels.</li><li>• No—Use this option to exclude the channel in the scan for less-congested channels</li></ul>                                                                                                                                                                                                                                                            |

**Step 4** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Configuring the 11a Radio

Use this option to configure the device's 11a radio.

### Procedure

- Step 1** Select **11a Radio**. The menu expands and the 11a Radio dialog box displays in the right pane.
- Step 2** Click **See details** to see for which versions this option is valid.
- Step 3** Select one of the following from the Radio menu:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

- Identification—See [Identifying the 11a Radio Port](#), page 4-176.
- Filters—See [Setting Up 11a Radio Filters](#), page 4-179.
- Hardware—See [Defining the 11a Radio Hardware Settings](#), page 4-180.
- Advanced—See [Defining the 11a Radio Advanced Settings](#), page 4-185.
- Searched Channels—See [Defining the 11a Radio Searched Channels Settings](#), page 4-192.
- Data Encryption—See [Defining the 11a Radio Data Encryption Settings](#), page 4-195.
- Module Service Sets—See [Defining the 11a Radio Module Service Sets](#), page 4-199.
- Primary Service Set—See [Defining the 11a Radio Primary Service Set](#), page 4-204.
- Module QoS—See [Configuring 11a Radio QoS](#), page 4-206.

### Identifying the 11a Radio Port

Use this option to define basic identity information for the Ethernet port.



**Note** Changing this setting may cause the access point to reboot.

## Procedure

- Step 1** Select **11a Radio > Identification**. The 11a Radio: Identification dialog box displays in the right pane.
- Step 2** Click **See detail** to see for which versions this option is valid.
- Step 3** Enter the following information to identify the port:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-66** 11a Radio Identification Settings

| Field        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Primary Port | <p>From the list, select one of the following:</p> <p><b>Note</b> If the primary port was set using <b>Ethernet &gt; Identification</b>, the selected value is displayed.</p> <ul style="list-style-type: none"><li>• Ethernet—Sets the Ethernet port for all access points other than AP1200's as the primary port.</li><li>• Ethernet AP 1200—Sets the Ethernet port for AP1200 access points as the primary port.</li><li>• Radio 11b—Sets the 11b radio port as the primary port.</li><li>• Radio 11a—Sets the 11a radio port as the primary port.</li></ul> |

**Table 4-66 11a Radio Identification Settings (continued)**

| Field                       | Description                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Adopt Primary Port Identity | <p><b>Note</b> This setting may cause the device to reboot.</p> <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>yes—This adopts the primary port settings (MAC and IP addresses) for the Ethernet port.</li> <li>no—This uses different MAC and IP addresses for the Ethernet port.</li> </ul> <p>Click <b>See detail</b> to see for which versions this setting is valid.</p> |
| LEAP User Name              | <p>Use this field if the radio is set up as a repeater and authenticates to the network using LEAP. When the radio authenticates using LEAP, the access point sends this user name to the authentication server.</p> <p>Click <b>See detail</b> to see for which versions this option is valid.</p>                                                                                                                      |
| LEAP Password               | <p>Enter the LEAP password.</p> <p>Click <b>See detail</b> to see for which versions this option is valid.</p>                                                                                                                                                                                                                                                                                                           |

**Step 4** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).



## Setting Up 11a Radio Filters

### Procedure

- Step 1** Select **11a Radio > Filters**. The 11a Radio Filters dialog box displays in the right pane.
- Step 2** Click **See detail** to see for which versions this option is valid.
- Step 3** Complete the following:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-67 11a Radio Filters Settings**

| Field       | Description                                                                                                                                |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Ethertype   |                                                                                                                                            |
| Receive     | Enter the ID of a defined Ethertype filter, or select one of the filters you created using <b>Association &gt; Ethertype Filters</b> .     |
| Transmit    | Enter the ID of a defined Ethertype filter, or select one of the filters you created using <b>Association &gt; Ethertype Filters</b> .     |
| IP Protocol |                                                                                                                                            |
| Receive     | Enter the ID of a defined IP protocol filter, or select one of the filters you created using <b>Association &gt; IP Protocol Filters</b> . |
| Transmit    | Enter the ID of a defined IP protocol filter, or select one of the filters you created using <b>Association &gt; IP Protocol Filters</b> . |

**Table 4-67 11a Radio Filters Settings (continued)**

| Field    | Description                                                                                                                                 |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------|
| IP Port  |                                                                                                                                             |
| Receive  | Enter the ID of a defined IP port protocol filter, or select one of the filters you created using <b>Association &gt; IP Port Filters</b> . |
| Transmit | Enter the ID of a defined IP port protocol filter, or select one of the filters you created using <b>Association &gt; IP Port Filters</b> . |

**Step 4** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Defining the 11a Radio Hardware Settings

### Procedure

- Step 1** Select **11a Radio > Hardware**. The 11a Radio: Hardware dialog box displays in the right pane.
- Step 2** Click **See detail** to see for which versions this option is valid.

**Step 3** Complete the following:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-68 11a Radio Hardware Settings**

| Field                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service Set ID (SSID)               | <p>Enter a unique identifier client devices use to associate with the access point. It can be any alphanumeric, case-sensitive string, from 1 to 32 characters long.</p> <p>Several access points on a network or sub-network can share an SSID.</p>                                                                                                                                                                                                                                                                                                                  |
| Allow “Broadcast” SSID to Associate | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"><li>• yes—Allows devices that do not specify an SSID (devices that are “broadcasting” in search of an access point) to associate with to associate with the access point.</li><li>• no—Does not allow devices that do not specify an SSID (devices that are “broadcasting” in search of an access point) to associate with to associate with the access point.</li></ul> <p>With no selected, the SSID used by the client device must match exactly the access point’s SSID.</p> |

**Table 4-68 11a Radio Hardware Settings (continued)**

| Field                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Rates (Mb/sec)                |                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 6.0                                | <p>From the list, select one of the following for each of the four rates in megabits per second:</p> <ul style="list-style-type: none"> <li>• basic—Allows transmission at this rate for all packets, both unicast and multicast. At least one data rate must be set to basic.</li> <li>• yes—Allows transmission at this rate for unicast packets only.</li> <li>• no—Does not allow transmission at this rate.</li> </ul> |
| 9.0                                |                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 12.0                               |                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 18.0                               |                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 24.0                               |                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 36.0                               |                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 48.0                               |                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 54.0                               |                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Transmit Power                     | <p>From the list, select one of the following milliwatt settings: 5, 10, 20, 40.</p> <p>To reduce interference or to conserve power, select a lower power setting.</p> <p>Click <b>See details</b> to see for which versions this setting is valid.</p>                                                                                                                                                                     |
| Fragmentation Threshold (256-2338) | <p>Enter a setting to determine the size at which packets are fragmented (sent as several pieces instead of as one block).</p> <p>Use a low setting in areas where communication is poor or where there is a great deal of radio interference.</p>                                                                                                                                                                          |
| RTS Threshold (0-2339)             | <p>Enter a setting to determine the packet size at which the access point issues a request to send (RTS) before sending the packet.</p> <p>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.</p>                                                     |

**Table 4-68 11a Radio Hardware Settings (continued)**

| Field                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maximum RTS Retries (1-128)              | Enter the maximum number of times the access point issues an RTS before stopping the attempt to send the packet through the radio.                                                                                                                                                                                                                                                                                                                                                              |
| Max. Data Retires (1-128)                | Enter the maximum number of attempts the access point makes to send a packet before giving up and dropping the packet.                                                                                                                                                                                                                                                                                                                                                                          |
| Beacon Period (Kusec)                    | Enter the amount of time between beacons in kilomicroseconds. (One kilomicrosecond equals 1,024 microseconds.)                                                                                                                                                                                                                                                                                                                                                                                  |
| Data Beacon Rate (DTIM)                  | <p>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).</p> <p>The DTIM tells power-save client devices that a packet is waiting for them.</p> <p>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 Kmsecs. (One Kmsec equals 1,024 microseconds.)</p> |
| Default Radio Channel                    | From the list, select the radio channel you want for a default.                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Search for less-congested Radio Channel? | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• yes—Allows the access point to scan for the radio channel that is least busy and selects that channel for use.</li> <li>• no—Will not allow the access point to scan for a radio channel that is least busy.</li> </ul>                                                                                                                                                                             |

**Table 4-68 11a Radio Hardware Settings (continued)**

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Receive Antenna  | From the list, select one of the following:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Transmit Antenna | <ul style="list-style-type: none"> <li> <b>Right</b>—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.)<br/><br/>           Use this setting for both receive and transmit.         </li> <li> <b>Left</b>—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's left connector. (When you look at the access point's back panel, the left antenna is on the left.)<br/><br/>           Use this setting for both receive and transmit.         </li> <li> <b>Diversity</b>—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.<br/><br/>           Use this setting for both receive and transmit.         </li> </ul> |

- Step 4** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Defining the 11a Radio Advanced Settings

Use this option to define the settings and operational status of the Ethernet port.

### Procedure

---

- Step 1** Select **11a Radio > Advanced**. The 11a Radio: Advanced dialog box displays in the right pane.

Click **See detail** to see for which versions this setting is valid.

- Step 2** Complete the following:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

---

**Table 4-69 11a Radio Advanced Settings**

| Field  | Description                                                                                                                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status | From the list, select one of the following: <ul style="list-style-type: none"><li>• up—Enables the Radio port for normal operation.</li><li>• down—Disables the device's Radio port.</li></ul> |

**Table 4-69 11a Radio Advanced Settings (continued)**

| Field                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Packet Forwarding                | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>enabled—Allows normal operation.</li> <li>disabled—Prevents data from moving between the Ethernet and the radio, which is useful in troubleshooting.</li> </ul>                                                                                                                                                                     |
| Default Multicast Address Filter | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed under <b>Association &gt; Address Filters</b>.</li> <li>Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed under <b>Association &gt; Address Filters</b>.</li> </ul> |
| Maximum Multicast Packets/Second | <p>Use this setting to control the number of multicast packets that can pass through the Ethernet port each second.</p> <p>If you enter 0, the access point passes an unlimited number of multicast packets.</p> <p>If you enter a number other than 0, the device passes only that number of multicast packets per second.</p>                                                                                               |



**Table 4-69 11a Radio Advanced Settings (continued)**

| Field                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Radio Cell Role                | <p>From the list, enter one of the following:</p> <ul style="list-style-type: none"><li>• Client/Non-Root—use this setting for diagnostics or site surveys, such as when you need to test and access point by having it communicate with another access point or bridge without accepting associations from client devices.</li><li>• Repeater/Non-Root—Use this setting for access points that are not connected to a wired LAN and which transfer data between another access point or repeater.</li><li>• Access Point/Root—Use this setting if the access point is connected to a wired LAN.</li></ul> |
| Maximum Number of Associations | <p>Enter the maximum number of wireless networking devices that are allowed to associate to the access point.</p> <p>If you enter 0 it means that the maximum possible number of associations is allowed.</p> <p>Click <b>See details</b> to see for which versions this setting is valid.</p>                                                                                                                                                                                                                                                                                                             |
| Use Aironet Extensions         | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"><li>• yes—Enable load balancing, Message Integrity Check (MIC), and WEP key hashing.</li><li>• no—Does not enable the features listed above.</li></ul>                                                                                                                                                                                                                                                                                                                                                                |

**Table 4-69 11a Radio Advanced Settings (continued)**

| Field                                                | Description                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Classify Workgroup Bridges as network infrastructure | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• yes—Use this setting to limit the number of workgroup bridges that can associate to the access point to 20 or less.</li> <li>• no—Use this setting to allow more than 20 workgroup bridges to associate to the access point.</li> </ul>       |
| Ethernet encapsulation transform                     | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• 802.1H—Provides optimum performance for Cisco Aironet wireless products.</li> <li>• RFC1042—Ensures interoperability with non-Cisco Aironet wireless equipment.</li> </ul>                                                                    |
| Enhanced MIC verification for WEP                    | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• None—Does not enable MIC.</li> <li>• NMH—Enables MIC (Message Integrity Check), a security feature that protects your WEP keys by preventing attacks on encrypted packets called bit-flip attacks.</li> </ul>                                 |
| Temporal Key Integrity Protocol                      | <p>From the list, select the following:</p> <ul style="list-style-type: none"> <li>• None—Does not enable WEP key hashing.</li> <li>• Cisco—Enables WEP key hashing that defends against an attack on WEP in which the intruder uses the unencrypted initialization vector (IV) in encrypted packets to calculate the WEP key.</li> </ul> |

**Table 4-69 11a Radio Advanced Settings (continued)**

| Field                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Broadcast WEP Key rotation interval (sec) | <p>Enter a rotation interval in seconds.</p> <ul style="list-style-type: none"> <li>If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes.</li> <li>If you enter 0, you disable broadcast WEP key rotation.</li> </ul>                                                                                                                                                                                                                 |
| Accept Authentication Type                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Open                                      | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting.</li> <li>No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.</li> </ul>                                                                                                                                                                  |
| Shared                                    | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Yes—Tells the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting.</li> <li>No—Does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.</li> </ul> |

**Table 4-69 11a Radio Advanced Settings (continued)**

| Field       | Description                                                                                                                                                                                                                                                                                                                                     |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network-EAP | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Allows EAP-enabled client devices to authenticate through the access point.</li> <li>• No—Does not allow EAP-enabled client devices to authenticate through the access point.</li> </ul>                                                        |
| Require EAP |                                                                                                                                                                                                                                                                                                                                                 |
| Open        | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point.</li> <li>• No—Use this option if you do not use open and EAP authentication.</li> </ul>     |
| Shared      | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point.</li> <li>• No—Use this option if you do not use shared and EAP authentication.</li> </ul> |

**Table 4-69 11a Radio Advanced Settings (continued)**

| Field                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default Unicast Address Filter |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Open                           | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters.</li> <li>Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed with the Address Filters or on your authentication server.</li> </ul> <p>Select Disallowed for each authentication type that also uses MAC-based authentication.</p> |
| Shared                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Network-EAP                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Specified Access Point 1       | <p>If this access point is a repeater, enter the MAC address of one or more root-unit access points with which you want this access point to associate.</p>                                                                                                                                                                                                                                                                                                                                                         |
| Specified Access Point 2       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Specified Access Point 3       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Specified Access Point 4       | <p>With MAC addresses in these fields, the repeater access point always tries to associate with the specified access points instead of with other less-efficient access points.</p>                                                                                                                                                                                                                                                                                                                                 |

**Table 4-69 11a Radio Advanced Settings (continued)**

| Field             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Non-Root Mobility | <p>This setting applies mainly to repeater access points that you intend to use in a roaming environment.</p> <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Stationary</b>—Use this setting to specify that the radio firmware not aggressively scan for a better root association, which makes the association more stable but does not allow the access point to roam.</li> <li>• <b>Mobile</b>—Use this setting to specify that the radio firmware aggressively scan for a better root association, which allows the access point to roam throughout the wireless network.</li> </ul> <p>Click <b>See detail</b> to see for which versions this setting is valid.</p> |

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Defining the 11a Radio Searched Channels Settings

Use this option to limit the channels that the access point scans when Search for less-congested radio channel is enabled.

The access point uses this setting to scan for the radio channel that is least busy and selects that channel for use.



**Note** Not all channels are available for all geographic domains.

### Procedure

**Step 1** Select **11a Radio > Searched Channels**. The 11a Radio: Searched Channels dialog box displays in the right pane.

Click **See detail** to see for which versions this setting is valid.

**Step 2** Complete the following:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-70 11a Radio Searched Channels Settings**

| Field          | Description                             |
|----------------|-----------------------------------------|
| Channel Number | Lists the available channels by number. |

**Table 4-70 11a Radio Searched Channels Settings (continued)**

| Field           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Frequency (mHz) | <p>Lists the channel frequency.</p> <p>For a list of channel frequency, refer to one of the following:</p> <ul style="list-style-type: none"> <li>• URL:<br/> <a href="http://www.cisco.com/en/US/products/hw/wireless/ps430/products_command_reference_chapter09186a0080147d8b.html#2450296">http://www.cisco.com/en/US/products/hw/wireless/ps430/products_command_reference_chapter09186a0080147d8b.html#2450296</a> </li> <li>• Cisco IOS Commands for Access in the <i>Cisco Aironet 1200 Series Access Point Command Reference</i>.</li> </ul> |
| Search?         | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this option to include the channel in the scan for less-congested channels.</li> <li>• No—Use this option to exclude the channel in the scan for less-congested channels</li> </ul>                                                                                                                                                                                                                                                              |



**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Defining the 11a Radio Data Encryption Settings

Use this option to limit the channels that the access point scans when Search for less-congested radio channel is enabled.

The access point uses this setting to scan for the radio channel that is least busy and selects that channel for use.

### Procedure

---

- Step 1** Select **11a Radio > Data Encryption**. The 11a Radio: Data Encryption dialog box displays in the right pane.
- Step 2** Click **See detail** to see for which versions this setting is valid.

**Step 3** Complete the following:

**Table 4-71 11a Radio Data Encryption Settings**

| Field                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Encryption by Stations | <p>From the list, select the encryption type:</p> <ul style="list-style-type: none"> <li>• No Encryption—Requires clients to communicate with the Access Point without any data encryption. This setting is not recommended.</li> <li>• Optional—Allows clients to communicate with the Access Point either with or without data encryption. Typically, this option is used when you have client devices that cannot make a WEP connection, such as non-Cisco clients in a 128-bit WEP environment.</li> <li>• Full Encryption—Requires clients to use data encryption when communicating with the Access Point. Clients not using data encryption are allowed to communicate. This option is recommended if you want to maximize the security of your Wireless LAN.</li> </ul> |
| Authentication Type         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Open                        | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting.</li> <li>• No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                             |

**Table 4-71 11a Radio Data Encryption Settings (continued)**

| Field       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Shared      | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—This setting enables the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting.</li> <li>• No—This setting does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.</li> </ul> |
| Network EAP | <p>From the list, select one of the following:</p> <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Allows EAP-enabled client devices to authenticate through the access point.</li> <li>• No—Does not allow EAP-enabled client devices to authenticate through the access point.</li> </ul>                                                                                                                                                                                                      |
| Require EAP |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Open        | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point.</li> <li>• No—Use this option if you do not use open and EAP authentication.</li> </ul>                                                                                                                                                                                                      |

**Table 4-71 11a Radio Data Encryption Settings (continued)**

| Field                       | Description                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Shared                      | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point.</li> <li>• No—Use this option if you do not use shared and EAP authentication.</li> </ul> |
| Encryption Keys 1 through 4 |                                                                                                                                                                                                                                                                                                                                                 |
| Transmit Key                | Click to indicate this is the key you want to use to transmit packets. Only one key can be selected at a time.                                                                                                                                                                                                                                  |
| Encryption Key              | <p>Enter the type of encryption key used:</p> <ul style="list-style-type: none"> <li>• For 40-bit WEP keys, enter as 10 hexadecimal digits (0-9, a-f, or A-F).</li> <li>• For 128-bit WEP keys, enter as 26 hexadecimal digits (0-9, a-f, or A-F).</li> </ul>                                                                                   |
| Key Size                    | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• 40 bit</li> <li>• 128 bit</li> <li>• Not set</li> </ul>                                                                                                                                                                                             |

**Step 4** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Defining the 11a Radio Module Service Sets

Use this option to limit the channels that the access point scans when Search for less-congested radio channel is enabled.

The access point uses this setting to scan for the radio channel that is least busy and to select that channel for use.

### Procedure

---

**Step 1** Select **11a Radio > Module Service Sets**. The 11a Radio: Module Service Sets dialog box displays in the right pane.

**Step 2** Click **See detail** to see which versions this option is valid for.



---

**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

---

**Step 3** Using this option you can:

- Add a new Service Set—See [Adding a New Service Set, page 4-200](#).
  - Delete an exiting Service Set from a device—See [Deleting an Existing Service Sets, page 4-203](#).
-

## Adding a New Service Set

### Procedure

**Step 1** To add a new module service set, enter the following:

**Table 4-72 New Module Service Sets**

| Field                                                       | Description                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device                                                      |                                                                                                                                                                                                                                                                |
| SSID for use by Infrastructure Stations (such as Repeaters) | Enter an identification number for the client radio SSID.                                                                                                                                                                                                      |
| Disallow Infrastructure Stations on any other SSID          | <p>From the list, select one of the following:</p> <p>Yes—Use this option to disallow infrastructure stations on any other SSID.</p> <p>No—Use this option to allow infrastructure stations on any other SSID.</p>                                             |
| Add New Service Set                                         |                                                                                                                                                                                                                                                                |
| Service Set ID (1-32)                                       | Enter an identification for the SSID.                                                                                                                                                                                                                          |
| Service Set Name                                            | Enter the SSID.                                                                                                                                                                                                                                                |
| Maximum Number of Associations                              | Enter a number to limit the maximum number of wireless clients per SSID.                                                                                                                                                                                       |
| Proxy Mobile IP Enabled                                     | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Yes—This setting allows proxy mobile IP use by all stations associated to this access point.</li> <li>No—This setting does not allow proxy mobile IP use.</li> </ul> |
| Default VLAN ID                                             | Enter the identification number for a defined VLAN, or select one of the VLAN IDs you created using <b>Association &gt;VLANs</b> .                                                                                                                             |

**Table 4-72 New Module Service Sets (continued)**

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default Policy Group       | Enter the identification number of a defined policy group, or select one of the policy groups you created using <b>Association &gt; Policy Groups</b> .                                                                                                                                                                                                                                                                                                                                                              |
| Accept Authentication Type |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Open                       | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting.</li> <li>• No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.</li> </ul>                                                                                                                                                                  |
| Shared                     | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Tells the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting.</li> <li>• No—Does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.</li> </ul> |
| Network-EAP                | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Allows EAP-enabled client devices to authenticate through the access point.</li> <li>• No—Does not allow EAP-enabled client devices to authenticate through the access point.</li> </ul>                                                                                                                                                                                                                             |

**Table 4-72 New Module Service Sets (continued)**

| Field                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Require EAP                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Open                           | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point.</li> <li>• No—Use this option if you do not use open and EAP authentication.</li> </ul>                                                                                                                                                                             |
| Shared                         | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point.</li> <li>• No—Use this option if you do not use shared and EAP authentication.</li> </ul>                                                                                                                                                                         |
| Default Unicast Address Filter |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Open                           | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters.</li> <li>• Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed with the Address Filters or on your authentication server.</li> </ul> <p>Select Disallowed for each authentication type that also uses MAC-based authentication.</p> |
| Shared                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Network-EAP                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

**Step 2** Click **Add** to add the Service Set to the Service Sets to Add list.

**Step 3** To delete a group from the list, select the name, then click **Delete**.



**Step 4** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

### Deleting an Existing Service Sets

#### Procedure

---

**Step 1** Enter the Service Set number in the **Service Set ID** text box, then click **Add** to add it to the Service Sets to Delete list.

**Step 2** To delete an identification number from the list, select it, then click **Delete**.

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
-

## Defining the 11a Radio Primary Service Set

Use this option to set a default VLAN for the primary SSID on an access point.

### Procedure

- Step 1** Select **11a Radio > Primary Service Set**. The 11a Radio: Primary Service Set dialog box displays in the right pane.



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

- Step 2** Enter the following information:

**Table 4-73 Primary Service Set**

| Field                          | Description                                                                                                                                                                                                                                             |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service Set Name               | Enter the name.                                                                                                                                                                                                                                         |
| Maximum Number of Associations | Enter a number to limit the maximum number of wireless clients per SSID.                                                                                                                                                                                |
| Proxy Mobile IP Enabled        | From the list, select one of the following: <ul style="list-style-type: none"> <li>Yes—This setting allows proxy mobile IP use by all stations associated to this access point.</li> <li>No—This setting does not allow proxy mobile IP use.</li> </ul> |
| Default VLAN ID                | Enter the identification number for a defined VLAN, or select one of the VLAN IDs you created using <b>Association &gt; VLANs</b> .                                                                                                                     |
| Default Policy Group           | Enter the identification number of a defined policy group, or select one of the policy groups you created using <b>Association &gt; Policy Groups</b> .                                                                                                 |

**Table 4-73 Primary Service Set (continued)**

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Accept Authentication Type |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Open                       | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting.</li> <li>• No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.</li> </ul>                                                                                                                                                                  |
| Shared                     | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Tells the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting.</li> <li>• No—Does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.</li> </ul> |
| Network-EAP                | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Allows EAP-enabled client devices to authenticate through the access point.</li> <li>• No—Does not allow EAP-enabled client devices to authenticate through the access point.</li> </ul>                                                                                                                                                                                                                             |
| Require EAP                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Open                       | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point.</li> <li>• No—Use this option if you do not use open and EAP authentication.</li> </ul>                                                                                                                                                                          |

**Table 4-73 Primary Service Set (continued)**

| Field                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Shared                         | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b>—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point.</li> <li>• <b>No</b>—Use this option if you do not use shared and EAP authentication.</li> </ul>                                                                                                                      |
| Default Unicast Address Filter |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Open                           | From the list, select one of the following:                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Shared                         | <ul style="list-style-type: none"> <li>• <b>Allowed</b>—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters.</li> <li>• <b>Disallowed</b>—The access point discards all traffic except packets sent to the MAC addresses set as allowed with the Address Filters or on your authentication server.</li> </ul> <p>Select Disallowed for each authentication type that also uses MAC-based authentication.</p> |
| Network-EAP                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Configuring 11a Radio QoS

Use this option to define traffic class QoS policies.

## Procedure

**Step 1** Select **11a Radio > Module QoS**. The 11a Radio: Quality of Service dialog box appears.

Click **See detail** to see which versions this option is valid for.

**Step 2** Complete the following:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-74 11a Radio QoS**

| Field                   | Description                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Generate QBBS Element   | From the list, select one of the following: <ul style="list-style-type: none"> <li>• Yes—Use this setting to enable support for basic 802.11 Quality of Service.</li> <li>• No—Use this setting to disable support for basic 802.11 Quality of Service.</li> </ul>                                                                                             |
| User Symbol Extensions  | From the list, select one of the following: <ul style="list-style-type: none"> <li>• Yes—Use this setting enables support for Symbol Voice over IP (VoIP phones).</li> <li>• No—Use this setting to disable support for Symbol VoIP phones.</li> </ul>                                                                                                         |
| Send IGMP General Query | From the list, select one of the following: <ul style="list-style-type: none"> <li>• Yes—Use this setting to allow the access point to send an IGMP General Query to all associated stations when they complete all required high-level authentication.</li> <li>• No—Use this setting to not allow the access point to send an IGMP General Query.</li> </ul> |

**Table 4-74 11a Radio QoS (continued)**

| Field                 | Description                                                                                                                                                                                                   |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Background            | <ul style="list-style-type: none"> <li>Min Contention Window—Enter the minimum contention window value. The value listed is to the power of 2. The access point computes Contention Window values.</li> </ul> |
| (spare)               |                                                                                                                                                                                                               |
| Best Effort (default) |                                                                                                                                                                                                               |
| Excellent Effort      | <ul style="list-style-type: none"> <li>Max Contention Window—Enter the maximum contention window value. The value listed is to the power of 2. The access point computes Contention Window values.</li> </ul> |
| Controlled Load       |                                                                                                                                                                                                               |
| Interactive Video     |                                                                                                                                                                                                               |
| Interactive Voice     | <ul style="list-style-type: none"> <li>Fixed Slot Time—Enter a value for a fixed slot time.</li> </ul>                                                                                                        |
| Network Control       |                                                                                                                                                                                                               |

**Step 3** Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-3](#).

## Defining the Security Settings

Use this option to configure the device's security settings.

### Procedure

**Step 1** Select **Security**. The menu expands and the Security dialog box displays in the right pane.

**Step 2** Select one of the following from the Security menu:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

- Local Admin Access—See [Setting Local Admin Access, page 4-209](#).
- Local AP/Client Security—See [Setting Local AP/Client Security, page 4-213](#).
- Authentication Server Security—See [Setting Authentication Server Security, page 4-216](#).

## Setting Local Admin Access

Use this option to enable or disable local admin access.

### Procedure

**Step 1** Select **Security > Local Admin Access**. The Security: Local Admin Access 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 Template windows up until that point.

**Table 4-75 Local Admin Access Settings**

| Field                                  | Description                                                                                                                                                                                                                           |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Local Admin Authentication             | From the list, select one of the following: <ul style="list-style-type: none"><li>• Enable—Use this setting to enable local admin authentication.</li><li>• Disable—Use this setting to disable local admin authentication.</li></ul> |
| Allow read-only browsing without login | From the list, select one of the following: <ul style="list-style-type: none"><li>• Yes—Use this setting to allow read-only browsing.</li><li>• No—Use this setting to disallow read-only browsing.</li></ul>                         |

**Step 3** Using this option you can:

- Add Users—See [Adding Users](#), page 4-211.
  - Delete Users—See [Deleting Users](#), page 4-212.
-



## Adding Users

### Procedure

**Step 1** To add a new user, enter the following:

| Field                 | Description                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add Users             | Click <b>See user details</b> for information about existing user IDs. See <a href="#">Understanding the User Details Window, page 4-212</a> for information about the table.                                                                                                                                                                                     |
| User Identifier       | Enter an identification number for the user. Use the table in the User Details window to help assign a number. If you use an existing identifier number, you will modify the current setting.<br><br><b>Tip</b> If you want to set the same user name on all access points and do not know which user ID's may already be in use, enter a very high value (2000). |
| User name             | Enter the name for the user.                                                                                                                                                                                                                                                                                                                                      |
| User password         | Enter a password for the user.                                                                                                                                                                                                                                                                                                                                    |
| Confirm User Password | Reenter the password.                                                                                                                                                                                                                                                                                                                                             |
| Capabilities          | Select the capabilities you want to allow the user.                                                                                                                                                                                                                                                                                                               |

**Step 2** Click >> to add the users to the Users to Add list.

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Deleting Users

### Procedure

- 
- Step 1** Click **See detail** to see which versions this option is valid for.
- Click **See user details** Click **See user details** for information about existing user IDs. See [Understanding the User Details Window, page 4-212](#) for information about the table.
- Step 2** Enter the user's identification number in the **User Identifier** text box, then click >> to add it to the Users to Delete list.
- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

### Understanding the User Details Window

When you click **see user details**, a window appears with the following table:

| Field           | Description                                                                     |
|-----------------|---------------------------------------------------------------------------------|
| Device Name     | The device name.                                                                |
| IP Address      | The IP address of the device.                                                   |
| User Identifier | The currently assigned user identifier.                                         |
| Username        | The user name.                                                                  |
| Timestamp       | The time and date in which the information was collected from the access point. |

## Setting Local AP/Client Security

Use this option to set up the local access point and client security.

### Procedure

**Step 1** Select **Security > Local AP/Client Security**. The Security: Local AP/Client Security 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 Template windows up until that point.

**Table 4-76 Local AP /Client Security Settings**

| Field                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Encryption by Stations | <p>From the list, select the encryption type:</p> <ul style="list-style-type: none"><li>• No Encryption—Requires clients to communicate with the Access Point without any data encryption. This setting is not recommended.</li><li>• Optional—Allows clients to communicate with the Access Point either with or without data encryption. Typically, this option is used when you have client devices that cannot make a WEP connection, such as non-Cisco clients in a 128-bit WEP environment.</li><li>• Full Encryption—Requires clients to use data encryption when communicating with the Access Point. Clients not using data encryption are allowed to communicate. This option is recommended if you want to maximize the security of your Wireless LAN.</li></ul> |
| Authentication Type         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

**Table 4-76 Local AP /Client Security Settings (continued)**

| Field       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Open        | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting.</li> <li>• No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.</li> </ul>                                                                                                                                                                  |
| Shared Key  | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Tells the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting.</li> <li>• No—Does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.</li> </ul> |
| Network-EAP | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Allows EAP-enabled client devices to authenticate through the access point.</li> <li>• No—Does not allow EAP-enabled client devices to authenticate through the access point.</li> </ul>                                                                                                                                                                                                                             |
| Require EAP |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Open        | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point.</li> <li>• No—Use this option if you do not use open and EAP authentication.</li> </ul>                                                                                                                                                                          |

**Table 4-76 Local AP /Client Security Settings (continued)**

| Field                       | Description                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Shared                      | From the list, select one of the following: <ul style="list-style-type: none"><li>• Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point.</li><li>• No—Use this option if you do not use shared and EAP authentication.</li></ul> |
| Encryption Keys 1 through 4 |                                                                                                                                                                                                                                                                                                                                       |
| Transmit Key                | Click 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: <ul style="list-style-type: none"><li>• For 40-bit WEP keys, enter as 10 hexadecimal digits (0-9, a-f, or A-F).</li><li>• For 128-bit WEP keys, enter as 26 hexadecimal digits (0-9, a-f, or A-F).</li></ul>                                                                                   |
| Key Size                    | From the list, select one of the following: <ul style="list-style-type: none"><li>• Not set</li><li>• 40 bit</li><li>• 128 bit</li></ul>                                                                                                                                                                                              |

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Setting Authentication Server Security

Use this option to set up authentication server security.

**Note**

---

Changing this setting may cause the access point to reboot.

---

### Procedure

---

**Step 1** Select **Security > Authentication Server**. The Security: Authentication Server 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 Template windows up until that point.

---

**Table 4-77 Authentication Server Settings**

| Field                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 802.1X Protocol Version (For EAP Authentication) | <p><b>Note</b> This setting may cause the device to reboot.</p> <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Draft 7—No radio firmware versions compliant with Draft 7 have LEAP capability, so you should not need to select this setting.</li> <li>• Draft 8—Select this option if LEAP-enabled client devices that associate with this access point use radio firmware versions 4.13, 4.16, or 4.23, or if workgroup bridges associating with this access point use firmware version 8.58 or earlier.</li> <li>• Draft 10—Select this option if client devices that associate with this access point or bridge use Microsoft Windows XP EAP authentication, if LEAP-enabled client devices that associate with this bridge use radio firmware version 4.25 or later, or if workgroup bridges associating with this access point use firmware version 8.65 or later.</li> </ul> <p>Click <b>See detail</b> for information on which version this setting is valid</p> |
| Primary Server Reattempt Period (Min)            | <p>Enter the amount of time a before another attempt is made if the server is not responding.</p> <p>Click <b>See detail</b> for information on which version this setting is valid.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Table 4-77 Authentication Server Settings (continued)**

| Field            | Description                                                                                                                                                                                                             |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Name/IP   | Enter the name or IP address of the server.                                                                                                                                                                             |
| Server Type      | Enter the type of server.<br><br>Click <b>See detail</b> for information on which version this setting is valid                                                                                                         |
| Port             | Enter the port number your server uses for authentication.                                                                                                                                                              |
| Shared Secret    | Enter the shared secret used by your server. It must match the shared secret on the RADIUS server.                                                                                                                      |
| Retran Int (sec) | Enter the number of seconds the access point should wait before retransmitting.<br><br>Click <b>See detail</b> for information on which version this setting is valid.                                                  |
| Max Retran       | Enter the number of times the access point should attempt to contact the server before giving up.<br><br>Click <b>See detail</b> for information on which version this setting is valid.                                |
| Time Out (sec's) | Enter the number of seconds the access point should wait before authentication fails.<br><br>If the server does not respond within this time, the access point tries to contact the next defined authentication server. |



**Table 4-77 Authentication Server Settings (continued)**

| Field     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EAP Auth. | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"><li>• Yes—Use this server for EAP authentication.</li></ul> <p>In this type of authentication, the access point relays authentication messages between the server and the authenticating client device.</p> <ul style="list-style-type: none"><li>• No—Do not use this server for EAP authentication.</li></ul> <p>Click <b>See detail</b> for information on which version this setting is valid.</p>                                                                                                                   |
| MAC Auth. | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"><li>• Yes—Use this server for MAC-based authentication.</li></ul> <p>This allows only client devices with specified MAC addresses to associate and pass data through the access point. Client devices with MAC addresses not in a list of allowed MAC addresses are not allowed to associate with the access point.</p> <ul style="list-style-type: none"><li>• No—Do not use this server for MAC-based authentication.</li></ul> <p>Click <b>See detail</b> for information on which version this setting is valid.</p> |

**Table 4-77 Authentication Server Settings (continued)**

| Field      | Description                                                                                                                                                                                                                                                                                                                                                             |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Auth. | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this setting to allow user authentication.</li> <li>• No—Use this setting to disallow user authentication.</li> </ul> <p>Click <b>See detail</b> for information on which version this setting is valid.</p>                                                        |
| MIP Auth.  | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this setting to authenticate proxy Mobile IP configured clients.</li> <li>• No—Use this setting to disallow authentication of proxy Mobile IP configured clients.</li> </ul> <p>Click <b>See detail</b> for information on which version this setting is valid.</p> |

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Configuring 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 Services dialog box displays in the right pane.
- Step 2** Select one of the following from the Services menu:
- Start-Up—See [Configuring Start-Up Settings, page 4-222](#).
  - Console/Telnet—See [Configuring Console/Telnet Settings, page 4-225](#).
  - Hot Standby—See [Configuring Hot Standby Settings, page 4-227](#).
  - Routing—See [Configuring Routing Settings, page 4-229](#).
  - CDP—See [Configuring CDP Settings, page 4-230](#).
  - DNS—See [Configuring DNS Settings, page 4-231](#).
  - FTP—See [Configuring FTP Settings, page 4-233](#).
  - HTTP—See [Configuring HTTP Settings, page 4-234](#).
  - SNMP—See [Configuring SNMP Settings, page 4-235](#).
  - Sntp—See [Configuring Sntp Settings, page 4-236](#).
  - Accounting—See [Configuring Accounting Settings, page 4-238](#).
  - ProxyMobile IP Setup—See [Setting Up Proxy Mobile IP, page 4-242](#).
  - ProxyMobile SA Bind—See [Configuring Proxy Mobile SA Bindings, page 4-243](#).
-

## Configuring Start-Up Settings

Use this option to configure the access point for your network's BOOTP or DHCP servers for automatic assignment of IP addresses.

### Procedure

**Step 1** Select **Services > Start-Up**. The Services: Start-Up 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 Template windows up until that point.

**Table 4-78 Start-Up Settings**

| Field                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuration Server Protocol                           | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>None</b>—Use this setting if your network does not have an automatic system for IP address assignment.</li> <li>• <b>BOOTP</b>—Use this setting if IP addresses are hard-coded based on MAC addresses.</li> <li>• <b>DHCP</b>—Use this setting if IP addresses are “leased” for predetermined periods of time.</li> </ul> |
| Use prior Config Server settings if no server responds? | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>yes</b>—Use this setting to have the access point save the boot server's most recent response.</li> <li>• <b>no</b>—Use this setting to not use the most recent response.</li> </ul>                                                                                                                                      |

**Table 4-78 Start-Up Settings (continued)**

| Field                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Read “.ini” file from file server?    | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>always</b>—Use this setting for the access point to always load configuration settings from an .ini file on the server.</li> <li>• <b>never</b>—Use this setting for the access point to never load configuration settings from an .ini file on the server.</li> <li>• <b>if specified by server</b>—Use this setting for the access point to load configuration settings from an .ini file on the server if the server’s DHCP or BOOTP response specifies that an .ini file is available.</li> </ul> |
| BOOTP Server Timeout (sec’s)          | Enter the length of time the access point waits to receive a response from a single BOOTP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| DHCP Multiple-Offer Timeout (sec’s)   | Enter the length of time the access point waits to receive a response when there are multiple DHCP servers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| DHCP Requested Lease Duration (min’s) | Enter the length of time the access point requests for an IP address lease from your DHCP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| DHCP Minimum Lease Duration (min’s)   | Enter the shortest amount of time the access point accepts for an IP address lease. The access point ignores leases shorter than this period.                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| DHCP Client Identifier Type           | <p>From the list, select one of the client identifier types.</p> <p>Click <b>See detail</b> to see for which versions this setting is valid.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

**Table 4-78 Start-Up Settings (continued)**

| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DHCP Client Identifier Value | <p>Use this setting to include a unique identifier in the access point's DHCP request packet.</p> <ul style="list-style-type: none"><li>• If you select Other-Non Hardware from the DHCP Client Identifier Type list, you can enter up to 255 alphanumeric characters.</li><li>• If you select any other option from the DHCP Client Identifier Type list, you can enter up to 12 hexadecimal characters (numbers 0 through 9, and the letters A through F).</li></ul> <p>Click <b>See detail</b> to see for which versions this setting is valid.</p> |
| DHCP Class Identifier        | <p>Enter the access point's group name.</p> <p>The DHCP server uses the group name to determine the response to send to the access point.</p>                                                                                                                                                                                                                                                                                                                                                                                                          |

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Configuring Console/Telnet Settings

Use this option to configure the access point to work with a terminal emulator or through Telnet.

### Procedure

---

- Step 1** Select **Services > Console/Telnet**. The Services: Console/Telnet 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 Template windows up until that point.

---

**Table 4-79 Console/Telnet Settings**

| Field     | Description                                                                                                                                                                                  |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Baud Rate | Enter a rate from 110 to 115,200, expressed in bits per second.<br><br>The rate you enter is dependent on the capability of the computer you use to open the access point management system. |

**Table 4-79 Console/Telnet Settings (continued)**

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parity           | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• None—Use this setting to use no parity bit.</li> <li>• Even—Use this setting to make the total number of bits even.</li> <li>• Odd—Use this setting to make the total number of bits odd.</li> </ul>                                                                            |
| Data Bits        | From the list, select one of the data bit settings.                                                                                                                                                                                                                                                                                                                         |
| Stop Bits        | From the list, select one of the stop bit settings.                                                                                                                                                                                                                                                                                                                         |
| Flow Control     | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• None—Use this setting to indicate no flow control is used.</li> <li>• SW Xonn/Xoff—Use this setting to indicate the method information is sent between pieces of equipment to prevent loss of data when too much information arrives at the same time on one device.</li> </ul> |
| Terminal Type    | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• teletype—Use this setting if your terminal emulator does not support ANSI.</li> <li>• ANSI—Use this setting to offer graphic features such as reverse video buttons and underlined links.</li> </ul>                                                                            |
| Columns (64-132) | Enter a number to define the width of the terminal emulator display within the range of 64 characters to 132 characters.                                                                                                                                                                                                                                                    |
| Lines (16-50)    | Enter a number to define the height of the terminal emulator display within the range of 16 characters to 50 characters.                                                                                                                                                                                                                                                    |



**Table 4-79 Console/Telnet Settings (continued)**

| Field  | Description                                                                                                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Telnet | From the list, select one of the following: <ul style="list-style-type: none"><li>• <b>Enable</b>—Use this setting to enable Telnet access to the management system.</li><li>• <b>Disable</b>—Use this setting to prevent Telnet access to the management system.</li></ul> |

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Configuring Hot Standby Settings

Use this option to configure a standby access point as a client device associated to a monitored access point.

**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 current entries in the window and any entries you have made in other Template windows up until that point.

**Table 4-80 Hot Standby Settings**

| Field                            | Description                                                                                                                                                                                                         |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hot Standby Mode                 | From the list, select one of the following: <ul style="list-style-type: none"> <li>• Enable—Use this setting to allow hot standby mode.</li> <li>• Disable—Use this setting to disable hot standby mode.</li> </ul> |
| Service Set ID (SSID)            | Enter the monitored access point's SSID.                                                                                                                                                                            |
| MAC Address for the Monitored AP | Enter the monitored access point's MAC address.                                                                                                                                                                     |
| Polling Frequency (1-30)         | Enter the number of seconds between each query the standby access point sends to the monitored access point.                                                                                                        |
| Timeout for Each Polling (1-600) | Enter the number of seconds the standby access point should wait for a response from the monitored access point before it assumes that the monitored access point has malfunctioned.                                |

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Configuring Routing Settings

Use this option to configure the access point to communicate with the IP network routing system.

### Procedure

---

**Step 1** Select **Services > Routing**. The Services: Routing 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 Template windows up until that point.

---

**Table 4-81 Routing Settings**

| Field               | Description                                                                                                                        |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Default Gateway     | Enter the IP address of your network's default gateway in this entry field.<br><br>The entry 255.255.255.255 indicates no gateway. |
| New Network Route   |                                                                                                                                    |
| Destination Network | Enter the IP address of the destination network.                                                                                   |

**Table 4-81 Routing Settings (continued)**

| Field       | Description                                                                |
|-------------|----------------------------------------------------------------------------|
| Gateway     | Enter the IP address of the gateway used to reach the destination network. |
| Subnet Mask | Enter the subnet mask associated with the destination network.             |

**Step 3** Click >> to add an additional network route for the access point.

**Step 4** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Configuring CDP Settings

Use this option to enable, disable, or adjust the access point's CDP settings.

### Procedure

**Step 1** Select **Services > CDP**. The Services: CDP 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 Template windows up until that point.

**Table 4-82 CDP Settings**

| Field                          | Description                                                                                                                                                                                           |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco Discovery Protocol (CDP) | From the list, select one of the following: <ul style="list-style-type: none"><li>• <b>Enable</b>—Use this setting to enable CDP.</li><li>• <b>Disable</b>—Use this setting to disable CDP.</li></ul> |
| Packet Hold Time               | Enter the number of seconds other CDP-enabled devices should consider the access point's CDP information valid.                                                                                       |
| Packet Sent Every              | Enter the number of seconds between each CDP packet the access point sends.<br><br>This value should always be less than the packet hold time.                                                        |

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Configuring DNS Settings

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 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 Template windows up until that point.

**Table 4-83 DNS Settings**

| Field                    | Description                                                                                                                                                                                                                   |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Domain Name System (DNS) | From the list, select one of the following: <ul style="list-style-type: none"> <li>• <b>Enable</b>—Use this option if your network DNS.</li> <li>• <b>Disable</b>—Use this option if you network does not use DNS.</li> </ul> |
| Default Domain           | Enter the name of your network's IP domain. Your entry might look like this:<br>mycompany.com                                                                                                                                 |
| Domain Name Servers      | Enter the IP addresses of up to three domain name servers on your network.                                                                                                                                                    |
| Domain Suffix            | Enter the portion of the full domain name that you would like omitted from access point displays.                                                                                                                             |

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Configuring FTP Settings

Use this option to configure File Transfer Protocol settings for the access point. All non-browser file transfers are governed by these settings.

### Procedure

**Step 1** Select **Services > FTP**. The Services: FTP 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 Template windows up until that point.

**Table 4-84 FTP Settings**

| Field                        | Description                                                                                                                                   |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| File Transfer Protocol (FTP) | From the list select one of the protocols.                                                                                                    |
| Default File Server          | Enter the IP address or DNS name of the file server where the access point should look for FTP files.                                         |
| FTP Directory                | Enter the file server directory that contains the firmware image files.                                                                       |
| FTP User Name                | Enter the username assigned to your FTP server.<br><br>You do not need to enter a name in this field if you selected TFTP.                    |
| FTP User Password            | Enter the password associated with the file server's username.<br><br>You do not need to enter a password in this field if you selected TFTP. |

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Configuring HTTP Settings

Use this option to configure HTTP settings for the access point.

### Procedure

**Step 1** Select **Services > HTTP** The Services: HTTP 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 Template windows up until that point.

**Table 4-85 HTTP Settings**

| Field                      | Description                                                                                                                                                                                                                                                                                                    |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Allow Non-Console Browsing | From the list, select one of the following: <ul style="list-style-type: none"> <li>• <b>Enable</b>—Use this setting to allow browsing to the management system.</li> <li>• <b>Disable</b>—Use this setting to make the management system accessible only through the console and Telnet interfaces.</li> </ul> |
| HTTP Port                  | Enter the port through which the access point provides web access.                                                                                                                                                                                                                                             |



- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Configuring SNMP Settings

Use this option to configure settings for notifications to be sent to an SNMP server.

### Procedure

---

**Step 1** Select **Services > SNMP**. The Services: SNMP 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 Template windows up until that point.

---

**Table 4-86** *SNMP Settings*

| Field                                     | Description                                                                                                                                                                                                                                                                                      |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Simple Network Management Protocol (SNMP) | From the list, select one of the following: <ul style="list-style-type: none"><li>• <b>Enable</b>—Use this setting to allow event notifications to be sent to an SNMP server.</li><li>• <b>Disable</b>—Use this setting to not allow event notifications to be sent to an SNMP server.</li></ul> |
| SNMP Trap Destination                     | Enter the IP address or the host name of the server running the SNMP Management software.                                                                                                                                                                                                        |

**Table 4-86** *SNMP Settings (continued)*

| Field               | Description                    |
|---------------------|--------------------------------|
| SNMP Trap Community | Enter the SNMP community name. |
| SysName             | Enter the system name.         |
| SysLocation         | Enter the system location.     |
| SysContact          | Enter the system contact.      |

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Configuring SNTP Settings

Use this option to configure time server settings.

## Procedure

**Step 1** Select **Services > SNTP**. The Services: SNTP 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 Template windows up until that point.

**Table 4-87 SNTP Settings**

| Field                               | Description                                                                                                                                                                                                                                                                                                     |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Simple Network Time Protocol (SNTP) | From the list, select one of the following: <ul style="list-style-type: none"> <li>• Enable—Use this setting if your network uses Simple Network Time Protocol.</li> <li>• Disable—Use this setting if your network does not use Simple Network Time Protocol.</li> </ul>                                       |
| Default Time Server                 | Enter enter the server's IP address.                                                                                                                                                                                                                                                                            |
| GMT Offset (hr)                     | From the list, select the time zone in which the access point operates.                                                                                                                                                                                                                                         |
| Use Daylight Savings Time           | From the list, select one of the following: <ul style="list-style-type: none"> <li>• Enable—Use this setting to have the access point automatically adjust to Daylight Savings Time.</li> <li>• Disable—Use this setting to not have the access point automatically adjust to Daylight Savings Time.</li> </ul> |

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Configuring Accounting Settings

Use this option to configure settings that enable you to send network accounting information about wireless client devices to a RADIUS server on your network.

### Procedure

- Step 1** Select **Services > Accounting**. The Services: Accounting dialog box appears. Click **See detail** to see for which versions this setting is valid.
- Step 2** Complete the following:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

---

**Table 4-88 Accounting Settings**

| Field             | Description                                                                                                                                                                                                                                                   |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable accounting | From the list, select one of the following: <ul style="list-style-type: none"> <li>• enable—Use this setting to turn on accounting for your wireless network.</li> <li>• disable—Use this setting to turn off accounting for your wireless network</li> </ul> |

**Table 4-88 Accounting Settings (continued)**

| Field                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable delaying to report STOP          | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>enable—Use this setting to delay sending a stop report to the server when a client device disassociates from the access point.</li> </ul> <p>The delay reduces accounting activity for client devices that disassociate from the access point and then quickly reassociate.</p> <ul style="list-style-type: none"> <li>disable—Use this setting to not delay sending a stop report to the server when a client device disassociates from the access point.</li> </ul> |
| Minimum delay time to report STOP (sec) | Enter the number of seconds the access point waits before sending a stop report to the server when a client device disassociates from the access point.                                                                                                                                                                                                                                                                                                                                                                                                         |
| Server Name/IP                          | Enter the name or IP address of the server to which the access point sends accounting data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Server Type                             | <p>Select RADIUS from the list.</p> <p>(Additional types may be added in future software releases.)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Port                                    | <p>Enter the communication port setting used by the access point and the server.</p> <p>The default setting, 1813, is the correct setting for Cisco Aironet access points and Cisco secure ACS.</p>                                                                                                                                                                                                                                                                                                                                                             |
| Shared Secret                           | Enter the shared secret used by your server. It must match the shared secret on the RADIUS server.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

**Table 4-88 Accounting Settings (continued)**

| Field              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Retran (sec)       | Enter the amount of time to wait before retransmitting.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Max Retran         | Enter the maximum number of times to attempt retransmissions.<br><br>Click <b>See detail</b> for information on which version this setting is valid.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Enable Update      | From the list, select one of the following: <ul style="list-style-type: none"> <li>enable—Use this setting to allow accounting update messages for wireless clients.<br/><br/>With updates enabled, the access point sends an accounting start message when a wireless client associates to the access point, sends updates at regular intervals while the wireless client is associated to the access point, and sends an accounting stop message when the client disassociates from the access point.</li> <li>disable—Use this setting to not allow accounting update messages.<br/><br/>With updates disabled, the access point sends only accounting start and accounting stop messages to the server.</li> </ul> |
| Update Delay (sec) | Enter the update interval in seconds.<br><br>If you use 360, the access point sends an accounting update message for each associated client device every 6 minutes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Table 4-88 Accounting Settings (continued)**

| Field         | Description                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EAP Auth.     | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"><li>• Yes—Use this server for EAP authentication.</li></ul> <p>In this type of authentication, the access point relays authentication messages between the server and the authenticating client device.</p> <ul style="list-style-type: none"><li>• No—Do not use this server for EAP authentication.</li></ul> |
| Non-EAP Auth. | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"><li>• Yes—Use this server for non-EAP authentication.</li><li>• No—Do not use this server for non-EAP authentication.</li></ul>                                                                                                                                                                                 |

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Setting Up Proxy Mobile IP

Use this option to enable the access points to work in conjunction with Mobile IP configured on your network routers.

### Procedure

- Step 1** Select **Services > ProxyMobileIP Setup**. The Services: Proxy Mobile IP Setup 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 Template windows up until that point.

**Table 4-89 Proxy Mobile IP Setup**

| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Proxy Mobile IP       | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this setting to enable proxy mobile IP.</li> <li>• No—Use this setting to disable proxy mobile IP.</li> </ul>                                                                                                                                                                                                                                                    |
| Authoritative IP 1 through 3 | <p>Enter the IP address of the authoritative access point.</p> <p>Proxy Mobile IP must be enabled on the wireless SSID. Since multiple SSIDs may exist on the access point and not all SSIDs may have to accommodate mobile clients, you must enable proxy Mobile IP per SSID. The authoritative access point is used to communicate with new access points to update subnet map records and send the new access points a new and complete subnet mapping table.</p> |



- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Configuring Proxy Mobile SA Bindings

Use this option to identify the clients that are able to establish contact with a foreign agent in another network segment or network other than the client's home network.

### Procedure

---

- Step 1** Select **Services > ProxyMobile SA Bind.** The Services: Proxy Mobile SA Bindings 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 Template windows up until that point.

---

**Table 4-90 Proxy Mobile SA Bindings**

| Field                    | Description                                                                                            |
|--------------------------|--------------------------------------------------------------------------------------------------------|
| IP Address Range - Start | Enter the beginning IP address of the range in which client devices must reside in order to be valid.  |
| IP Address Range - End   | Enter the ending IP address of the range in which the client devices must reside in order to be valid. |

**Table 4-90 Proxy Mobile SA Bindings (continued)**

| Field                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group SPI                              | <p>Enter the security parameter index of the IP address range entered in the IP Address Range - Start and End fields.</p> <p>The SPI is a 32-bit number (8 hexadecimal digits) assigned to the initiator of the security association request by the receiving IPSec endpoint. On receiving a packet, the destination address, protocol, and SPI are used to determine the security association.</p> <p>The security association allows the node to authenticate or decrypt the packet according to the security policy configured for that security association.</p> |
| Group Key                              | <p>Enter an authentication key that the group specified in the security association uses to access a foreign agent.</p> <p>The group key is a 128-bit key entered as 32 hexadecimal digits (0-9, a-f, or A-F).</p> <p>To add to the current SA Bindings, click &gt;&gt;.</p>                                                                                                                                                                                                                                                                                         |
| Current SA Bindings                    | <p>Lists previously configured security association bindings.</p> <p>To remove a binding from the list, select it, then click &lt;&lt;.</p>                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Delete Existing SA Binding from Device |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SA Binding ID                          | Enter the identification number of the SA binding to delete, then click >>.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SA Bindings To Delete                  | Lists the SA bindings to be deleted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
  - **Save** to save the template. See [Saving the Template, page 4-253](#).
  - Another template category to configure more options. See [Template Categories, page 4-100](#).
- 

## Configuring Events

This option enables you to customize the display of access point events (alerts, warnings, and normal activity).

### Procedure

---

- Step 1** Select **Events**. The menu expands and the Events dialog box displays in the right pane.
- Step 2** Select one of the following from the Events menu:



**Note** Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

---

- Event Handling—See [Configuring Event Handling, page 4-245](#).
  - Event Notifications—See [Configuring Event Notification, page 4-250](#).
- 

## Configuring Event Handling

The event settings control how events are handled by the access point: counted, displayed in the log, recorded, or announced in a notification. The settings are color coded: red for fatal errors, magenta for alerts, blue for warnings, and green for information.

## Procedure

**Step 1** Select **Events > Event Handling**. The Events: Event Handling 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 Template windows up until that point.

**Table 4-91 Event Handling Settings**

| Field                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System Fatal             | From the list, select one of the following: <ul style="list-style-type: none"> <li>Count—Use this option to tally the total events occurring in this category without any form of notification or display.</li> <li>Display Console—Use this option to provide a read-only display of the event but not record it.</li> <li>Record—Use this option to make a record of the event in the log and provide a read-only display of the event.</li> <li>Notify—Use this option to makes a record of the event in the log, display the event, and tell the access point to notify someone of the occurrence.</li> </ul> |
| Protocol Fatal           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Network Port Fatal       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| System Alert             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Protocol Alert           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Network Port Alert       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| External Alert           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| System Warning           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Protocol Warning         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Network Port Warning     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| External Warning         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| System Information       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Protocol Information     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Network Port Information |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| External Information     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

**Table 4-91 Event Handling Settings (continued)**

| Field                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Handle Alerts as Severity Level | <p>From the list, select one of the following:</p> <ul style="list-style-type: none"><li>• <b>systemFatal</b>—Indicates an event that prevents operation of the device as a whole.</li><li>• <b>protocolFatal</b>—Indicates an event that prevents operation of a specific communications protocol in use, such as HTTP or IP.</li><li>• <b>portFatal</b>—Indicates an event that prevents operation of the Ethernet or radio network interface.</li><li>• <b>systemAlert</b>—Indicates that you need to take action to correct a condition on the device as a whole.</li><li>• <b>protocolAlert</b>—Indicates that you need to take action to correct a condition on a specific communications protocol in use, such as HTTP or IP.</li><li>• <b>portAlert</b>—Indicates that you need to take action to correct the condition on the Ethernet or radio network interface.</li><li>• <b>externalAlert</b>—Indicates that you need to take action to correct the condition on a device on the network.</li></ul> |

**Table 4-91 Event Handling Settings (continued)**

| Field | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <ul style="list-style-type: none"> <li>• <code>systemWarning</code>—Indicates that an error or failure may have occurred on the device as a whole.</li> <li>• <code>protocolWarning</code>—Indicates that an error or failure may have occurred on a specific communications protocol in use, such as HTTP or IP.</li> <li>• <code>portWarning</code>—Indicates that an error or failure may have occurred on an Ethernet or radio network interface.</li> <li>• <code>externalWarning</code>—Indicates that an error or failure may have occurred on a device.</li> <li>• <code>systemInfo</code>—Notification that some sort of event has occurred on a device.</li> <li>• <code>protocolInfo</code>—Notification that some sort of event has occurred on a communications protocol in use, such as HTTP or IP.</li> <li>• <code>portInfo</code>—Notification that some sort of event has occurred on an Ethernet or radio network interface.</li> <li>• <code>externalInfo</code>—Notification that some sort of event has occurred on a device.</li> </ul> |

**Table 4-91 Event Handling Settings (continued)**

| Field                                                                          | Description                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maximum Number of Bytes Stored per Alert Packet<br>(0- 2312)                   | <p>Enter the maximum number of bytes the access point stores for each Station Alert packet when packet tracing is enabled.</p> <p>If you use 0, the access point does not store bytes for Station Alert packets; it only logs the event.</p>                                                   |
| Maximum Memory Reserved for Detailed Event Trace Buffer<br>(bytes) (0-8388608) | <p>Enter the number of bytes reserved for the Detailed Event Trace Buffer.</p> <p>The Detailed Event Trace Buffer is a tool for tracing the contents of packets between specified stations on your network.</p> <p><b>Note</b> Changing this setting may cause the access point to reboot.</p> |

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Configuring Event Notification

Use this option to enable and configure notification of fatal, alert, warning, and information events to destinations external to the access point, such as an SNMP server or a Syslog system.

### Procedure

**Step 1** Select **Events > Event Notification**. The Events: Event Notification 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 Template windows up until that point.

**Table 4-92 Events > Event Notification Settings**

| Field                                                      | Description                                                                                                                                                                                                                                                           |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Should Notify-Disposition Events generate SNMP Traps?      | From the list, select one of the of the following: <ul style="list-style-type: none"> <li>• Yes—Use this option to send event notifications to an SNMP server.</li> <li>• No—Use this option if you do not want to send notifications to an SNMP server.</li> </ul>   |
| SNMP Trap Destination                                      | Enter the IP address or the host name of the server running the SNMP Management software.                                                                                                                                                                             |
| SNMP Trap Community                                        | Enter the SNMP community name.                                                                                                                                                                                                                                        |
| Should Notify-Disposition Events generate Syslog Messages? | From the list, select one of the of the following: <ul style="list-style-type: none"> <li>• Yes—Use this option to send event notifications to a Syslog server.</li> <li>• No—Use this option if you do not want to send notifications to a Syslog server.</li> </ul> |



**Table 4-92 Events > Event Notification Settings (continued)**

| Field                      | Description                                                         |
|----------------------------|---------------------------------------------------------------------|
| Syslog Destination Address | Enter the IP address or the host name of the server running Syslog. |
| Syslog Facility Number     | Enter the Syslog Facility number for the notifications.             |

**Step 3** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## Configuring Custom Values

This option enables to 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

This option should be used only by advanced users who have a good understanding of the MIB variables they are setting.

Templates with custom key values are not validated.

### Procedure

**Step 1** Select **Configure > Templates > Custom Values**. The Custom Values dialog box appears.



### Note

Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

**Step 2** Complete the following:



**Note** You must enter the exact syntax for the setting to work properly.

| Field | Description              |
|-------|--------------------------|
| Key   | Enter a valid MIB key.   |
| Value | Enter a valid MIB value. |

**Step 3** Click >> to add the custom value to the list.



**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 4** Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 4-252](#).
- **Save** to save the template. See [Saving the Template, page 4-253](#).
- Another template category to configure more options. See [Template Categories, page 4-100](#).

## 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 4-253](#).

## Saving the 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 4-274](#).
  - Click **No** if you want to save the template only.
  - Click **Cancel** to cancel the operation and then display the previous screen.
- 

## 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** Select **IOS** or **non-IOS** depending upon the type of template you want to create.
- Step 3** Enter a unique name. See [Naming Guidelines, page A-1](#) for details.

- Step 4** Click **Create 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 4-2](#).
- 

## 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 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 A-1](#) for details.
- Step 4** Click **OK**. The Templates window refreshes and the new name appears in the Existing Templates list.
- Step 5** Click **Edit**. See [Editing a Template, page 4-255](#).
-

## 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 box, 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 4-2](#).
-

## Converting a Template

Use this option to convert a non-IOS configuration template to an IOS template. You cannot convert an IOS template to a non-IOS 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 non-IOS template you want to convert from the Existing Templates box, then click **Convert**.

A dialog box appears with the following fields:

| Field                   | Description                                                                                                                                                                                                                                                      |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                    | Enter a name for the converted template.                                                                                                                                                                                                                         |
| Description             | Enter a description for the template.                                                                                                                                                                                                                            |
| Converted Configuration | Displays the non-IOS configurations that have been converted to IOS.                                                                                                                                                                                             |
| Commands Not Converted  | <p>Displays the non-IOS configurations that were not converted to IOS.</p> <p>These commands are not converted for one of two reasons:</p> <p>There is no equivalent command for IOS.</p> <p>The command conversion is not supported by the conversion tool.</p> |

- Step 3** To save the template, click **Save**.
- The Templates window displays and the new name appears in the Existing Templates list.

## 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 box, 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 an IOS access point, the imported configuration options are displayed in the Custom Values template screen.

When you import a configuration from a non-IOS access point, the configuration options are displayed in their corresponding template screens. However, if the imported configuration options do not have corresponding template screens, they 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 or Non-IOS.
- Step 3** Click **Import**. The Import Template window appears and varies depending upon which type you selected.
- For IOS, go to step 4.
  - For Non-IOS go to step 6.
- Step 4** Complete the following:

| Field                    | Description                                                                                                                                                                                                                                                                                                                     |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Template Name            | <p>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.</p> <p>If you are importing from a device, you must enter a template name.</p>                                                                                                               |
| Description              | <p>Enter a description for the template.</p> <p>Do not click the Enter key at the end of the description; it will generate an error.</p>                                                                                                                                                                                        |
| From file                | Enter the template filename or browse to find the file, then click <b>Import</b> .                                                                                                                                                                                                                                              |
| From device (IP Address) | Enter a device name or IP address, then click <b>Import</b> .                                                                                                                                                                                                                                                                   |
| Non-IP-Identity          | <p>Select this option if you do not want to download identity parameters, such as IP address, from the access point.</p> <p>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.</p> |



| Field              | Description                                                                                                                                                                                                                                                                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Full               | <p>Select this option to import a full configuration from the access point.</p> <p>This type of import includes the access point's identity parameters, such as sysname, IP address, etc.</p> <p>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.</p> |
| 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** Go to step [7](#).

**Step 6** Complete the following:

| Field                    | Description                                                                                                                                                                                                       |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Template Name            | <p>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.</p> <p>If you are importing from a device, you must enter a template name.</p> |
| Description              | <p>Enter a description for the template.</p> <p>Do not click the Enter key at the end of the description; it will generate an error.</p>                                                                          |
| From file                | Enter the template filename or browse to find the file, then click <b>Import</b> .                                                                                                                                |
| From device (IP Address) | Enter a device name or IP address, then click <b>Import</b> .                                                                                                                                                     |

| Field              | Description                                                                                                                                                                                                                                                                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Non-IP-Identity    | <p>Select this option if you do not want to download identity parameters, such as IP address, from the access point.</p> <p>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.</p>                            |
| Full               | <p>Select this option to import a full configuration from the access point.</p> <p>This type of import includes the access point's identity parameters, such as sysname, IP address, etc.</p> <p>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.</p> |
| Device 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 access point.                                                                                                                                                                                                       |
| User Password      | If the device is not managed by the WLSE, enter the user password on the access point.                                                                                                                                                                                                                                                                     |

**Step 7** To import another template, click **Back** and go to [Step 3](#).

**Step 8** When you are finished, click **Done**.

**Step 9** View the template you imported by selecting **Configure > Templates** and selecting it in the Existing Templates list.

## 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**. You will be prompted for a location to export the.ini file.
- Step 4** Click **Done**.
- 

## 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 4-262](#).
- Scheduling a configuration archive job—[Scheduling an Archive Collection, page 4-263](#).

- Viewing the status of a configuration archive job—[Viewing Archive Status, page 4-264](#).

## 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 4-263](#) 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.
- For information on how to search or use the device selector, see [Exporting URL-Based Report Data, page 6-94](#).
- 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.<br>Click the <b>Archive Name</b> 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: IOS or non-IOS.                                                                                                                               |

| Field     | Description                                                                                                                                                                |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.<br>See <a href="#">Editing the Archive, page 4-264</a> .                                       |

- 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 4-265](#).
  - Delete an archived configuration—See [Deleting Archived Configurations, page 4-265](#).
  - Compare configurations—See [Comparing Configurations, page 4-266](#).
  - Export a configuration to a file—See [Exporting a Configuration to a File, page 4-266](#).
  - Export a configuration to a template—See [Exporting a Configuration to a Template, page 4-266](#).

## Scheduling an Archive Collection



### Note

Archive collection for non-IOS access points is supported only for device versions 11.23T and higher (AP350/BR350) and 11.56 and higher (AP1200).

### 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 4-288](#).

- 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 4-293](#).
- 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:<br><br>Yes—Use this setting to indicate that the configuration archive is available to be overwritten.<br><br>No—Use this setting to indicate that it will not be overwritten. |

| Field       | Description                                            |
|-------------|--------------------------------------------------------|
| 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: IOS or non-IOS.     |
| 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**.

---

## 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

- 
- |               |                                                                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Select a configuration you want to from the table.                                                                       |
| <b>Step 2</b> | Click <b>Export to Template</b> . The configuration is exported to a template.                                           |
| <b>Step 3</b> | To view the exported template, select <b>Configure &gt; Templates</b> 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 4-267](#).
- Archive Jobs—[Managing Archive Jobs, page 4-285](#).

## 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 topics covered in this section are:

- [How Do WLSE Configuration Jobs Work?, page 4-268](#)
- [Recommendations For Running Configuration Jobs, page 4-269](#)
- [Creating a Configuration Job, page 4-277](#)
- [Viewing Configuration Job Status, page 4-278](#)
  - [Filtering a Configuration Job, page 4-281](#)
  - [Editing a Configuration Job, page 4-281](#)
  - [Running a Configuration Job Again, page 4-282](#)
  - [Deleting a Configuration Job, page 4-282](#)
  - [Copying a Configuration Job, page 4-283](#)
  - [Viewing Job Run Details, page 4-283](#)

### Related Topics

- [Using the Templates, page 4-1.](#)
- [Configuration FAQs and Troubleshooting, page 10-19](#)

## How Do WLSE Configuration Jobs Work?

Both IOS and non-IOS access points use jobs created by the **Configure > Jobs** option to make configuration updates. The process by which the configurations are updated, however, differs for IOS and non-IOS access points.

### IOS-Based Access Points

When the WLSE configures IOS-based 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.

### Non-IOS-Based Access Points

To configure non-IOS-based access points:

1. The WLSE places the configuration template in the local /tftpboot directory.
2. The WLSE starts the configuration job using either the SNMP set or HTTP post operation.
  - When using SNMP, the SNMP set operation includes the WLSE IP address as the TFTP server and the template filename to download from the /tftpboot directory of the WLSE.
  - When using HTTP, because of limitations on the access point, you cannot specify the WLSE as the TFTP server *when you start the configuration job*. Instead, you must configure each separate access point to use the WLSE as a TFTP server *first*, before you can use HTTP to start the job.
3. The devices use TFTP to download the configuration updates from the WLSE.
4. When the job completes, the WLSE removes the template from the /tftpboot directory to prevent an unauthorized client from connecting to the WLSE and downloading the configuration template.

To make configuration updates for non-IOS-based access points, the WLSE requires these access point credentials:

- When using SNMP: SNMP-write access.
- When using HTTP:
  - The HTTP username and password
  - WLSE configured as a TFTP server on each access point

#### Related Topics

- [Recommendations For Running Configuration Jobs, page 4-269](#)
- [Creating a Configuration Job, page 4-277](#)

## 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.

#### 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:



---

**Note**

All these steps, except Schedule Job, must be completed but do not have to be done in order.

---

1. **Job Name**—See [Naming the Configuration Job](#), page 4-272.
2. **Select Template**—See [From the menu in the left pane, go to the next step, Select Devices. For additional information, see Selecting Devices, page 4-274., page 4-273.](#)
3. **Select Devices**—See [Selecting Devices](#), page 4-274.
4. **Schedule Job**—See [Scheduling a Configuration Job](#), page 4-275.
5. **Options**—See [Setting Configuration Job Options](#), page 4-276.
6. **Save**—See [Saving the Configuration Job](#), page 4-277.



---

**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.

---

## 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 4-93** *Job Name*

| Field       | Description                                                                          |
|-------------|--------------------------------------------------------------------------------------|
| Job Name    | Enter a name for the job.<br>See <a href="#">Naming Guidelines, page A-1</a> .       |
| Description | Enter a description of the job.<br>See <a href="#">Naming Guidelines, page A-1</a> . |

**Step 3** From the menu in the left pane, go to the next step, Select Template. For additional information, see [Selecting a Template, page 4-272](#).

## 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 4-94 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.                                                                                                                  |
| Device Versions        | Displays the device versions for the device types listed in the Device Type field.<br><br>Each device type's valid versions are displayed in sequence and grouped using parentheses. |
| 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 4-274](#).

## Selecting Devices

### 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 4-275](#).

---



## 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 4-95** *Schedule Job*

| Field      | Description                                                                                                                                     |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Run Now    | Click to run the job.<br><b>Note</b> 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 4-277](#).

## 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.

**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.                                          |
| Apply Configuration using | Select either Telnet or SSH.                                                                                               |
| Write NVRAM on Success    | Check if you want the this template, after the job has succeeded, to be used by the access point in the event of a reload. |



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

**Step 3** From the menu in the left pane, go to the next step, Save. For additional information, see [Saving the Configuration Job, page 4-277](#).

## Saving the Configuration Job

### 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.
- Step 2** Click **Save**. A window displays comments to indicate whether the job has passed the validation tests.

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 by the WLSE. You can work around this by importing the latest supported device version from Cisco.com. See [Updating Supported Firmware Versions](#), page 8-38.
    - 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.
- 

## Creating a Configuration Job

Using this option, you can create a configuration job or an archive job.

**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 4-271](#).
- 

## Viewing Configuration Job Status

This window allows you to view job status. It also allows you to filter a job, edit a job, view details about the job and undo a 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 [Updating Supported Firmware Versions, page 8-38](#).

The topics covered in this section are:

- [Creating a Configuration Job, page 4-277](#)
- [Viewing the Configuration Job, page 4-279](#)
- [Filtering a Configuration Job, page 4-281](#)
- [Editing a Configuration Job, page 4-281](#)
- [Running a Configuration Job Again, page 4-282](#)
- [Deleting a Configuration Job, page 4-282](#)
- [Copying a Configuration Job, page 4-283](#)
- [Viewing Job Run Details, page 4-283](#)

**Note**

Your login determines whether you can use this option.

### Related Topics

[Using the Templates, page 4-1](#)

## 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.

**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.<br><b>Note</b> Jobs that cause an access point to reboot are listed as Unverified.        |

- Running



**Tip** You can stop a running job by clicking **Stop Job**.

| Field          | Description               |
|----------------|---------------------------|
| Job Name       | The job name.             |
| Recurring      | Whether the job recurs.   |
| Job Start Time | The time the job started. |

| Field            | Description                                        |
|------------------|----------------------------------------------------|
| Percent Complete | The percent of the job that has completed running. |
| Next Schedule    | The next time the job is scheduled to run.         |

- All

| Field           | Description                                                                                                                    |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------|
| Job Name        | The job name.                                                                                                                  |
| Recurring       | Whether the job recurs.                                                                                                        |
| Job State       | The state of the job.<br><b>Note</b> A job in a DidNotStart state must be rescheduled.                                         |
| 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.<br><b>Note</b> Jobs that cause an access point to reboot are listed as Unverified. |

**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 4-281](#).
- Edit the job—See [Editing a Configuration Job, page 4-281](#).
- Run the job again—See [Running a Configuration Job Again, page 4-282](#).

- Delete the job—See [Deleting a Configuration Job](#), page 4-282.
  - Copy a job—See [Copying a Configuration Job](#), page 4-283.
  - View the run details—See [Viewing Job Run Details](#), page 4-283.
  - Refresh the screen—Click **Refresh**.
- 

## 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 4-271](#).
- 

**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 from the list which you would like to edit.
- 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; they can be stopped.

**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 Job Run Details

Use this option to view details about a job, or to undo a job from the displayed list of jobs.

### 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 or to undo a job, select the job, then click **Show Run Details**. The Job Run details table displays the information. See [Viewing the Job Run Details Table, page 4-284](#).
- 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.
- To select all the jobs in the table, click **Select All**.
- To deselect all the jobs in the table, click **DeSelect All**.



---

**Note** If you have multiple screens, you must Select All or DeSelect All one screen at a time.

---

- To undo the selected configuration job, click **Undo**.

The Undo feature is not supported for the following:

- Custom Values
- Security options: Local Admin Authentication under the Local Admin Access; Encryption Key Values under Local AP/Client Security; Shared Secret under Server-Based Security; and Shared Secret under Accounting.
- FTP username and password
- Previously undone jobs
- Routing table configurations (for versions prior to 11.23T only)
- Adding a user in place of an existing user on the access point. The Undo feature works for new users.

## 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 4-286](#)
- [Recommendations For Using Configuration Archives, page 4-286](#)
- [Creating an Archive Job, page 4-293](#)
- [Viewing Archive Job Status, page 4-293](#)
  - [Filtering an Archive Job, page 4-296](#)
  - [Editing an Archive Job, page 4-296](#)
  - [Running an Archive Job Again, page 4-297](#)
  - [Deleting an Archive Job, page 4-297](#)
  - [Copying a Configuration Job, page 4-283](#)
  - [Viewing Job Run Details, page 4-283.](#)

## 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 4-286](#)
- [Scheduling an Archive Collection, page 4-263](#)

## 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 do I work with the limitations of non-IOS-based access points?
- A.** Due to limitations imposed by the device operating system, not all configured attributes on a non-IOS-based access point are archived. Security related parameters, for example, such as user names and passwords, WEP keys, and AAA servers are not archived. Other non-security related parameters also are not archived. If you create configuration templates for any unrattified configuration parameters, you can apply these templates to the appropriate devices when necessary.
- 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 4-269](#), 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 4-285](#)

## Archive Job Choices

When you create or edit an archive job, the following choices appear in the left pane of the Jobs window:



#### Note

---

Archive collection for non-IOS access points is supported only for device versions 11.23T and higher (AP350/BR350) and 11.56 and higher (AP1200).

---

1. **Job Name**—See [Naming the Archive Job, page 4-289](#).
2. **Select Devices**—See [Selecting Devices, page 4-289](#).
3. **Schedule Job**—See [Scheduling an Archive Job, page 4-291](#).
4. **Finish**—See [Finishing the Archive Job, page 4-292](#).

**Note**

All these steps, except Schedule Job, must be completed but do not have to be

**Related Topics**

[Recommendations For Using Configuration Archives, page 4-286](#)

## 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 4-96 Job Name**

| Field       | Description                                                                         |
|-------------|-------------------------------------------------------------------------------------|
| Job Name    | Enter a name for the job.<br><a href="#">See Naming Guidelines, page A-1.</a>       |
| Description | Enter a description of the job.<br><a href="#">See Naming Guidelines, page A-1.</a> |

**Step 3** From the menu in the left pane, go to the next step, Select Devices. For additional information, see [Selecting Devices, page 4-274](#).

## Selecting Devices

**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, Schedule Job. For additional information, see [Scheduling a Configuration Job, page 4-275](#).
-



## 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 4-97** *Schedule Job*

| Field      | Description                                                                                                                                     |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Run Now    | Click to run the job.<br><b>Note</b> 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 4-292](#).

## Finishing the Archive Job


**Note**

Archive jobs use SNMP, and will only work properly for non-IOS devices with software releases 11.23T and higher.

**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.<br><br><b>Note</b> This setting applies to IOS devices only; for non-IOS devices, select either one. |


**Tip**

If email notification is not working, you may need to configure the mailroute by selecting **Administration > 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 4-288](#).
- 

### Related Topics

[Recommendations For Using Configuration Archives, page 4-286](#)

## 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 4-294](#)
- [Filtering an Archive Job, page 4-296](#)
- [Editing an Archive Job, page 4-296](#)
- [Running an Archive Job Again, page 4-297](#)
- [Deleting an Archive Job, page 4-297](#)
- [Copying an Archive Job, page 4-297](#)
- [Viewing Job Run Details, page 4-283](#)

**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.                                                                                           |

- Running



**Tip** You can stop a running job by clicking **Stop Job**.

| 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.         |

- All

| Field           | Description                                                                                                                        |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------|
| Job Name        | The job name.                                                                                                                      |
| Recurring       | Whether the job recurs.                                                                                                            |
| Job State       | The state of the job.<br><br><b>Note</b> A job in a DidNotStart state must be rescheduled.                                         |
| 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.<br><br><b>Note</b> Jobs that cause an access point to reboot are listed as Unverified. |

**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 greyed.

- Filter the job—See [Filtering an Archive Job, page 4-296](#).
- Edit the job—See [Editing a Configuration Job, page 4-281](#).
- Delete the job—See [Deleting a Configuration Job, page 4-282](#).
- Run the job again—See [Running an Archive Job Again, page 4-297](#).
- Copy a job—See [Copying an Archive Job, page 4-297](#).
- View the run details—See [Viewing Job Run Details, page 4-298](#).
- 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 4-288](#).
-

## 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 from the list which you would like to edit.
- 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; they can be stopped.

**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 or to undo a job, select the job, then click **Show Run Details**. The Job Run details table displays the information. See [Viewing the Job Run Details Table, page 4-299](#).
  - 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 after they are discovered, auto managed, and the WLSE has their inventory information.

The topics covered in this section are:

- [Assigning a Startup Configuration, page 4-300](#)
- [Assigning an Auto-Managed Configuration, page 4-306](#)

## 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 non-IOS access points: Prevent the initial configuration from being uploaded to devices after a reboot by setting the **bootconfigReadINI** variable to **never** by auto-managed configuration or regular configuration.

For IOS access points (Version 12.2(3)JA or later): Prevent the initial configuration from being uploaded to devices after a reboot by using the IOS config command **no boot upgrade**.

### Before You Begin

1. Create a template for the startup configuration. See [Creating a Startup Configuration Template, page 4-302](#).

2. If you are configuring
  - A DHCP server, go to step 4.
  - A router as a DHCP server, go to step 3.
3. 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.

4. 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 4-302](#)
- [Assigning an Auto-Managed Configuration, page 4-306](#)

**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.<br><br><b>Note</b> For non-IOS access points, this name must have an.ini extension. There are no restrictions for IOS access points. |
| Description            | Enter a description for the configuration.                                                                                                                                                              |
| Configuration Template | From the list select the startup template to assign to the configuration file.<br><br>Click <b>Details</b> to see the device types and device versions for which the template is valid.                 |

**Step 3** To save the template, click **Save**.

**Step 4** To delete the template, click **Delete**.

## 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 [Setting Up Devices, page 3-5](#).)

You can create a startup configuration for:

- IOS devices—See [Creating an IOS Startup Template, page 4-303](#).
- Non-IOS devices—See [Creating a Non-IOS Startup Template, page 4-305](#).

## Creating an IOS Startup Template

Use the following table to guide you in creating a startup configuration template for IOS devices:

| Tasks                                 | Template Choice                          | Notes                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Cisco Discovery Protocol (CDP) | Select <b>Services &gt; CDP</b> .        | CDP is required for the WLSE to discover devices on the network.                                                                                                                                                                                                                                                                                                 |
| Enable Telnet                         | Select <b>Services &gt; Telnet/</b> .    | Select <b>Enable</b> for Telnet.                                                                                                                                                                                                                                                                                                                                 |
| Enable SSH                            | Select <b>Services &gt; Telnet/SSH</b> . | Do the following: <ol style="list-style-type: none"><li>1. Select <b>Enabled</b> for Secure Shell.</li><li>2. Enter the system name.</li><li>3. Enter the domain name.</li></ol> <p><b>Note</b> For any version lower 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.</p> |
| Enable SNMP                           | Select <b>Services &gt; SNMP</b> .       | SNMP is required for the WLSE to discover and manage the device.<br><br>Select <b>Enabled</b> for Simple Network Management Protocol (SNMP).                                                                                                                                                                                                                     |

| Tasks                           | Template Choice                    | Notes                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create a Read community string  | Select <b>Services &gt; SNMP</b> . | <p>Do the following:</p> <ol style="list-style-type: none"> <li>1. Enter a community string in the SNMP Community field.</li> <li>2. Enter <b>iso</b> in the Object Identifier field.</li> <li>3. Select <b>Read-Only</b>.</li> </ol> <p><b>Note</b> The read community string must be specified under <b>Administration &gt; Device Credentials</b>.</p> |
| Create a Write community string | Select <b>Services &gt; SNMP</b> . | <p>Do the following:</p> <ol style="list-style-type: none"> <li>1. Enter a community string in the SNMP Community field.</li> <li>2. Select <b>Write-Only</b>.</li> </ol> <p><b>Note</b> The write community string must be specified under <b>Administration &gt; Device Credentials</b>.</p>                                                            |

## Creating a Non-IOS Startup Template

Use the following table to guide you in creating a non-IOS startup configuration template:

| Tasks                                                                                              | Template Choice                                                                                                                                                                                                | Notes                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Cisco Discovery Protocol (CDP)                                                              | Select <b>Services &gt; CDP</b> .                                                                                                                                                                              | CDP is required for the WLSE to discover devices on the network.                                                                                                                                                                                                                                                                                              |
| Enable SNMP.<br>(Optional Set the location.)<br>(Optional Set the system name and system contact.) | Select <b>Services &gt; SNMP</b> .                                                                                                                                                                             | SNMP is required for the WLSE to discover and manage the device.<br><br>Setting the location enables proper grouping of devices into the system-defined Location group. For more information, see <a href="#">Managing Groups, page 3-97</a> .                                                                                                                |
| Set the community string by creating a user with all privileges.                                   | Select <b>Security &gt; Local Admin Access</b> .<br><br>To create an user with SNMP read/write privileges, enter a username and password and select the Write, SNMP, Firmware, and Administrator capabilities. | The username of the user with Write and SNMP privileges is used as the SNMP read/write community string.<br><br>This community string should also have been configured on the WLSE using <b>Administration &gt; Discover &gt; Device Credentials &gt; SNMP Communities</b> .<br><br>The Firmware privilege is required for configuring devices from the WLSE. |
| Set up TFTP as the transfer protocol between the WLSE and access points.                           | Select <b>Services &gt; FTP</b> .                                                                                                                                                                              | TFTP is used for transferring configuration changes to access points.                                                                                                                                                                                                                                                                                         |

## Assigning an Auto-Managed Configuration

Use this option to automatically apply a customized configuration to auto-managed devices after their inventory information has been collected by the WLSE.

The configuration which is applied to the devices is based on the system-defined group with which the devices are associated.



### Tip

It is recommended that as part of the auto-managed configuration template, you create an HTTP user and password by selecting **Security > Local Admin Access**. You also enter this user and password on the WLSE by selecting **Administration > Discover > Device Credentials > HTTP User/Password**.

The following topics are covered in this section:

- Assigning a Configuration Template—See [Assigning Auto-Managed Configurations, page 4-306](#)
- Emailing the Configuration Job Results—See [Using Auto-Managed Options, page 4-308](#)

## Assigning Auto-Managed Configurations

### Procedure

- Step 1** Select **Configure > Auto Update > Auto-Managed Configuration**. 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 4-98 Auto-Managed Configuration**

| Field                  | Description                                              |
|------------------------|----------------------------------------------------------|
| Auto-Managed Templates | Lists the auto-managed templates that have been created. |
| Name                   | Enter a name for the auto-managed configuration.         |



**Table 4-98 Auto-Managed Configuration (continued)**

| Field                                                                                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                                                                                                  | Enter a description for the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Automatically apply configuration template to devices matching the criteria below when they get auto managed | <ol style="list-style-type: none"> <li>1. Select the checkbox if you want to automatically apply a template.</li> <li>2. From the list select the template you want to assign.</li> <li>3. Click <b>Details</b> to see the device types and device versions for which this template is valid.</li> </ol>                                                                                                                                                                                                                                                                                                                                          |
| Device Types                                                                                                 | <p><b>Note</b> Auto-managed templates for AP 350's 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.</p> <ol style="list-style-type: none"> <li>1. Select the checkbox to enable the device types.</li> <li>2. From the list, select the device and click &gt;&gt; to add it to the list of valid devices for that template.</li> <li>3. To remove devices from the list, select the device, then click <b>Remove</b>.</li> </ol> |
| Software Versions                                                                                            | <ol style="list-style-type: none"> <li>1. Select the checkbox to enable the software versions.</li> <li>2. Enter the version numbers if they are not in the list, or from the list, select the version number, then click &gt;&gt; to add it to the list of valid versions for that template.</li> <li>3. To remove version numbers, select the version number from the list, then click <b>Remove</b>.</li> </ol>                                                                                                                                                                                                                                |
| Subnet                                                                                                       | <ol style="list-style-type: none"> <li>1. Select the checkbox to enable subnets.</li> <li>2. From the list, select the subnet.</li> <li>3. To remove version numbers, select the version number from the list, then click <b>Remove</b>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                               |

- 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 checkbox to enable email notification.
- Step 3** 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 **Administration > Appliance > Configure Mailroute**.

---

- Step 4** Click **Save**.
-



# Updating Device Firmware

You can use the WLSE to upgrade the firmware on one or more access points, either as a scheduled operation or on demand. The firmware options on the WLSE are:

- Upgrading IOS and non-IOS access points.
- Converting non-IOS access points to IOS.
- Displaying firmware versions supported by the WLSE and updating the firmware versions support on the WLSE.

The topics in this section are:

| Topic                                                                                                    | Reference                                                                                |
|----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Overview                                                                                                 | <a href="#">About Firmware Upgrades, page 5-2</a>                                        |
| Managing normal firmware upgrades:                                                                       |                                                                                          |
| <ul style="list-style-type: none"><li>• Downloading images to the WLSE or a remote TFTP server</li></ul> | <a href="#">Managing Firmware Images, page 5-5</a>                                       |
| <ul style="list-style-type: none"><li>• Running firmware jobs</li></ul>                                  | <a href="#">Managing Firmware Jobs, page 5-14</a>                                        |
| Converting Cisco Aironet 1200 and Aironet 350 access points from non-IOS to IOS firmware                 | <a href="#">Converting Access Points to IOS, page 5-35</a>                               |
| Viewing and updating the WLSE's firmware support data                                                    | <a href="#">Viewing and Updating Firmware Versions that the WLSE Supports, page 5-14</a> |

**Note**

One or both of the firmware subtabs may not be visible to some users. Your login determines whether you can view and use WLSE options.

## About Firmware Upgrades

The topics covered in this section are:

- [How Firmware Upgrades Work, page 5-2](#)
- [Recommendations For Running Firmware Upgrades, page 5-3](#)

For overview information on converting non-IOS access points to IOS, see [Converting Access Points to IOS, page 5-35](#)

## How Firmware Upgrades Work

To use the firmware upgrade feature, you must:

1. Download the firmware image to the WLSE and import it to the WLSE or import the image directly from Cisco.com. 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 locally 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.

The WLSE usually initiates the download and reboot by using an SNMP set operation. For older non-IOS APs that do not support such SNMP operations, you can use HTTP to initiate the download. In that case, each access point in the job must have the WLSE configured as the TFTP server. It is recommended that you migrate to newer access point firmware and use SNMP instead of HTTP.

## Recommendations For Running Firmware Upgrades

The topics in this section concern the number of devices to include in firmware jobs and the amount of time it takes to run a job:

- [Number of Devices in a Job, page 5-3](#)
- [How Much Time to Allocate, page 5-3](#)
- [Calculating the Estimated Time, page 5-4](#)

### 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, its 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?

The 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 also 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 [Firmware jobs over slow links do not succeed.](#), page 10-28). 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

Suppose a WLAN administrator plans to upgrade 200 AP1100 access points. After preliminary testing, it is determined 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:

- View images downloaded to the WLSE—See [Viewing Images Downloaded to the WLSE](#), page 5-6.
- Edit images on the WLSE—See [Editing Image Details on the WLSE](#), page 5-6.
- Delete images from the WLSE—See [Deleting Images from the WLSE](#), page 5-8.
- Download images to the WLSE—See [Importing Images to the WLSE](#), page 5-8.
- 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 5-13.

### Related Topics

- [Managing Firmware Jobs](#), page 5-14
- [Converting Access Points to IOS](#), page 5-35
- [About Firmware Upgrades](#), page 5-2

## Viewing Images Downloaded to the WLSE

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 on an image, select the image. The Image Details window opens, showing the image name, image version, image size, and a description.
- 

### Related Topics

[Editing Image Details on the WLSE, page 5-6](#)

## Editing Image Details on the WLSE

### Procedure

- 
- Step 1** Select **Firmware > Images**.
- Step 2** Expand the folder that contains the image you want to edit, then select the image. The Image Details window opens.
- Step 3** You can edit the image name, image version, device type, and description as described in [Table 5-1 on page 5-7](#).



**Table 5-1** Image Details

| Field       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name        | By default, the name of the image file or of the image file in a zipped file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Device Type | <p>The device type to which the firmware applies. 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.</p> <p>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.</p>                                                                                                                                                                                                                                                                                                                                      |
| Version     | <p>Edit 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. 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.</p> <p><b>Note</b> To prevent errors when importing, do not rename IOS images.</p> <p>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:</p> <ul style="list-style-type: none"><li>• Official format—12.2(4)JA1</li><li>• Cisco.com format—12.2.4-JA1</li></ul> |
| Size        | Size of the image (read-only field).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 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 5-8](#)
- [Viewing and Updating Firmware Versions that the WLSE Supports, page 5-14](#)

## Deleting Images from the WLSE

### Procedure

---

- Step 1** Select **Firmware > Images**.
- Step 2** Expand the folder that contains the image you want to delete, then select the image. The Image Details window opens.
- Step 3** Click **Delete**, then click **OK**. 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 5-6](#)
- [Editing Image Details on the WLSE, page 5-6](#)

## 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 5-9](#).
- Download images to the WLSE directly from Cisco.com—see [Importing Images Directly from Cisco.com to the WLSE, page 5-11](#).

### Related Topics

- [Viewing Images Downloaded to the WLSE, page 5-6](#)
- [Editing Image Details on the WLSE, page 5-6](#)

## Importing Images from the Client System Desktop to the WLSE

### 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://www.cisco.com/public/sw-center/sw-wireless.shtml>
- You can also locate images on Cisco.com by selecting **Products and Services > Network Management Cisco Works > Wireless LAN Solution Engine > Software Center**.



**Note** Only the combined images from Cisco.com are supported for importing to the WLSE. If you download an image component from another site and then try to import a component, the operation will fail.

For information about supported versions of images, see the Supported Devices document 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 5-2 on page 5-10](#).

**Table 5-2 Desktop Import Window**

| Field                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device Type              | Select the device type from the list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Version                  | <p>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. 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.</p> <p><b>Note</b> To prevent errors when importing, do not rename IOS images.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• Official format—12.2(4)JA1</li> <li>• Cisco.com format—12.2.4-JA1</li> </ul> <p><b>Note</b> If you are importing an image to convert non-IOS access points to IOS, see <a href="#">Converting Access Points to IOS, page 5-35</a> for information about the images for conversion and how to enter the version.</p> |
| File Location            | <p>Enter the path to the image on the desktop or click <b>Browse</b>.</p> <p>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 <a href="#">Editing Image Details on the WLSE, page 5-6</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Overwrite Existing Image | <p>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.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**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 5-14](#).

## Importing Images Directly from Cisco.com to the WLSE

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.



### Note

The special images for converting non-IOS access points to IOS are not available for import directly from CCO to the WLSE. Use the special conversion procedures in [Converting Access Points to IOS, page 5-35](#).

### Procedure

**Step 1** Select **Firmware > Images > Import > From Cisco.com**. Complete the following:

**Table 5-3** *Cisco.com Import Window*

| Field                          | Description                                                                                                                                                      |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco.com Username             | Your Cisco.com username.                                                                                                                                         |
| Cisco.com Password             | Your Cisco.com password                                                                                                                                          |
| Proxy IP/Hostname <sup>1</sup> | 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                     |                                                                                                                                                                  |

**Table 5-3 Cisco.com Import Window (continued)**

| Field          | Description                                                                              |
|----------------|------------------------------------------------------------------------------------------|
| 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 5-9](#)).

**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** 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 5-6](#).

**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**.

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 8** 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 9** Click **Refresh** to refresh the Import Status window; click **Close** to close it.

**Step 10** For information on uploading firmware to access points and bridges, see [Managing Firmware Jobs, page 5-14](#).

---

## 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>

- Navigate to the images by selecting **Products and Services > Network Management CiscoWorks > Wireless LAN Solution Engine > Software Center**.

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 5-14](#). You specify the TFTP server and provide the filename when you specify job options (for more information, see [5. Set Options, page 5-20](#)).

## Viewing and Updating Firmware Versions that the WLSE Supports

You can:

- Import support for new versions by selecting **Administration > System > New Version Support**. See [Updating Supported Firmware Versions, page 8-38](#).
- View version support by selecting **Administration > System > Firmware Supported Versions**. See [Viewing Supported Firmware Versions, page 8-39](#).

## Managing Firmware Jobs

The Jobs subtab allows you to:

- Create firmware jobs—See [Creating and Running a Firmware Job, page 5-15](#).  
If you are using a firmware job to convert non-IOS access points to IOS, follow the procedures in [Converting Access Points to IOS, page 5-35](#) before creating a firmware job.
- View a list of firmware jobs—See [Viewing Job Status Information, page 5-28](#).



- Filter the list of firmware jobs—See [Filtering Jobs](#), page 5-30.
- Edit firmware jobs—See [Editing a Job](#), page 5-31.
- Copy firmware jobs—see [Copying a Job](#), page 5-32.
- Delete firmware jobs—See [Deleting a Job](#), page 5-31.
- View firmware jobs details—See [Viewing Job Run Details](#), page 5-32.

### Related Topics

[Managing Firmware Images](#), page 5-5

## 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 IOS and non-IOS access points.

Use the procedure in [Converting Access Points to IOS](#), page 5-35 to convert access points to IOS.



### 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

Each job name (configuration, firmware, or AP radio scan) must be unique.

For other guidelines on job names, see [Appendix A, “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 5-16](#).
- 

## 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 [Firmware Version Support, page 8-37](#).

1. **Job Name**—See [1. Name the Job and Select the Protocol, page 5-17](#).
2. **Select Image**—See [2. Select the Image, page 5-18](#).
3. **Select Devices**—See [3. Select Devices, page 5-18](#).
4. **Schedule Job**—See [4. Schedule the Job, page 5-19](#).
5. **Options**—See [5. Set Options, page 5-20](#).
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 5-22](#).



### Caution

Clicking on 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 and Select the Protocol

**Note**

Each job name (configuration, firmware, or AP radio scan) must be unique.

**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 5-4 on page 5-17](#).

**Table 5-4 Job Name Parameters**

| Field       | Description                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Job Name    | Enter a name for the job. For guidelines on naming jobs, see <a href="#">Appendix A, “Naming Guidelines.”</a>                                                                                                                                                                                                                                                                                               |
| Description | Enter a description of the job. For guidelines on entering descriptions, see <a href="#">Appendix A, “Naming Guidelines.”</a>                                                                                                                                                                                                                                                                               |
| Protocol    | Select the protocol to be used for the job: HTTP or SNMP. For IOS firmware upgrades and conversions from non-IOS firmware to IOS firmware, you must select SNMP.<br><br><b>Note</b> After a job runs once, the protocol cannot be changed. To change the protocol, make a copy of the job and select a different protocol. For information on copying a job, see <a href="#">Copying a Job, page 5-32</a> . |

**Step 3** Go to the next step, Select Image. See [2. Select the Image, page 5-18](#).

## 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.



**Note** If you are converting Cisco Aironet 1200 access points from non-IOS firmware to IOS firmware, you must select a special upgrade image (for example, AP1200-Cisco-IOS-Upgrade-v1). Do not use a regular IOS image upgrade file.

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 5-8](#).

- Step 3** From the menu in the left pane, go to the next step, Select Devices. See [3. Select Devices, page 5-18](#).

## 3. Select Devices

### 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 and Search, page 1-9](#).

**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 3-97](#).

**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 5-19](#).

---

### Related Topics

[Managing Groups, page 3-97](#)

## 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 5-20](#).

## 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 5-5 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 8-35.

**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 5-6 on page 5-21](#). For information about storing images on the remote TFTP server, see [Using a Remote TFTP Server for Updating Devices](#), page 5-13.

**Table 5-6 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. |
| Recently used servers                 |                                                                                                                                                                                                                  |
| 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 5-22.

## 6. Save the Job and Finish

### Procedure

**Step 1** Select **SAVE** from the left pane.

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 [Firmware Version Support, page 8-37](#).

- 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 5-25](#).

**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:



**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 <b>Yes</b> . The Job Summary window appears.                                                                                                                          |
| Skip devices with warnings and only apply image to devices without warnings. | Click <b>No</b> . The Job Summary window appears.                                                                                                                           |
| Correct warnings before proceeding.                                          | <ol style="list-style-type: none"> <li>1. Click <b>Cancel</b>. The Save window appears.</li> <li>2. Return to job choices, make corrections, and save job again.</li> </ol> |

– If there are warnings and errors:

| Desired Action                                                                             | Steps                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Skip devices with errors. Apply image to all other devices, including those with warnings. | Click <b>Yes</b> . The Job Summary window appears.<br><b>Note</b> Image will <i>not</i> be applied to devices with errors.                                                          |
| Skip devices with warnings or errors. Apply image to all other devices.                    | Click <b>No</b> . The Job Summary window appears.<br><b>Note</b> Image will <i>not</i> be applied to devices with errors.                                                           |
| Correct warnings or errors before proceeding.                                              | <ol style="list-style-type: none"> <li>1. Click <b>Cancel</b>. The Save window appears.</li> <li>2. Return to the job choices, make corrections, and save the job again.</li> </ol> |

– If there are only errors:

| Desired Action                                              | Steps                                                                                                                                                                       |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Skip devices with errors. Apply image to all other devices. | Click <b>OK</b> . The Job Summary window appears.<br><b>Note</b> Image will <i>not</i> be applied to devices with errors.                                                   |
| Correct errors before proceeding.                           | <ol style="list-style-type: none"> <li>1. Click <b>Cancel</b>. The Save window appears.</li> <li>2. Return to job choices, make corrections, and save job again.</li> </ol> |

- 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 5-28](#).

**Table 5-7 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.
- Non-IOS devices will be rebooted by using SNMP.
  - IOS devices will be rebooted by 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 5-28](#).

To view the status of jobs at any time, select **Firmware > Jobs**.

#### Related Topics

- [Deleting a Job, page 5-31](#)
- [Viewing Job Status Information, page 5-28](#)
- [Viewing Job Run Details, page 5-32](#)

## 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 5-9 on page 5-26](#).

**Table 5-8 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.<br><br>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:<br><br><code>This job can take as long as xx minutes to complete.</code>                                                                                                                                                                                                                                                             |
| 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.<br><br>For information on importing updated information on supported firmware versions and viewing information on versions supported by the WLSE, see <a href="#">Updating Supported Firmware Versions, page 8-38</a> and <a href="#">Viewing Supported Firmware Versions, page 8-39</a> . |
| Image known bugs validation              | Any major caveats for this image.                                                                                                                                                                                                                                                                                                                                                                                               |
| Job protocol validation                  | Whether the selected job protocol (HTTP or SNMP) is valid for this device.<br><br><b>Note</b> Firmware upgrade via SNMP is supported for firmware versions 11.08T and later. SNMP is required for IOS firmware upgrades and conversions from non-IOS to IOS.                                                                                                                                                                    |
| Device-Image validation                  | Whether the selected image is valid for this device: <ul style="list-style-type: none"><li>• <i>Error</i> if the image is not valid for the selected device type.</li><li>• <i>Warning</i> if the image is not recognized by the WLSE.</li><li>• <i>Information</i> if the same image is already installed on the devices.</li></ul>                                                                                            |

Messages in the Save window show the status of each item that is tested by the job validation process:

**Table 5-9 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <i>Warning</i>     | <p>The operation is permitted but may not be advisable; for example, downgrading to an earlier image.</p> <p>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 <b>Save</b> in this window and you can decide whether to ignore warnings.</p> <p>The warning messages are:</p> <ul style="list-style-type: none"> <li>• Device is running a software version that is not currently supported by WLSE—The WLSE does not recognize this software version. You can click <b>Yes</b> when prompted to ignore warnings.</li> <li>• 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 <b>Yes</b> when prompted to ignore warnings.</li> <li>• Selected firmware image version is the same as the image running on the device—You can click <b>Yes</b> when prompted to ignore warnings.</li> </ul> |

**Table 5-9 Messages in the Save Window (continued)**

| Message Type | Description and Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Error</i> | <p>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.</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>SNMP/HTTP protocol not supported for firmware upload on device—Remove the device from the job.</li> <li>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 <b>Devices &gt; Discover &gt; Device Credentials</b> before you can upgrade this device. For more information, see <a href="#">Enter Telnet and SSH Usernames and Passwords—IOS Access Points</a>, page 3-33.</li> </ul> |

## 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 30 days by default. To change the retention period, see [Managing Polling Parameters](#), page 3-87.



### Note

Your login determines whether you can use the following options.

- To check the status of jobs, see [Viewing Job Status Information, page 5-28](#).
- To filter the list of jobs, see [Filtering Jobs, page 5-30](#).
- To edit a job, see [Editing a Job, page 5-31](#).
- To delete a job, see [Deleting a Job, page 5-31](#).
- To see the details of a job, see [Viewing Job Run Details, page 5-32](#).

### Related Topics

[Creating and Running a Firmware Job, page 5-15](#)

## Viewing Job Status Information

For information about specific job states, see [Job Status Information and Job Run Log Messages, page 5-33](#).

### 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.                                                                                 |

- 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.                                                                                 |

- 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.                   |

- All

| Field           | Description                                                                                             |
|-----------------|---------------------------------------------------------------------------------------------------------|
| Job Name        | The job name.                                                                                           |
| Job State       | The state of the job.<br><b>Note</b> 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.                                                             |

**Step 3** 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 4** The following options are provided:
- Filter jobs—See [Filtering Jobs](#), page 5-30.
  - Edit a job—See [Editing a Job](#), page 5-31.
  - Delete a job—See [Deleting a Job](#), page 5-31.
  - Copy a job—See [Table 5-9 on page 5-32](#).
  - View job run details—See [Viewing Job Run Details](#), page 5-32.
- Step 5** To refresh the screen, click **Refresh**.
- 

### Related Topics

[Using the Functions in the Main Jobs Window](#), page 5-27

## Filtering Jobs

Use this option to display a limited set of jobs, making it easier to search for a particular job by name.

### 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 5-27



## 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.

**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 5-16](#).
- 

**Related Topics**

[Using the Functions in the Main Jobs Window, page 5-27](#)

## 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.

**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 5-27](#)

## Copying a Job

Use this option to copy a job. You can use this option to change the protocol in a job that has already run.



### 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.

### 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 5-27](#)

## Viewing Job Run Details

Use this option to view details about a job.

### 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.                 |
| Percent Complete | The percent of the job that completed. |

**Step 4** To view details for a particular job run, select the job and click **Show Run Details**.

**Step 5** To view the job run log, click **Job Run Log**. A window displays all the details for the selected job number. For information on the messages in the job run log, see [Job Status Information and Job Run Log Messages, page 5-33](#).

**Step 6** To refresh the table, click **Refresh**.

### Related Topics

[Using the Functions in the Main Jobs Window, page 5-27](#)

## Job Status Information and Job Run Log Messages

This section provides information about:

- [Job Status “Not Verified”, page 5-33](#)
- [Job Run Log Messages, page 5-34](#)

### Job Status “Not Verified”

If a job ends with the status “not verified,” or fails because of timeouts caused by slow links, you can change the values of the job properties parameters in the WLSE and rerun the job.



#### Note

A status of “not verified” does not always mean that the job failed. The WLSE may have timed out before verifying whether the job succeeded.

To change job properties parameters that affect timeouts, access the WLSE through the following URL:

`http://your_wlse:1741/debug/jobprops.jsp`

where *your\_wlse* is the name of the WLSE.

- 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 5-10 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 in <b>Devices &gt; Device Credentials</b> . For more information about the required community strings, see <a href="#">Setting Up Devices</a> , page 3-5. |
| 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 <a href="#">Job Status “Not Verified”</a> , page 5-33.                                                                |

# Converting Access Points to IOS

**Caution**

After you convert a non-IOS access point to IOS, you cannot reverse the process. The access point cannot be converted back to non-IOS firmware.

**Caution**

The conversion job might fail if the non-IOS access point does not have at least 4 MB (DRAM) of free space. To check the free space in the device, use the CLI command `:vxdiag memshow`. You can free up space by temporarily removing the 11a radio. For more information, see the access point documentation on Cisco.com.

This section contains the following topics:

- Overview information—see [About Conversion](#), page 5-35.
- Step-by-step conversion procedure—see [Conversion Procedure](#), page 5-37.

## About Conversion

This section contains the following topics:

- [Overview: Converting Non-IOS Access Points](#), page 5-36
- [Converting Cisco Aironet 1200 and 1220 Access Points](#), page 5-36
- [Converting Cisco Aironet 350 Access Points](#), page 5-37

## Overview: Converting Non-IOS Access Points

There are two options for converting non-IOS access points to IOS:

- You can download the Cisco Aironet Conversion Tool (CAC Tool) from Cisco.com, and convert one access point at a time.
- You can use the WLSE, which can convert multiple access points to IOS.

Conversion from non-IOS to IOS firmware requires a special upgrade image (for example, AP1200-Cisco-IOS-Upgrade-v1). Do not use a regular IOS image upgrade file.

Conversion takes more time than normal upgrades because:

- Conversion images are larger than normal images.
- The access point must be rebooted twice during a conversion, while it is rebooted only once during normal upgrades.

The WLSE automatically converts most of the non-IOS configuration data to IOS-style configuration. However, certain key data are not automatically converted and must be specified as part of the upgrade job. Therefore, when you use WLSE to convert to IOS, you must define a non-IOS configuration template that includes the following parameters: HSRP configuration, LEAP configuration, User Manager configuration AAA server configurations, WEP key configuration, and per-VLAN security settings. This template is assigned to the devices during the upgrade process.

The WLSE has an internal timeout parameter for firmware upgrades. If the WLSE is unable to communicate successfully with the access point within the period specified by the timeout, it will declare the upgrade job unverified.

## Converting Cisco Aironet 1200 and 1220 Access Points

After conversion, a Cisco Aironet 1200 becomes a Cisco Aironet 1210, and a Cisco Aironet 1220 becomes a Cisco Aironet 1230. As a result, the following changes occur:

- The sysOID after conversion is the same as the sysOID of an access point with native IOS.
- Software images listed in the WLSE Supported Device Table for 1210 and 1230 access points will now apply to the converted access points.
- Converted devices will be placed in different system groups.

The Cisco Aironet 1200 and 1220 access points to be converted must be running 11.56, 12.01T1, or 12.02T1 non-IOS (VxWorks) firmware. The upgrade images are:

| Image Name                              | IOS Version after Conversion  |
|-----------------------------------------|-------------------------------|
| AP1200-Cisco-IOS-Upgrade-Image-v1.img   | Cisco IOS Release 12.2(11)JA  |
| AP1200-Cisco-IOS-Upgrade-Image-v1.1.img | Cisco IOS Release 12.2(11)JA1 |

## Converting Cisco Aironet 350 Access Points

After conversion, Cisco Aironet 350 access points will be removed from the AP350 system group and placed in the AP350-IOS group. The Cisco Aironet 350 access points to be converted must be running 11.23T, 12.01T1, or 12.02T1 non-IOS (VxWorks firmware). The upgrade image is:

| Image Name                           | IOS Version after Conversion |
|--------------------------------------|------------------------------|
| AP350-Cisco-IOS-Upgrade-Image-v1.img | Cisco IOS Release 12.2(13)JA |

## Conversion Procedure

The major tasks in the conversion process are listed in [Table 5-11 on page 5-38](#).

**Note**

An estimate of the time required to complete the firmware job is displayed during the last task, [4. Create and Run the Conversion Job, page 5-43](#).

**Table 5-11 Quick Reference for Converting an Access Point to IOS**

| Task |                                                                                                                                                                                                                                                                                                       | Reference                                                              |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| 1    | Configure the access points to be converted.                                                                                                                                                                                                                                                          | <a href="#">1. Configure Access Points To Be Converted, page 5-38.</a> |
| 2    | Configure the WLSE by downloading a special conversion image to your local system, importing it into the WLSE, and entering the community strings for all access points to be converted.<br><br><b>Note</b> Downloading the image directly from Cisco.com is not supported for the conversion images. | <a href="#">2. Configure the WLSE for IOS Conversions, page 5-39.</a>  |
| 3    | Create a template for the conversion.                                                                                                                                                                                                                                                                 | <a href="#">3. Create a Conversion Template, page 5-41.</a>            |
| 4    | Create and schedule the conversion job.                                                                                                                                                                                                                                                               | <a href="#">4. Create and Run the Conversion Job, page 5-43.</a>       |

## 1. Configure Access Points To Be Converted

For each non-IOS access point to be converted, make sure the access point is configured properly for conversion:

### Procedure

---

**Step 1** After an image is uploaded to an access point, the access point is rebooted. If you are using **DHCP** to assign IP addresses to the access points to be converted, make sure that the IP addresses do not expire during the time required to run the firmware job and reboot the access points.

You can set the DHCP lease period accordingly or use the DHCP reservation feature. The WLSE firmware module provides IP and MAC addresses for the reservation feature.

**Step 2** Log in to each access point and set the following:

- a. Under **Setup > Express Setup**, set the SNMP admin community string.

This creates a user under **Setup > Security > User Information** whose username is the community string.

You will need this community string for the next task, [2. Configure the WLSE for IOS Conversions, page 5-39](#).

- b. Select the user created in Step 2b. Under Capability Settings, select **Firmware**.
- 

Next, configure the WLSE. See [2. Configure the WLSE for IOS Conversions, page 5-39](#).

## 2. Configure the WLSE for IOS Conversions

On the WLSE, import the image and make sure access point community strings are entered:

### Procedure

---

**Step 1** Locate the special conversion image on Cisco.com at the following URL:



<http://www.cisco.com/public/sw-center/sw-wireless.shtml>

For information on the images to use for conversion, see [Converting Cisco Aironet 1200 and 1220 Access Points, page 5-36](#) or [Converting Cisco Aironet 350 Access Points, page 5-37](#).

**Step 2** Import the image:

- a. Download the image to the desktop from Cisco.com. You can download firmware images from the following URL:

<http://www.cisco.com/public/sw-center/sw-wireless.shtml>



**Note**

Conversion images cannot be imported directly from CCO because these images lack an appropriate version identifier.



**Note**

Use of a remote TFTP server is not supported for conversion jobs.

- b. Import the image to the WLSE by selecting **Firmware > Images > Import > From Desktop**.
- c. For converting AP 350s, make sure you select AP 350 from the Device Type list. Do not select AP350-IOS.



**Caution**

The Version field must be set correctly. Otherwise, the image will be incompatible with the access points that you are converting.

| Image                                   | Version <sup>1</sup> |
|-----------------------------------------|----------------------|
| AP1200-Cisco-IOS-Upgrade-Image-v1.img   | 12.2(11)JA           |
| AP1200-Cisco-IOS-Upgrade-Image-v1.1.img | 12.2(11)JA1          |
| AP350-Cisco-IOS-Upgrade-Image-v1.img    | 12.2(13)JA           |

1. You can also enter the image version as 12.2.

- d. For more information about downloading and importing firmware, see [Importing Images to the WLSE, page 5-8](#).

**Step 3** Select **Administration > Discover > Device Credentials > SNMP Communities**.

Make sure the community strings for all access points to be converted are entered into the SNMP Communities table. These are the community strings you entered in [1. Configure Access Points To Be Converted, page 5-38](#).

For more information on entering community strings on the WLSE, see [Enter SNMP Communities, page 3-56](#).

---

Next, create a conversion template on the WLSE; see [3. Create a Conversion Template, page 5-41](#).

### 3. Create a Conversion Template

Create a *non-IOS* template that contains the security parameters for the level of security that you require.

It is necessary to set these security parameters because the parameters set on the access point might have write-only permissions. During the firmware conversion job, write-only parameters cannot be extracted from the access point. Therefore, such parameters must be re-entered by applying a template so the access point is configured correctly after the conversion.

All other parameters on the access points will retain their values after conversion. If you set parameters in the conversion template in addition to those described in the following procedure, the extra parameters will be ignored.

To create the conversion template.

#### Procedure

---

- Step 1** Select **Configure > Templates**.
- Step 2** Select **non-IOS**.
- Step 3** Enter a unique name. See [Naming Guidelines, page A-1](#) for details.
- Step 4** Click **Create New**.
- Step 5** From the left pane, select **Security > Local Admin Access > Add Users** and set the following parameters.

**Caution**

You must set the following three parameters in the template. Otherwise, the conversion will fail and you will have to log in to each access point and configure it manually.

- a. Enter a User Identifier (any integer but 0). If you want to set the same user name on all the access points to be converted and do not know which user identifiers are already in use, enter a very high value (such as 2000).
- b. Enter the User Name. After conversion, this username will be the Telnet user name and the read/write community string on the access points. These credentials are necessary for the WLSE to communicate with the access points.

**Note**

This user name must be the same as the community string you entered on the WLSE in [2. Configure the WLSE for IOS Conversions, page 5-39](#).

- c. Enter a password. After conversion, this password will be the Telnet user password on the access points.

**Step 6**

Using the choices in the left pane, set the necessary parameters from [Table 5-12 on page 5-42](#). The parameters you set depend on the level of security that you need on your access points.

**Note**

When you validate the conversion job, any parameters listed in the table that are not set in the template will cause informational messages during the last task. These messages will not prevent the firmware jobs from running successfully.

**Table 5-12 Other Conversion Template Settings**

| Template Choice                     | Setting                                                                                                                                                                                                                                          |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Association > VLANs                 | <ul style="list-style-type: none"> <li>• Enter WEP Key 1 through WEP Key 4.</li> <li>• Select the size of each WEP key.</li> </ul>                                                                                                               |
| 11a Radio > Data Encryption         | <ul style="list-style-type: none"> <li>• Enter Encryption Key 1 through Encryption Key 4.</li> <li>• Select the Transmit Key.</li> <li>• Select the Key Size for each encryption key.</li> </ul>                                                 |
| Security > Local AP/Client Security | <ul style="list-style-type: none"> <li>• Enter Encryption Key 1 through Encryption Key 4.</li> <li>• Select the Transmit Key.</li> <li>• Select the Key Size for each encryption key.</li> </ul>                                                 |
| Security > Authentication Server    | <ul style="list-style-type: none"> <li>• Enter server name or IP address.</li> <li>• Select Server Type.</li> <li>• Enter Port, Share Secret, Retran Int, Max Retran.</li> <li>• Specify EAP Auth, MAC Auth, User Auth, and MIP Auth.</li> </ul> |

**Step 7** Select **Preview** to see your changes before you apply them.

**Step 8** Select **Finish** to save the template.

---

For more information about configuration templates, see [Using the Templates, page 4-1](#).

After you create the template, you can create and run the firmware job; see [4. Create and Run the Conversion Job, page 5-43](#).

## 4. Create and Run the Conversion Job

For more details on the steps in this procedure, see the complete descriptions in [Job Creation Tasks, page 5-16](#).

To create, save, and run the conversion job:

---

**Step 1** Select **Firmware > Jobs**.

**Step 2** Enter a name for the job and an optional description, and select **SNMP**.



---

**Note** Each job name (configuration, firmware, or AP radio scan) must be unique.

---

**Step 3** Click **Select Image**. Expand the device folder and select the special conversion image.

**Step 4** Click **Select Devices**.

- a. Expand the folder that contains the access points to be converted.
- b. From the Available Devices list, select a group or individual devices and click **Add**.

**Step 5** Click **Schedule Job**.

- To run the job right after you finish the job creation process, select **Run Now**.
- To schedule the job for later, select the date and time.

**Step 6** Click **Options**. To specify job options:

- a. (Optional) In the Email settings section, you can specify email notification upon completion of the job.
- b. The Remote Server option cannot be used for conversion jobs.
- c. In the IOS Security Parameters section, enter the enable password and select the conversion template from the Select Config Template list.



---

**Note** This section appears only if you selected a valid conversion image in [Step 3](#). If it does not appear, return to Select Image and select the correct image.

---

- Step 7** Click **Save** to validate the job settings, view a job summary, and run the job immediately or add it to the list of scheduled jobs.

The Save window shows information about the job. For details about the messages in this window, see [Table 5-8 on page 5-25](#).

If there are warning or error messages in the Save window, the job will fail or only succeed on some of the devices. Edit your job choices and click **Save** in the left pane.

- Step 8** When the job is ready to run, click **Save** in the Save window. The Job Summary page displays basic information about the job, and the job will run immediately or will be added to the job list.

- Step 9** To check job status, select **Firmware > Jobs**.

- If the job status is “not verified”:
  - First, *check the access points* to find out if they have been converted to IOS.
  - If they have *not* been converted, run the job again.
  - If they have been converted, *do not run the job again*.



**Note**

A job status of “not verified” does not always mean the job failed. The WLSE may have timed out before confirming that the job succeeded. For more information, see [Job Status Information and Job Run Log Messages, page 5-33](#).

- If the job status is “failed,” you can increase the value of the Vxworks to IOS time out parameter and run the job again.

To change this parameter, access the WLSE through the following URL:

`http://your_wlse:1741/debug/jobprops.jsp`

where *your\_wlse* is the name of the WLSE.

- Step 10** After the job finishes successfully:

- All access points in the job will be rebooted.
- An inventory will run automatically.
- The access points will be in the managed state.

- Cisco Aironet 1200 access points that were converted will be removed from the AP 1200 system group and placed in the AP 1210 group. Cisco Aironet 1220 access points will be in the AP 1230 group. Cisco Aironet 350 access points will be in the AP 350-IOS group.
-







## 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.

Following are the subtabs under Reports:



### Note

---

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

---

- **Device Center**—See [Using the Device Center, page 6-2](#)
- **Radio Manager**—See [Displaying Radio Manager Reports, page 6-8](#)
- **Wireless Clients**—See [Displaying Wireless Client Reports, page 6-13](#)
- **Current**—See [Displaying Current Reports, page 6-19](#)
- **Trends**—See [Displaying Trends, page 6-72](#)
- **Scheduled Email Jobs**—See [Scheduling Email Jobs, page 6-91](#)

The WLSE also has a feature that allows the system administrator, with the username admin, to manually enter a URL in the WLSE to export report data, rather than using the UI export function. For information, see [Exporting URL-Based Report Data, page 6-95](#).

# Using the Device Center

The device center enables you to quickly access various types of reports for a particular device.

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 1-10](#).

For information about the folders for device groups in the device selector, see [System-Defined Groups, page 3-86](#).



## 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. For information on how to search or use the device selector, see [Using the Device Selector and Search, page 1-9](#).
- Step 3** Click on the buttons for different report types:
  - For access points and bridges:
    - Summary report—See [Displaying an AP Summary Report, page 6-40](#)
    - Detailed report—See [Displaying a Detailed Report, page 6-43](#)
    - WDS Summary report—See [Viewing the WDS Summary Report, page 6-4](#).
    - Fault Status—See [Viewing the Fault Status Report, page 6-6](#)
    - Device History—See [Viewing Device History, page 6-6](#)
    - Config History—See [Viewing Config History, page 6-7](#)
    - Firmware History—See [Viewing Firmware History, page 6-8](#)
    - AP Web Page—Opens up a browser window to the AP Summary Status.

**Tip**

The HTTP port on IOS access points must be set to 80 for this link to work. For information on setting up the HTTP port, see [Enter HTTP Port Settings—IOS Access Points, page 3-24](#).

- For switches:
  - Summary report—See [Displaying a Switch Summary Report, page 6-66](#)
  - Fault Status—See [Viewing the Fault Status Report, page 6-6](#)
  - Device History—See [Viewing Device History, page 6-6](#)
- For routers:
  - Summary Report—See [Displaying a Router Summary Report, page 6-68](#)
  - Fault Status—See [Viewing the Fault Status Report, page 6-6](#)
  - Device History—See [Viewing Device History, page 6-6](#)
- For servers:
  - Summary Report—See [Displaying a Server Summary Report, page 6-70](#).

## Viewing the WDS Summary Report

The following table is displayed for the device's wireless domain services (WDS) summary:

**Table 6-1 WDS Summary**

| Column      | Description                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name        | The access point name.                                                                                                                                                                                                                                                                                                                                                                         |
| As Of       | <p>The time the WLSE polled information from the device.</p> <p>For more information, see <a href="#">Time Display, page 1-8</a></p>                                                                                                                                                                                                                                                           |
| MAC Address | The MAC address of the access point.                                                                                                                                                                                                                                                                                                                                                           |
| IP Address  | <p>The IP address of the access point.</p> <p>Click to open a browser window to the AP Summary Status.</p> <p><b>Tip</b> The HTTP port on IOS access points must be set to 80 for this link to work. For information on setting up the HTTP port, see <a href="#">Enter HTTP Port Settings—IOS Access Points, page 3-24</a>.</p>                                                               |
| Status      | <p>The operational status of the device:</p> <ul style="list-style-type: none"> <li>• Admin standalone—Configured as the WDS but with no other devices participating.</li> <li>• Active—The WDS is actively performing as the WDS on the subnet.</li> <li>• Backup—The WDS is acting as a backup to the main WDS.</li> <li>• Candidate—The device is configured as a WDS candidate.</li> </ul> |

**Table 6-1 WDS Summary (continued)**

| Column                                             | Description                                                |
|----------------------------------------------------|------------------------------------------------------------|
| 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.                                |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

## Viewing the Fault Status Report

The following table is displayed for the device’s fault status:

**Table 6-2    Device Fault Status**

| Column      | Description                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type        | The fault type.                                                                                                                                                                                      |
| Description | A description of the fault.<br><br>Click to see fault details. See <a href="#">Viewing Fault Details, page 2-10</a> .                                                                                |
| Severity    | The fault severity level.                                                                                                                                                                            |
| State       | The current state of the fault.                                                                                                                                                                      |
| Timestamp   | The time the fault was reported.<br><br>Click to see fault details. See <a href="#">Viewing Fault Details, page 2-10</a> .<br><br>For more information, see <a href="#">Time Display, page 1-8</a> . |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

## Viewing Device History

The following table is displayed for the device’s history:

**Table 6-3    Device History**

| Column      | Description                                                                                                         |
|-------------|---------------------------------------------------------------------------------------------------------------------|
| Timestamp   | The time the device’s state last changed.<br><br>For more information, see <a href="#">Time Display, page 1-8</a> . |
| Device Name | The name of the device.                                                                                             |

**Table 6-3** *Device History (continued)*

| Column     | Description                      |
|------------|----------------------------------|
| IP Address | The IP address of the device.    |
| State      | The current state of the device. |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

## Viewing Config History

The following table is displayed for the device's configuration history:

**Table 6-4** *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.   |
| Job Name      | The name of the configuration job.             |
| Job Type      | The type of configuration job.                 |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

## Viewing Firmware History

The following table is displayed for the device's firmware history:

**Table 6-5** *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.                         |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

## Displaying Radio Manager Reports

This window allows you to view radio management information. You can view, export, and email the reports.

Using this option, you can view the following types of radio management reports:

- Configured Radio Parameters Report (11b)—See [Displaying a Configured Radio Parameters Report \(11b\), page 6-9](#).
- Path Loss Between Managed APs Report (11b)—See [Displaying a Path Loss Between Managed APs Report \(11b\), page 6-10](#).
- Channel Loading Report (11b)—See [Displaying a Channel Loading Report \(11b\), page 6-11](#).



The folders and devices in the device selector display icons indicating the alarm status of the devices. For an explanation of the icons, see [Understanding the Icons, page 1-10](#).

For information about the folders for device groups in the device selector, see [System-Defined Groups, page 3-86](#).

**Note**

Your login determines whether you can use this option.

## Displaying a Configured Radio Parameters Report (11b)

### Procedure

- Step 1** Select **Reports > Radio Manager**. 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 **Configured Radio Parameters Report (11b)**.
- Step 4** Click **View**. The following report displays.

**Table 6-6** *Configured Radio Parameters Report (11b)*

| 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 (11b).                       |
| Channel        | The radio channel used.                                  |
| Transmit Power | The power level of the radio transmission in milliwatts. |
| Data Rate      | The data rate in Mbps.                                   |
| Beacon         | The amount of time between beacons in kilomicroseconds.  |

**Table 6-6 Configured Radio Parameters Report (11b) (continued)**

| Column             | Description                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Admin Status       | The administrative status of the access point.                                                                                  |
| Operational Status | The operational status of the access point.                                                                                     |
| As Of              | The time the WLSE polled information from the device.<br><br>For more information, see <a href="#">Time Display, page 1-8</a> . |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

- Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## Displaying a Path Loss Between Managed APs Report (11b)

### Procedure

- Step 1** Select **Reports > Radio Manager**. 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 **Path Loss Between Managed APs Report (11b)**.
- Step 4** Click **View**. The following report displays.

**Table 6-7 Path Loss Between Managed APs Report (11b)**

| Column         | Description                      |
|----------------|----------------------------------|
| AP Name        | The name of the access point.    |
| Interface Name | The name of the radio interface. |

**Table 6-7 Path Loss Between Managed APs Report (11b) (continued)**

| Column                  | Description                                                                                                                     |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| PHY                     | The physical interface type (11b).                                                                                              |
| 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.<br><br>For more information, see <a href="#">Time Display, page 1-8</a> . |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

**Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## Displaying a Channel Loading Report (11b)

### Procedure

- Step 1** Select **Reports > Radio Manager**. 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 **Channel Loading Report (11b)**.

**Step 4** Click **View**. The following report displays.

**Table 6-8 Channel Loading Report (11b)**

| Column           | Description                                                                                                                     |
|------------------|---------------------------------------------------------------------------------------------------------------------------------|
| AP Name          | The name of the access point.                                                                                                   |
| PHY              | The physical interface type (11b).                                                                                              |
| 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.<br><br>For more information, see <a href="#">Time Display, page 1-8</a> . |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

**Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

# Displaying Wireless Client Reports

Wireless client reports provide information about the type of client that is associating with an access point, information about how much bandwidth the client is using, and a history of which access points the client has been associated with.

Wireless client reports are not real-time reports. The data is only as fresh as the last client polling cycle, which means the client polling interval can greatly determine the accuracy of the client reports. Therefore:

- In environments where clients are highly mobile, such as health care and retail deployments, set the client inventory 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 fairly stationary for longer periods of time, so the client polling cycles should be more infrequent.

Wireless client polling is a fairly heavy-weight process. If you have many access points to poll for client associations, the interval will need to be set more infrequently, and as a result, the client data will not be as accurate. To set the client polling interval, see [Changing the Polling Intervals for Automatic Inventories, page 3-70](#).

Wireless Clients reports are updated every 51 minutes by default. To change the default setting, select **Devices > Discover > Inventory > Polling**.

**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 6-14](#)
- Client Statistics Report—See [Displaying a Client Statistics Report, page 6-16](#)
- Client Historical Association Report—See [Displaying a Client Historical Association Report, page 6-18](#)

## 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.

### 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 MAC address, IP address, or name. 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.



### Note

Searching for clients based on names works only for clients associated to IOS devices.

- Step 4** Click **Search**. A list appears in the left pane.
- Step 5** Click the MAC address, IP address or name. The right pane refreshes and displays the Client Detail Report, which is the default report.

The reports for wireless clients associated to IOS and to non-IOS devices are different:

- IOS Client Detail Report—See [Table 6-9 on page 6-15](#).
- Non-IOS Client Detail Report—See [Table 6-10 on page 6-15](#).

**Table 6-9 IOS Client Detail Report**

| Column         | Description                                                                                                                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name           | The client name.                                                                                                                                                                                                |
| IP Address     | The client IP address.                                                                                                                                                                                          |
| Client Type    | The type of client.                                                                                                                                                                                             |
| Connected to   | <p>The name or IP address of the AP.</p> <p>Click on this link to view the AP Detail Report and the Fault Summary.</p> <p>For more information, see <a href="#">Displaying a Detailed Report, page 6-43</a></p> |
| Role           | Indicates the role of the device.                                                                                                                                                                               |
| Radio Type     | The type of client radio type.                                                                                                                                                                                  |
| Time last seen | The time the client was last seen by the system.                                                                                                                                                                |
| MAC Address    | The MAC address of the client.                                                                                                                                                                                  |

**Table 6-10 Non-IOS Client Detail Report**

| Column         | Description                                                                                                                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name           | The name of the client.                                                                                                                                                                                         |
| IP Address     | The IP address of the client.                                                                                                                                                                                   |
| Client Type    | The type of client.                                                                                                                                                                                             |
| Connected to   | <p>The name or IP address of the AP.</p> <p>Click on this link to view the AP Detail Report and the Fault Summary.</p> <p>For more information, see <a href="#">Displaying a Detailed Report, page 6-43</a></p> |
| State          | The current state of the client.                                                                                                                                                                                |
| Time last seen | The time the client was last seen by the system.                                                                                                                                                                |

**Table 6-10 Non-IOS Client Detail Report (continued)**

| Column           | Description                              |
|------------------|------------------------------------------|
| Software Version | The version of software for this device. |
| MAC Address      | The MAC address of the wireless client.  |

- Step 6

To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 7

To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## 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 MAC address, IP address, or name. You can use an asterisk (\*) as a wildcard to denote numbers and letters.



**Note**

Searching for clients based on names works only for clients associated to IOS devices.

- Step 4

Click **Search**. A list appears in the left pane.
- Step 5

Select the MAC address, IP address, or name. The right pane refreshes.



- Step 6** From the Report Name list, select **Client Statistics Report**.
- Step 7** Click **View**. The reports for wireless clients associated to IOS and to non-IOS devices are different:
- IOS Client Statistics Report—See [Table 6-11 on page 6-17](#).
  - Non-IOS Client Statistics Report—See [Table 6-12 on page 6-17](#).

**Table 6-11 IOS Client Statistics Report**

| Column                                | Description                                               |
|---------------------------------------|-----------------------------------------------------------|
| Name                                  | The client name.                                          |
| IP Address                            | The client IP address.                                    |
| MAC Address                           | The MAC address of the client.                            |
| 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 (dBm) | A tally of the received signal power.                     |
| Latest Signal Quality (%)             | The current index of radio signal quality.                |
| Received WEP Errors                   | The number of received encryption errors.                 |
| Packet Errors                         | The number of packet errors.                              |

**Table 6-12 Non-IOS Client Statistics Report**

| Column         | Description                                               |
|----------------|-----------------------------------------------------------|
| Name           | The name of the client.                                   |
| IP Address     | The IP address of the client.                             |
| Time last seen | The time the wireless client was last seen by the system. |

- Step 8** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 9** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).
- 

## 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.

---

### 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 MAC address, IP address, or name. You can use an asterisk (\*) as a wildcard to denote numbers and letters.



### Note

Searching for clients based on names works only for clients associated to IOS devices.

---

- Step 4** Click **Search**. A list appears in the left pane.
- Step 5** Select the MAC address, IP address, or name. The right pane refreshes.
- Step 6** From the Report Name list, select **Client Historical Association Report**.

- Step 7** Click **View**. The Client Historical Association Report displays in the right pane with the following information:

**Table 6-13 Client Historical Association Report**

| Column          | Description                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AP IP Address   | The IP address of the access point.                                                                                                                                                                                                                                                                                                                         |
| AP Name         | The name of the access point.                                                                                                                                                                                                                                                                                                                               |
| Associated Time | <p>The time when the WLSE has polled the access point to retrieve the client association time.</p> <p><b>Tip</b> To ensure that you are viewing the most up-to-date information, verify when the last inventory cycle occurred. Client inventory status can be seen by selecting <b>Administration &gt; Discover &gt; Tasks History &gt; Inventory</b>.</p> |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

- Step 8** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 9** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## 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 \(Non-IOS Devices\), page 6-20](#)
- [Group Reports \(IOS Devices\), page 6-20](#)
- [Access Point Reports \(Non-IOS Devices\), page 6-21](#)

- [Access Point Reports \(IOS Devices\)](#), page 6-21
- [Switch Reports](#), page 6-22
- [Router Reports](#), page 6-22
- [Server Reports](#), page 6-22

The folders and devices in the device selector display icons indicating the alarm status of the devices. For an explanation of the icons, see [Understanding the Icons](#), page 1-10.

For information about the folders for device groups in the device selector, see [System-Defined Groups](#), page 3-86.

**Note**


---

Your login determines whether you can use this option.

---

**Group Reports (Non-IOS Devices)**

- Group Client Association—See [Displaying a Group Client Association Report](#), page 6-22
- Group Security Report—See [Displaying a Group Security Report](#), page 6-26
- Group SSID Report—See [Displaying a Group SSID Report](#), page 6-29
- Group VLAN Report—See [Displaying a Group VLAN Report](#), page 6-32
- Per VLAN Client Report—See [Displaying a Per VLAN Client Report](#), page 6-35
- Group Policy Report—See [Displaying a Group Policy Report](#), page 6-38

**Group Reports (IOS Devices)**

- Group Client Association—See [Displaying a Group Client Association Report](#), page 6-22
- Group Security Report—See [Displaying a Group Security Report](#), page 6-26
- Group SSID Report—See [Displaying a Group SSID Report](#), page 6-29
- Group VLAN Report—See [Displaying a Group VLAN Report](#), page 6-32
- Per VLAN Client Report—See [Displaying a Per VLAN Client Report](#), page 6-35

**Access Point Reports (Non-IOS Devices)**

- Summary Report—See [Displaying an AP Summary Report](#), page 6-40
- Detailed Report—See [Displaying a Detailed Report](#), page 6-43
- AP Associations—See [Displaying an AP Associations Report](#), page 6-49
- EAP Authentication Report—See [Displaying an EAP Authentication Report](#), page 6-50
- AP Ethertype Protocol Filters—See [Displaying an AP Ethertype Protocol Filters Report](#), page 6-52
- AP IP Protocol Filters—See [Displaying an AP IP Protocol Filters Report](#), page 6-53
- AP IP Port Filters—See [Displaying an AP IP Port Filters Report](#), page 6-54
- AP Policy Report—See [Displaying an AP Policy Report](#), page 6-55
- AP QoS Report—[Displaying an AP QoS Report](#), page 6-57
- AP SSID Report—[Displaying an AP SSID Report](#), page 6-59
- AP VLAN Report—[Displaying an AP VLAN Report](#), page 6-61
- Per VLAN Client Report—[Displaying a Per VLAN Client Report](#), page 6-63
- AP Hot Standby Report—[Displaying an AP Hot Standby Report](#), page 6-65

**Access Point Reports (IOS Devices)**

- Summary Report—See [Displaying an AP Summary Report](#), page 6-40
- Detailed Report—See [Displaying a Detailed Report](#), page 6-43
- AP Associations—See [Displaying an AP Associations Report](#), page 6-49
- EAP Authentication Report—See [Displaying an EAP Authentication Report](#), page 6-50
- AP QoS Report—[Displaying an AP QoS Report](#), page 6-57
- AP SSID Report—[Displaying an AP SSID Report](#), page 6-59
- AP VLAN Report—[Displaying an AP VLAN Report](#), page 6-61
- Per VLAN Client Report—[Displaying a Per VLAN Client Report](#), page 6-63
- AP Hot Standby Report—[Displaying an AP Hot Standby Report](#), page 6-65

**Switch Reports**

- Switch Summary Report—See [Displaying a Switch Summary Report, page 6-66](#)
- AP and Bridge Connected to Switch Report—See [Displaying an AP and Bridge Connected to Switch Report, page 6-67](#)

**Router Reports**

- Router Summary Report—See [Displaying a Router Summary Report, page 6-68](#)
- AP and Bridge Connected to Router Report—See [Displaying an AP and Bridge Connected to Router Report, page 6-69](#)

**Server Reports**

- Server Summary Report—See [Displaying a Server Summary Report, page 6-70](#)
- AP Usage Report—See [Displaying an AP Usage Report, page 6-71](#)

## 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**.
- Step 4** Click **View**. The following report displays. The reports for IOS and non-IOS devices are different:
- IOS Group Client Association Report—See [Table 6-14 on page 6-23](#).
  - Non-IOS Group Client Association Report—See [Table 6-15 on page 6-24](#).

**Table 6-14 IOS Group Client Association Report**

| Column                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Number of Clients Associated to this Group | The total number of clients associated with the group of access points or bridges.                                                                                                                                                                                                                                                                                                                         |
| Count of Active Stations in this Group     | The number of access points or bridges currently in the group.                                                                                                                                                                                                                                                                                                                                             |
| As Of                                      | The time the WLSE polled information from the device.<br><br>For more information, see <a href="#">Time Display, page 1-8</a> .                                                                                                                                                                                                                                                                            |
| AP Name                                    | The name of the access point.<br><br>Click to view the following: <ul style="list-style-type: none"> <li>• AP Detailed Report—See <a href="#">Displaying a Detailed Report, page 6-43</a>.</li> <li>• Fault Summary—See <a href="#">Viewing the Fault Status Report, page 6-6</a>.</li> <li>• EAP Authentication Report—See <a href="#">Displaying an EAP Authentication Report, page 6-50</a>.</li> </ul> |
| AP IP Address                              | The IP address of the access point.<br><br>Click to open a browser window to the AP Summary Status.<br><br><b>Tip</b> The HTTP port on IOS access points must be set to 80 for this link to work. For information on setting up the HTTP port, see <a href="#">Enter HTTP Port Settings—IOS Access Points, page 3-24</a> .                                                                                 |
| 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.                                                                                                                                                                                                                                                                                                                                                       |

**Table 6-14 IOS Group Client Association Report (continued)**

| Column                           | Description                                                                                                                 |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Number of AP-Repeaters Connected | The number of repeaters connected to the access point.                                                                      |
| Status (Fault)                   | Click to view the Fault Summary.<br>For more information, see <a href="#">Viewing the Fault Status Report, page 6-6</a> .   |
| As Of                            | The time the WLSE polled information from the device.<br>For more information, see <a href="#">Time Display, page 1-8</a> . |

**Table 6-15 Non-IOS Group Client Association Report**

| Column                                     | Description                                                                                                                 |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Number of Clients Associated to this Group | The total number of clients currently associated with the group of access points or bridges.                                |
| Count of Active Stations in this Group     | The number of access points or bridges currently in the group.                                                              |
| As Of                                      | The time the WLSE polled information from the device.<br>For more information, see <a href="#">Time Display, page 1-8</a> . |



**Table 6-15 Non-IOS Group Client Association Report (continued)**

| Column                           | Description                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AP Name                          | <p>The name of the access point.</p> <p>Click to view the following:</p> <ul style="list-style-type: none"> <li>• AP Detailed Report—See <a href="#">Displaying a Detailed Report</a>, page 6-43.</li> <li>• Fault Summary—See <a href="#">Viewing the Fault Status Report</a>, page 6-6.</li> <li>• EAP Authentication Report—See <a href="#">Displaying an EAP Authentication Report</a>, page 6-50.</li> </ul> |
| AP IP Address                    | <p>The IP address of the access point.</p> <p>Click to open a browser window to the AP Summary Status.</p>                                                                                                                                                                                                                                                                                                        |
| 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)                   | <p>Click to view the Fault Summary.</p> <p>For more information, see <a href="#">Viewing the Fault Status Report</a>, page 6-6.</p>                                                                                                                                                                                                                                                                               |
| As Of                            | <p>The time the WLSE polled information from the device.</p> <p>For more information, see <a href="#">Time Display</a>, page 1-8.</p>                                                                                                                                                                                                                                                                             |

For information on how to sort table data, see [Sorting Table Data](#), page 1-11.

**Step 5** To export the report, click **Export**. See [Exporting a Report](#), page 6-89.

**Step 6** To email the report, click **Email Report**. See [Emailing a Report](#), page 6-89.

# 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**.
- Step 4

Click **View**. The following report displays. The reports for IOS and non-IOS devices are different:
 
  - IOS Group Security Report—See [Table 6-16 on page 6-26](#).
  - Non-IOS Group Security Report—See [Table 6-17 on page 6-28](#).

**Table 6-16 IOS Group Security Report**

| Column  | Description                                                                                                                                                                                                                                                                                                                                                                               |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AP Name | <p>The name of the device.</p> <p>Click to view the following:</p> <ul style="list-style-type: none"> <li>AP Detailed Report—<a href="#">Displaying a Detailed Report, page 6-43</a>.</li> <li>Fault Summary—<a href="#">Viewing the Fault Status Report, page 6-6</a>.</li> <li>EAP Authentication Report—<a href="#">Displaying an EAP Authentication Report, page 6-50</a>.</li> </ul> |

**Table 6-16 IOS Group Security Report (continued)**

| Column                            | Description                                                                                                                                                                                                                                                                                                                |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AP IP Address                     | <p>The IP address of the device.</p> <p>Click to open a browser window to the AP Summary Status.</p> <p><b>Tip</b> The HTTP port on IOS access points must be set to 80 for this link to work. For information on setting up the HTTP port, see <a href="#">Enter HTTP Port Settings—IOS Access Points, page 3-24</a>.</p> |
| RF Interface                      | The radio interface name.                                                                                                                                                                                                                                                                                                  |
| Encryption Type                   | Indicates that devices using WEP are allowed to communicate with the access point.                                                                                                                                                                                                                                         |
| 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.                                                                                                                                                                                                                      |
| Status (Fault)                    | <p>Click to view the Fault Summary.</p> <p>For more information, see <a href="#">Viewing the Fault Status Report, page 6-6</a>.</p>                                                                                                                                                                                        |
| Link to EAP Authentication Report | <p>Click to view the EAP Authentication report.</p> <p>For more information, see <a href="#">Displaying an EAP Authentication Report, page 6-50</a>.</p>                                                                                                                                                                   |
| As Of                             | <p>The time the fault was reported.</p> <p>For more information, see <a href="#">Time Display, page 1-8</a>.</p>                                                                                                                                                                                                           |

**Table 6-17 Non-IOS Group Security Report**

| Column                            | Description                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AP Name                           | <p>The name of the device.</p> <p>Click to view the following:</p> <ul style="list-style-type: none"> <li>• AP Detailed Report—<a href="#">Displaying a Detailed Report, page 6-43.</a></li> <li>• Fault Summary—<a href="#">Viewing the Fault Status Report, page 6-6.</a></li> <li>• EAP Authentication Report—<a href="#">Displaying an EAP Authentication Report, page 6-50.</a></li> </ul> |
| AP IP Address                     | <p>The IP address of the device.</p> <p>Click to open a browser window to the AP Summary Status.</p>                                                                                                                                                                                                                                                                                            |
| RF Interface                      | The radio interface name.                                                                                                                                                                                                                                                                                                                                                                       |
| 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.                                                                                                                                                                                                                                                                                           |
| Status (Fault)                    | <p>Click to view the Fault Summary.</p> <p>For more information, see <a href="#">Viewing the Fault Status Report, page 6-6.</a></p>                                                                                                                                                                                                                                                             |

**Table 6-17 Non-IOS Group Security Report (continued)**

| Column                            | Description                                                                                                                                    |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Link to EAP Authentication Report | Click to view the EAP Authentication report.<br>For more information, see <a href="#">Displaying an EAP Authentication Report</a> , page 6-50. |
| As Of                             | The time the fault was reported.<br>For more information, see <a href="#">Time Display</a> , page 1-8.                                         |

For information on how to sort table data, see [Sorting Table Data](#), page 1-11.

- Step 5** To export the report, click **Export**. See [Exporting a Report](#), page 6-89.
- Step 6** To email the report, click **Email Report**. See [Emailing a Report](#), page 6-89.

## 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**.
- Step 3** Click **View**. The following report displays. The reports for IOS and non-IOS devices are different:
- IOS Group SSID Report—See [Table 6-18 on page 6-30](#).
  - Non-IOS Group SSID Report—See [Table 6-19 on page 6-31](#).

**Table 6-18 IOS Group SSID Report**

| Column        | Description                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSID          | The unique identifier the client device uses to associate with the access point.                                                                                                                                                                                                                                                                                                                                  |
| AP Name       | <p>The name of the access point.</p> <p>Click to view the following:</p> <ul style="list-style-type: none"> <li>• AP Detailed Report—See <a href="#">Displaying a Detailed Report, page 6-43</a>.</li> <li>• Fault Summary—See <a href="#">Viewing the Fault Status Report, page 6-6</a>.</li> <li>• EAP Authentication Report—See <a href="#">Displaying an EAP Authentication Report, page 6-50</a>.</li> </ul> |
| AP IP Address | <p>The IP address of the access point.</p> <p>Click to open a browser window to the AP Summary Status.</p> <p><b>Tip</b> The HTTP port on IOS access points must be set to 80 for this link to work. For information on setting up the HTTP port, see <a href="#">Enter HTTP Port Settings—IOS Access Points, page 3-24</a>.</p>                                                                                  |
| RF Interface  | The radio interface name.                                                                                                                                                                                                                                                                                                                                                                                         |
| VLAN ID       | The identification number of the VLAN.                                                                                                                                                                                                                                                                                                                                                                            |
| As Of         | <p>The time the WLSE polled information from the device.</p> <p>For more information, see <a href="#">Time Display, page 1-8</a>.</p>                                                                                                                                                                                                                                                                             |

**Step 4** Go to [Step 5](#).

**Table 6-19 Non-IOS Group SSID Report**

| Column                      | Description                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSID                        | The unique identifier the client device uses to associate with the access point.                                                                                                                                                                                                                                                                                                                                  |
| VLAN ID                     | The identification number of the VLAN.                                                                                                                                                                                                                                                                                                                                                                            |
| VLAN Name                   | The name of the VLAN.                                                                                                                                                                                                                                                                                                                                                                                             |
| AP Name                     | <p>The name of the access point.</p> <p>Click to view the following:</p> <ul style="list-style-type: none"> <li>• AP Detailed Report—See <a href="#">Displaying a Detailed Report, page 6-43</a>.</li> <li>• Fault Summary—See <a href="#">Viewing the Fault Status Report, page 6-6</a>.</li> <li>• EAP Authentication Report—See <a href="#">Displaying an EAP Authentication Report, page 6-50</a>.</li> </ul> |
| AP IP Address               | <p>The IP address of the access point.</p> <p>Click to open a browser window to the AP Summary Status.</p>                                                                                                                                                                                                                                                                                                        |
| RF Interface                | The radio interface name.                                                                                                                                                                                                                                                                                                                                                                                         |
| Number of Clients Connected | The number of wireless clients connected to the device.                                                                                                                                                                                                                                                                                                                                                           |
| Priority                    | The priority configuration based on the traffic type.                                                                                                                                                                                                                                                                                                                                                             |
| Default Policy Group        | <p>The number of the default policy group (which contains access parameters).</p> <p>Click to view the Policy Report—See <a href="#">Displaying a Group Policy Report, page 6-38</a>.</p>                                                                                                                                                                                                                         |
| As Of                       | <p>The time the WLSE polled information from the device.</p> <p>For more information, see <a href="#">Time Display, page 1-8</a>.</p>                                                                                                                                                                                                                                                                             |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

- Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).
- 

## 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**.
- Step 3** Click **View**. The following report displays. The reports for IOS and non-IOS devices are different:
- IOS Group VLAN Report—See [Table 6-20 on page 6-33](#).
  - Non-IOS Group VLAN Report—See [Table 6-21 on page 6-34](#).



**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 IOS access points, VLAN information is accessible by SNMP.

---



**Table 6-20 IOS Group VLAN Report**

| Column           | Description                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLAN ID          | The identification number of the VLAN.                                                                                                                                                                                                                                                                                                                                                                            |
| AP Name          | <p>The name of the access point.</p> <p>Click to view the following:</p> <ul style="list-style-type: none"> <li>• AP Detailed Report—See <a href="#">Displaying a Detailed Report, page 6-43</a>.</li> <li>• Fault Summary—See <a href="#">Viewing the Fault Status Report, page 6-6</a>.</li> <li>• EAP Authentication Report—See <a href="#">Displaying an EAP Authentication Report, page 6-50</a>.</li> </ul> |
| AP IP Address    | <p>The IP address of the access point.</p> <p>Click to open a browser window to the AP Summary Status.</p> <p><b>Tip</b> The HTTP port on IOS access points must be set to 80 for this link to work. For information on setting up the HTTP port, see <a href="#">Enter HTTP Port Settings—IOS Access Points, page 3-24</a>.</p>                                                                                  |
| 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            | <p>The time the WLSE polled information from the device.</p> <p>For more information, see <a href="#">Time Display, page 1-8</a>.</p>                                                                                                                                                                                                                                                                             |

**Step 4** Go to [Step 5](#).

**Table 6-21 Non-IOS Group VLAN Report**

| Column                      | Description                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLAN ID                     | The identification number of the VLAN.                                                                                                                                                                                                                                                                                                                                                                            |
| VLAN Name                   | The name of the VLAN.                                                                                                                                                                                                                                                                                                                                                                                             |
| AP Name                     | <p>The name of the access point.</p> <p>Click to view the following:</p> <ul style="list-style-type: none"> <li>• AP Detailed Report—See <a href="#">Displaying a Detailed Report</a>, page 6-43.</li> <li>• Fault Summary—See <a href="#">Viewing the Fault Status Report</a>, page 6-6.</li> <li>• EAP Authentication Report—See <a href="#">Displaying an EAP Authentication Report</a>, page 6-50.</li> </ul> |
| AP IP Address               | <p>The IP address of the access point.</p> <p>Click to open a browser window to the AP Summary Status.</p>                                                                                                                                                                                                                                                                                                        |
| SSID                        | The unique identifier the client device uses to associate with the access point.                                                                                                                                                                                                                                                                                                                                  |
| RF Interface                | The radio interface name.                                                                                                                                                                                                                                                                                                                                                                                         |
| Number of Clients Connected | The number of wireless clients connected to the device.                                                                                                                                                                                                                                                                                                                                                           |
| Priority                    | The priority configuration based on the traffic type.                                                                                                                                                                                                                                                                                                                                                             |
| Default Policy Group        | <p>The number of the default policy group (which contains access parameters).</p> <p>Click to view the Policy Report—See <a href="#">Displaying a Group Policy Report</a>, page 6-38.</p>                                                                                                                                                                                                                         |
| As Of                       | <p>The time the WLSE polled information from the device.</p> <p>For more information, see <a href="#">Time Display</a>, page 1-8.</p>                                                                                                                                                                                                                                                                             |

For information on how to sort table data, see [Sorting Table Data](#), page 1-11.

- Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).
- 

## 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**.
- Step 3** Click **View**. The following report displays. The reports for IOS and non-IOS devices are different:
- IOS Per VLAN Client Report—See [Table 6-22 on page 6-35](#).
  - Non-IOS Per VLAN Client Report—See [Table 6-23 on page 6-36](#).

**Table 6-22 IOS Per VLAN Client Report**

| Column  | Description                            |
|---------|----------------------------------------|
| VLAN ID | The identification number of the VLAN. |

**Table 6-22 IOS Per VLAN Client Report (continued)**

| Column             | Description                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AP Name            | <p>The name of the access point.</p> <p>Click to view the following:</p> <ul style="list-style-type: none"> <li>• AP Detailed Report—See <a href="#">Displaying a Detailed Report, page 6-43</a>.</li> <li>• Fault Summary—See <a href="#">Viewing the Fault Status Report, page 6-6</a>.</li> <li>• EAP Authentication Report—See <a href="#">Displaying an EAP Authentication Report, page 6-50</a>.</li> </ul> |
| SSID               | The unique identifier the client device uses to associate with the access point.                                                                                                                                                                                                                                                                                                                                  |
| Client MAC Address | The MAC address of the client.                                                                                                                                                                                                                                                                                                                                                                                    |
| ClientType         | The type of client.                                                                                                                                                                                                                                                                                                                                                                                               |
| As Of              | <p>The time the WLSE polled information from the device.</p> <p>For more information, see <a href="#">Time Display, page 1-8</a>.</p>                                                                                                                                                                                                                                                                             |

**Step 4** Go to [Step 5](#).

**Table 6-23 Non-IOS Per VLAN Client Report**

| Column    | Description                            |
|-----------|----------------------------------------|
| VLAN ID   | The identification number of the VLAN. |
| VLAN Name | The name of the VLAN.                  |

**Table 6-23 Non-IOS Per VLAN Client Report (continued)**

| Column             | Description                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AP Name            | <p>The name of the access point.</p> <p>Click to view the following:</p> <ul style="list-style-type: none"> <li>• AP Detailed Report—See <a href="#">Displaying a Detailed Report, page 6-43</a>.</li> <li>• Fault Summary—See <a href="#">Viewing the Fault Status Report, page 6-6</a>.</li> <li>• EAP Authentication Report—See <a href="#">Displaying an EAP Authentication Report, page 6-50</a>.</li> </ul> |
| 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.                                                                                                                                                                                                                                                                                                                                                                                     |
| RF Interface       | The radio interface name.                                                                                                                                                                                                                                                                                                                                                                                         |
| SSID               | The unique identifier the client device uses to associate with the access point.                                                                                                                                                                                                                                                                                                                                  |
| Client Type        | The type of client.                                                                                                                                                                                                                                                                                                                                                                                               |
| As Of              | <p>The time the WLSE polled information from the device.</p> <p>For more information, see <a href="#">Time Display, page 1-8</a>.</p>                                                                                                                                                                                                                                                                             |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

**Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

# Displaying a Group Policy Report

This report lists all the policy groups configured on each of the non-IOS 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 Policy Report**.
- Step 3

Click **View**. The following report displays the following:

**Table 6-24** Group Policy Report

| Column                   | Description                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AP Name                  | <p>The name of the access point.</p> <p>Click to view the following:</p> <ul style="list-style-type: none"> <li>AP Detailed Report—See <a href="#">Displaying a Detailed Report, page 6-43</a>.</li> <li>Fault Summary—See <a href="#">Viewing the Fault Status Report, page 6-6</a>.</li> <li>EAP Authentication Report—See <a href="#">Displaying an EAP Authentication Report, page 6-50</a>.</li> </ul> |
| AP IP Address            | <p>The IP address of the access point.</p> <p>Click to open a browser window to the AP Summary Status.</p>                                                                                                                                                                                                                                                                                                  |
| Policy Group Id          | The identification number of the policy group.                                                                                                                                                                                                                                                                                                                                                              |
| Policy Group Name        | The name of the policy group.                                                                                                                                                                                                                                                                                                                                                                               |
| Ethertype Filter Id (In) | <p>The identification number of the (receive) Ethertype filter.</p> <p>Click to view the AP Ethertype Protocol Filters Report—See <a href="#">Displaying an AP Ethertype Protocol Filters Report, page 6-52</a>.</p>                                                                                                                                                                                        |

**Table 6-24 Group Policy Report (continued)**

| Column                      | Description                                                                                                                                                                                                           |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ethertype Filter Id (Out)   | <p>The identification number of the (transmit) Ethertype filter.</p> <p>Click to view the AP Ethertype Protocol Filters Report—See <a href="#">Displaying an AP Ethertype Protocol Filters Report, page 6-52</a>.</p> |
| IP Protocol Filter Id (In)  | <p>The identification number of the (receive) IP protocol filter.</p> <p>Click to view the AP IP Protocol Filters Report—See <a href="#">Displaying an AP IP Protocol Filters Report, page 6-53</a>.</p>              |
| IP Protocol Filter Id (Out) | <p>The identification number of the (transmit) IP protocol filter</p> <p>Click to view the AP IP Protocol Filters Report—See <a href="#">Displaying an AP IP Protocol Filters Report, page 6-53</a>.</p>              |
| IP Port Filter Id (In)      | <p>The identification number of the (receive) IP port filter.</p> <p>Click to view the AP IP Port Filters Report—See <a href="#">Displaying an AP IP Port Filters Report, page 6-54</a>.</p>                          |
| IP Port Filter Id (Out)     | <p>The identification number of the (transmit) IP port filter.</p> <p>Click to view the AP IP Port Filters Report—See <a href="#">Displaying an AP IP Port Filters Report, page 6-54</a>.</p>                         |
| As Of                       | <p>The time the WLSE polled information from the device.</p> <p>For more information, see <a href="#">Time Display, page 1-8</a>.</p>                                                                                 |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

- Step 4** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 5** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## Displaying an AP 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 and Search, page 1-9](#).
- Step 3** From the Report Name list, select **Summary Report**.
- Step 4** Click **View**.
- If viewing from the Device Center tab, the AP Summary Report is displayed.
  - If viewing from the Current tab, the AP Summary Report and the Fault Summary are displayed.



**Note** If the selected device has dual interfaces, two summary reports are displayed, one for each interface.

**Table 6-25 AP Summary Report**

| Column      | Description                                                                                                                     |
|-------------|---------------------------------------------------------------------------------------------------------------------------------|
| Name        | The system name for the device.                                                                                                 |
| As Of       | The time the WLSE polled information from the device.<br><br>For more information, see <a href="#">Time Display, page 1-8</a> . |
| MAC Address | The device's MAC address.                                                                                                       |



**Table 6-25 AP Summary Report (continued)**

| Column                                                                                                        | Description                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP Address                                                                                                    | <p>The device's IP address.</p> <p>Click to open a browser window to the AP Summary Status.</p> <p><b>Tip</b> The HTTP port on IOS access points must be set to 80 for this link to work. For information on setting up the HTTP port, see <a href="#">Enter HTTP Port Settings—IOS Access Points, page 3-24</a>..</p> |
| Parent WDS for the Access Point<br><b>Note</b> This column displays only on the Device Center summary report. | The access point that provides Wireless Domain Services.                                                                                                                                                                                                                                                               |
| Version                                                                                                       | <ul style="list-style-type: none"> <li>For IOS devices, the IOS version on the device.</li> <li>For non-IOS devices, the software version on the device.</li> </ul>                                                                                                                                                    |
| 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.                                                                                                                                                                                                                                                                    |
| Model                                                                                                         | Model number of the device.                                                                                                                                                                                                                                                                                            |
| SSID                                                                                                          | The unique identifier the client device uses to associate with the access point.                                                                                                                                                                                                                                       |
| SSID Associated to the Native Vlan                                                                            | The SSID that is mapped to the native VLAN.                                                                                                                                                                                                                                                                            |
| Radio Cell Role                                                                                               | Indicates whether the device is used as a root or repeater.                                                                                                                                                                                                                                                            |

**Table 6-25 AP Summary Report (continued)**

| Column                            | Description                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Link to the Detailed Report       | <p>Click to see details.</p> <p><b>Note</b> This link is not available from the Device Center.</p> <p>For more information, see <a href="#">Displaying a Detailed Report, page 6-43</a>.</p>                                                                                                                                                                |
| Link to the Association Report    | <p>Click to see associations.</p> <p><b>Note</b> This link is not available from the Device Center.</p> <p>For more information, see <a href="#">Displaying an AP Associations Report, page 6-49</a>.</p>                                                                                                                                                   |
| Link to the Access Point Web Page | <p>Click to open a browser window to the AP Summary Status.</p> <p><b>Tip</b> The HTTP port on IOS access points must be set to 80 for this link to work. For information on setting up the HTTP port, see <a href="#">Enter HTTP Port Settings—IOS Access Points, page 3-24</a>.</p> <p><b>Note</b> This link is not available from the Device Center.</p> |

For information on the Fault Summary, see [Viewing the Fault Status Report, page 6-6](#).

**Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## Displaying a Detailed 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 and Search, page 1-9](#).
- Step 3** From the Report Name list, select **Detailed Report**.
- Step 4** Click **View**.
  - The Detailed Reports for IOS and non-IOS devices are different:
    - IOS Detailed Report—See [Table 6-26 on page 6-43](#).
    - Non-IOS Detailed Report—See [Table 6-27 on page 6-46](#).
  - 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 6-26 IOS Detailed Report**

| Column      | Description                                                                                                                     |
|-------------|---------------------------------------------------------------------------------------------------------------------------------|
| Name        | The system name for the device.                                                                                                 |
| As Of       | The time the WLSE polled information from the device.<br><br>For more information, see <a href="#">Time Display, page 1-8</a> . |
| MAC Address | The device's MAC address.                                                                                                       |

**Table 6-26 IOS Detailed Report (continued)**

| Column                              | Description                                                                                                                                                                                                                                                                                                           |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP Address                          | <p>The device's IP address.</p> <p>Click to open a browser window to the AP Summary Status.</p> <p><b>Tip</b> The HTTP port on IOS access points must be set to 80 for this link to work. For information on setting up the HTTP port, see <a href="#">Enter HTTP Port Settings—IOS Access Points, page 3-24</a>.</p> |
| Number of Clients Connected         | The number of wireless clients connected to the device.                                                                                                                                                                                                                                                               |
| Number of Bridges Connected         | The number of bridges connected to the device.                                                                                                                                                                                                                                                                        |
| Number of AP-Repeaters Connected    | The number of AP repeaters connected to the device.                                                                                                                                                                                                                                                                   |
| Software Version                    | The IOS version on the device.                                                                                                                                                                                                                                                                                        |
| SSID                                | The unique identifier the client device uses to associate with the access point.                                                                                                                                                                                                                                      |
| SSID Associated to the Native Vlan  | The SSID that is mapped to the native VLAN.                                                                                                                                                                                                                                                                           |
| Radio Cell Role                     | Indicates the role of the device.                                                                                                                                                                                                                                                                                     |
| Subnet Mask                         | The subnet mask.                                                                                                                                                                                                                                                                                                      |
| Hot StandBy                         | <p>Indicates whether the hot standby unit is in monitoring mode.</p> <p>If true, the current unit is in monitoring mode.</p>                                                                                                                                                                                          |
| Current operating frequency channel | The radio channel being used.                                                                                                                                                                                                                                                                                         |
| Ethernet Port Status                | The operational status of the Ethernet port.                                                                                                                                                                                                                                                                          |
| Radio Port Status                   | The operational status of the radio port.                                                                                                                                                                                                                                                                             |

**Table 6-26 IOS Detailed Report (continued)**

| Column                                     | Description                                                                                                                                                                                                                                                                           |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Transmit Power (mW)                        | The access point's transmission power setting in milliwatts.                                                                                                                                                                                                                          |
| Switch IP (to which this AP is attached)   | <p>The IP address of the switch to which this access point is attached.</p> <p><b>Note</b> CDP must be enabled for the switch information to be collected for this report.</p>                                                                                                        |
| Switch Name (to which this AP is attached) | <p>The name of the switch to which this access point is attached.</p> <p><b>Note</b> CDP must be enabled for the switch information to be collected for this report.</p>                                                                                                              |
| Length of WEP key 1 through 4 (in bits)    | The WEP key length.                                                                                                                                                                                                                                                                   |
| 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.                                                                                                                                                                                 |
| Link to the Access Point Web Page          | <p>Click to open a browser window to the AP Summary Status.</p> <p><b>Tip</b> The HTTP port on IOS access points must be set to 80 for this link to work. For information on setting up the HTTP port, see <a href="#">Enter HTTP Port Settings—IOS Access Points, page 3-24</a>.</p> |

**Step 5** Go to [Step 6](#).

**Table 6-27 Non-IOS Detailed Report**

| Column                                    | Description                                                                                                                     |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Name                                      | The system name for the device.                                                                                                 |
| As Of                                     | The time the WLSE polled information from the device.<br><br>For more information, see <a href="#">Time Display, page 1-8</a> . |
| MAC Address                               | The device's MAC address.                                                                                                       |
| IP Address                                | The device's IP address.<br><br>Click to open a browser window to the AP Summary Status.                                        |
| Subnet Mask                               | The subnet mask.                                                                                                                |
| Software Version                          | The software version on the device.                                                                                             |
| Number of Clients Connected               | The number of wireless clients connected to the device.                                                                         |
| Number of Bridges Connected               | The number of bridges connected to the device.                                                                                  |
| Number of AP-Repeaters Connected          | The number of AP repeaters connected to the device.                                                                             |
| Model                                     | The hardware model of the device.                                                                                               |
| SNMP Trap Destination                     | The IP address or host name of the server running the SNMP Management software.                                                 |
| HTTP Port                                 | The device's HTTP setting.                                                                                                      |
| Hot StandBy                               | Indicates whether the hot standby unit is in monitoring mode.<br><br>If true, the current unit is in monitoring mode.           |
| Count of Access Point observed by this AP | Number of access points seen by the access points.                                                                              |
| Ethernet Port Status                      | The operational status of the Ethernet port.                                                                                    |

**Table 6-27 Non-IOS Detailed Report (continued)**

| Column                                       | Description                                                                                                                                                                    |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch IP (to which this AP is attached)     | <p>The IP address of the switch to which this access point is attached.</p> <p><b>Note</b> CDP must be enabled for the switch information to be collected for this report.</p> |
| Switch Name (to which this AP is attached)   | <p>The name of the switch to which this access point is attached.</p> <p><b>Note</b> CDP must be enabled for the switch information to be collected for this report.</p>       |
| Radio Port                                   | The radio port.                                                                                                                                                                |
| SSID                                         | The unique identifier the client device uses to associate with the access point.                                                                                               |
| SSID Associated to the Native Vlan           | The SSID that is mapped to the native VLAN.                                                                                                                                    |
| Radio Cell Role                              | Indicates the role of the device.                                                                                                                                              |
| Ensure Compatibility With 2Mbps Clients      | Indicates whether it is compatible with 2Mbps clients.                                                                                                                         |
| Ensure Compatibility With non-Aironet 802.11 | Indicates whether it is compatible with 802.11.                                                                                                                                |
| Current operating frequency channel          | The radio channel being used.                                                                                                                                                  |
| Radio Port Status                            | The operational status of the radio port.                                                                                                                                      |
| Transmit Power (mW)                          | The access point's transmission power setting in milliwatts.                                                                                                                   |
| Encryption type                              | Indicates that devices using WEP are allowed to communicate with the access point.                                                                                             |
| Length of WEP key 1 through 4 (in bits)      | The WEP key length.                                                                                                                                                            |

**Table 6-27 Non-IOS Detailed Report (continued)**

| Column                            | Description                                                                                                  |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------|
| 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.        |
| Link to the Access Point Web Page | Click to open a browser window to the AP Summary Status.                                                     |

- Step 6** For Fault Summary information, see [Viewing the Fault Status Report, page 6-6](#).
- Step 7** For EAP Authentication Report, see [Displaying an EAP Authentication Report, page 6-50](#).
- Step 8** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 9** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## Displaying an AP 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 and Search, page 1-9](#).
- Step 3** From the Report Name list, select **AP Associations Report**.



**Step 4** Click **View**. The report is displayed. The reports for IOS and non-IOS devices are different:

- IOS AP Associations Report—See [Table 6-28 on page 6-49](#).
- Non-IOS AP Associations Report—See [Table 6-29 on page 6-49](#).

**Table 6-28 IOS AP 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 type.                                                                                         |
| As Of       | The time the client was last seen by the system.<br>For more information, see <a href="#">Time Display, page 1-8</a> . |

**Table 6-29 Non-IOS AP Associations Report**

| Column      | Description                                                                                                            |
|-------------|------------------------------------------------------------------------------------------------------------------------|
| Name        | The name of the client associated with the access point.                                                               |
| IP Address  | The IP address of the wireless client.                                                                                 |
| MAC Address | The wireless client's MAC address.                                                                                     |
| Device Type | The wireless client device type.                                                                                       |
| State       | The operational state of the device.                                                                                   |
| As Of       | The time the device was last seen by the system.<br>For more information, see <a href="#">Time Display, page 1-8</a> . |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

**Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## Displaying an EAP Authentication Report

This device report lists all the authentication servers that are configured for the access point.

### 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 and Search, page 1-9](#).
- Step 3** From the Report Name list, select **EAP Authentication Report**.
- Step 4** Click **View**. The report is displayed. The reports for IOS and non-IOS devices are different:
  - IOS EAP Authentication Report—See [Table 6-30 on page 6-51](#).
  - Non-IOS EAP Authentication Report—See [Table 6-31 on page 6-51](#).

**Table 6-30 IOS EAP 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.          |

**Step 5** Go to [Step 6](#).

**Table 6-31 Non-IOS EAP Authentication Report**

| Column          | Description                                                                                                                                                                                                          |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Name     | The name of the authentication server or the IP address. The IP address is displayed if the server name is not configured or if Reverse DNS is not enabled under <b>Administration &gt; Discover &gt; Discover</b> . |
| Server Protocol | The protocol used by the server.                                                                                                                                                                                     |
| Server Priority | The priority of the server when multiple servers are configured for the same service.                                                                                                                                |
| Server Port     | The port setting used by the access point and the server for authentication.                                                                                                                                         |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

**Step 6** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 7** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## Displaying an AP Ethertype Protocol Filters Report

This non-IOS device report lists the Ethertype protocol filters configured on the access point.

### 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 and Search, page 1-9](#).
- Step 3** From the Report Name list, select **AP Ethertype Protocol Filters**.
- Step 4** Click **View**. The report is displayed with the following headings:

**Table 6-32 AP Ethertype Protocol Filters Report**

| Column                          | Description                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Filter Set Id                   | The identification number of the filter set.                                                                                |
| Filter Set Name                 | The name of the filter set.                                                                                                 |
| Default Disposition             | The type of disposition configured: Forward (to forward protocol traffic, or Block (to block protocol traffic).             |
| Filter Special Case Ethertype   | The special case configuration.                                                                                             |
| Filter Special Case Disposition | The special case disposition.                                                                                               |
| Filter Special Case Priority    | The priority configuration based on the traffic type.                                                                       |
| As Of                           | The time the WLSE polled information from the device.<br>For more information, see <a href="#">Time Display, page 1-8</a> . |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

**Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## Displaying an AP IP Protocol Filters Report

This non-IOS device report lists the IP protocol filters configured on the access point.

### 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 and Search, page 1-9](#).
- Step 3** From the Report Name list, select **AP IP Protocol Filters**.
- Step 4** Click **View**. The report is displayed with the following headings:

**Table 6-33 AP IP Protocol Filters Report**

| Column                          | Description                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Filter Set Id                   | The identification number of the filter set.                                                                                |
| Filter Set Name                 | The name of the filter set.                                                                                                 |
| Default Disposition             | The type of disposition configured: Forward (to forward protocol traffic, or Block (to block protocol traffic).             |
| Filter Special Case IP Protocol | The special case configuration.                                                                                             |
| Filter Special Case Disposition | The special case disposition.                                                                                               |
| Filter Special Case Priority    | The priority configuration based on the traffic type.                                                                       |
| As Of                           | The time the WLSE polled information from the device.<br>For more information, see <a href="#">Time Display, page 1-8</a> . |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

- Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## Displaying an AP IP Port Filters Report

This non-IOS device report lists the various IP port filters configured on the access point.

### 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 and Search, page 1-9](#).
- Step 3** From the Report Name list, select **AP IP Port Filters**.
- Step 4** Click **View**. The report is displayed with the following headings:

**Table 6-34 AP IP Port Filters Report**

| Column                          | Description                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Filter Set Id                   | The identification number of the filter set.                                                                                |
| Filter Set Name                 | The name of the filter set.                                                                                                 |
| Default Disposition             | The type of disposition configured: Forward (to forward protocol traffic, or Block (to block protocol traffic).             |
| Filter Special Case IP Port     | The special case configuration.                                                                                             |
| Filter Special Case Disposition | The special case disposition.                                                                                               |
| Filter Special Case Priority    | The priority configuration based on the traffic type.                                                                       |
| As Of                           | The time the WLSE polled information from the device.<br>For more information, see <a href="#">Time Display, page 1-8</a> . |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

- Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).
-

## Displaying an AP Policy Report

This non-IOS device report lists all the policy groups configured on the access point.

### 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 and Search, page 1-9](#).
- Step 3** From the Report Name list, select **AP Policy Report**.
- Step 4** Click **View**. The report is displayed with the following headings:

**Table 6-35** AP Policy Report

| Column                     | Description                                                                                                                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policy Group Id            | The identification number for the policy group.                                                                                                                                                            |
| Policy Group Name          | The name of the policy group.                                                                                                                                                                              |
| Ethertype Filter Id (In)   | The identification number of the (receive) Ethertype filter.<br>Click to see the AP Ethertype Protocol Filters Report—See <a href="#">Displaying an AP Ethertype Protocol Filters Report, page 6-52</a> .  |
| Ethertype Filter Id (Out)  | The identification number of the (transmit) Ethertype filter.<br>Click to see the AP Ethertype Protocol Filters Report—See <a href="#">Displaying an AP Ethertype Protocol Filters Report, page 6-52</a> . |
| IP Protocol Filter Id (In) | The identification number of the (receive) IP protocol filter.<br>Click to see the AP Ethertype Protocol Filters Report—See <a href="#">Displaying an AP IP Protocol Filters Report, page 6-53</a> .       |

**Table 6-35 AP Policy Report (continued)**

| Column                   | Description                                                                                                                                                                                        |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP Protocol Filter (Out) | The identification number of the (transmit) IP protocol filter.<br><br>Click to see the AP IP Protocol Filters Report—See <a href="#">Displaying an AP IP Protocol Filters Report, page 6-53</a> . |
| IP Port Filter Id (In)   | The identification number of the (receive) IP port filter.<br><br>Click to see the AP IP Port Filters Report—See <a href="#">Displaying an AP IP Port Filters Report, page 6-54</a> .              |
| IP Port Filter Id (Out)  | The identification number of the (transmit) IP port filter.<br><br>Click to see the AP IP Port Filters Report—See <a href="#">Displaying an AP IP Port Filters Report, page 6-54</a> .             |
| As Of                    | The time the WLSE polled information from the device.<br><br>For more information, see <a href="#">Time Display, page 1-8</a> .                                                                    |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

**Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## Displaying an AP QoS Report

This device report displays the configured QoS parameters.

### 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 and Search, page 1-9](#).



- Step 3** From the Report Name list, select **AP QoS Report**.
- Step 4** Click **View**. The report is displayed. The reports for IOS and non-IOS devices are different:
- IOS AP QoS Report—See [Table 6-36 on page 6-57](#).
  - Non-IOS AP QoS Report—See [Table 6-37 on page 6-58](#).

**Table 6-36 IOS AP QoS Report**

| Column                | Description                                                                                                                 |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------|
| RF Interface          | The radio interface name.                                                                                                   |
| Traffic Class         | The category of traffic.                                                                                                    |
| 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.<br>For more information, see <a href="#">Time Display, page 1-8</a> . |

- Step 5** Go to [Step 6](#).

**Table 6-37 Non-IOS AP QoS Report**

| Column                | Description                                                                                                                 |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------|
| RF Interface          | The radio interface name.                                                                                                   |
| Traffic Category      | The category of traffic.                                                                                                    |
| CWmin                 | The minimum contention window value.                                                                                        |
| CWmax                 | The maximum contention window value.                                                                                        |
| Generate QBSS Element | Indicates if basic 802.11 quality of service is enabled or disabled.                                                        |
| As Of                 | The time the WLSE polled information from the device.<br>For more information, see <a href="#">Time Display, page 1-8</a> . |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

- Step 6** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 7** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).
- 

## Displaying an AP 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 and Search, page 1-9](#).
- Step 3** From the Report Name list, select **AP SSID Report**. Click **View**. The report is displayed. The reports for IOS and non-IOS devices are different:
- IOS AP SSID Report—See [Table 6-38 on page 6-59](#).
  - Non-IOS AP SSID Report—See [Table 6-37 on page 6-58](#).

**Table 6-38 IOS AP SSID Report**

| Column       | Description                                                                                                                 |
|--------------|-----------------------------------------------------------------------------------------------------------------------------|
| SSID         | The unique identifier the client device uses to associate with the access point.                                            |
| RF Interface | The radio interface name.                                                                                                   |
| VLAN ID      | The VLAN identification number.                                                                                             |
| As Of        | The time the WLSE polled information from the device.<br>For more information, see <a href="#">Time Display, page 1-8</a> . |

**Step 4** Go to [Step 5](#).

**Table 6-39 Non-IOS AP SSID Report**

| Column                      | Description                                                                                                                                                                          |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSID                        | The unique identifier the client device uses to associate with the access point.                                                                                                     |
| VLAN ID                     | The VLAN identification number.                                                                                                                                                      |
| VLAN Name                   | The VLAN name.                                                                                                                                                                       |
| RF Interface                | The radio interface name.                                                                                                                                                            |
| Number of Clients Connected | The number of wireless clients connected to the device.                                                                                                                              |
| Priority                    | The priority configuration based on the traffic type.                                                                                                                                |
| Default Policy Group        | The number of the default policy group (which contains access parameters).<br><br>Click to view the AP Policy Report—See <a href="#">Displaying an AP Policy Report, page 6-55</a> . |
| As Of                       | The time the WLSE polled information from the device.<br><br>For more information, see <a href="#">Time Display, page 1-8</a> .                                                      |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

**Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

# Displaying an AP 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 and Search, page 1-9](#).
- Step 3

From the Report Name list, select **AP VLAN Report**.
- Step 4

Click **View**. The report is displayed. The reports for IOS and non-IOS devices are different:
 
  - IOS AP VLAN Report—See [Table 6-40 on page 6-61](#).
  - Non-IOS AP VLAN Report—See [Table 6-41 on page 6-62](#).



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 IOS access points, VLAN information is accessible by SNMP.

**Table 6-40** *IOS AP VLAN Report*

| Column           | Description                                                                                                                 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------|
| VLAN ID          | The identification number 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.<br>For more information, see <a href="#">Time Display, page 1-8</a> . |

**Table 6-41 Non-IOS AP VLAN Report**

| Column                      | Description                                                                                                                 |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| VLAN ID                     | The identification number of the VLAN.                                                                                      |
| VLAN Name                   | The name of the VLAN.                                                                                                       |
| SSID                        | The unique identifier the client device uses to associate with the access point.                                            |
| RF Interface                | The radio interface name.                                                                                                   |
| Number of Clients Connected | The number of wireless clients connected to the device.                                                                     |
| Priority                    | The priority configuration based on the traffic type.                                                                       |
| Default Policy Group        | The number of the default policy group (which contains access parameters).                                                  |
| As Of                       | The time the WLSE polled information from the device.<br>For more information, see <a href="#">Time Display, page 1-8</a> . |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

**Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## 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 and Search, page 1-9](#).
- Step 3

From the Report Name list, select **Per VLAN Client Report**.
- Step 4

Click **View**. The report is displayed. The reports for IOS and non-IOS devices are different:
 
  - IOS Per VLAN Report—See [Table 6-42 on page 6-63](#).
  - Non-IOS Per VLAN Report—See [Table 6-43 on page 6-64](#).

**Table 6-42 IOS Per VLAN Report**

| Column             | Description                                                                      |
|--------------------|----------------------------------------------------------------------------------|
| VLAN ID            | The identification number 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.                                                    |

**Table 6-42 IOS Per VLAN Report (continued)**

| Column      | Description                                                                                                                 |
|-------------|-----------------------------------------------------------------------------------------------------------------------------|
| Client Type | The type of client associated to the access point.                                                                          |
| As Of       | The time the WLSE polled information from the device.<br>For more information, see <a href="#">Time Display, page 1-8</a> . |

**Step 5** Go to [Step 6](#).

**Table 6-43 Non-IOS Per VLAN Client Report**

| Column             | Description                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------|
| VLAN ID            | The identification number of the VLAN.                                                                                      |
| VLAN Name          | The name of the VLAN.                                                                                                       |
| 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.                                                                                               |
| SSID               | The unique identifier the client device uses to associate with the access point.                                            |
| Client Type        | The type of client associated to the access point.                                                                          |
| As Of              | The time the WLSE polled information from the device.<br>For more information, see <a href="#">Time Display, page 1-8</a> . |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

**Step 6** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 7** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

# Displaying an AP 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 and Search, page 1-9](#).
- Step 3** From the Report Name list, select **AP HotStandby Report**.
- Step 4** Click **View**. The report is displayed with the following headings:

**Table 6-44 AP Hot Standby Report**

| Column                             | Description                                                                                                                                                                                                 |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hot StandBy                        | Indicates whether the access is enabled for hot standby.                                                                                                                                                    |
| Monitored AP Mac Address           | <p>The MAC address of the access point this access point is monitoring.</p> <p><b>Note</b> This field displays the value 000000000000 when the MAC Address has not been configured on the access point.</p> |
| Monitored AP IP Address (IOS only) | <p>The IP address of the access point this access point is monitoring.</p> <p><b>Note</b> This field is empty if the monitored device is not in the list of devices discovered by the WLSE.</p>             |
| Monitored AP Name                  | <p>The name of the access point this access point is monitoring.</p> <p><b>Note</b> This field is empty if the monitored device is not in the list of devices discovered by the WLSE.</p>                   |
| 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.                                   |



**Table 6-44 AP Hot Standby Report (continued)**

| Column             | Description                                                                                                                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hot Standby Status | The current status of the hot standby access point: Normal, Initializing, Takeover, Stopped, Associating, RootMacFailed, InterfaceMerge, AssociationFail, EtherTestFail, RadioTestFail, or Error. |
| Hot Standby State  | The current state of the hot standby access point: Running, Initializing, Stopped, or NotRunning.                                                                                                 |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

**Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## 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 and Search, page 1-9](#).
- Step 3** From the Report Name list, select **Switch Summary Report**.
- Step 4** Click **View**. The group report is displayed with the following headings:

**Table 6-45 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.       |

**Table 6-45** *Switch Summary Report (continued)*

| Column                              | Description                                                                                                                         |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| 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.<br>For more information, see <a href="#">Displaying an AP and Bridge Connected to Switch Report</a> , page 6-67. |

- Step 5** For information on the Fault Summary table, see [Viewing the Fault Status Report](#), page 6-6.
- Step 6** To export the report, click **Export**. See [Exporting a Report](#), page 6-89.
- Step 7** To email the report, click **Email Report**. See [Emailing a Report](#), page 6-89.

## 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 and Search](#), page 1-9.
- Step 3** From the Report Name list, select **AP and Bridge Connected to Switch Report**.

**Step 4** Click **View**. The report is displayed with the following headings:

**Table 6-46 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.<br><br>Click for details. For more information, see <a href="#">Viewing the Fault Status Report, page 6-6</a> . |

**Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## 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 and Search, page 1-9](#).

**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 6-47 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.          |

**Step 5** For information on the Fault Summary table, see [Viewing the Fault Status Report, page 6-6](#)

**Step 6** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 7** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## 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 and Search, page 1-9](#).

**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 6-48 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.<br><br>Click for details. For more information, see <a href="#">Viewing the Fault Status Report, page 6-6</a> . |

**Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## 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 and Search, page 1-9](#).

**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 6-49 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.   |

**Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## 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 and Search, page 1-9](#).

**Step 3** From the Report Name list, select **AP Usage Report**.

**Step 4** Click **View**. The report is displayed with the following headings:

**Table 6-50 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.<br>For more information, see <a href="#">Time Display, page 1-8</a> . |

- Step 5** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 6** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).
- 

## 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 6-73](#)). 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
  - Group Performance Report: RF Utilization—[Displaying a Group Performance Report: RF Utilization, page 6-74](#)
  - Group Performance Report: Ethernet Utilization—See [Displaying a Group Performance Report: Ethernet Utilization, page 6-75](#)
  - Top N Number of Associations—See [Displaying a Top N Number of Associations Report, page 6-76](#)
  - Top N Percentage Errors—See [Displaying a Top N Percentage Errors Report, page 6-78](#)

- Access Point and Bridge Reports
  - AP and Bridge RF Transmission Statistics—See [Displaying an AP and Bridge RF Transmission Statistics Report](#), page 6-79
  - AP and Bridge Ethernet Transmission Statistics—See [Displaying an AP and Bridge Ethernet Transmission Statistics Report](#), page 6-80
  - AP and Bridge Performance: Graph—See [Displaying an AP and Bridge Performance Graph](#), page 6-81
  - AP and Bridge Performance: Tabular—See [Displaying an AP and Bridge Performance: Tabular](#), page 6-82
  - Top N Busiest Clients—See [Displaying Top N Busiest Clients](#), page 6-83
  - Top N Client Error Rate—See [Displaying Top N Client MIC Error Rate](#), page 6-85
- Server Report
  - Server Response Time Graph—See [Displaying a Server Response Time Graph](#), page 6-87

The folders and devices in the device selector display icons indicating the alarm status of the devices. For an explanation of the icons, see [Understanding the Icons](#), page 1-10.

For information about the folders for device groups in the device selector, see [System-Defined Groups](#), page 3-86.

**Note**


---

Your login determines whether you can use this option.

---

**Related Topics**

[Using Trend Reports For Capacity Planning](#), page 6-73

## 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.
  - 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.

**Step 6** Click **View**. The table is displayed:

**Table 6-51 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.<br>For more information, see <a href="#">Time Display, page 1-8</a> . |
| RF Utilization (%)     | The percentage of radio frequency utilization.                                                                              |
| Number of Associations | Shows the number of associations with clients.                                                                              |
| SSID                   | The unique identifier the client device uses to associate with the access point.                                            |
| Channel Number         | The channel being used.                                                                                                     |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

**Step 7** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 8** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## 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.
- 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.
- Step 6** Click **View**. The table is displayed:

**Table 6-52 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.<br>For more information, see <a href="#">Time Display, page 1-8</a> . |
| Ethernet Utilization (%) | The percentage of Ethernet utilization.                                                                                     |
| Number of Associations   | Shows the number of associations with clients.                                                                              |
| SSID                     | The unique identifier the client device uses to associate with the access point.                                            |
| Channel Number           | The channel being used.                                                                                                     |

- Step 7** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 8** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## Displaying a Top N Number of Associations 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**.
- 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.
- Step 7** Click **View**. The table is displayed:

**Table 6-53** *Top N Number of Associations*

| 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. |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

- Step 8** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 9** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).
-

## 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.
- Step 7** Click **View**. The table is displayed:

**Table 6-54 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. |

For information on how to sort table data, see [Sorting Table Data](#), page 1-11.

- Step 8** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 9** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).
- 

## Displaying an AP and Bridge 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 and Search, page 1-9](#).
- Step 3** From the Report Name list, select **AP and Bridge 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.
- Step 6** Click **View**. A graph is displayed:

**Table 6-55 AP and Bridge RF Transmission Statistics**

| Column        | Description                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------------------|
| Transmit Rate | The x-axis displays the time intervals.<br>The y-axis displays the number of packets transmitted per second. |

**Table 6-55 AP and Bridge RF Transmission Statistics (continued)**

| Column        | Description                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------|
| Receive Rate  | The x-axis displays the time intervals.<br>The y-axis displays the number of packets received per second.         |
| Packet Errors | The x-axis displays the time intervals.<br>The y-axis displays the number of error packets per number of packets. |

**Step 7** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 8** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## Displaying an AP and Bridge 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 and Search, page 1-9](#).
- Step 3** From the Report Name list, select **AP and Bridge 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.

**Step 6** Click **View**. A graph is displayed:

**Table 6-56 AP and Bridge Ethernet Transmission Statistics**

| Column        | Description                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------|
| Transmit Rate | The x-axis displays the time intervals.<br>The y-axis displays the number of packets transmitted per second.      |
| Receive Rate  | The x-axis displays the time intervals.<br>The y-axis displays the number of packets received per second.         |
| Packet Errors | The x-axis displays the time intervals.<br>The y-axis displays the number of error packets per number of packets. |

**Step 7** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 8** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## Displaying an AP and Bridge Performance 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 and Search, page 1-9](#).
- Step 3** From the Report Name list, select **AP and Bridge Performance 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.

**Step 6** Click **View**. A graph is displayed:

**Table 6-57 AP and Bridge Performance Graph**

| Column                 | Description                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------------|
| Ethernet Utilization   | The x-axis displays the time intervals.<br>The y-axis displays the percent of Ethernet utilization.        |
| RF Utilization         | The x-axis displays the time intervals.<br>The y-axis displays the percent of radio frequency utilization. |
| Number of Associations | The x-axis displays the time intervals.<br>The y-axis displays the number of client associations           |

**Step 7** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 8** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## Displaying an AP and Bridge Performance: Tabular

### 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 and Search, page 1-9](#).

**Step 3** From the Report Name list, select **AP and Bridge Performance: 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.
- Step 6** Click **View**. The report is displayed:

**Table 6-58 AP and Bridge Performance: 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.<br>For more information, see <a href="#">Time Display, page 1-8</a> . |
| 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.                                                                                  |

- Step 7** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 8** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## 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 and Search, page 1-9](#).
- 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.
- Step 7** Click **View**. The table is displayed:

**Table 6-59 Top N Busiest Clients**

| Column                   | Description                          |
|--------------------------|--------------------------------------|
| 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. |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

- Step 8** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 9** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## 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.

This report is for IOS access points only.

### 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 and Search, page 1-9](#).
  - 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.
  - Step 7** Click **View**. The report 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 6-60 IOS Top N Client MIC Error Rate**

| Column                               | Description                                                                                    |
|--------------------------------------|------------------------------------------------------------------------------------------------|
| Client MAC Address                   | The MAC address of the client.                                                                 |
| MIC Error Rate (Avg)<br>(per second) | The average value of the rate of Message Integrity Check (MIC) errors recorded for the client. |
| MIC Error Rate (Min)<br>(per second) | The minimum value of the rate of Message Integrity Check (MIC) errors recorded for the client. |
| MIC Error Rate (Max)<br>(per second) | The maximum value of the rate of Message Integrity Check (MIC) errors recorded for the client. |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

**Step 8** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).

**Step 9** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## Displaying Top N Client Bit 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 bit error rate as perceived by the access point for the selected period of time.

This report is for non-IOS access points only.

### 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 and Search, page 1-9](#).
- Step 3** From the Report Name list, select **Top N Client 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.
- Step 7** Click **View**. The report is displayed.

**Table 6-61 Non-IOS Top N Client Bit Error Rate**

| Column                         | Description                                |
|--------------------------------|--------------------------------------------|
| Client MAC Address             | The MAC address of the client.             |
| Bit Error Rate (Avg) (in kbps) | The average bit error rate for the client. |
| Bit Error Rate (Min) (in kbps) | The minimum bit error rate for the client. |
| Bit Error Rate (Max) (in kbps) | The maximum bit error rate for the client. |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

- Step 8** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 9** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

## Displaying a Server Response Time Graph

This graph plots the response time of the server over the period of time specified.

### 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 and Search, page 1-9](#).
- 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.
- Step 6** Click **View**. The following report displays:

**Table 6-62** *Server Response Time Graph*

| Column               | Description                                                                                       |
|----------------------|---------------------------------------------------------------------------------------------------|
| Server Response Time | The x-axis displays the time intervals.<br>The y-axis displays the response time in milliseconds. |

- Step 7** To export the report, click **Export**. See [Exporting a Report, page 6-89](#).
- Step 8** To email the report, click **Email Report**. See [Emailing a Report, page 6-89](#).

# Exporting a Report

- 
- 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 in the requested format and displays the output.
- 

# 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.<br><br>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.<br><br>For more information, see <a href="#">Naming Guidelines, page A-1</a> .                      |
| Specify the Days Worth or Report Data | Enter the number of days for which you want data emailed.<br><br><b>Note</b> 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.                                                              |

| Field  | Description                                                                |
|--------|----------------------------------------------------------------------------|
| 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 6-91](#)
- 

## 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.

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.<br>For more information, see <a href="#">Naming Guidelines, page A-1</a> . |
| Recurring     | Indicates whether it is a recurring job.                                                        |
| Next Schedule | Indicates when the job runs again.                                                              |

For information on how to sort table data, see [Sorting Table Data, page 1-11](#).

**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 6-92](#).

**Step 4** To edit a job, select it, then click **Edit Email Job**. See [Editing an Email Job, page 6-93](#).

## 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.                                           |

| Field           | Description                                                                                 |
|-----------------|---------------------------------------------------------------------------------------------|
| 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.

# Exporting URL-Based Report Data



## 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 | AccessPoint | 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 }**

An example of a URL to generate CSV output for Group Performance Report: RF Utilization, for a group of 350 access points, with start date and time of July 21 00:00:00 GMT+05:30 2003, and an end date and time of July 21 23:59:59 GMT+05:30 2003 is as follows:

```
http://172.10.29.117:1741/servlet/com.cisco.nm.wlse.util.WLSEReportsExportServlet?id=350%20AP&reporttype=group&family=group&reportName=Group%20Performance%20Report%20%3A%20RF%20Utilization&tzOffset=330&filetype=csv&reportcategory=trends&startdate=2003-7-21-00-00-00&enddate=2003-7-21-23-59-59
```







# Radio Management

---

The Radio Manager tab displays information to help you manage your WLAN radio environment. All the device information shown under this tab is polled from the managed devices in your network.

The Radio Manager tab includes these options:



## Note

---

Some subtabs may not be visible to some users.

---

- Radio Monitoring—See [Radio Monitoring](#), page 7-6
- AP Radio Scan—See [AP Radio Scan](#), page 7-9
- Client Walkabout—See [Client Walkabout](#), page 7-24
- Location Manager—See [Location Manager](#), page 7-39
- RM Assisted Configuration—See [Radio Management Assisted Configuration](#), page 7-60
- Manage RM Measurements—See [Managing RM Measurements](#), page 7-71

## Related Topics

[Understanding the Radio Manager](#), page 7-2

# Understanding the Radio Manager

The Radio Manager features simplify the deployment, expansion, and day-to-day management of the WLAN by:

- Automatically configuring network-wide radio parameters during initial deployment and network expansion.
- Continuously monitoring the radio environment, detecting interference and rogue APs, and alerting the WLAN administrator to radio network changes.
- Providing information to help visualize the network radio topology, including the path loss between APs and RF coverage.

The following topics provide a high-level overview of how the Radio Manager collects data and uses this data to help you manage your WLAN:

- [Understanding the Radio Manager Features, page 7-2](#)
- [Collecting Radio Location Measurements, page 7-4](#)

## Understanding the Radio Manager Features

The Radio Manager provides these features:

- **Rogue AP detection**

The Radio Monitoring feature uses the radio measurement capabilities on Cisco IOS APs (1100, 1200) and Cisco client adaptors to discover any new 802.11 APs that are transmitting beacons. Both clients and APs periodically scan for other 802.11 beacon frames on both serving channels and neighboring channels. Reports of detected beacons are returned to the Radio Manager, which validates the detected beacons against a list of APs known to be authorized to provide wireless access.

A newly discovered AP that cannot be qualified as being a known authorized AP generates an administrator alert. You can categorize this new AP as one of the following AP types:

- **Managed AP**—An AP that is authorized to provide wireless access to the LAN and requires management services provided by the WLSE.
- **Unmanaged AP**—An AP that is authorized to provide wireless access to the LAN but does *not* require any management services from the WLSE.

- Friendly AP—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, but that you are not going to modify in any way.
- Rogue AP—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 unknown radios are classified as Rogue until you change them to Friendly.

- **Interference detection**

You can initiate interference detection when you activate Radio Monitoring. Only APs in the radio monitoring list participate in interference detection; clients can detect interference as well. You can define what level of signal strength and duration of signal is required to detect interference. When interference is determined to be present, an alert is generated.

- **Automatic radio parameter generation**

The Radio Manager can generate optimal values for the radio parameters of a given group of APs. Each set of radio parameters can modify the following:

- AP frequency
- AP transmit power
- AP beacon interval

When computing new radio configuration parameters, select any combination of parameters that may be altered. After the desired parameters are selected, the Radio Manager is given free reign to alter each parameter as it sees fit.

### **Related Topics**

- [Collecting Radio Location Measurements, page 7-4](#)

# Collecting Radio Location Measurements

The Radio Manager characterizes the WLAN radio environment using the following radio location measurements obtained from Cisco APs and Cisco clients:

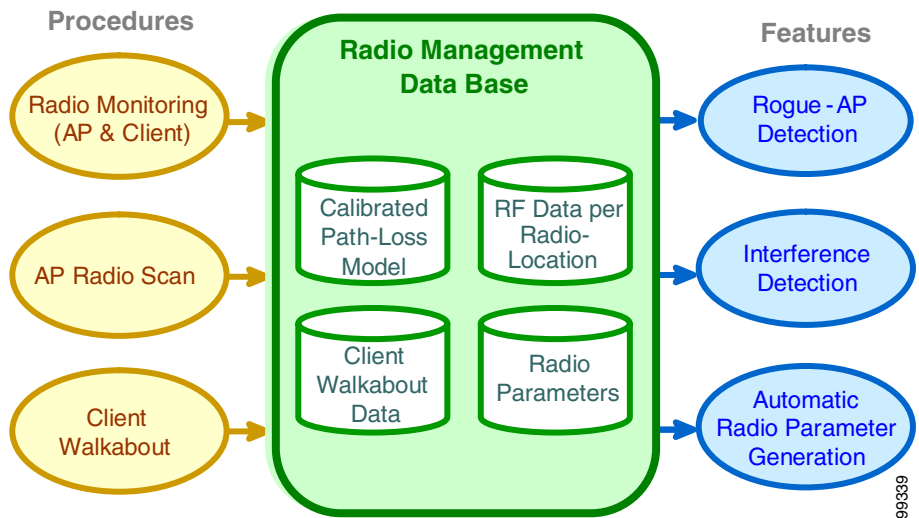
- Beacon—To determine path loss and detect AP rogues (serving channel and non-serving channels).
- Channel load and noise histogram—To characterize the degree of contention and interference (serving channel only).

The Assisted Site Survey (see [Using the Assisted Site Survey Wizard, page 7-55](#)) can walk you through the process of determining the optimal radio transmit power and channel selection. It helps you select APs, run an AP radio scan job, perform a client walkabout, and generate radio parameters for the selected APs.

You can also choose to run these features manually. The following table summarizes which procedures produce the data required by the different Radio Manager features:

| Feature                              | Run these procedures           | Results are used in:                      |
|--------------------------------------|--------------------------------|-------------------------------------------|
| Rogue AP detection                   | Radio Monitoring               | Location Manager                          |
|                                      | AP Radio Scan                  | Faults                                    |
| Interference detection               | Radio Monitoring               | Faults                                    |
| Automatic radio parameter generation | AP Radio Scan                  | RM Assisted Configuration                 |
|                                      | Client Walkabout (recommended) | Location Manager<br>Radio Manager Reports |

The results produced by these features constitute the radio knowledge base. This knowledge base (see [Figure 7-1](#)) is saved in the WLSE database and accessed by other Radio Manager features.

**Figure 7-1 Radio Data Collection and Knowledge Base**

Several Radio Manager procedures are used solely to generate measurement requests and collect the results:

- **Radio Monitoring** periodically gathers radio frequency statistics and identifies specific signal sources. It continuously monitors the radio frequency environment and generates alerts when new APs appear.

**Tip**

This feature is your primary means of detecting rogue APs.

- **AP Radio Scan** sets selected APs to transmit beacons on the same channel and detects all neighboring APs. This feature measures the path loss between each AP and every other AP it can hear and scans other channels to detect rogue APs.

**Tip**

Run AP radio scans during initial setup, then periodically to capture any changes made to the APs (added, deleted, or moved).

- **Client Walkabouts** provide optimal coverage for the radio parameter generator (see [Radio Management Assisted Configuration, page 7-60](#)). During a walkabout, the client (typically a laptop) is carried throughout the desired coverage area and continuously reports radio measurements back to its serving AP.

**Tip**

If you do not perform a client walkabout, you *must* enter a floor plan that includes the distances between APs (see [Adding Building Information, page 7-47](#)).

**Related Topics**

- [Understanding the Radio Manager Features, page 7-2](#)
- [Using the Assisted Site Survey Wizard, page 7-55](#)
- [Radio Monitoring, page 7-6](#)
- [AP Radio Scan, page 7-9](#)
- [Client Walkabout, page 7-24](#)

## Radio Monitoring

Radio Monitoring runs on the specified Cisco IOS APs and its associated CCX-compliant clients to continuously monitor the WLAN radio environment and discover any new APs that are transmitting beacons. The channel measurements are used for radio configuration, rogue AP discovery, and interference detection.

**Note**

Radio Monitoring is your primary means of detecting rogue APs.

Use the Radio Monitoring option to:

- Specify the serving channel monitoring option (APs, clients, or both)
- Specify the non-serving channel monitoring option (to monitor channels the AP is not transmitting on)
- Specify the group of APs and clients to perform the channel measurements

**Tip**

Leave Radio Monitor continuously running on your network so new APs are discovered promptly, the necessary faults are generated, and your reports are accurate and up-to-date.

An AP can be added to the Radio Monitoring list and also be included on an AP Radio Scan or Client Walkabout; the measurement requests for these two features supersede the monitoring measurement requests. When the other, shorter term procedures end, the APs are returned to the normal radio monitoring mode.

**Note**

Your login determines whether you can use this option.

**Related Topics**

- [Setting Radio Monitoring Options, page 7-7](#)
- [Collecting Radio Location Measurements, page 7-4](#)

## Setting Radio Monitoring Options

To detect interference and rogue APs, radio monitoring must be running.

**Tip**

Leave Radio Monitor continuously running on your network so new APs are discovered promptly, the necessary faults are generated, and your reports are accurate and up-to-date.

**Prerequisites**

Before you can select devices to be included in radio monitoring, you must have already:

- Discovered the devices (see [Managing Device Discovery, page 3-30](#)).
- Made the devices managed (see [Managing and Unmanaging Devices, page 3-64](#)).
- Authenticated the devices with WDS (see [Setting WDS Thresholds, page 2-46](#)).

## Procedure

- 
- Step 1** Select **Radio Manager > Radio Monitoring**. The Radio Monitoring Options window appears.
- Step 2** Click **Enable** to monitor your WLAN environment.
- Step 3** For **Serving Channel Monitoring**, select one or both of the following check boxes for measurements on the channel the devices are configured to:
- **APs** to perform monitoring measurements on the Cisco IOS APs on the serving channel.
  - **Clients** to perform monitoring measurements on CCX-compliant clients on the serving channel.
- Step 4** For **Non-Serving Channel Monitoring**, select one or both of the following check boxes to measure other channels in the band:
- **APs** to perform monitoring measurements on the Cisco IOS APs on the non-serving channels.
  - **Clients** to perform monitoring measurements on CCX-compliant clients on the non-serving channels.
-  **Note** 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).
- 
- Step 5** Click **Select AP**. All managed devices are listed in the Device selector in the middle pane.
- Step 6** Select the devices you want to monitor (see [Using the Device Selector and Search, page 1-9](#)).
- Now that you have selected your radio monitoring options, you need to save your settings.
- Step 7** Click **Finish**. The Finish dialog box appears.
- Step 8** Click **Save** to save your radio monitoring options.



Radio Monitor will now begin monitoring the devices you selected. Radio Monitoring takes measurements every 90 seconds.

---

#### Related Topics

- [Collecting Radio Location Measurements, page 7-4](#)
- [Client Walkabout, page 7-24](#)
- [Location Manager, page 7-39](#)

## AP Radio Scan

The AP Radio Scan feature produces path loss data used for rogue location estimations, radio parameter generation data, and coverage display data.



#### Note

The Assisted Site Survey wizard can walk you through the process of determining the optimal radio transmit power and channel selection. It helps you select APs, run an AP radio scan job, perform a client walkabout, and generate radio parameters for the selected APs. See [Using the Assisted Site Survey Wizard, page 7-55](#).

---

#### Related Topics

- [Understanding AP Radio Scans, page 7-9](#)
- [Creating a New AP Radio Scan, page 7-11](#)
- [Viewing AP Radio Scan Jobs, page 7-16](#)
- [Editing AP Radio Scan Jobs, page 7-19](#)

## Understanding AP Radio Scans

AP radio scans produce path loss data used for rogue location estimations, radio parameter generation data, and coverage display data. This data is used to determine:

- How an AP is positioned related to other APs

- The amount of path loss due to obstructions (such as walls) between APs

These channel measurements, when combined with other data generated by Radio Monitoring and Client Walkabout, are used for radio configuration, rogue AP discovery, and interference detection.

The AP Radio Scan option allows you to:

- Specify a group of APs that will participate in the scan procedure.
- Change the maximum transmit power level.
- Schedule the new job to run immediately or at a certain date and time. You can also specify whether this job will run only once or periodically.

During the scanning process, an AP radio scan performs the following tasks:

1. Sets the selected APs to the same channel at maximum power.

During a scan, AP frequencies and power levels are temporarily changed but no data rates are modified. For each AP, the channel is fixed and the procedure steps through the power levels up to the maximum transmit power level you have specified.

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 of each AP.
3. Calculates the path loss of each AP.
4. Steps through the power levels to determine the power step calibration of each AP.
5. Saves this information in the database as AP radio locations.
6. Sets all APs back to their original power and channel settings.

### Related Topics

- [Creating a New AP Radio Scan, page 7-11](#)

## Creating a New AP Radio Scan

You should run an AP Radio scan:

- During initial setup.
- After adding, deleting, or moving APs.

You might also choose to run an AP scan periodically to capture any changes made to the APs. You can create multiple scan jobs, but only one job can be run at a time.

**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.

**Note**

Your login determines whether you can use this option.

### Prerequisites

Before you can run an AP Radio scan job, you must have already:

- Discovered the devices (see [Managing Device Discovery, page 3-30](#)).
- Made the devices managed (see [Managing and Unmanaging Devices, page 3-64](#)).
- Authenticated the devices with WDS (see [Setting WDS Thresholds, page 2-46](#)).

### Procedure

- 
- Step 1** Select **Radio Manager > AP Radio Scan**.
- Step 2** Enter a name for the job and click **New Job**. For guidelines on job names, see [Appendix A, “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 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 [1. Name the Job and Select the Maximum Transmit Power, page 7-12](#).
2. **Select Devices**—See [2. Select the APs, page 7-13](#).
3. **Schedule Job**—See [3. Schedule the Job, page 7-14](#).
4. **Finish**—See [4. Finish the Job, page 7-15](#).



**Caution** 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.

### Related Topics

[Understanding AP Radio Scans, page 7-9](#).

## 1. Name the Job and Select the Maximum Transmit Power

### Procedure

- Step 1** 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 <a href="#">Appendix A, “Naming Guidelines.”</a> |

| Field                  | Description                                                                                                                                                                                                                                                      |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description            | Enter a description of the job. For guidelines on entering descriptions, see <a href="#">Appendix A, “Naming Guidelines.”</a>                                                                                                                                    |
| Maximum Transmit Power | By default, the power level is set to the maximum value allowed on the AP or the maximum allowed by the regulatory domain.<br><br>You might choose to enter a lower power setting when, for example, the default power level might affect a neighboring network. |

- Step 3** From the menu in the left pane, go to the next step, Select AP. (See [2. Select the APs, page 7-13.](#))

#### Related Topics

- [Copying AP Radio Scan Jobs, page 7-21](#)
- [Creating a New AP Radio Scan, page 7-11](#)

## 2. Select the APs

#### Procedure

- Step 1** 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 and Search, page 1-9](#)).
- Step 3** From the menu in the left pane, go to the next step, Schedule Job. (See [3. Schedule the Job, page 7-14.](#))

#### Related Topics

- [Creating a New AP Radio Scan, page 7-11](#)

### 3. Schedule the Job

When scheduling an AP radio scan job, you can select Run Now to start the job immediately, or you can schedule the job for a future date and time. You can also 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** Click **Schedule Job**.
- Step 2** Enter the following information:

| Field      | Description                                                                                                                                                                                                                                                                                                  |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Run Now    | Click to run the job. The job will run immediately after you click <b>Save</b> (see <a href="#">4. Finish the Job, page 7-15</a> ).<br><br><b>Note</b> 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.<br><br><b>Note</b> 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** From the menu in the left pane, select the next task, Finish. (See [4. Finish the Job](#), page 7-15.)
- 

#### Related Topics

- [Editing AP Radio Scan Jobs](#), page 7-19
- [Deleting AP Radio Scan Jobs](#), page 7-20
- [Creating a New AP Radio Scan](#), page 7-11

## 4. Finish the Job

Before selecting this option, you must name the job and select the maximum transmit power, select the devices, and schedule the job.

#### Procedure

---

- Step 1** Click **Finish** in the left pane to complete job creation.
- Step 2** Click **Save** to add the job to the list of scheduled jobs or run the job now, depending on whether you scheduled the job for a later time or chose Run Now in the scheduling screen.

The screen refreshes and the AP Radio Scan Job Save Summary window shows 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. |

- Step 3** To view the job run log, see [Viewing the AP Radio Scan Job Run Log](#), page 7-21.

The job stops automatically after all the required APs respond with the appropriate radio measurements. To stop the job manually, see [Stopping AP Radio Scan Jobs, page 7-20](#).

- Step 4** After the AP Radio Scan has completed successfully, you are ready to run a client walkabout (see [Client Walkabout, page 7-24](#)).
- 

#### Related Topics

- [Viewing AP Radio Scan Jobs, page 7-16](#)
- [Deleting AP Radio Scan Jobs, page 7-20](#)
- [Creating a New AP Radio Scan, page 7-11](#)

## Viewing AP Radio Scan Jobs

Use this screen to view AP radio scan jobs.



#### Note

Your login determines whether you can use this option.

---

#### Procedure

---

- Step 1** Select **Radio Manager > AP Radio Scan**.

- 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 Job State you selected: [Scheduled and Unscheduled](#), [Running](#), or [All](#).



- 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.                                                                           |

- 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.    |
| Next Schedule    | Firmware jobs are not recurring.                      |
| Owner            | The user who last edited the job.                     |

- 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.<br><br><b>Note</b> 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** To sort table data, click on the corresponding heading (see [Sorting Table Data, page 1-11](#)).
- Step 4** From this window, you can:
- Filter the list of AP radio scan jobs—See [Filtering AP Radio Scan Jobs, page 7-18](#)
  - Edit a job—See [Editing AP Radio Scan Jobs, page 7-19](#)
  - Stop a job—See [Stopping AP Radio Scan Jobs, page 7-20](#)
  - Delete a job—See [Deleting AP Radio Scan Jobs, page 7-20](#)
  - Copy a job to create a new job—See [Copying AP Radio Scan Jobs, page 7-21](#)
  - View the AP radio scan job run log—See [Viewing the AP Radio Scan Job Run Log, page 7-21](#)
  - Refresh the screen—See [Refreshing the AP Radio Scan Job Summary, page 7-23](#)
- 

## Filtering AP Radio Scan Jobs

Use this option to display a limited set of AP radio scan 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 **Radio Manager > AP Radio Scan**.
- Step 2** Click **Filter**.
- 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**. 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.

---

## Editing AP Radio Scan Jobs

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 **Radio Manager > AP Radio Scan**.
  - Step 2** From the list of jobs, select the job you want to edit.
  - Step 3** Click **Edit**.
  - Step 4** Select choices in the Job Creation Menu. For descriptions of the choices, see [Creating a New AP Radio Scan, page 7-11](#).
-

## Stopping AP Radio Scan Jobs

Use this option to stop a running AP Radio Scan job.

**Note**

Your login determines whether you can use this option.

**Procedure**

- 
- Step 1** Select **Radio Manager > AP Radio Scan**.
  - Step 2** From the Job State list, select **Running**.
  - Step 3** Select the job you want to stop.
  - Step 4** Click **Stop**.
  - Step 5** Click **OK** in the popup window.
- 

## Deleting AP Radio Scan Jobs

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 **Radio Manager > AP Radio Scan**.
  - Step 2** From the list of jobs, select the job you want to delete.
  - Step 3** Click **Delete**.
  - Step 4** Click **OK** in the popup window.
-

## Copying AP Radio Scan Jobs

Use this option to create a new job using the data (maximum transmit power and selected APs) from a previously-created job. This option does not copy the schedule data.

**Note**

Your login determines whether you can use this option.

**Procedure**

- 
- Step 1** Select **Radio Manager > AP Radio Scan**.
- Step 2** From the list of jobs, select the job you want to copy.
- Step 3** Click **Copy Job**.

**Note**

This option does *not* copy the schedule data.

- Step 4** Enter the name for the new job in the popup window.
- Step 5** Click **OK**.
- 

## Viewing the AP Radio Scan Job Run Log

Use this option to view the run logs for a selected job.

**Note**

Your login determines whether you can use this option.

**Procedure**

- 
- Step 1** Select **Radio Manager > AP Radio Scan**.
- Step 2** From the All AP Radio Scan Jobs table, select a job, then click **Job Run Log**.

- Step 3** 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.<br><br>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.                                                                                                      |

This table also provides the following options:

- To sort table data, click on the corresponding heading (see [Sorting Table Data, page 1-11](#)).
- To view the details for a different job run, select another run and click **Job Run Log**. The details for the selected run appear below the list of runs.
- To view the AP location information collected during a job run, select the run and click **AP Location Information**.



**Note**

AP location information is available only for the most recently completed AP radio scan job.

The AP Location Information table contains the following information:

| Field         | Description                                                        |
|---------------|--------------------------------------------------------------------|
| AP Name       | The name of the access point                                       |
| IP Address    | The IP address for that access point.                              |
| Has Scan Data | Whether scan data was collected for this access point (YES or NO). |

| Field          | Description                                                      |
|----------------|------------------------------------------------------------------|
| Neighbors      | The number of neighboring access points that have been detected. |
| Last Scan Time | The date and time this scan was run.                             |

- To refresh the table, click **Refresh**.

## Refreshing the AP Radio Scan Job Summary

If you made recent changes to one or more AP radio scan jobs, you can refresh the job list to make sure you are looking at the latest information.

**Note**

Your login determines whether you can use this option.

**Procedure**

- Step 1** Select **Radio Manager > AP Radio Scan**. The list of AP radio scan jobs appears.
- Step 2** From the Job State list, select the type of job you want to view.
- Step 3** Click **Refresh**. The screen shows an updated list of the currently displayed jobs.

# Client Walkabout

Client Walkabout measurements are used to determine AP coverage. This data is used to provide optimal coverage for the radio parameter generator.

**Note**

The Assisted Site Survey wizard can walk you through the process of determining the optimal radio transmit power and channel selection. It helps you select APs, run an AP radio scan job, perform a client walkabout, and generate radio parameters for the selected APs. See [Using the Assisted Site Survey Wizard, page 7-55](#).

**Related Topics**

- [Understanding Client Walkabouts, page 7-24](#)
- [Client Walkabout Guidelines, page 7-25](#)
- [Creating a New Client Walkabout, page 7-26](#)
- [Viewing Client Walkabouts, page 7-33](#)
- [Editing Client Walkabouts, page 7-34](#)

## Understanding Client Walkabouts

The Client Walkabout option allows you to:

- Specify a group of APs that will participate in the walkabout.
- Specify the maximum transmit power level.

During a client walkabout, up to five client stations, each identified by its 802.11 MAC address, are walked around the coverage area of the WLAN or a portion of the WLAN. The APs are set to the same channel and the transmit power in the APs is increased so that the power required to cover the edges of the WLAN can be determined.

A client walkabout station continuously reports radio measurements back to its serving AP as it roams throughout the coverage area. All measurements are passed to the Radio Manager, which incorporates them into its radio environment database.



**Note**

If you choose not to perform a client walkabout, you must enter a floor plan that includes the distances between APs (see [Adding Floor Information, page 7-49](#)).

**Related Topics**

- [Creating a New Client Walkabout, page 7-26](#)
- [Client Walkabout Guidelines, page 7-25](#)
- [Collecting Radio Location Measurements, page 7-4](#)

## Client Walkabout Guidelines

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 session does affect the processing time of RM Assisted Configuration—the larger the data set, the longer it takes to calculate the parameters.

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 Assisted Site Survey Wizard, page 7-55](#)), 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 RM Assisted Configuration either on a per-building or per-floor basis. You will usually get better channel combinations if you run RM 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 WLSE1105 will take 10 to 12 minutes or less to complete the parameter generation process—*without* other jobs, such as inventory, configuration, discovery, or another Radio Manager task running simultaneously.

**Note**

Because the WLSE1130 is a higher performance product, its parameter generation speed will be significantly better than a WLSE1105.

**Related Topics**

- [Creating a New Client Walkabout, page 7-26](#)
- [Understanding Client Walkabouts, page 7-24](#)

## Creating a New Client Walkabout

Use this option to create a client walkabout session.

**Note**

Your login determines whether you can use this option.

**Prerequisites**

Before you can run a client walkabout, you must have already:

- Discovered the devices (see [Managing Device Discovery, page 3-30](#)).
- Made the devices managed (see [Managing and Unmanaging Devices, page 3-64](#)).
- Authenticated the devices with WDS (see [Setting WDS Thresholds, page 2-46](#)).
- Configured the walkabout client to associate with the APs selected for the walkabout.

## Procedure

---

**Step 1** Select **Radio Manager > 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.

**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 [1. Name the Walkabout, page 7-28](#).
2. **Select AP**—See [2. Select the APs, page 7-28](#).
3. **Enter Client MAC**—See [3. Enter Client MAC Addresses, page 7-29](#).
4. **Options**—See [4. Enter Walkabout Options, page 7-30](#).
5. **Finish**—See [5. Finish Creating the Walkabout, page 7-30](#).



### Caution

---

Clicking on a 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 4** To run the client walkabout, see [Running the Walkabout, page 7-31](#).

---

## Related Topics

- [Client Walkabout Guidelines, page 7-25](#)

# 1. Name the Walkabout

Procedure

- Step 1
- Click **Name**.
- Step 2
- Enter the following data:

| Field       | Description                                                                                                                                                                                                                                                                |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Job Name    | Enter a unique name for the walkabout.<br><br>To make each session easy to identify, consider including the floor number or a similar identifier in the job name.<br><br>For additional naming convention guidelines, see <a href="#">Appendix A, “Naming Guidelines.”</a> |
| Description | Enter a description of the walkabout. For guidelines on entering descriptions, see <a href="#">Appendix A, “Naming Guidelines.”</a>                                                                                                                                        |

- Step 3
- From the menu in the left pane, go to the next step, Select AP. (See [2. Select the APs, page 7-28.](#))

Related Topics

[Creating a New Client Walkabout, page 7-26](#)

# 2. Select the APs

Procedure

- Step 1
- 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 session (see [Using the Device Selector and Search, page 1-9](#)).



---

**Note** In each walkabout session, include only the APs on that floor (see [Client Walkabout Guidelines, page 7-25](#)).

---

- Step 3** From the menu in the left pane, go to the next step, Enter Client MAC. (See [3. Enter Client MAC Addresses, page 7-29](#).)
- 

#### Related Topics

[Creating a New Client Walkabout, page 7-26](#)

## 3. Enter Client MAC Addresses

#### Procedure

---

- Step 1** 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 dropdown list.



---

**Note** Entering a MAC address that consists of more than 12 characters will generate an error message.

---

- Step 3** From the menu in the left pane, select the next task, Options. (See [4. Enter Walkabout Options, page 7-30](#).)
- 

#### Related Topics

[Creating a New Client Walkabout, page 7-26](#)

## 4. 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** Click **Options**.
  - Step 2** Select the AP power setting.  
  
By default, the power level is set to the maximum value allowed on the AP or the maximum allowed by the regulatory domain. You might choose to enter a lower power setting when, for example, the default power level might affect a neighboring network.
  - Step 3** From the menu in the left pane, select the next task, Finish. (See [5. Finish Creating the Walkabout](#), page 7-30.)
- 

### Related Topics

[Creating a New Client Walkabout](#), page 7-26

## 5. 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** Click **Finish** in the left pane.
  - Step 2** Click **Save** to add the walkabout to the list of client walkabouts. The screen refreshes and the Client Walkabout Summary window shows the following information:

| Field | Description            |
|-------|------------------------|
| Name  | Name of the walkabout. |

| Field              | Description                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 <a href="#">4. Enter Walkabout Options, page 7-30</a> ). |
| 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** To run the walkabout, see [Running the Walkabout, page 7-31](#).

### Related Topics

[Creating a New Client Walkabout, page 7-26](#)

## Running the Walkabout

When you start a client walkabout, the walkabout session starts immediately and continues until you stop the procedure. Only one client walkabout session 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 session during off-hours to minimize any disruptions to the network.

### Prerequisites

- You must have successfully created a client walkabout session (see [Creating a New Client Walkabout, page 7-26](#)).

### Procedure

**Step 1** Take the client (typically a laptop) to the area where the walkabout will be run.

- Step 2** Select **Radio Manager > Client Walkabout**. A list of the current Client Walkabout sessions appears.
- Step 3** Select the name of the client walkabout session 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. Use these guidelines as you walk:
- 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 the edges of the network.
  - Emphasize areas where you want coverage, such as conference rooms and other enclosed areas.
  - For more information about collecting walkabout data, see [Client Walkabout Guidelines, page 7-25](#).
- Step 6** When you have finished collecting the data, *stop the walkabout*. Select the walkabout session 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 [Viewing Walkabout Session Details, page 7-36](#).)
  - Click **Walkabout Details** to view the AP locations collected during a walkabout (see [Viewing AP Location Details, page 7-37](#)).

You can also use the Location Manager (see [Location Manager, page 7-39](#)) to view the results of the walkabout session.

---

### Related Topics

- [Viewing Client Walkabouts, page 7-33](#)
- [Starting Client Walkabouts, page 7-35](#)
- [Stopping Client Walkabouts, page 7-36](#)



## Viewing Client Walkabouts

Use this screen to view client walkabout sessions.

**Note**

Your login determines whether you can use this option.

**Procedure**

**Step 1** Select **Radio Manager > Client Walkabout**.

**Step 2** From the Client Walkabout State list, select the type of walkabout whose status you want to check (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** To sort table data, click on the corresponding heading (see [Sorting Table Data, page 1-11](#)).

**Step 4** From this window, you can:

- Edit a walkabout—See [Editing Client Walkabouts, page 7-34](#).
- Delete a walkabout—See [Deleting Client Walkabouts, page 7-35](#).
- Start a walkabout—See [Starting Client Walkabouts, page 7-35](#).
- Stop a walkabout—See [Stopping Client Walkabouts, page 7-36](#).
- View walkabout run details—See [Viewing Walkabout Session Details, page 7-36](#).

- View the AP locations collected during a walkabout—See [Viewing AP Location Details, page 7-37](#)
  - Refresh the screen—See [Refreshing the Walkabouts Summary, page 7-38](#).
- 

## Editing Client Walkabouts

Use this option to edit a walkabout from the displayed list of walkabouts.

**Note**

Your login determines whether you can use this option.

---

**Procedure**

---

- Step 1** Select **Radio Manager > Client Walkabout**.
- Step 2** From the list of walkabouts, select the walkabout that you want to edit.
- Step 3** Click **Edit**.
- Step 4** Select choices in the Client Walkabout Creation Menu. For descriptions of the choices, see [Creating a New Client Walkabout, page 7-26](#).
- Step 5** Click **Save** to save your changes. The Client Walkabout Save Summary displays the new settings for this walkabout.
- 

## Deleting Client Walkabouts

Use this option to delete a walkabout from the displayed list of walkabouts. Walkabouts that are running cannot be deleted.

**Note**

Your login determines whether you can use this option.

---

### Procedure

---

- Step 1** Select **Radio Manager > Client Walkabout**.
  - Step 2** From the list of walkabouts, select the walkabout that you want to delete.
  - Step 3** Click **Delete**.
  - Step 4** Click **OK** in the popup window.
- 

## Starting Client Walkabouts

Use this option to start a client walkabout.

**Note**

Your login determines whether you can use this option.

---

### Procedure

---

- Step 1** Select **Radio Manager > Client Walkabout**.
  - Step 2** From the list of walkabouts, select the walkabout that you want to start.
  - Step 3** Click **Start**.
- 

## Stopping Client Walkabouts

Use this option to stop a running walkabout.

**Note**

Your login determines whether you can use this option.

---

### Procedure

---

- Step 1** Select **Radio Manager > Client Walkabout**.

- Step 2** From the list of walkabouts, select the walkabout that you want to stop.
- Step 3** Click **Stop**.
- 

## Viewing Walkabout Session Details

Use this option to view the details of a client walkabout session.

**Note**

Your login determines whether you can use this option.

---

**Procedure**

- 
- Step 1** Select **Radio Manager > Client Walkabout**.
- Step 2** Select a walkabout, then click **Detailed**.

**Step 3** The Client Walkabout Details 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.                                                                                                                                   |
| 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 4. <a href="#">Enter Walkabout Options, page 7-30</a> ). |
| 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.                                                                                                                    |

## Viewing AP Location Details

Use this option to view the AP locations collected during a client walkabout session.



**Note**

Your login determines whether you can use this option.

**Procedure**

**Step 1** Select **Radio Manager > Client Walkabout**.

**Step 2** Select a walkabout, then click **Walkabout Details**.



**Note** AP location information is available only for the *most recently completed* walkabout. If a new walkabout session is in progress, this information is not available for the latest completed walkabout.

**Step 3** 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. |

## Refreshing the Walkabouts Summary

You can refresh the list of walkabouts to make sure you are looking at the latest information.



**Note** Your login determines whether you can use this option.

### Procedure

- Step 1** Select **Radio Manager > Client Walkabout**. The list of client walkabout sessions appears.
- Step 2** From the Client Walkabout State list, select the type of walkabouts you want to view (Running or All).
- Step 3** Click **Refresh**. The screen shows an updated list of the currently displayed walkabouts.

# Location Manager

The Location Manager gives you a graphical view of the APs on each floor of your building(s). Location Manager also uses the radio monitoring channel measurements supplied by all managed devices and client stations to calculate the location of unknown APs in your network. It provides a location estimate using measurements from as few as one station, regardless of type. The accuracy of the measurements depends on the number of devices that the measuring entity can detect from the given location.

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.

Location Manager allows you to

- View the location of APs in your building (see [Adding Building Information, page 7-47](#).)
- View the relative location of unknown or rogue APs (see [Finding Unknown Radios, page 7-52](#))
- Determine optimal radio transmit power and channel selection (see [Using the Assisted Site Survey Wizard, page 7-55](#))
- Display the predicted coverage of APs (see [Modifying AP Coverage Display Options, page 7-46](#))

## Prerequisites

Before you can use Location Manager, you must have already:

- Discovered the devices (see [Managing Device Discovery, page 3-30](#)).
- Authenticated the devices with WDS (see [Setting WDS Thresholds, page 2-46](#)).

For more information about navigating in the Location Manager window, see [Understanding the Location Manager Window, page 7-39](#).

## Understanding the Location Manager Window

In the upper left pane of the Location Manager window, you expand the All Locations folder to display the buildings and corresponding floors that you added.

Managed devices appear in the pane in the lower left pane of the Location Manager window. You need to initiate a discovery before they appear in this window. See [Managing Device Discovery, page 3-30](#) for more information.

The summary window in the right pane displays the number of APs in Managed state and Unmanaged state. You can double-click on the name of an AP to center the AP in the display of the floor map. For more information about adding devices to the floor map, see [Adding Devices to the Floor Map, page 7-51](#).

In addition, the All Locations Summary also gives you the number of

- Access Points in Managed State—The number of managed APs
- Access Points in Unmanaged State—The number of unmanaged APs
- Active Alarm Counts—The number of major and minor alarms currently in your network.
- Major Alarm Counts—P1 and P2 alarms (see [Viewing Fault Information, page 2-1](#))
- Minor Alarm Counts—P3, P4, and P5 alarms (see [Viewing Fault Information, page 2-1](#))

Location Manager includes several tools that you can use:

- Measuring Tool (See [Using Location Manager Measuring Tool, page 7-40](#).)
- Modify Contrast Tool (See [Using Location Manager Contrast Sliding Tool, page 7-41](#).)
- Channel Color Key (See [Using Location Manager Channel Color Key, page 7-41](#).)
- Locate Device Tool (See [Locating Devices in Location Manager, page 7-42](#).)

## 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 building(s). (See [Adding Floor Information, page 7-49](#).)



### 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 building 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.

## Using Location Manager Channel Color Key

Each AP on your floor map has a color associated with it. The color indicates the channel the AP is transmitting on. To verify which color corresponds with which channel, click on the Channel Color Key icon or select **Help > Channel Color Key**. The Channel Color Key legend appears showing you which color represents which channel.

## Using Location Manager Radio Location Color Key

The Location Manager Unknown Radio Location Color Key shows you the possible location of an unknown radio. The color gradations correspond to the percentage of probability that the unknown radio exists in the specified region. Click on the Unknown Radio Location Color Key, located next to the Channel Color Key, or select **Help > Unknown Radio Location Color Key** to view this information.

## 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.

## 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 Device**. The Find Device 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 Device 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 Device** at the bottom of the form.

The device 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.

#### Related Topics

- [Changing Location Manager Display Options, page 7-44](#)
- [Adding Devices to the Floor Map, page 7-51](#)

## Obtaining Server Information

From Location Manager, you can

- Verify Server Status (See [Verifying Server Status, page 7-43](#).)
- View Server Messages (See [Viewing Server Messages, page 7-44](#).)

## Verifying Server Status

You can verify the status of your server by selecting **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—The username of the person who launched Location Manager
- Client Address—The address of the client machine that launched Location Manager
- Login Time—The time that the user launched Location Manager

**Related Topics**

- [Viewing Server Messages, page 7-44](#)

## Viewing Server Messages

You can view server messages after you configure your floor plan with APs by selecting **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.

**Related Topics**

- [Verifying Server Status, page 7-43](#)

## Changing Location Manager Display Options

Location Manager allows you to modify how devices are displayed. You can

- Modify how device names are displayed (See [Modifying Device Name Display, page 7-44](#).)
- Modify what AP information is displayed on the floor map (See [Modifying Floor Map Display Options, page 7-45](#).)
- Modify AP coverage display options (See [Modifying AP Coverage Display Options, page 7-46](#).)

## Modifying Device Name Display

You can select how you want your devices displayed in the Location Manager window by selecting **View > Device Label** and clicking on one of these options:

- Name— Device Names are displayed
- IP Address—IP Addresses of devices are displayed
- MAC Address—MAC addresses of devices are displayed

## Modifying Floor Map Display Options

You can specify what AP information you want displayed on the floor map:

- Channel frequency (See [Displaying Channel Frequency, page 7-45.](#))
- Transmit power (See [Displaying Transmit Power, page 7-45.](#))
- Data rate (See [Displaying Data Rate, page 7-45.](#))
- Coverage display (See [Displaying Coverage, page 7-45.](#))
- Displaying RSS (See [Displaying RSSI from Selected AP, page 7-46.](#))

### Displaying Channel Frequency

To display the channel frequency of the APs on the floor map, select **Display > Channel Frequency**.

The floor map refreshes to show the channel frequency of each AP. The color of the channel frequency number corresponds to the channel. For more information about the colors and what they mean, see [Using Location Manager Channel Color Key, page 7-41.](#)

### Displaying Transmit Power

To display the transmit power of the APs on the floor map, select **Display > Transmit Power**.

The floor map refreshes to show the transmit power (in mW) of each AP.

### Displaying Data Rate

To display the highest basic rate set of the APs on the floor map, select **Display > Data Rate**.

The floor map refreshes to show the data rate (in Mbps) of each AP.

### Displaying Coverage

To display a graphic representation of the transmit coverage of the APs on the floor map, select **Display > Coverage Display**.

The floor map refreshes to show the coverage area of each AP. To learn more about modifying the coverage display, see [Changing Location Manager Display Options, page 7-44.](#)

## Displaying RSSI from Selected AP

To display a numeric value of the received signal strength on the floor map, select **Display > Show RSSI from Selected AP**.

The floor map refreshes to show the received signal strength of each AP.

## Modifying AP Coverage Display Options

You can modify how the coverage of each AP is displayed in the floor map.

### Procedure

- 
- Step 1** Next to the Coverage Display pulldown, click **Options**. The Coverage Display Options form appears.
- Step 2** Select a value in the Display Signal Strength Threshold pulldown. The default is 80% (-55dBm), which means that the coverage area displayed on floor map encompasses the area in which the AP signal stretch is at 80% (-55dBm) of its threshold.
- You can select a different signal strength threshold, which will change the coverage area displayed on the floor map. If, for example, you select 20% (-85dBm) in the Display Signal Strength Threshold field, the coverage area around the AP will increase because it indicates the area in which the AP signal strength is at 20% (or -85dBm) or more of its threshold.
- Step 3** Change the display coloring method by choosing one of these options:
- Use Gradient Color (default)—Uses one color with varying degrees of darkness based on the receiving signal range
  - Use Solid Color—Uses one color with the boundary drawn within the range of the signal strength threshold you selected
- Step 4** Change the Calculation Grid Size by clicking on a value in the pulldown menu. Changing the size to a larger value, for example 8ft., gives you a more general coverage that is not as granular as if you had picked a smaller value, for example 2 ft. The smaller the value you choose, the more time it will take for the floor map to refresh because it will display a more specific coverage area.

- Step 5** Click **Apply**. The floor map refreshes to show the display options you selected.
- 

#### Related Topics

- [Changing Location Manager Display Options, page 7-44](#)

## Adding Building Information

When you start Location Manager, the first thing you need to do is add information about your building(s) and its floor(s).

#### Procedure

---

- Step 1** Select **Radio Manager > Location Manager**. A page appears telling you about the necessary Java plug-in version required to use Location Manager, and it displays the Java version you are currently running.
- Step 2** When you are sure you are running the correct version of the Java plug-in, click **Launch** to start Location Manager. The Location Manager window opens.
- Step 3** The first time you launch Location Manager, a dialog box appears saying that no building or floor information was found. It asks if you want to add a new building.
- Step 4** Click **Yes**.
- On subsequent launches, the buildings, corresponding floors, and relevant devices appear under All Locations.
- Step 5** The Building Tool opens displaying the Create Building Information form. Enter information about the building.

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 6** To import an image of the building, click **Upload/Select**. For more information about importing an image, see [Importing an Image of the Building, page 7-48](#).



**Note** The image filename cannot have any spaces in it. If your image filename has a space in it, rename the file before uploading it.

- Step 7** Click **Add Floor** to add information about the floor of the building. For more information about adding information about the floor, see [Adding Floor Information, page 7-49](#).

- Step 8** Click **Save**. You'll see the name of building appear under All Locations in the left pane of the Location Manager window.

#### Related Topics

- [Importing an Image of the Building, page 7-48](#)
- [Adding Floor Information, page 7-49](#)

## Importing an Image of the Building

To use Location Manager, you need an image (.gif, .jpg, .jpeg, or .png) of the layout of your building. You can import this image into the Location Manager by following these steps.



**Note** The image filename cannot have any spaces in it. If your image filename has a space in it, rename the file before uploading it.



**Note** If you import an image at the building level (not a *floor*), that image is the default for all floors in the building.



### Procedure

- 
- Step 1** In the Location Manager window, right click on a building or floor name and select **Edit Building** (or Edit Floor if you right-clicked on a floor). The Building Tool opens with the Create Floor Information form.
  - Step 2** Click **Upload/Select**. The Select Image File screen appears.
  - Step 3** Click **Upload** to browse to the location of your image file.
  - Step 4** Click on your image file, then click **Select**. You'll see your file added to the Select Image file window.
  - Step 5** Click **Select** on the Select Image file window. The image is uploaded. You'll see the name of your image file in the Default Floor Map Image field on the Building Tool window, and your image file should appear in the Map Image Preview field.
  - Step 6** On the Map Image preview, drag the red rectangle to cover just the edges of your building, or if desired, drag the rectangle over just a portion of your building. This is particularly important if your image has white space around the building because it helps Location Manager more accurately determine the location of any interferers.
- 

### Related Topics

- [Adding Devices to the Floor Map, page 7-51](#)
- [Adding Floor Information, page 7-49](#)

## Adding Floor Information

After importing an image file of your building, you need to specify the dimensions of the floor(s) so that Location Manager knows the scale of the image you imported and can more accurately report the location of any interferers. When you first import an image file into Location Manager, the floor dimensions are the pixel size of the imported image.

If you don't know the dimensions of your floor, see [When You Don't Know Floor Dimensions, page 7-50](#) for more information.

## Procedure

- Step 1** In the Location Manager window, right click on the building name and select **Add Floor**. The Building Tool opens with the Create Floor Information form.
- Step 2** Enter the name of the floor and import an image map. For more information, see [Importing an Image of the Building, page 7-48](#).



**Note** The image filename cannot have any spaces in it. If your image filename has a space in it, rename the file before uploading it.



**Note** If you previously imported an image to your building, that image is the default for all floors in the building. To upload a new image for the floor, import a new image.

- Step 3** Select whether the measurement is in feet or meters using the pull-down menu, and then enter the dimensions of your floor in the Floor Dimensions field.
- Step 4** On the Map Image preview, drag the red rectangle to cover just the edges of your floor, or if desired, drag the rectangle over just a portion of your floor, for example, a conference room. This is particularly important if your image has white space around the building or conference room because it helps Location Manager more accurately determine the location of any interferers.

## Related Topics

- [When You Don't Know Floor Dimensions, page 7-50](#)

## When You Don't Know Floor Dimensions

If you don't know the dimensions of the floor, you can add dimension information to Location Manager using:

- The dimensions of a smaller area, for example, a conference room.
- The distance between two points, for example, two devices.

### Procedure

- 
- Step 1** If you know the dimensions of a portion of the floor (or the distance between two devices), in the Building Tool, enter that measurement (or the distance between the two devices) in the Floor Dimension field. To improve accuracy, specify a measurement for the largest area possible.
- Step 2** On the imported image map, drag the red rectangles to cover just the area that you specified the dimensions for. Or if using the distance between two devices, put two corners of the rectangle at each AP location.
- 

## Adding Devices to the Floor Map

After you add a new building and new floor and import an image map, you can place the devices on the floor map for each floor.

You need to initiate a discovery before you can add them to a building or floor. See [Managing Device Discovery, page 3-30](#) for more information.

### Procedure

- 
- Step 1** From the list of devices in the bottom left window of Location Manager, click on a device name and drag it to its approximate location on the image of the floor map.
- You do not need to place the devices in the exact location on the image map, but the closer the device on the map matches its location on the floor, the more accurately Location Manager will be when giving you information about unknown radios and interferers.
- Step 2** Continue to drag and drop devices on to the floor map.
- 

The floor map indicates the alarm status of each device:

- Red indicates the device has faults with major alarms.
- Yellow indicates the device has faults with minor alarms.
- Green indicates the device has no faults.

- Grey indicates the device is unmanaged.

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.

#### Related Topics

- [Moving Devices on Image Map, page 7-52](#)
- [Using Location Manager Channel Color Key, page 7-41](#)

## Moving Devices on Image Map

If you already placed a device on your image map and need to change its location, you can move it to a new location by following these steps:

#### Procedure

---

- Step 1** Click on the Enable Edit Location Mode icon.
- 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**.
- Step 4** If you select **Edit > Cut**, click on the new location for the device, then select **Edit > Paste**.

The device appears in the new location on the image map.

---

#### Related Topics

- [Adding Devices to the Floor Map, page 7-51](#)

## Finding Unknown Radios

Location Manager helps you find unknown 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.

### Procedure

**Step 1** In the Location Manager window, click on the Unknown Radio List icon or select **Tools > Unknown Radio List**. The Unknown Radio List window opens displaying a list of all unknown radios found.

**Step 2** At the top of the Unknown Radio List window, select which devices you want to view:

- **Rogue**—An APs that has not been identified as Friendly. By default, all unknown radios are classified as Rogue until you change them to Friendly.
- **Friendly**—An AP 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 device name. The Unknown Radio List window refreshes with data specific to that device.

The **Reported By** field shows the device or devices that detected the unknown radio:

- If the **APs** checkbox is selected, the Reported By field displays the APs that detected the selected unknown radio.
- If the **Clients** checkbox is selected, clients detected the selected unknown radio.

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 building map. You'll see the possible location of the unknown radio shaded in color. The darkest shade indicates the most probable location.

Because Location Manager does not know the transmit power of the unknown radio, you might need to change the display options as explained in [Changing Location Manager Display Options, page 7-44](#).



**Note** 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

- [Displaying Unknown Radios in the Floor Map, page 7-54](#)

## Displaying Unknown Radios in the Floor Map

You can view the location of unknown radios in the Location Manager window by following these steps:

#### Procedure

**Step 1** In the Location Manager window, select the unknown radio type that you want to view in the Unknown Radios pulldown menu. The pulldown menu might contain MAC addresses or IP addresses of devices in your network.



**Note** You might need to zoom out if you cannot see the possible location of the unknown radio in the Location Manager window. See [Zooming In and Out, page 7-42](#).

**Step 2** Click **Options** to modify the display options for the unknown radio. The default transmit power selected is 50mW and 100mW.

**Step 3** Click on different transmit power options to increase the area on the floor map in which the unknown radio might be located. If you select all transmit powers, the floor map will display all possible areas that the unknown radio might be located.

- Step 4** Select whether to use the 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.
- 

#### Related Topics

- [Finding Unknown Radios, page 7-52](#)

## Using the Assisted Site Survey Wizard

The Assisted Site Survey walks you through the process of determining the optimal radio transmit power and channel selection. 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 [1. Selecting the APs, page 7-55](#).
2. **AP Radio Scan**—See [2. Viewing Radio Scan Data, page 7-56](#).
3. **Client Walkabout**—See [3. Performing a Client Walkabout, page 7-57](#).
4. **Radio Parameter Generation**—See [4. Generating Radio Parameters, page 7-58](#).

### 1. Selecting the APs

#### Procedure

---

- Step 1** Select **Radio Manager > Location Manager > 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 ([2. Viewing Radio Scan Data, page 7-56](#)).
- 

## 2. Viewing Radio Scan Data

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                                                                                                 |
| 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 old radio scan data—The wizard uses the data collected from the most recent radio scan job. Use this option if the number of neighbors is accurate.



**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.

---

- 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. By default, the power level is set to the maximum value allowed on the AP. See [Understanding AP Radio Scans, page 7-9](#).



- 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                        |
| Last Scan Time | Time the most recent radio scan job started |

- Step 4** Click **Next** to go to the next step ([3. Performing a Client Walkabout, page 7-57](#)).

#### Related Topics

- [Understanding AP Radio Scans, page 7-9](#)

## 3. 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 7-24](#).

#### 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 [Client Walkabout Guidelines, page 7-25](#).
  - Skip Client Walkabout—If the location data is accurate, you can skip the client walkabout and go directly to [4. Generating Radio Parameters, page 7-58](#).
- Step 2** If you select to start Client Walkabout Setup, you need to enter at least one client MAC address, and up to five addresses, that will move around during the walkabout.

- Step 3** Select the AP power setting. By default, the power level is set to the maximum value allowed on the AP or the maximum allowed by the regulatory domain. 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 |

- Step 5** Click **Next** to go to the next step ([4. Generating Radio Parameters, page 7-58](#)).

#### Related Topics

- [Client Walkabout Guidelines, page 7-25](#)

## 4. 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 internally utilizing 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.



#### 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.

#### 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** Enter a value in the Minimum and Maximum Transmit Power fields. By default, the transmit power is set to the maximum value allowed on the AP or the maximum allowed by the regulatory domain. You might choose to enter a lower power setting when, for example, the default power level might affect a neighboring network.
- Step 3** Under Goal, enter a numerical value for the expected maximum number of clients per AP, and a numerical value for the expected average number of clients per AP.
- Step 4** Select whether to enable black hole mitigation. If you select this option, Radio Manager 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, Radio Manager will not recommend a beacon interval.
- Step 5** Click **Start** to start the configuration parameter calculation. When the radio parameter generation is complete, a message appears at the bottom of the screen.
- Step 6** Click **Next** to view the calculation results and apply the configuration to the APs.
- Step 7** After reviewing the calculation results, 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**.

---



---

**Note** To view the changes from the Assisted Site Survey displayed graphically in Location Manager, in the Location Manager window, select **View > Refresh Data**.

---

#### Related Topics

- [AP Radio Scan, page 7-9](#)
- [Client Walkabout, page 7-24](#)
- [Radio Management Assisted Configuration, page 7-60](#)

# Radio Management Assisted Configuration

RM Assisted Configuration can help you configure your APs by internally utilizing measurement data collected from a Client Walkabout and AP radio scanning. RM Assisted Configuration recommends optimal radio transmit power, channel selection, and beacon interval (optional), and then applies these configuration settings to the APs, if desired.

**Tip**

To get optimal channel settings, run RM Assisted Configuration on a per building basis. That is, include all APs in one building in a single RM Assisted Configuration job.

**Note**

Your login determines whether you can use this option.

**Related Topics**

- [Creating a New Assisted Configuration Task, page 7-65](#)
- [Viewing Assisted Configuration Tasks, page 7-60](#)
- [Editing Assisted Configuration Tasks, page 7-61](#)

## Viewing Assisted Configuration Tasks

You can view RM assisted configuration tasks.

**Note**

Your login determines whether you can use this option.

**Procedure**

- Step 1** Select **Radio Manager > RM Assisted Configuration**. The RM Assisted Configuration screen appears.
- Step 2** From the pulldown menu, select what 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 RM 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. You can sort the configuration tasks by name, status, next schedule, or owner by clicking on the corresponding column heading.

#### Related Topics

- [Editing Assisted Configuration Tasks, page 7-61](#)
- [Copying Assisted Configuration Tasks, page 7-62](#)
- [Creating a New Assisted Configuration Task, page 7-65](#)

## Editing Assisted Configuration Tasks

You can edit assisted configuration tasks that were previously created.



**Note**

Your login determines whether you can use this option.

#### Procedure

- Step 1** Select **Radio Manager > RM Assisted Configuration**. The RM Assisted Configuration screen appears.
- Step 2** From the RM Assisted Configuration pulldown menu, select the configuration tasks you want to edit. The screen refreshes to show the corresponding tasks.

- Step 3** Click on the radio button next to the task you want to modify, then click **Edit**. See [Radio Management Assisted Configuration, page 7-60](#) for more information about completing the task.
- 

#### Related Topics

- [Copying Assisted Configuration Tasks, page 7-62](#)
- [Deleting Assisted Configuration Tasks, page 7-63](#)
- [Creating a New Assisted Configuration Task, page 7-65](#)

## Copying Assisted Configuration Tasks

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.



#### Note

Your login determines whether you can use this option.

---

#### Procedure

---

- Step 1** Select **Radio Manager > RM Assisted Configuration**. The RM Assisted Configuration screen appears.
- Step 2** From the RM Assisted Configuration pulldown menu, select the configuration tasks you want to copy. The screen refreshes to show the corresponding tasks.
- Step 3** Click on the radio button next to the task you want to modify, then click **Copy**.
- Step 4** Enter a new name for the copied configuration, then click **OK**. The copied configuration appears in the task list.
- 

#### Related Topics

- [Editing Assisted Configuration Tasks, page 7-61](#)
- [Creating a New Assisted Configuration Task, page 7-65](#)

- [Refreshing the List of Configuration Tasks, page 7-64](#)

## Deleting Assisted Configuration Tasks

You can delete assisted configuration tasks that were previously created.

**Note**

Your login determines whether you can use this option.

### Procedure

- Step 1** Select **Radio Manager > RM Assisted Configuration**. The RM Assisted Configuration screen appears.
- Step 2** From the RM Assisted Configuration pulldown menu, select the configuration tasks you want to delete. The screen refreshes to show the corresponding tasks.
- Step 3** Click on the radio button next to the task you want to remove, then click **Delete**. A dialog box appears asking if you want to delete the selected task.
- Step 4** Click **OK**. The configuration is deleted from the task list.

### Related Topics

- [Refreshing the List of Configuration Tasks, page 7-64](#)
- [Creating a New Assisted Configuration Task, page 7-65](#)

## Viewing Details of a Configuration Task

You can view details of selected configuration tasks.

**Note**

Your login determines whether you can use this option.

### Procedure

- 
- Step 1** Select **Radio Manager > RM Assisted Configuration**. The RM Assisted Configuration screen appears.
- Step 2** From the RM Assisted Configuration pulldown menu, select the configuration tasks you want to view. The screen refreshes to show the corresponding tasks.
- Step 3** Click on the radio button next to the task you want to view details of, then click **Details**.

The Radio Management Assisted Configuration Details window appears listing information about the configuration task.

---

### Related Topics

- [Editing Assisted Configuration Tasks, page 7-61](#)
- [Copying Assisted Configuration Tasks, page 7-62](#)
- [Refreshing the List of Configuration Tasks, page 7-64](#)
- [Creating a New Assisted Configuration Task, page 7-65](#)

## Refreshing the List of Configuration Tasks

If you made recent changes to configuration tasks, you can refresh the list of configuration tasks to make sure you're looking at the latest information. You might also need to refresh the configuration tasks if you have a configuration in the Planning state.



### Note

Your login determines whether you can use this option.

---

### Procedure

- 
- Step 1** Select **Radio Manager > RM Assisted Configuration**. The RM Assisted Configuration screen appears.
- Step 2** From the RM Assisted Configuration pulldown menu, select **All**. The screen updates to show all the RM assisted configuration tasks.



- Step 3** Click on **Refresh**. The screen refreshes and shows an updated list of all configuration tasks.
- 

#### Related Topics

- [Editing Assisted Configuration Tasks, page 7-61](#)
- [Creating a New Assisted Configuration Task, page 7-65](#)

## Creating a New Assisted Configuration Task

When you have a APs or a group of APs that you want to configure, you can use RM Assisted Configuration to configure the APs. Using AP Scan and Client Walkabout data, RM Assisted Configuration generates optimal values for the radio parameters of a given group of APs.



#### Tip

To get optimal channel settings, run RM Assisted Configuration on a per building basis. That is, include all APs in one building in a single RM Assisted Configuration job.

---



#### Note

The Assisted Site Survey wizard can walk you through the process of determining the optimal radio transmit power and channel selection. It helps you select APs, run an AP radio scan job, perform a client walkabout, and generate radio parameters for the selected APs. See [Using the Assisted Site Survey Wizard, page 7-55](#).

---



#### Note

Your login determines whether you can use this option.

---

#### Prerequisites

Before you can create a new RM assisted configuration task, you must have already:

- Discovered the devices (see [Managing Device Discovery, page 3-30](#))

- Made the devices managed (see [Managing and Unmanaging Devices](#), page 3-64)
- Perform an AP Radio Scan (see [AP Radio Scan](#), page 7-9)
- Perform a Client Walkabout (optional but recommended) or add device information in Location Manager. See [Client Walkabout](#), page 7-24 and [Location Manager](#), page 7-39.

### Procedure

- 
- Step 1** Select **Radio Manager > RM Assisted Configuration**. The RM assisted configuration information appears.
- 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 RM assisted configuration task:
1. **Job Name**—[1. Naming the Configuration Task](#), page 7-67.
  2. **Select Devices**— See [2. Selecting Devices](#), page 7-67.
  3. **Constraints and Goals**—See [3. Assigning Constraints and Goals](#), page 7-68.
  4. **Calculated Parameters**—See [4. Calculating Parameters](#), page 7-69.
  5. **Calculated Results**— See [5. Viewing the Calculated Results](#), page 7-69.
  6. **Schedule**—See [6. Scheduling the Assisted Configuration](#), page 7-70.
  7. **Done**— See [7. Finishing the Task](#), page 7-70.



### Caution

---

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.

---

## 1. Naming the Configuration Task

### Procedure

---

**Step 1** Click **Name**.

The screen refreshes so you can enter information about the new task. You'll see the name you entered in the Task Name field.

**Step 2** Enter the following information:.

| Field       | Description                                                                                                                   |
|-------------|-------------------------------------------------------------------------------------------------------------------------------|
| Job Name    | Enter a unique name for the job. For guidelines on naming jobs, see <a href="#">Appendix A, "Naming Guidelines."</a>          |
| Description | Enter a description of the job. For guidelines on entering descriptions, see <a href="#">Appendix A, "Naming Guidelines."</a> |

---

**Step 3** From the menu in the left pane, go to the next step, Selecting Devices. (See [2. Selecting Devices, page 7-67](#))

---

## 2. Selecting Devices

### Procedure

---

**Step 1** 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 and Search, page 1-9](#)).**Step 3** From the menu in the left pane, go to the next step, Constraints and Goals. See [3. Assigning Constraints and Goals, page 7-68](#).)

---

### Related Topics

- [Creating a New Assisted Configuration Task, page 7-65](#)

### 3. Assigning Constraints and Goals

After selecting the devices for the assisted configuration task, you need to specify the constraints and goals of the task.

#### Procedure

- 
- Step 1** Determine whether you want to apply the constraints to all APs that you selected in Step 2 or if you want to apply the constraints to individual APs that you selected in Step 2.
- Step 2** If you selected to apply the constraints to individual APs, a list box appears in which you can select the AP on which to apply the constraints. Click on the AP name in the list box.
- Step 3** For the Channel Set, select either option:
- **Recommended**—Use the channels Radio Manager 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.
- Step 4** Enter a number for the minimum transmit power and a number for the maximum transmit power. By default, the power level is set to the maximum value allowed on the AP or the maximum allowed by the regulatory domain. You might choose to enter a lower power setting when, for example, the default power level might affect a neighboring network.
- Step 5** Enter a numerical value for the expected maximum number of clients per AP and a numerical value for the expected average number of clients per AP.
- Step 6** Select whether to enable black hole mitigation. If you select this option, Radio Manager 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, Radio Manager displays the beacon interval the AP is currently configured to.
- 

#### Related Topics

- [Creating a New Assisted Configuration Task, page 7-65](#)
- [Editing Assisted Configuration Tasks, page 7-61](#)

- [Deleting Assisted Configuration Tasks, page 7-63](#)

## 4. Calculating Parameters

After you assign the constraints and goals, the next step is for Radio Manager to calculate the parameters. In this step, you will see a progress bar that indicates the progress Radio Manager 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.

To stop the parameter calculation, click on the **Stop** button.

When the parameter calculation is complete, the results are displayed. For more information about the parameter results, see [5. Viewing the Calculated Results, page 7-69](#).

**Related Topics**

- [Creating a New Assisted Configuration Task, page 7-65](#)
- [Editing Assisted Configuration Tasks, page 7-61](#)
- [Deleting Assisted Configuration Tasks, page 7-63](#)

## 5. Viewing the Calculated Results

After Radio Manager calculates the parameters for the assisted configuration job, it displays the calculation results. The calculation results specify the following information:

| Field          | Description                            |
|----------------|----------------------------------------|
| Name           | Name of the AP                         |
| Transmit Power | Recommended transmit power for this AP |
| Channel        | Recommended channel for the AP         |

| Field                        | Description                                                                                                                                                                                                                                                         |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Beacon Interval              | Recommended beacon interval for the AP. If you did not select the Enable Black Hole Mitigation option, this column displays the value the AP is currently configured to. (See <a href="#">3. Assigning Constraints and Goals</a> , page 7-68 for more information.) |
| Estimated Maximum Throughput | The estimated maximum megabytes per second that the AP can process                                                                                                                                                                                                  |

## 6. Scheduling the Assisted Configuration

After you have viewed the calculation results of the assisted configuration task (see [4. Calculating Parameters](#), page 7-69 for more information) and want to apply these changes, you need to determine when to apply configuration changes.

### Procedure

- 
- Step 1** Click on **6. Schedule**. The Schedule RM Assisted Configuration Job form 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.
- 

## 7. Finishing the Task

Before selecting this option, you must name the assisted configuration task, select the devices, enter constraints and goals, and schedule the assisted configuration task.

### Procedure

- 
- Step 1** Click **Finish** in the left pane.

The Done form appears indicating that the job has completed or it has been scheduled (if you scheduled it to run later).

---

## Managing RM Measurements

Use the Manage RM Measurements tab to delete previously-collected radio location measurements, including links and path loss data. You might need to delete radio location data, for example:

- When APs have been added, deleted, or physically moved.

**Note**

If you run a new AP radio scan, the radio location information for the selected APs is deleted automatically.

---

- If the number of walkabout locations is slowing down the RM Assisted Configuration. You can use the Location Manager's RM Assisted Wizard (see [Using the Assisted Site Survey Wizard, page 7-55](#)), to view the walkabout results, including each AP and the number of walkabout locations that can hear that AP.

### Procedure

---

**Step 1** Select **Radio Manager > Manage RM Measurements**.

**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.
- **Delete Walkabout Measurements**—Deletes the client radio locations collected during client walkabouts.

**Step 3** Click **Select Devices**. All managed devices are listed in the Device selector in the middle pane.

**Note**

In a multi-storied building, in addition to selecting the APs for that floor, select the APs for the floors above and below as well.

---

- Step 4** Select the devices you want to include in the job (see [Using the Device Selector and Search, page 1-9](#)).
- Step 5** Click **Finish** in the left pane. The selected data is deleted immediately.
- 

**Related Topics**

- [AP Radio Scan, page 7-9](#)
- [Client Walkabout, page 7-24](#)
- [Using the Assisted Site Survey Wizard, page 7-55](#)





# Managing the WLSE System

---

The following subtabs are displayed when you select the Administration tab:



## Note

---

Some of these subtabs may not be visible to some users; what you see under the Administration tab depends on your login.

---

- **Appliance**—Manage the Wireless LAN Solution Engine system (see [Managing the Appliance, page 8-2](#)).
- **System**—View information about supported firmware versions, and update firmware support to add newly supported versions (see [Updating Supported Firmware Versions, page 8-38](#)).
- **User Admin**—Manage users and user roles (see [Managing Users, page 8-39](#)).
- **My Profile**—Set preferences for an individual user: password, email address, and appearance of the interface at login (see [Modifying Your Profile, page 8-46](#)).
- **Links**—Set up links to other systems (such as CiscoWorks servers) and display their desktops and run ACS failed login reports (see [Creating Links, page 8-48](#)).

# Managing the Appliance

Options under the Appliance subtab allow you to manage the WLSE system and use connectivity tools. When you select **Administration > Appliance**, the following options are displayed:

- **Status**—Gather and view WLSE statistics and restart the WLSE (see [Using Log Files, page 8-3](#) and [Restarting the WLSE, page 8-5](#)).
- **Software**—Update, reinstall, view status, and define the repository for the WLSE software (see [Managing WLSE Software, page 8-5](#)).
- **Security**—Manage WLSE security features, such as telnet, SSL, and authentication modules (see [Managing Security, page 8-15](#)).
- **Backup and Restore**—Configure backup location, backup data, and restore data (see [Backing Up and Restoring Data, page 8-21](#)).
- **Diagnostics**—Troubleshoot, run self-tests, view process status (see [Using WLSE Diagnostics Options, page 8-28](#)).
- **Splash Screen**—Customize the splash screen message (see [Specifying a Splash Screen Message, page 8-32](#)).
- **Time/NTP/Name**—Set the current time (see [Set the Current Local and UTC Time, page 8-33](#)), specify **NTP** servers (see [Specify NTP Time Servers, page 8-34](#)), and specify IP name servers (see [Specify Name Servers, page 8-34](#)).
- **Configure Mailroute**—Specify an **SMTP** server for handling email notifications (see [Configuring the Mail Route, page 8-35](#)).
- **Connectivity Tools**—Test device connectivity and reachability and find the values of SNMP variables (see [Using Connectivity Tools, page 8-35](#)).

**Note**

---

Your login determines whether you can use these options.

---

## Using Log Files

This option allows you to view the contents of WLSE log files, download logs, search for data in logs, and email logs.

### Procedure

- Step 1** Select **Administration > Appliance > Status > View Log File**. The following information is displayed:

| Field     | Description                                         |
|-----------|-----------------------------------------------------|
| Log file  | 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, see [About Log Files, page 8-4](#).

- 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 the 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 Selected Log Files textbox. Click **Send**.

## About Log Files

The WLSE maintains the following log files.

| Log File             | Content                                                                                                      |
|----------------------|--------------------------------------------------------------------------------------------------------------|
| access_log           | Web server user access log.                                                                                  |
| backup.log           | Log that appears after you back up WLSE data, restore data, or test the reachability of the backup location. |
| daemons.log          | Log for messages that dmgttd does not log.                                                                   |
| dataUpdate.log       | Log that appears after you upgrade WLSE software.                                                            |
| db2.log              | Log showing database startups due to installations or reboots.                                               |
| dmgttd.log           | Process Management daemon log file.                                                                          |
| error_log            | Web server error log.                                                                                        |
| faults.log           | Device fault log.                                                                                            |
| install.log          | Software package installation log.                                                                           |
| jobvm.log            | Scheduled tasks log.                                                                                         |
| mfgtest.log          | Manufacturing test log.                                                                                      |
| mod_jk.log           | Message log for hook between Tomcat and Apache.                                                              |
| snmpd.log            | <a href="#">SNMP</a> agent log file.                                                                         |
| ssl_request_log      | Log for secure HTTPS socket layer web server events.                                                         |
| swan.log             | Radio management log.                                                                                        |
| tomcat.log           | Java servlet messages log.                                                                                   |
| updateWLSE-x.x.x.log | Appears after you upgrade WLSE software; for example, updateWLSE-2.0.2.log.                                  |

## Restarting the WLSE

This option allows you to restart the WLSE. After restart, discovery and inventory will resume at the next scheduled time.

### Procedure

**Step 1** Select **Administration > 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. (See the *User Guide for the Wireless LAN Solution Engine, Release 2.5* on Cisco.com or by clicking **View PDF** in the online help.)

## Managing WLSE Software



### Caution

Before attempting to upgrade WLSE software, check the readme file associated with the software on Cisco.com for changes to the procedures and caveats. Some procedures in this guide may not be applicable to certain software upgrades.



### Note

Upgrade from a pre-release software version to an FCS version is not supported.

The software 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 8-6](#).
- **Define Repository**—Specify the repository location. The repository provides software update services to the WLSE—See [Managing the Repository, page 8-8](#).

- **Upgrading Software**—Select and install a software image from the repository—See [Installing the Software Update, page 8-12](#).
- **Browse Repository**—Browse the available complete images in the repository—See [Browsing the Repository, page 8-13](#).
- **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 8-14](#).

The topics in this section are:

- [Viewing Status of Installed Software, page 8-6](#)
- [Downloading the Upgrade Image, page 8-8](#)
- [Creating the Repository, page 8-9](#)
- [Defining the Repository, page 8-11](#)
- [Installing the Software Update, page 8-12](#)

For more information on installing WLSE software, including other installation methods, see the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*.

## Viewing Status of Installed Software

You can view information about the software currently installed on the WLSE.

### Procedure

- Step 1** Select **Administration > 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. |

| Field   | Description                                                                                                                                                                                              |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status  | Status of the installation:<br><br>Success—Software was installed with no errors.<br><br>Warning—Software installed successfully with minor errors.<br><br>Error—Software 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:<br><br>Success—Software installed with no errors.<br><br>Warning—Software installed successfully with minor errors.<br><br>Error—Software 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 8-14](#)
- [Installing the Software Update, page 8-12](#)
- [Managing WLSE Software, page 8-5](#)

## 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. | <a href="#">Downloading the Upgrade Image, page 8-8</a> |
| 2.   | Create repository.                | <a href="#">Creating the Repository, page 8-9</a>       |
| 3.   | Define repository.                | <a href="#">Defining the Repository, page 8-11</a>      |

## Downloading the Upgrade Image

To locate the upgrade files, follow the navigation path **Products and Services > Network Management CiscoWorks > CiscoWorks Wireless LAN Solution Engine > Software Center** or use one of the following URLs:

- [http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod\\_upgrades\\_and\\_downloads.html](http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_upgrades_and_downloads.html)
- <ftp://ftp.cisco.com/cisco/crypto/3DES/cw2000/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 the *User Guide for the Wireless LAN Solution Engine, Release 2.5* on Cisco.com or click **View PDF** in the online help.

The topics in this section are:

- [Creating a Local Repository, page 8-9](#)
- [Creating a Repository on a Windows Server, page 8-10](#)

### Creating a Local Repository

To create a local repository on the WLSE:

#### Procedure

- 
- |               |                                                                                                                                                                                                                                                                                                                                   |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Open a <a href="#">CLI</a> window to the WLSE, using Telnet or <a href="#">SSH</a> .                                                                                                                                                                                                                                              |
| <b>Step 2</b> | Specify the FTP site that will be the source of the software updates. Enter the following CLI command:<br><br><b>repository source ftp://hostname/path</b><br><br>where <i>hostname</i> is the name of the remote FTP server and <i>path</i> is the directory path on the remote FTP where you placed the zip file and info file. |
| <b>Step 3</b> | 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.<br><br><b>repository list remote</b>                                                                                                                                  |
| <b>Step 4</b> | Download the software to the local repository using the following command. This command requires a valid username and password on the remote FTP server.<br><br><b>repository add package</b>                                                                                                                                     |

For example, if the name of the zip file is WLSE-2.5-K9.zip, the *package* is WLSE-2.5-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.

Use the following procedure to set up a Windows NT, Windows 2000, or Windows XP server as a remote repository.

### Procedure

**Step 1** If you are using a Windows XP or Windows 2000 server as a repository and you are using the Internet Explorer 6.0 browser on the client, configure the browser *on the repository* as follows to make sure the update process works properly. Otherwise, the display during the update process does not work properly.

- a. Install Java Plugin 1.3.1\_08 or later.
- b. In the browser, select **Tools > Internet Options > Privacy** and lower the slider all the way down to achieve the **Accept all Cookies** setting.



### Note

For information on supported browsers, see [Supported Browsers, page 1-3](#).

**Step 2** Extract the zip file to any empty directory; for example, D:\WLSE\_repository.

**Step 3** Open a command window, create a virtual drive, and map the virtual drive to the drive containing the update file; for example:

```
subst f: d:\WLSE_repository
```



### Note

The virtual drive (f: in this example) will be removed after you reboot the Windows 2000, Windows NT, or Windows XP server.

**Step 4** Double-click the virtual drive icon. Then, double-click the autorun.bat file if it does not automatically run.

The Appliance Update screen appears in a browser.

---

## Defining the Repository

By defining the repository, you are telling the WLSE where to look for available software updates.

### Procedure

---

**Step 1** Select **Administration > 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 <code>localhost</code> . 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 **Administration > Appliance > Software > Browse Repository** to check the update image.

---

### Related Topics

- [Installing the Software Update, page 8-12](#)
- [Browsing the Repository, page 8-13](#)
- [Managing WLSE Software, page 8-5](#)

## Installing the Software Update



### Caution

Before upgrading WLSE software, back up the configuration. The upgrade attempts to preserve the WLSE database, but a backup is needed in case of errors during the upgrade. For information on backing up the WLSE's configuration, see [Backing Up and Restoring Data, page 8-21](#).

Before upgrading WLSE software, check the readme file that accompanies the image on Cisco.com for possible changes to the procedure, caveats, and new features.

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.

### Procedure

- Step 1** If you are using Internet Explorer 6.0 on a Windows XP client to update WLSE software, make sure Java Plugin 1.3.1\_08 is installed on the browser. Otherwise, certain displays during the upgrade process do not work properly.
- Step 2** Select **Administration > 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.
- Step 3** 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 4** To view details on an image in the table, click **README** in the Details field.
- Step 5** To begin the installation, make a selection from the Compatible Updates table, Compatible Reinstallations table, or Complete Images table.
- Step 6** To install the selected software, click **Install**. The Install Software Updates window opens.
- Step 7** Click **Confirm** to continue the installation. Click **Cancel** to cancel the installation.
- Step 8** 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 9** To view details of the installation after the installation is complete, select **Administration > Appliance > Software > Status > View Log**.
- 

#### Related Topics

- [Managing the Repository, page 8-8](#)
- [Viewing Status of Installed Software, page 8-6](#)
- [Viewing Software Update History, page 8-14](#)
- [Browsing the Repository, page 8-13](#)
- [Managing WLSE Software, page 8-5](#)

## 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 8-8](#).

---

#### Procedure

---

- Step 1** Select **Administration > Appliance > Software > Browse Repository**.

- 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 <b>README</b> to display details. |

#### Related Topics

- [Installing the Software Update, page 8-12](#)
- [Managing WLSE Software, page 8-5](#)

## 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.

#### Procedure

- Step 1** Select **Administration > Appliance > Software > Software Update History**. The following information is displayed:

**Table 8-1 Software Update History Window**

| Field   | Description          |
|---------|----------------------|
| Name    | Software identifier. |
| Version | Software version.    |

**Table 8-1 Software Update History Window (continued)**

| Field        | Description                                                                                                                                                                                                  |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Summary      | Summary of the installed software.                                                                                                                                                                           |
| Install Date | Date and time ( <a href="#">UTC</a> ) the software was installed.                                                                                                                                            |
| Status       | Status of the installed software.                                                                                                                                                                            |
| Status       | The status of the installation:<br><br>Success—Software was installed with no errors.<br><br>Warning—Software installed successfully with minor errors.<br><br>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.

#### Related Topics

- [Viewing Status of Installed Software, page 8-6](#)
- [Browsing the Repository, page 8-13](#)
- [Managing WLSE Software, page 8-5](#)

## Managing Security

You can manage the following security options under **Administration > Appliance > Security**:

- **Authentication Modules**—Set up the authentication module to be used (see [Setting Up an Authentication Module, page 8-17](#)).
- **SSL (HTTPS)**—Obtain a permanent, signed Certificate Signed Request for secure Web access (see [Managing SSL \(HTTPS\), page 8-18](#)).
- **Telnet and SSH**—Configure Telnet and [SSH](#) settings (see [Enabling Telnet and Selecting SSH Type, page 8-20](#)).

- **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 8-20](#)).

### Related Topics

[Overview: Security, page 8-16](#)

## Overview: Security

The WLSE provides the following security features:

- Optional secure connection through the Web browser—See [Managing SSL \(HTTPS\), page 8-18](#).
- Connection through the CLI via Telnet or SSH—See [Enabling Telnet and Selecting SSH Type, page 8-20](#).
- Authentication through the local database or alternative authentication services—See [Setting Up an Authentication Module, page 8-17](#) and [Managing User Accounts, page 8-42](#).
- Flexible user access to managed devices and WLSE services through configurable roles—See [Managing Roles, page 8-40](#).

## 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
- MS NT Domain

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.



The WLSE determines user roles; therefore, all users must be in the local database of user IDs and passwords. A user's role determines the services and devices that the user can access. Users must have the same user ID locally as they have in the alternative authentication source, but the local password and authentication service password do not have to be same.

Users who are authenticated by an alternative service and who are not in the local database have no roles assigned to them. Users who have no roles see only the splash screen after logging in and cannot view screens or perform tasks.

If the alternative authentication service fails, the Wireless LAN Solution Engine defaults to the Local authentication module. Even if the local user database fails, you can always log in as the admin user.

### Related Topics

- [Setting Up an Authentication Module, page 8-17](#)
- [Managing Users, page 8-39](#)

## Setting Up an Authentication Module

You can use your existing authentication method to authenticate WLSE users by selecting and configuring one of the WLSE's login modules.

To configure an authentication module for users logging in to the CLI via Telnet or SSH, see the chapter titled "Managing the WLSE via the CLI" or the appendix titled "Using the Command Line Interface" in the *User Guide for the Wireless LAN Solution Engine, Release 2.5*. To view the user guide from the online help, click **View PDF**.



### Note

Even if you are using your own authentication service, all users must still be in the local database of users. For information on adding users to the local database, see [Managing Users, page 8-39](#).

### Procedure

- 
- Step 1** Select **Administration > Appliance > Security > Authentication Modules**.
- Step 2** Select an authentication module from the Select Module drop down list, then click **Submit**.

- Step 3** Depending on the authentication module you selected, enter the following data, then click **Submit**:
- **RADIUS** module or **TACACS+** module:
    - 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.
  - MS NT Domain module:
    - Domain—Name of the Windows domain.
    - Primary Domain Controller and Backup Domain Controller—Names of the primary and backup Windows domain controllers. A backup domain controller is optional.
- 

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.

### Related Topics

[Overview: Authentication Modules, page 8-16](#)

## Managing SSL (HTTPS)

SSL (secure socket layer) protocol provides a secure connection between Web clients and the WLSE. When you initially install and set up the WLSE, 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, see [Unsigned Certificate Not Generated, page 8-20](#) before attempting this procedure.

---

## Procedure

- 
- Step 1** Select **Administration > Appliance > Security > SSL (HTTPS)**.
- Step 2** Click **View CSR**. The encrypted CSR is displayed.
- If the following error message appears, see [Unsigned Certificate Not Generated, page 8-20](#):
- ```
No certificate signing request was found. Please contact your administrator.
```
- 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:
- Copy it into an ASCII file on a client system.
 - On the same client, select **Administration > Security**.
 - Under SSL (HTTPS), type the path to the signed certificate or click **Browse** to locate the file, then click **Submit Certificate**.
 - To use the new certificate, you need to restart the Wireless LAN Solution Engine 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):
- Log in to the WLSE's CLI by using the console or by using Telnet or SSH.
 - Enter the following CLI command:

```
# firewall eth0 1741
```
- For more information on this command, see Appendix B in the *User Guide for the Wireless LAN Solution Engine, Release 2.5*. To view this guide from the online help, click **View PDF**.
- Step 6** To establish a connection to the WLSE 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.
-

Unsigned Certificate Not Generated

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. For information on using the **mkcert** command, see Appendix B in the *User Guide for the Wireless LAN Solution Engine, Release 2.5*. To view this guide from the online help, click **View PDF**.

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.

Procedure

- Step 1** Select **Administration > 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 take place immediately.
-

Viewing the Last 10 Logged-On Users

To view information about the last 10 users who have logged on to the WLSE:

Procedure

- Step 1** Select **Administration > 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.

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 8-22](#)).
- **Backup**—Schedule a backup of WLSE data or run an immediate backup (see [Scheduling and Running Backups, page 8-24](#)).
- **Restore**—Restore an available backup image (see [Restoring Data, page 8-26](#)).

Related Topics

[About Backup and Restore, page 8-21](#)

About Backup and Restore



Note

Backups from pre-release software cannot be restored on the FCS version.

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.

You can restore data backed up on one WLSE to another WLSE. You cannot, however, restore backup data from a WLSE 1130 to a WLSE 1105. For information on restoring from one WLSE to another, see [Copying Configuration Data from One WLSE to Another](#), page 8-27.

Specifying the Backup Location

You must set the backup location before you can run backups. The backup location must be an FTP server because the WLSE uses FTP to transfer the data.



Note

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 2000 or Windows XP Server as a Backup Location](#), page 8-24.

Procedure

-
- Step 1** Select **Administration > 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 machine.
Password	Valid password on the backup location machine.
Verify Password	
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.

Step 3 Click **Save**, or click **Erase** to clear your entries or remove the previously configured backup location.

Step 4 To verify that the backup location is reachable and is configured as an FTP server, click **Test**.

Related Topics

- [Scheduling and Running Backups, page 8-24](#)
- [Restoring Data, page 8-26](#)
- [Configuring a Windows 2000 or Windows XP Server as a Backup Location, page 8-24](#)
- [About Backup and Restore, page 8-21](#)

Configuring a Windows 2000 or Windows XP Server as a Backup Location

To serve as a backup location, a Windows 2000 or Windows XP server must be configured for UNIX directory mode.

Procedure

Step 1 On the server, select **Start > Settings > Control Panel > Administrative Tools > Internet Services Manager**.

If this option is not available on the server, first enable it as follows:

- a. Select **Start > Settings > Control Panel > Add/Remove Programs**.
- b. On the left side of the Add/Remove window, click **Add/Remove Windows Components**. The Windows Components wizard starts.
- c. 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**.

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.



Note

Normal operations continue during backup.

**Note**

You should perform a backup whenever you add users.

Procedure

-
- Step 1** Make sure the backup location has been specified (see [Specifying the Backup Location, page 8-22](#)).
- Step 2** Select **Administration > Appliance > Backup and Restore > Backup**.
- Step 3** To run an immediate backup, click **Backup Now**.
- Step 4** To schedule automatic backups:
- 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).
 - Click **Schedule Backup**.
- Step 5** To cancel a scheduled backup, click **Remove Scheduled Backup**.
- Step 6** There are several ways to verify that the backup succeeded:
- Check the log file under backup.log file under **Administration > Appliance > Status > View Log File**.
 - Select **Administration > 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 8-26](#)
- [About Backup and Restore, page 8-21](#)

Restoring Data

**Note**

The WLSE shuts down and restarts while data is being restored.

To restore the WLSE's configuration data from a backup:

Procedure

-
- Step 1** Select **Administration > Appliance > Backup and Restore > Restore**.
- 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.
 - Users' CLI access 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 8-27](#).

- Step 4** Click **Restore**. The Restore Backup window opens.
- Step 5** Click **OK**.

The Wireless LAN Solution Engine shuts down and restarts while data is being restored.

Related Topics

- [Scheduling and Running Backups, page 8-24](#)
- [Specifying the Backup Location, page 8-22](#)
- [About Backup and Restore, page 8-21](#)

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 the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine, 2.5*.

**Note**

You cannot restore a backup from a WLSE 1130 to a WLSE 1105.

-
- Step 1** Back up the data on the source WLSE. For more information, see [Backing Up and Restoring Data, page 8-21](#).
- Step 2** If you have installed a new WLSE and have not configured it yet, run the setup program and complete the initial configuration.
- For information on the setup program and initial configuration, see the *Installation and Configuration Guide for the Cisco Works Wireless LAN Solution Engine, 2.5*.
- 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 8-26](#).

Using WLSE Diagnostics Options

The options under **Administration > Appliance > Diagnostics** are:

- **WLSE Info**—Gather troubleshooting information about the WLSE status and create status reports (see [Viewing and Creating a Status Report, page 8-28](#)).
- **Self Test**—Create and display self tests (see [Viewing and Creating a Self-Test Report, page 8-29](#)).
- **Processes**—View WLSE process status, stop and start processes (see [Managing Processes, page 8-29](#)).

Viewing and Creating a Status Report

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.

Procedure

- Step 1** Select **Administration > 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 8-29](#)
- [Managing Processes, page 8-29](#)

Viewing and Creating a Self-Test Report

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.

Procedure

-
- Step 1** Select **Administration > 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 8-28](#)
- [Managing Processes, page 8-29](#)

Managing Processes

You can view the status of the major processes running on the WLSE, start and stop processes, and access complete reports.

Procedure

-
- Step 1** Select **Administration > Appliance > Diagnostics > Processes**. The Process Report displays the following information.

Column	Description
Process name	Describes how a process is registered. For information on the processes displayed, see Processes Displayed, page 8-31 .
State	Process status and a summary of the log file entries for the process.
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 8-32 .
View process status.	Click process state. See System Log, page 8-32 .
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 .

Processes Displayed

The Process Report table displays the status of the following major WLSE processes:

Process Name	Description
WirelessSvcMgr	Process that manages the internal radio management tasks.
WLSEjobvm	The job virtual machine.
WLSEFaults	The fault manager.
WebServer	The Web Server.
Tomcat	The Java servlet engine.
ExcepReporter	The process that forwards traps.
CDPbrdcast	The CDP daemon that identifies Cisco devices to their immediate neighbors.
PerfMon	The process that monitors performance.

Daemon Information

The Daemon Information dialog box displays the following:

Field	Description
Process	Process name.
Path	File location.
Flags	Flags used to register the process with the Daemon Manager.
Startup	Method used to start the process.
Dependencies	Other processes that must be running for this process to run.

System Log

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.

Procedure

-
- Step 1** Select **Administration > 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 the Time and Specifying Name Servers

The **Administration > Appliance > Time/NTP/NAME** option allows you to:

- [Set the Current Local and UTC Time, page 8-33](#)
- [Specify NTP Time Servers, page 8-34](#)
- [Specify Name Servers, page 8-34](#)

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 **Administration > Appliance > TIME/NTP/NAME**.
- Step 2** In the Current Time area, select the new time and date parameters from the lists and click **Update**.

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 **Administration > Appliance > TIME/NTP/NAME**.
- 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**.
-

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 **Administration > Appliance > TIME/NTP/NAME**.
- 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**.
-

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 Administration > 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 .
-

Using Connectivity Tools

When you select **Administration > 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 8-36](#)).
- **SNMP Query Tool**—query a device's SNMP variables (see [Using the SNMP Query Tool, page 8-37](#)).

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 **Administration > 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 8-2 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.
TCP Port Scan	Finds the active ports on a device.	Displays the active ports.
SNMP Reachable	Tries to reach a device by using SNMP . To reach a device by using SNMP, the device's credentials must be in the WLSE database. To check credentials, select Administration > 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 **Administration > 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.
-

Firmware Version Support

You can use the WLSE to upgrade and update the firmware on one or more access points, either as a scheduled operation or on demand. To accomplish this, information about supported firmware versions is stored on the WLSE. You can:

- View the versions currently supported by the WLSE.
- Update the version support on the WLSE.

The topics covered in this section are:

- [Updating Supported Firmware Versions, page 8-38](#)
- [Viewing Supported Firmware Versions, page 8-39](#)

Updating Supported Firmware Versions

When WLSE 2.5 was released, support was included for the access point firmware versions that were available at that time. The WLSE can be updated to add support for firmware versions that are released later. When support is available for newer versions, an update file will be posted on Cisco.com. You can download this file and import it into the WLSE to update versions supported by the firmware module.

**Note**

Your login determines whether you can use this option.

To import new firmware support information:

Procedure

-
- Step 1** To download the firmware version update file to your desktop or another network computer from Cisco.com, you can either:
- Enter this URL in the browser:
`www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_upgrades_and_downloads.html`
 - Navigate to **Products and Services > Network Management CiscoWorks > CiscoWorks Wireless LAN Solution Engine > Software Center**.
- The firmware version update file is listed along with the WLSE software update files.
- Step 2** Select **Administration > System > New Version Support**.
- Step 3** Enter the path to the device support file or click **Browse**.
- Step 4** Click **Import**.
- Step 5** To display the firmware versions currently supported by the WLSE, see [Viewing Supported Firmware Versions, page 8-39](#).
-

Related Topics

[Viewing Supported Firmware Versions, page 8-39](#)

Viewing Supported Firmware Versions

**Note**

Your login determines whether you can use this option.

To display firmware versions currently supported by the WLSE:

-
- Step 1** Select **Administration > System > Firmware Supported Versions**.
- Step 2** The access point firmware versions that are supported by this WLSE are displayed.
- Step 3** To import updated firmware support, see [Updating Supported Firmware Versions, page 8-38](#).
-

Related Topics

[Updating Supported Firmware Versions, page 8-38](#)

Managing Users

The options displayed when you select **Administration > User Admin** allow you to manage user roles and logins:

- [Managing Roles, page 8-40](#)—Add, modify, and delete user roles.
- [Managing User Accounts, page 8-42](#)—Add, modify, and delete user accounts.

Related Topics

[Modifying Your Profile, page 8-46](#)

[Overview: Authentication Modules, page 8-16](#)

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 8-41](#).
- About roles—See [Overview: Roles, page 8-40](#).

Overview: 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.

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 in the Software Center on Cisco.com.

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 8-42](#)). You cannot modify the privileges of this role.
- 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 Administrator role.

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 **Administration > 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 can view all roles.
- Other users can only view the roles assigned to them and any 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 A-1](#)
- [Managing User Accounts, page 8-42](#)

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:

- [Add Users, page 8-43](#)
- [Modify Users, page 8-44](#)
- [Delete Users, page 8-45](#)
- [Overview: User Accounts, page 8-42](#)

Related Topics

- [Overview: Authentication Modules, page 8-16](#)
- [Modifying Your Profile, page 8-46](#)
- [Appendix A, “Naming Guidelines”](#)

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—Limited access to viewing basic WLSE configuration.
- 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 when the setup script is run. 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.

Add Users



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Administration > User Admin > Manage Users**. The Users list displays the current users.
- The admin user can view and modify all existing users.
 - 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:

Field	Information to Enter
User Name	Name of the new user.
User Password	Password for the new user.
Confirm Password	
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 subset of commands. ¹
Roles	One or more roles for the user. 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 B in the *User Guide for the Wireless LAN Solution Engine, Release 2.5*

- 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**.

Related Topics

- [Modifying Your Profile, page 8-46](#)
- [Appendix A, “Naming Guidelines”](#)

Modify Users



Note

Your login determines whether you can use these options.

Procedure

To modify a user:

- Step 1** Select **Administration > User Admin > Add/Modify/Delete**. The Users list displays the current users.



Note

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. The admin user can view all logins.

- Step 2** Select the user from the Users list and make the desired changes:

Field	Information to Enter
User Name	User's name.
User Password	New password for user.
Confirm Password	
Email	Enter or change the user's email address.

Field	Information to Enter
CLI Access	User's access to the WLSE CLI : None, Level 0, or Level 15. By default, Level 15 is selected for System Administrator, 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 available for each privilege level, see the <i>User Guide for the Wireless LAN Solution Engine, Release 2.5</i> —From the online help, click View PDF .
Roles	User's roles. 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 A-1](#)
- [Managing Roles, page 8-40](#)
- [Modifying Your Profile, page 8-46](#)

Delete Users

Use the following procedure to delete users.



Caution

If a user is deleted, all the users created by the deleted user are also removed. For example, if userA creates userB and then userA is deleted, userB is also deleted.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > 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 8-46](#).
- Change your email address—See [Changing Your Email Address, page 8-47](#).
- Set your home page preferences—See [Changing the Default Tab and Subtab, page 8-47](#).

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 **Administration > 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 A-1](#).
- Step 3** Click **Apply** to save your changes or **Reset** to discard your changes.
-

Related Topics

- [Modify Users, page 8-44](#)
- [Naming Guidelines, page A-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 **Administration > 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

- [Modify Users, page 8-44](#)

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 **Administration > 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 ACS, or to another WLSE.

There is one preconfigured link for running the ACS Failed Login Report, which generates a report on failed logins on an ACS server. For more information, see [Running the ACS Failed Login Report, page 8-49](#).



Note

This feature is available to all users.

Procedure

Step 1 Select **Administration > 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**.
- Step 5** To activate a link and connect to the other system, click the link name in the left pane.
- Step 6** To configure the ACS Failed Login Report link, click **Edit** under ACS Failed Login Report and enter the following information:

Field	Description
URL	URL of the ACS server.
Username	Administrator username created when ACS software was installed on the ACS server.
Password	Password for the administrator username.

- Step 7** Click **Save**.

Running the ACS Failed Login Report

The ACS failed login report shows failed logins on a specified Cisco Access Control Server (ACS).

To configure the link for an ACS failed login report:

- Step 1** Select **Administration > Links**.
- Step 2** Under ACS Failed Login Report in the left panel, click **Edit**.
- Step 3** Enter the following information:
- The URL of the ACS server.
 - The username of a user on the ACS server.
 - The password of the user.
- Step 4** Click **Save**.

Step 5 To run the ACS failed login report on a server, click the link name.



Managing the WLSE via the CLI

This chapter describes the major system administration tasks that you can perform by using the command line interface (CLI). These tasks are for both WLSE 1105 and WLSE 1130. For details on all CLI commands, see [Appendix B, “Using the Command Line Interface \(CLI\).”](#)



Note

For administrative tasks performed from the Web interface, see the WLSE online help or the preceding chapters in this guide.

This chapter contains the following topics:

- [Logging In and Out via CLI, page 9-2](#)
- [User Management via CLI, page 9-3](#)
- [Backing Up and Restoring via CLI, page 9-5](#)
- [Upgrading WLSE Software via CLI, page 9-10](#)
- [Shutting Down and Powering Off the WLSE, page 9-11](#)
- [Rebooting the WLSE via CLI, page 9-11](#)
- [Setting WLSE System Date and Time, page 9-12](#)
- [Configuring Ethernet Interfaces, page 9-14](#)
- [Administering Management Services via CLI, page 9-16](#)
- [Viewing System Information via CLI, page 9-17](#)
- [Recovery Management, page 9-18](#)

Logging In and Out via CLI

Use the following commands to log in and out of the WLSE.

Logging In

To use the CLI to log in:

Step 1 Attach a console or connect via Telnet or SSH to the WLSE.

If you are using a console, make sure you are attaching it to the correct port:

- For the WLSE 1105, use the serial port on the front panel; do not use the serial port on the back panel as the console port.
- For the WLSE 1130, use the serial port on the back panel as the console port.

For more information about the location of the serial ports and connecting to them, see the *Installation and Configuration Guide for the Wireless LAN Solution Engine, Release 2.5* for CiscoWorks 1130 information or the *Quick Start Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*.

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 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 9-3](#). For information on setting CLI privileges via the Web interface, see [Managing User Accounts, page 8-42](#).

Logging Out

To log out, use the **exit** command.

User Management via CLI

This section contains the following topics:

- [Managing User Accounts, page 9-3](#)
- [Setting Up TACACS+ or RADIUS Authentication for CLI Login, page 9-4](#)

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

To create or modify user accounts:

-
- Step 1** Log in. For more information, see [Logging In and Out via CLI, page 9-2](#).
- Step 2** Enter 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.
  - *password* is the user's password.
  - **privilege 0** allows access to a subset of the CLI commands (see [Privilege Level 0 Commands, page B-10](#)). This is the default and is assigned to the account even if you omit this argument.
  - **privilege 15** allows access to all CLI commands.
- Step 3** 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 8-42](#) 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 9-3](#).

To set up the WLSE's RADIUS module, enter the following command:

```
auth cli 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 tacacs secret server
```

where *secret* is the shared secret and *server* is the hostname or IP address of the authentication server.

For more information about using alternative authentication, see [auth, page B-17](#), and [Overview: Authentication Modules, page 8-16](#).

# 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 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.

**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 9-8](#).

**Note**

You can restore a backup made on one WLSE to another WLSE. For information, see [Copying Configuration Data to another WLSE, page 9-10](#).

## Setting Up the Backup Location

Before backing up, you must specify an FTP server as the backup location.

### Specifying the Backup Location

To specify the backup location:

---

**Step 1** Log in. For more information, see [Logging In and Out via CLI, page 9-2](#).

**Step 2** Enter the following command:

**backupconfig** *hostname username password 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.
- *directory* is the pathname of the backup directory, if different from user's default directory.

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 8-21](#).

**Note**

---

WLSE operations continue during the backup.

---

To back up the WLSE:

- 
- Step 1** Log in. For more information, see [Logging In and Out via CLI, page 9-2](#).
- Step 2** Make sure the backup location has been configured. See [Setting Up the Backup Location, page 9-6](#).
- Step 3** To test the availability of the backup location enter:
- ```
backup test
```
- Step 4** 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

**Note**

---

The WLSE shuts down during the restore operation and reboots afterwards.

---

To restore the WLSE configuration:

- 
- Step 1** Log in. For more information, see [Logging In and Out via CLI, page 9-2](#).
- 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 users' CLI privileges.

For information about restoring from WLSE to another, see:

- [Installing a Replacement WLSE, page 9-8](#)
- [Copying Configuration Data to another WLSE, page 9-10](#)

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, page 9-10](#).

Removing the Old WLSE

Before removing the old WLSE:

- Step 1** Log in to the old WLSE. For more information, see [Logging In and Out via CLI, page 9-2](#).
- Step 2** 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 3** Back up the data from the old WLSE. See [Backing Up and Restoring via CLI, page 9-5](#) for details.
- Step 4** Enter the following command:
- ```
shutdown
```
- Step 5** Power down and remove the old system.
-

Installing the Replacement WLSE

To install the replacement WLSE:

-
- Step 1** Install and power on the new WLSE, using the instructions in the *Installation and Configuration Guide for the Wireless LAN Solution Engine, Release 2.5*.
- Step 2** 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
```
- Step 3** 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
```
-

Copying Configuration Data to another WLSE

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 9-8](#).



Note

You cannot restore a backup from a WLSE 1130 to a WLSE 1105.

-
- Step 1** Back up the data on the original WLSE. For more information, see [Backing Up and Restoring via CLI, page 9-5](#).
- Step 2** If you have installed a new WLSE and have not configured it yet, run the setup program and complete the configuration.
- For information on the setup program and additional configuration steps, use the *Installation and Configuration Guide for the Wireless LAN Solution Engine, Release 2.5*.
- 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 *Installation and Configuration Guide for the Wireless LAN Solution Engine, Release 2.5*.

Rebooting the WLSE via CLI

Rebooting the system restarts its management services, even if the services were stopped prior to the reboot.

To restart the WLSE:

Step 1 Log in. See [Logging In and Out via CLI, page 9-2](#).

Step 2 Enter the following command:

reload

You are prompted to verify the reload. Enter **yes** to confirm or **no** to cancel the reload.



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.

Shutting Down and Powering Off the WLSE



Caution

If you power off the WLSE improperly, you might disable the system.

To shut down the WLSE:

Step 1 Log in. See [Logging In and Out via CLI, page 9-2](#).

Step 2 Enter the following command:

shutdown

Step 3 Power off the WLSE.

Setting WLSE System Date and Time

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, page 9-12](#) (the recommended method).
- [Setting the System Clock Manually, page 9-13](#).

**Note**

You can set the current local (browser) time on the Web interface. For information, see the online help or the *Installation and Configuration Guide for the Wireless LAN Solution Engine, Release 2.5*.

To display the system time, use the **show clock** command. For more information on this command, see [show clock, page B-11](#).

Setting the System Clock Using NTP

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, page 9-13](#).

To specify NTP servers:

Step 1 Log in. See [Logging In and Out via CLI, page 9-2](#).

Step 2 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:

-
- Step 1** Log in. See [Logging In and Out via CLI, page 9-21](#)
- Step 2** 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

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 to manually.

To set the date and time manually:

- 
- Step 1** Log in. See [Logging In and Out via CLI, page 9-2](#).
- 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).
- 

For more information about the **clock** command, see [show clock, page B-11](#).

# Configuring Ethernet Interfaces

The WLSE 1105 uses 10/100 Mbps Ethernet connectors. The WLSE 1130 uses 10/100/1000 Mbps Ethernet connectors. The Ethernet 0 interface is configured during initial setup of the WLSE, and all protocols are enabled on the Ethernet 0 interface.

**Note**

The Ethernet interface labeled “A” on the WLSE 1130 back panel corresponds to Ethernet 0 in software (such as CLI commands). The Ethernet interface labeled “B” corresponds to Ethernet 1 in software.

This section contains the following topics:

- [Configuring Protocols on Ethernet Interfaces, page 9-14.](#)
- [Configuring Interface Parameters, page 9-15.](#)
- [Managing Devices on Both Interfaces, page 9-15.](#)

## Configuring Protocols on Ethernet Interfaces

All protocols are enabled by default on the Ethernet 0 interface. On the Ethernet 1 interface of the WLSE 1130, 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

To allow or prevent protocols on an Ethernet interface:

---

**Step 1** Log in. See [Logging In and Out via CLI, page 9-2.](#)



**Step 2** To allow CDP on an interface, enter the following command:

```
cdp run port
```

where *port* is the Ethernet interface, either eth0 or eth1.

To disable CDP, enter the following command:

```
no cdp run port
```

For more information on this command, see [cdp](#), page B-20.

**Step 3** To allow or prevent any of the other protocols on an interface, use the **firewall** command. For information on this command, see [firewall](#), page B-25.

---

## Configuring Interface Parameters

To enable or disable Ethernet interfaces and set parameters on the interfaces (IP address, gateway information, speed, half/full duplex), use the following command.

```
interface eth[ernet][0-5] {[up | down] | ipaddress netmask
[default-gateway address] [up | down] }
[auto | speed [10 | 100 | 1000]] duplex [half | full]
mtu [46-1500]
```

For detailed information on this command, see [interface](#), page B-31.

## Managing Devices on Both Interfaces

The Ethernet 0 interface is configured by the setup program during initial setup of the WLSE. 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 9-14.
- Configure Ethernet 1 interface parameters—See [Configuring Interface Parameters](#), page 9-15.

- Use the following command to configure a static route to the default gateway for the Ethernet 1 interface to reach the networks connected to the Ethernet 1 interface:

```
route { network address } netmask { network netmask }
 gateway { gateway address }
```

If you do not configure the static route, the WLSE will use only the default gateway configured on the Ethernet 0 interface and will be unable to manage the devices on the networks connected to the Ethernet 1 interface. For more information on the **route** command, see [route](#), page B-49.

## 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.

To specify a mail server:

- 
- Step 1** Log in as the admin user.
- Step 2** Enter the following command:

```
mailroute server
```

where *server* is the IP address or hostname of the 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.

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, use the following CLI commands.

**Table 9-1** Commands for Viewing System Information

| Command                  | Information Displayed                              |
|--------------------------|----------------------------------------------------|
| <b>show anilog</b>       | ANI log                                            |
| <b>show auth-cli</b>     | Type of authentication used for secure CLI access  |
| <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 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 collectorlog</b> | Collector log                                      |
| <b>show config</b>       | System configuration                               |
| <b>show daemonslog</b>   | Daemons log                                        |
| <b>show dmgtldlog</b>    | Daemon manager log                                 |
| <b>show import</b>       | Imported hosts file                                |
| <b>show install logs</b> | Software updates and images in the repository      |
| <b>show ipchains</b>     | IP chains for Ethernet interface                   |
| <b>show hosts</b>        | System hosts file                                  |

**Table 9-1** *Commands for Viewing System Information (continued)*

| Command                     | Information Displayed                             |
|-----------------------------|---------------------------------------------------|
| <b>show maillog</b>         | Email log                                         |
| <b>show process</b>         | Statistics for active processes                   |
| <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-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 tomcatlog</b>       | Tomcat log                                        |
| <b>show telnetenable</b>    | Telnet status                                     |
| <b>show webaccesslog</b>    | Web access log                                    |
| <b>show weberror log</b>    | Web error log                                     |
| <b>show websslaccesslog</b> | Web SSL log                                       |

## Recovery Management

Use the following procedures to recover from problems:

- [Erasing System Configuration and Resetting to Factory Defaults, page 9-19](#)
- [Using the Maintenance Image, page 9-19.](#)
- [Reimaging the WLSE, page 9-21.](#)
- [Using the Rescue Image, page 9-22](#)
- [Recovering from the Loss of All Administrator Passwords, page 9-23](#)

## Erasing System Configuration and Resetting to Factory Defaults

To erase the system configuration and reset the WLSE to factory default:

**Step 1** Log in as the admin user.

**Step 2** Enter the following command. This command resets the WLSE to factory defaults, but leaves the database and logs in place.

```
erase config
```



**Note** This command stops and restarts system services.

**Step 3** To purge the database, enter the following command:

```
reinitdb
```



**Note** This command stops and restarts system services.



**Note** After the system reboots, you must reconfigure the system using the setup program, as described in the *Installation and Configuration Guide for the Wireless LAN Solution Engine, Release 2.5*.

## 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 9-23.
  - Perform disk filesystem integrity checks or recover from filesystem corruption. See [fsck](#), page B-79.

## 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's console port, and log on as **admin**.
- For the WLSE 1105, use the serial port on the front panel; do not use the serial port on the back panel as a console port.
  - For the WLSE 1130, the serial/console port is on the back panel.
- Step 2** 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 cannot log in because you have lost all user account passwords.
- Step 3** When the `LIL0 boot :` prompt appears, press the Tab key.
- Step 4** When the `boot :` prompt appears, enter:  

```
CiscoBreR
```
- Step 5** 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, page 9-21](#)) or boot from the rescue image (see [Using the Rescue Image, page 9-22](#)).

## Reimaging the WLSE

**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 9-7](#).

To reimage your WLSE, perform the following steps:

- 
- Step 1** Connect a console to the WLSE's serial port.
- For the WLSE 1105, use the serial port on the front panel; do not use the serial port on the back panel as a console port.
  - For the WLSE 1130, the serial/console port is on the back panel.
- 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. For the location of the CD drive, see the *Installation and Configuration Guide for the Wireless LAN Solution Engine, Release 2.5* for the WLSE 1130 or the *Quick Start Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*.
- Step 4** Enter the following command. The WLSE will reboot.
- ```
reload
```

Step 5 At the following prompt, enter **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 9-22](#).

Do you wish to continue (Yes/[No]/Rescue) **yes**

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.

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 9-19](#).

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 to the WLSE's serial port.

- For the WLSE 1105, use the serial port on the front panel; do not use the serial port on the back panel as a console port.
- For the WLSE 1130, the serial/console port is on the back panel.

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.

- For the location of the WLSE 1130 CD drive, see the *Installation and Configuration Guide for the Wireless LAN Solution Engine, Release 2.5* for the WLSE 1130.
- For the location of the WLSE 1105 CD drive, see the *Quick Start Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*.

Step 4 Enter the following command. The WLSE will reboot.

```
reload
```

Step 5 At the following prompt, enter **rescue**. The WLSE will reboot.

```
Do you wish to continue (yes/[no]/rescue):
```

Step 6 After the WLSE comes up, the setup login prompt appears. Configure the system from the setup program, as described in the *Installation and Configuration Guide for the Wireless LAN Solution Engine, Release 2.5*.

Recovering from the Loss of All Administrator Passwords

If you cannot log on to the system and perform administrative tasks, perform the following procedure:

- [Recovering on a WLSE 1130, page 9-23](#)
- [Recovering on a WLSE 1105, page 9-24](#)

Recovering on a WLSE 1130

To recover from the loss of all administrator passwords:

Step 1 Connect a console to the console port on the back panel.

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 and Up Arrow and Down Arrow keys to select **1** to boot into CiscoBreR and press Enter. The following prompt appears:

```
[root@CiscoMaintImage/]#
```

- Step 4** Enter the following command. This erases the WLSE's configuration, returns the WLSE to factory defaults, and reloads the WLSE.

```
[root@CiscoMaintImage/]# erase config
```

- Step 5** After the WLSE starts up, the setup login prompt appears. Use the setup program to configure the system. This allows you to add a password for the admin user.

Recovering on a WLSE 1105

To recover from the loss of all administrator passwords:

- Step 1** Connect a console to the serial port on the front panel; do not use the serial port on the back panel as a console port.

- Step 2** Put the recovery CD in the CD drive.

- Step 3** Enter the following command:

```
reload
```

- Step 4** When the “Yes/No/Rescue/Reboot” option appears, enter:

```
rescue
```

- Step 5** When the shell prompt appears, enter:

```
erase config
```

This command erases the WLSE's configuration.

- Step 6** When the “Yes/No/Rescue/Reboot” option appears, enter:

```
reboot
```

After the WLSE starts up, a long prompt appears:

```
localhostlogin:
```

- Step 7** Log in as the user “setup” and configure the system. This allows you to add a password for the admin user.

For more information about setup, see the *Installation and Configuration Guide for the Wireless LAN Solution Engine, Release 2.5*.



FAQs and Troubleshooting

This chapter provides troubleshooting and FAQs for WLSE software.



Note For the most up to date FAQs and troubleshooting information, see the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.5* on Cisco.com.

This chapter provides the following frequently asked questions and troubleshooting information:

- General Questions—See [General FAQs and Troubleshooting, page 10-2](#)
- Faults Tab—[Faults FAQs and Troubleshooting, page 10-11](#)
- Devices Tab—[Devices FAQs and Troubleshooting, page 10-14](#)
- Configuration Tab—[Configuration FAQs and Troubleshooting, page 10-19](#)
- Firmware Tab—[Firmware FAQs and Troubleshooting, page 10-23](#)
- Reports Tab—[Reports FAQs and Troubleshooting, page 10-30](#)
- Radio Manager Tab—[Radio Manager FAQs and Troubleshooting, page 10-34](#)
- Administration Tab—[Administration FAQs and Troubleshooting, page 10-39](#)

General FAQs and Troubleshooting

- [General FAQs, page 10-2](#)
- [General Troubleshooting, page 10-3](#)

General FAQs

- [Can several users be logged on and managing the same access point at once?](#)
 - [What ports and protocols does the WLSE use?](#)
 - [Can I use a different HTTP port to manage the access point?](#)
 - [Is Telnet enabled or disabled by default on the WLSE?](#)
 - [Can SSH be disabled?, page 10-3](#)
 - [Can I run a job to convert a number of access points from non-IOS to IOS?](#)
- Q.** Can several users be logged on and managing the same access point at once?
- A.** Yes, several users can view data and reports on the same access point. More than one user can create configuration and firmware update jobs for the same access point and these will be run in the order they are scheduled. Configuration templates may be modified by more than one user at the same time and the last write will overwrite the others.
- Q.** What ports and protocols does the WLSE use?
- A.** For discovery and fault monitoring, the WLSE primarily uses SNMP (UDP port 161). For applying configuration changes, the WLSE uses SNMP, HTTP (TCP port 80 or as configured), and TFTP (UDP port 69).
- Q.** Can I use a different HTTP port to manage the access point?
- A.** Yes, the HTTP port can be changed on the access point. The change will be reflected in WLSE after the next inventory cycle, or if you choose to run inventory now for the devices on which HTTP port was changed. This is assuming the inventory is done by SNMP and not HTTP.
- Q.** Is Telnet enabled or disabled by default on the WLSE?
- A.** Telnet is disabled by default for security reasons. SSH is enabled by default.

Q. Can SSH be disabled?

A. It cannot be disabled on the WLSE itself, but you can use the firewall command to deny all SSH connections. For example, the following CLI command will cause the WLSE to reject all incoming SSH connections on the Ethernet 0 interface but allows connections through other protocols and other ports:

```
firewall ethernet0 private firewall ethernet0 private ssh
```

Q. Can I run a job to convert a number of access points from non-IOS to IOS?

A. Yes, you can run a firmware job, using a special IOS upgrade image that is available on Cisco.com. For more information, see the firmware upgrade information in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*.

General Troubleshooting

This section provides the following troubleshooting information:

- After the WLSE reboots, the login screen appears, followed by an Internal Server Error message.
- A search for an access point using APs Based on Client IP, displays the following message, “search yielded no results.”
- When I try to access an access point web page through the WLSE, the following error message appears: Action Cancelled.
- Cannot recover after incorrect setup program entry.
- Cannot log into the system.
- Cannot log in as a system administrator.
- After the WLSE starts up, the setup login prompt appears. The WLSE cannot connect to the network.
- Cannot connect to the WLSE using a Web browser.
- The system time or date is incorrect.
- The system cannot boot from the hard drive during a reboot.

Symptom After the WLSE reboots, the login screen appears, followed by an Internal Server Error message.

Possible Cause The servlet engine in the WLSE is starting up.

Recommended Action Wait for 20 to 30 seconds, then log in again.

Symptom A search for an access point using APs Based on Client IP, displays the following message, “search yielded no results.”

Possible Cause The device you are searching for is an IOS device. This type of search only works for non-IOS devices.

Recommended Action None.

Symptom When I try to access an access point web page through the WLSE, the following error message appears: Action Cancelled.

Possible Cause The SNMP user on the access point does not have enough rights.

Recommended Action Log in to the access point web interface, select Setup > Security > User Information, and make sure that the user corresponding to the SNMP community (which is set up in the WLSE under Discovery > Device Credentials) has been granted rights for the following: firmware, admin, and snmp.

Symptom Cannot recover after incorrect setup program entry.

Possible Cause You entered incorrect text during the initial setup and want to fix the entry.

Recommended Action Exit setup by pressing **Ctrl-c**. Then run **erase config** to remove the incorrect installation information and rerun the setup program. If you use the erase config command to erase the previous WLSE configuration, and run the setup program again, you will be required to get a new certificate. Use the **mkcert** command or Administration > Appliance > Security > SSL (HTTPS).

Symptom Cannot log into the system.

Possible Cause You did not run the setup program to create an initial system configuration or you lost all the user account passwords.

Recommended Action

1. Did you run the setup program after booting the system for the first time?
If no, run the setup program.
If yes, continue to the next step.
2. Do you know the password for any system user accounts?
If no, see [Cannot log in as a system administrator., page 10-5](#).
If yes, continue to the next step.
3. If you are certain you entered a valid username and password, contact Cisco's Technical Assistance Center for assistance.

Symptom Cannot log in as a system administrator.

Possible Cause All administrator passwords have been lost.

Recommended Action Perform the following procedure:

1. Connect a console to the WLSE's console port.
For the WLSE 1105, use the serial port on the front panel; do not use the serial port on the back panel as a console port.
For the WLSE 1130, the serial/console port is on the back panel.
2. Power the system off, then power it back on. The following prompt appears:

`LIL0 boot:`
3. Press the Tab key. The following prompt appears:

`boot:`
4. Enter the following command. This puts the WLSE in maintenance image mode.

```
CiscoBreR  
[root@CiscoMaintImage/]#
```

5. Enter the following command. This erases the WLSE's configuration, returns the WLSE to factory defaults, and reloads the WLSE.

```
[root@CiscoMaintImage/]# erase config
```

Symptom After the WLSE starts up, the setup login prompt appears. The WLSE cannot connect to the network.

Possible Cause

- The network cable is not connected to the Ethernet 0 port.
- The Ethernet 0 interface is disabled or misconfigured.
- The system is configured correctly, but the network is down or misconfigured.
- DNS is misconfigured. Ping commands will result in a 50-70% failure rate in Pings from the WLSE (Web interface and CLI).

Recommended Action

1. Verify that the network cable is connected to the Ethernet 0 port and the Ethernet indicator is lit.
 - If the network cable is not connected, connect it.
 - If the network cable is connected but the Ethernet indicator is not lit, these are the probable causes:
 - The network cable is faulty.
 - The network cable is the wrong type (for example, a cross-over type, rather than the required straight-through type).
 - The port on the default gateway to which the system connects is down.
 - If the network cable is connected and the Ethernet indicator is on but the system cannot connect to the network, continue to the next step.
2. Use the **ping** command to perform the following tests:
 - Try to ping a well-known host on the network. A DNS server is a good target host.

If the ping command gets a response, the system is connected to the network. If the system cannot connect to a particular host, the problem is either with the network configuration or that host. Contact your network administrator for assistance.

If the ping command does not get a response, continue.

- Attempt to connect to another host on the same subnet as the system.

If the ping command can connect to a host on the same subnet, but cannot connect to a host on a different subnet, the default gateway is probably down.

If the ping command cannot connect to any hosts, continue to the next step.

3. Use the **show interfaces** command to determine if the Ethernet 0 interface is disabled or misconfigured.

For more information on the **show interfaces** command, see the CLI appendix in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

If the Ethernet 0 interface is disabled, enable it. If it is misconfigured, configure it correctly. For more information, see the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine*.

If the interface is enabled and correctly configured, continue to the next step.

4. Contact your network administrator to verify that there are no conditions on the network that prevent the system from connecting to the network.

If conditions prevent the system from connecting to the network, have your network administrator correct them.

5. If no conditions are preventing the system from connecting to the network, contact Cisco's Technical Assistance Center.

Symptom Cannot connect to the WLSE using a Web browser.

Possible Cause

- The system cannot connect to the network.
- HTTP or HTTPS is not enabled

- If connecting via HTTP, the IP address was not appended with **:1741**.
- The client system is not configured.

Recommended Action

1. Make sure that the system can connect to the network. Attempt to connect the system using a Web browser.
If you cannot connect, continue.
2. If you are attempting to connect via HTTP, verify that the IP address is appended with **:1741**.
3. If you are attempting to connect via HTTP, verify that HTTP is enabled. If you are attempting to connect via HTTPS, verify that HTTPS is enabled. For more information, see the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine*.
4. Verify that the browser is configured correctly, and attempt to connect to the WLSE. For more information, see these *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine*. If you cannot connect, continue to step 5.
5. At the system console, or through Telnet, verify that the Web Server and tomcat are running by entering the following:

```
# services status
```

If they are running, go to step 7. If they are not running continue to step 6.

6. Stop the system services by entering the following:

```
# services stop
```
7. Restart the system services by entering the following:

```
# services start
```
8. Try to connect the system using a Web browser.
If you cannot connect, continue to the next step.
9. Reboot the system by entering the **reload** command.

For more information on the **reload** command, see the CLI appendix in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

- d. If you still cannot connect to the system using a Web browser, contact Cisco's Technical Assistance Center for assistance.

Symptom The system time or date is incorrect.

Possible Cause

- NTP is misconfigured.
- The system clock is set incorrectly.

Recommended Action Make sure NTP is configured correctly and that the system clock is set correctly.

For information about maintaining the system time and date, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

Symptom The system cannot boot from the hard drive during a reboot.

Possible Cause

- The disk has a physical error.
- The disk image is corrupted.

Recommended Action If the WLSE cannot boot from the hard drive, the hard drive needs to be reimaged. Use the Recovery CD to reimage your WLSE. For more information, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

Symptom Cannot connect to system with Telnet or Telnet interaction is slow.

Possible Cause

- Telnet is disabled or configured incorrectly.
- The WLSE cannot recognize host names.

If you are not using name recognition, slow or non-existent telnet interaction is an expected problem.



Note Telnet is disabled by default. SSH is enabled by default.

Recommended Action

If the problem is not the network, perform the following steps. Connect to the console port if you cannot Telnet to the WLSE.

1. Check the Telnet settings to be sure Telnet is enabled and configured correctly. For more information, see the following

To check the Telnet settings, or to enable or disable Telnet on specific domains or IP addresses, use the **telnetenable** CLI command. [For more information on this command, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help](#)

To enable or disable Telnet on individual ports, use the **firewall** CLI command. [For more information on this command, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help](#)
2. If you have specified hosts using the **telnetenable** CLI command, make sure the host from which you are attempting to Telnet is on the list.
3. If you are using a DNS server, perform the following step:

Configure the system to use a functioning DNS server by entering:

```
# ip name-server ip-address
```

where *ip-address* is the IP address of the DNS server.

If you are using the import CLI command, proceed to the next step.

4. Verify that the system can get DNS services from the network by entering the following command:

```
# nslookup dns-name {hostname | ip-address}
```

where *dns-name* is the DNS name of a host on the network that is registered in DNS and *hostname* and *ip-address* is the same IP address specified in 2. The command returns the IP address of the host.

5. If the system cannot resolve DNS names to IP addresses, the DNS server it is using is not working properly.

Resolve the network DNS problem, then continue.

6. If you are using the **import** CLI command to resolve host names, verify that the WLSE can resolve host names by entering the following command:

```
ping hostname
```

where *hostname* is a host name that has been mapped to an IP address, or imported in a host file, using the **import** command.

7. If the system can resolve DNS names to IP addresses but you still cannot connect to the system using Telnet, or Telnet interaction with the system is extremely slow, contact Cisco's Technical Assistance Center.

Faults FAQs and Troubleshooting



Note

For an explanation of the faults displayed under **Faults > Display Faults**, see the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.5* on Cisco.com.

- [Faults FAQs, page 10-12](#)
- [Faults Troubleshooting, page 10-13](#)

Faults FAQs

- Does acknowledging a fault clear it?
- What traps are sent from the WLSE?
- What trap types are forwarded by the WLSE?
- Does a MIB or trap definition file exist for the WLSE?
- What information is emailed in a fault notification?

Q. Does acknowledging a fault clear it?

A. No, it only removes it from the Active list. For a description of fault states, see the information on understanding fault states in the online help.

Q. What traps are sent from the WLSE?

A. Traps are sent based on fault policy and threshold settings on the WLSE. The WLSE only sends out v2c traps, so make sure your trap listener is configured to accept v2c traps.

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

Q. What trap types are forwarded by the WLSE?

A. No traps are forwarded from other devices.

Q. What information is emailed in a fault notification?

A. For a description see the online help.

Q. Does a MIB or trap definition file exist for the WLSE?

A. Yes, from the Cisco.com download site, download MIB CISCO-DEVICE-EXCEPTION-REPORTING-MIB.my and load it into the trap receiver.

Faults Troubleshooting

- The Display Fault view is blank.
- Email fails to arrive at its destination.
- No VLAN fault information is displayed for IOS access points.

Symptom The Display Fault view is blank.

Possible Cause There are no faults to report based on the filtering criteria you entered.

Recommended Action Not applicable.

Symptom Email fails to arrive at its destination.

Possible Cause The SMTP server is not configured properly.

Recommended Action Configure the SMTP server by selecting Administration > Appliance > Configure Mailroute.

Symptom No VLAN fault information is displayed for IOS access points.

Possible Cause WEP keys have not been configured in each VLAN. When the WEP keys are configured in the IOS access points, VLAN information is accessible by SNMP.

Recommended Action Configure the WEP keys for the corresponding VLAN.

Devices FAQs and Troubleshooting

- [Devices FAQs, page 10-14](#)
- [Devices Troubleshooting, page 10-15](#)

Devices FAQs

- [Why is hostname \(device name\), sysContact, and sysLocation information not updated in the WLSE after I change these parameters on the access point?](#)
 - [What is an invalid CDP seed?](#)
 - [Can I discover devices if CDP is disabled?](#)
 - [What are the extra inventories listed in the Run Now folder?](#)
 - [What are the results of adding or removing an interface from an access point?](#)
- Q.** Why is hostname (device name), sysContact, and sysLocation information not updated in the WLSE after I change these parameters on the access point?
- A.** The hostname (device name), sysContact, and sysLocation parameters are updated during discovery, not during inventory. Make sure you schedule a periodic discovery under Administration > Discover > Scheduled Discovery.
- Q.** What is an invalid CDP seed?
- A.** An invalid seed is a device that does not run Cisco Discovery Protocol (CDP), such as a PC or workstation). Such a device does not function as a seed because it does not allow the WLSE to traverse the network and find other devices. In the discovery run log, invalid seeds are shown as SNMP unreachable.
- Q.** Can I discover devices if CDP is disabled?
- A.** If CDP is disabled on network devices, you can still discover access points by entering the IP addresses of all of them on the WLSE as seed values. However, the WLSE cannot discover switches directly attached to such access points, and switch-related reports will be empty.
- Q.** What are the extra inventories listed in the Run Now folder?
- A.** The radio management module runs periodic immediate inventories.

- Q.** What are the results of adding or removing an interface from an access point?
- A.** If you physically remove an interface (for example, removing 11b from a dual-interface AP 1200), the WLSE will automatically detect the change during the next inventory cycle. If you physically *add* an interface, you must delete the device and rediscover it. Otherwise, the inventory data might be invalid.

Devices Troubleshooting

This section contains the following troubleshooting information:

- [Devices were discovered but are not displayed in the GUI; for example, in Reports.](#)
- [There is a time discrepancy in the scheduled discovery jobs.](#)
- [Devices are placed in Misconfigured Devices group after discovery.](#)
- [The SNMP Query Authorization Exception is recorded in the discovery log.](#)
- [Frequent client inventories are causing too much network traffic or degrading WLSE performance.](#)
- [Inventory is taking longer than expected and a message about no logs available appears in the inventory log.](#)

Symptom Devices were discovered but are not displayed in the GUI; for example, in Reports.

Possible Cause The devices have not been moved to the Managed state.

Recommended Action Select Administration > Discover > Managed Devices. Move the devices from New or Unmanaged to Managed.

Intermediate switches with no access points directly connected to them are shown to be discovered in the Administration > Tasks History > Discovery logs but will not show up in Administration > Discover > Managed Devices > Manage/Unmanage.

Symptom There is a time discrepancy in the scheduled discovery jobs.

Possible Cause The local or system time is not set correctly on the WLSE.

Recommended Action

- a. Reset the WLSE system time (UTC) using CLI commands as follows:
 Enter **services stop** to stop services.
 Enter the **clock** command to reset the time.
 Enter **services start** to restart the services.
- b. Set the local browser time. Select Administration > Appliance > Time/NTP/Name.

Symptom Devices are placed in Misconfigured Devices group after discovery.

Possible Cause IOS devices are not configured correctly with an ISO view. The dot11mib fault appears for these devices.

Recommended Action Perform the following tasks on the devices and the WLSE. Either configure the devices individually or create a configuration template with the relevant custom values and create a job for the devices.

To configure devices individually:

- a. Use Telnet or SSH to log in to the device, then enter enable mode.
- b. In global configuration mode, enter the following commands in sequence:

```
# snmp-server view iso iso included
# snmp-server community community_string view iso RO
```

where *community_string* is the device's read-only community string. This is the same string that should exist in the WLSE's SNMP credentials screen (Devices > Discover > Device Credentials > SNMP Communities). If it is not entered there, see the following instructions for entering device credentials in the WLSE.

- c. Exit from the global configuration mode, and enter the following command:
- ```
write memory
```

To configure devices by using a template:

- a. Use the procedures in the configuration template instructions in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine*, 2.5 to create a template.
- b. Enter the following custom values in the template:

```
snmp-server view iso iso included
snmp-server community community_string view iso RO
```

Run a configuration job on the devices in the Misconfigured Devices group:

Select the template created in the previous step.

Either select the Misconfigured Devices group or the devices in the group.

Schedule the job to run at the desired time.

- c. After the configuration job finishes successfully, the dot11 mib fault will be cleared after the next discovery cycle. You can run a manual discovery immediately after the configuration job finishes; select Devices > Discover > Run Inventory > Run Now.

– Perform the following steps on the WLSE:

- a. If the device's ISO community string has not been entered on the WLSE, select Devices > Discover > Device Credentials > SNMP Communities. Then, enter the same community strings that you configured on the devices in the previous procedure.

Otherwise, the devices will be placed back in the Misconfigured Devices group after the next discovery cycle.

- b. Rediscover the devices by using them as seed devices in an immediate discovery. Select Devices > Discover > Run Inventory > Run Now. For more information on discovery, see the online help discovery section or the *User Guide for the CiscoWorks Wireless LAN Solution Engine*, Release 2.5.

**Symptom** The SNMP Query Authorization Exception is recorded in the discovery log.

**Possible Cause** The community string on the access point does not have admin and firmware rights.

**Recommended Action** In the configuration template or on the access point, assign the missing rights to the community string. For more information, see the information on setting up devices in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*.

**Symptom** Frequent client inventories are causing too much network traffic or degrading WLSE performance.

**Possible Cause** Running frequent client inventories when managing large numbers of access points (1,000 or more) generates a great deal of traffic and may degrade WLSE performance.

**Recommended Action** Increasing the Wireless Client Poll Interval in Devices > Discover > Inventory > Polling will reduce the polling frequency. If you need more frequent client polling for a subset of your access points, use the Scheduled Inventory feature instead (Devices > Discover > Inventory > Run Inventory).

**Symptom** Inventory is taking longer than expected and a message about no logs available appears in the inventory log.

No logs available. Waiting for resources to start job.

**Possible Cause** If there are also SNMP timeouts on the network, inventory jobs will take much longer. Other jobs may be using all of the available resources. Also, the next scheduled inventory will not run until the current inventory finishes.

**Recommended Action** None.

# Configuration FAQs and Troubleshooting

- [Configuration FAQs, page 10-19](#)
- [Configuration Troubleshooting, page 10-22](#)

## Configuration FAQs

- [If I create a configuration template that includes WEP key settings how can I verify that they were set on the access point \(the access point does not show WEP key settings on its web interface\)?](#)
  - [Can you undo a configuration update?](#)
  - [How long is the configuration job history kept in the WLSE?](#)
  - [Do jobs use HTTP or SNMP to initiate a configuration upload?](#)
  - [Is it necessary to validate a job?](#)
  - [What kinds of job logs are available?](#)
  - [What is startup configuration?](#)
  - [If I make changes to the startup template, will those modifications be automatically uploaded to the access points that already had that startup template applied?](#)
  - [What is auto configuration?](#)
- Q.** [If I create a configuration template that includes WEP key settings how can I verify that they were set on the access point \(the access point does not show WEP key settings on its web interface\)?](#)
- A.** For security reasons, the access point does not show or send WEP key information. One of the ways to verify the update is to look at the WEP Key length. The only way to verify the contents of the WEP key is to try associating a client that uses that WEP key.
- Q.** [Can you undo a configuration update?](#)
- A.** Yes, but only for successful jobs and device versions 11.23T and above for the 340 and 350 access points and bridges, and versions 11.56 and above for AP1200. The Undo feature cannot be used for IOS devices.

To undo a job, view the Job Run Details table under Configuration > Jobs, select the job you want to undo, and click Undo. For more specific information, see the online help.

- Q.** How long is the configuration job history kept in the WLSE?
- A.** The default time is 30 days. You can change this by navigating to Devices > Discover > Inventory > Polling > Job History Truncation Interval. Also, by default, for the recurring jobs, the last 30 runs are maintained in the database.
- Q.** Do jobs use HTTP or SNMP to initiate a configuration upload?
- A.** WLSE Configuration jobs can use either HTTP or SNMP as the mechanism to initiate a configuration template upload to an access point.
- The HTTP mechanism is valid for all supported device versions. The following setup parameters must be in place for HTTP mechanism to function properly:
    - HTTP credentials for the device (with admin and firmware privileges on the access point) must match those entered on the WLSE HTTP device credentials screen.
    - TFTP server settings on the access point (Setup > FTP), must refer to the WLSE's IP address.




---

**Note** Both username and password in the device credentials are case sensitive.

---

- The SNMP mechanism is valid for versions 11.08T and higher. The following setup parameters must be in place for SNMP to function properly:
  - SNMP credentials for the device (with admin and firmware privileges on the access point) must match those entered on the WLSE SNMP device credentials screen.
  - There is no need to change TFTP server settings for the SNMP mechanism, although you can use the SNMP mechanism to change the TFTP server settings on the AP to be used in the HTTP mechanism. Enter valid credentials in the Security > Local Admin Access template screen.

The SNMP job mechanism can be used to update TFTP settings, which are needed by HTTP-based jobs. This setting is available under Service > FTP in the configuration templates screens.



- Q.** Is it necessary to validate a job?
- A.** We recommend that you always validate a job before saving it. This will help in locating any possible problems before applying the job.
- Q.** What kinds of job logs are available?
- A.** There are two kinds of job logs: Job run log and the jobvm log.
- The job run log is where events are logged for a particular job's run. This log can be used to check what went wrong with the job and make any required corrections. The job run log can be viewed by selecting a particular job from the job list, then clicking **Job Run Detail**. From the window that pops up, select a particular run for the job, then click **Job Run Log**.
  - The jobvm.log is a global log for all types of jobs. It is used mainly for development troubleshooting. The jobvm.log can be viewed by selecting Administration > Appliance > View Log File, then clicking **jobvm.log**.
- Q.** What is startup configuration?

Startup configuration is used right after a device (access point) reboots. It requires DHCP server to be properly set up to allow the access point to pick its startup configuration from WLSE. For this to work, you must set up the following:

- a. Enter the `<IP address of the WLSE>` in the **Boot Server Host Name** field (option number 066) on the DHCP server.
- b. Enter `<startup file name>` in the **BootfileName** field (option number 067) on the DHCP server.

For additional information, or for information about configuring a router as a DHCP server, see the online help.

- Q.** What is auto configuration?
- A.** Auto configuration is used after the device has been discovered and inventory has been collected for it. This template can be applied based on criteria you define while saving your auto-configuration template.
- Q.** If I make changes to the startup template, will those modifications be automatically uploaded to the access points that already had that startup template applied?

- A.** No. If you make modifications to the startup template, you will have to reapply the template.

## Configuration Troubleshooting

- An IOS template job failed.
- A message indicates that the device version to which I am assigning a template is not supported.
- Configuration jobs fail because the Telnet/SSH credentials are not valid, even though credentials have been entered on the WLSE.

**Symptom** An IOS template job failed.

**Possible Cause** The template has the hostname configured instead of the IP address, and the DNS name resolution is not configured correctly on the access point.

**Recommended Action** Use the IP address or configure the DNS name correctly on the access point.

**Symptom** A message indicates that the device version to which I am assigning a template is not supported.

**Possible Cause** The device version was not supported at the time the WLSE was released.

**Recommended Action** Import the updated list of devices to the WLSE, select Administration > System > New Version Support.

**Symptom** Configuration jobs fail because the Telnet/SSH credentials are not valid, even though credentials have been entered on the WLSE.

**Possible Cause** The credentials entered on the WLSE do not exactly match the data entered in Devices > Discovery > Device Credentials > Telnet/SSH User/Password.

**Recommended Action** Make sure that the Telnet/SSH credentials data entered on the WLSE show the correct device login response. Match the device login sequence with the credential fields, as shown in [Firmware and configuration jobs fail because the Telnet/SSH credentials are not valid.](#), page 10-29.

## Firmware FAQs and Troubleshooting

- [Firmware FAQs, page 10-23](#)
- [Firmware Troubleshooting, page 10-25](#)

### Firmware FAQs

- [How can firmware images be imported?](#)
- [Are firmware jobs run by using both HTTP and SNMP?](#)
- [What kinds of job logs are available?](#)
- [How many devices can I have in one firmware job?](#)

**Q.** How can firmware images be imported?

**A.** Firmware images can be imported to WLSE from the desktop as well as Cisco.com. While importing any image from Cisco.com, the WLSE reads the version string and the device type for the image attributes. For imports from the desktop, you must make sure that the version and the device type strings are correctly entered in the image attributes. For example, for an AP350, image version 12.00T, the image string must be entered as 12.00T; not 12.0 or 12.00 or 12.0T.

**Q.** Are firmware jobs run by using both HTTP and SNMP?

- A.** Yes. Firmware jobs use both HTTP and SNMP protocols.
- HTTP is valid for all supported device versions. The following setup parameters must be in place for HTTP to function properly:
    - HTTP credentials for the device (with admin and firmware privileges on the AP) must match those entered on the WLSE HTTP device credentials screen.
    - TFTP server settings on the access point must reference the WLSE's IP address.




---

**Note** Both username and password in the device credentials are case sensitive.

---

- SNMP is valid for versions 11.08T and higher. The following setup parameters must be in place for SNMP to function properly:
  - SNMP credentials for the device (with admin and firmware privileges on the AP) must match those entered on the WLSE SNMP device credentials screen.
  - There is no need to change TFTP server settings for the SNMP mechanism, although you can use the SNMP mechanism to change the TFTP server settings on the AP to be used in the HTTP mechanism. Enter valid credentials in the Security > Local Admin Access template screen.




---

**Note** NOTE: Make sure to provide a numeric value in the user ID field (template screen).

---

- Q.** What kinds of job logs are available?
- A.** There are two kinds of job logs: Job run log and the jobvm log.
- The job run log is where events are logged for a particular job's run. This log can be used to check what went wrong with the job and make any required corrections. The job run log can be viewed by selecting a particular job from the job list, then clicking **Job Run Detail**. From the window that pops up, select a particular run for the job, then click **Job Run Log**.
  - The jobvm.log is a global log for all types of jobs. It is used mainly for development troubleshooting. The jobvm.log can be viewed by selecting Administration > Appliance > View Log File, then clicking **jobvm.log**.

- Q.** How many devices can I have in one firmware job?
- A.** There is no limit, although it is recommended that you work with device groups and set up jobs accordingly (for example, by location or building). While a job is running, the WLSE allocates resources for updating 20 devices in parallel. At any given time, 20 devices will be upgrading and the remainder will be waiting for resources to become available.

## Firmware Troubleshooting

- There is a time discrepancy in a job.
- Email about job completion fails to arrive at destination.
- Firmware is not updated on all the devices included in a job.
- An SNMP job fails..
- A firmware job ends with status “not verified.”
- Firmware jobs over slow links do not succeed.
- When downloading firmware from Cisco.com, an error message about cryptography permissions appears.
- When downloading firmware from Cisco.com, an error message about connectivity failure appears.
- Firmware and configuration jobs fail because the Telnet/SSH credentials are not valid.

**Symptom** There is a time discrepancy in a job.

**Possible Cause** The time was not set correctly on the WLSE.

### Recommended Action

- a. Reset the WLSE time to Universal Coordinated Time (UTC) using CLI commands as follows:  
Enter **services stop** to stop services.  
Enter the **clock** command to reset the time.  
Enter **services start** to restart the services.

- b. Set the time in local browser time, select Administration > Appliance > Time/NTP/Name.

For more information on setting the time, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

**Symptom** Email about job completion fails to arrive at destination.

**Possible Cause** The SMTP server is not specified.

**Recommended Action** Configure the mail route by selecting Administration > Appliance > Configure Mailroute.

**Symptom** Firmware is not updated on all the devices included in a job.

**Possible Cause** There were warnings displayed when the job was saved. Jobs for devices with warnings do not run; the job runs only for devices that do not have any warnings.

**Recommended Action** Solve the problems indicated in the warning messages before running the job.

**Possible Cause** If two firmware jobs were scheduled closely together, the second job contained some of the same devices as the first job. Those devices could not be updated because the first job was already running.

**Recommended Action** It is recommended that firmware jobs be run on groups of devices. Each group should be exclusive; that is, no device should be a member of more than one group.

For more information on upating firmware, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.5*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

**Symptom** An SNMP job fails.

**Possible Cause** The read community string does not have sufficient permissions.

**Recommended Action** The access point must have a user with at least SNMP, FIRMWARE, and ADMIN permissions for read-only access.

Access points with software releases prior to 12.01(T) must have a user with SNMP, FIRMWARE, ADMIN, and IDENT permissions for read-only access.

**Symptom** A firmware job ends with status “not verified.”



**Note**

The “not verified” status may not mean that the job has failed. The WLSE may time out before confirming whether the upgrade succeeded. To make sure, you can run an on-demand inventory on the devices in question to find out whether the firmware upgrade was installed. For more information, see the Inventory online help, or select Devices > DISCOVER > Inventory > Run Inventory Now.

**Possible Cause** The device may be taking a long time to reboot.



**Caution**

Do not take the following action for firmware jobs that you are running to convert non-IOS access points to IOS. See the special conversion instructions in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*.

**Recommended Action** Increase the value of the Device Reboot Wait Timeout parameter by accessing the WLSE through the following URL:

[http://your\\_wlse:1741/debug/jobprops.jsp](http://your_wlse:1741/debug/jobprops.jsp)

where *your\_wlse* is the name of the WLSE.

Increase the value of the Device Reboot Wait Timeout parameter and run the job again.



---

**Note** Do not make this value extremely high. It is advisable to keep this value to something slightly higher than the actual reboot time of the slowest access point.

---

**Symptom** Firmware jobs over slow links do not succeed.

**Possible Cause** The access points being upgraded are connected to the WLSE over a slow link (less than 1.544 Mbps) and the job is timing out.



**Caution**

---

Do not take the following action for firmware jobs that you are running to convert non-IOS access points to IOS. See the special conversion instructions in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine*, 2.5.

---

**Recommended Action**

- a. Access the WLSE through the following URL:  
`http://your_wlse:1741/debug/jobprops.jsp`
- b. Increase the value of the Per device job operation timeout parameter. For example, for a 56kbps link, the recommended value is 2400 seconds (40 minutes). On a 128kbps link, the recommended value is 1200 seconds (20 minutes).

**Symptom** When downloading firmware from Cisco.com, an error message about cryptography permissions appears.

**Possible Cause** The first time you attempt to download firmware, the WLSE displays this message: `Error while selecting or displaying image details. Please log into cisco.com and make sure your username has acknowledged cryptography permissions for downloading IOS images.`

**Recommended Action** Log into Cisco.com and acknowledge the cryptography permissions. After you have acknowledged these permissions, you can import IOS images to the WLSE.



**Symptom** When downloading firmware from Cisco.com, an error message about connectivity failure appears.

**Possible Cause** DNS is not configured on the WLSE.

**Recommended Action** Configure DNS on the WLSE and make sure the WLSE can resolve the cisco.com domain name. For information about configuring DNS, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5* or the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*.

**Symptom** Firmware and configuration jobs fail because the Telnet/SSH credentials are not valid.

**Possible Cause** The credentials entered on the WLSE do not exactly match the data entered in Devices > Discovery > Device Credentials > Telnet/SSH User/Password.

**Recommended Action** Make sure that the Telnet/SSH credentials data entered on the WLSE show the correct device login response. Match the device login sequence with the credential fields as follows.

| Device Login Sequence                                                            | Telnet Credential Fields Required                                     |
|----------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| Username:<br>Password:<br>prompt > <b>enable</b><br>Password:<br>enable prompt # | User Name<br>User Password<br>Enable Password                         |
| Password:<br>prompt > <b>enable</b><br>Password:<br>enable prompt #              | User Password<br>Enable Password<br>(leave the User Name field empty) |
| prompt > <b>enable</b><br>Password:<br>enable prompt #                           | Enable Password<br>(leave User Name and User Password fields empty)   |
| enable prompt #                                                                  | Not supported. Configure the device accordingly.                      |

# Reports FAQs and Troubleshooting

- [Reports FAQ, page 10-30](#)
- [Reports Troubleshooting, page 10-30](#)

## Reports FAQ

- Q.** Are any of the reports real-time reports?
- A.** The reports are not real time. They are based on data that is collected periodically. The frequency with which the data is collected is user configurable (see Devices > Discover > Inventory > Polling). The data shown in reports is as current as the time the data was collected from the devices.

## Reports Troubleshooting

- [The Top N Busiest Clients report and the Client Statistics report display 0 \(zero\) values.](#)
- [Some report fields are blank.](#)
- [The client association data in the Group Client Association report differs from the data shown in the Current Client Associations report.](#)
- [The access point data in the Historical Associations report is not accurate.](#)
- [The Summary and/or Detailed report for access points is empty.](#)
- [The group report for a user-defined group contains no data.](#)
- [After running a job, the updated data does not appear in a report.](#)
- [Email fails to arrive at its destination.](#)
- [There is a time discrepancy in the scheduled email jobs.](#)
- [No VLAN information is displayed for IOS access points.](#)

**Symptom** The Top N Busiest Clients report and the Client Statistics report display 0 (zero) values.

**Possible Cause** Wireless client polling frequency is set to 51 minutes by default. The counters could reset between two polling cycles which would cause zero values when the reports are run.

**Recommended Action** Increase the polling frequency by selecting Devices > Discover > Inventory > Polling.

**Caution**

---

Increasing the polling frequency could have an effect on performance.

---

**Symptom** Some report fields are blank.

**Possible Cause** The device is not configured properly for management by the WLSE; the ISO view has not been created.

**Recommended Action** See [Devices are placed in Misconfigured Devices group after discovery.](#), page 10-16 for information about how to correct the problem.

**Symptom** The client association data in the Group Client Association report differs from the data shown in the Current Client Associations report.

**Possible Cause** The data for the Group Client Association report is collected using performance attributes polling and the data shown in the Current Client Association report uses wireless client polling.

Whichever report has a higher polling frequency will contain the most up to date data. Select Devices > Discover > Inventory > Polling to view polling frequency.

**Recommended Action** None.

**Symptom** The access point data in the Historical Associations report is not accurate.

**Possible Cause** The wireless client was associated with an access point managed by the WLSE, but subsequently associated with an access point that was added to the network, but not yet managed by the WLSE.

**Recommended Action** Verify that the associated access points are in the managed devices folder by selecting Devices > Discover > Managed Devices > Manage/Unmanage.

**Symptom** The Summary and/or Detailed report for access points is empty.

**Possible Cause** The SNMP user may not have the correct rights assigned.

**Recommended Action**

- a. Open a browser window to the access point, and select Setup > Security > User Information.
- b. Make sure that the user corresponding to the SNMP community (which is set up in WLSE in Discovery > Device Credentials) has been granted rights for the following: Ident, firmware, admin, snmp, and write.
- c. If not, click on the user and assign all these rights.

**Symptom** The group report for a user-defined group contains no data.

**Possible Cause** Reports cannot be displayed for a user-defined group that contains another group.

**Recommended Action** Display individual reports for the sub-groups or devices within the user-defined group.

**Symptom** After running a job, the updated data does not appear in a report.

**Possible Cause** A full polling cycle has not completed and the new data has not been entered in the database.

**Recommended Action** Verify that the polling cycle has completed as follows:

- a. Select Administration > Appliance > Status > View Log File.
- b. Click **jobvm.log**.
- c. Scroll through the log to find the message: “Finished Inventory” for your particular job.

**Symptom** Email fails to arrive at its destination.

**Possible Cause** The SMTP server is not configured properly.

**Recommended Action** Configure the SMTP server by selecting Administration > Appliance > Configure Mailroute.

**Symptom** There is a time discrepancy in the scheduled email jobs.

**Possible Cause** The time is not set correctly on the WLSE.

**Recommended Action**

- a. Reset the WLSE time to Universal Coordinated Time (UTC) using CLI commands as follows:  
Enter **services stop** to stop services.  
Enter the **clock** command to reset the time.  
Enter **services start** to restart the services.
- b. Set the time in local browser time, select Administration > Appliance > Time/NTP/Name.

**Symptom** No VLAN information is displayed for IOS access points.

**Possible Cause** WEP keys have not been configured in each VLAN. When the WEP keys are configured in the IOS access points, VLAN information is accessible by SNMP.

**Recommended Action** Configure the WEP keys for the corresponding VLAN.

## Radio Manager FAQs and Troubleshooting

- [Radio Manager FAQs](#)
- [Radio Manager Troubleshooting](#)

### Radio Manager FAQs

- [Why don't I see the building or floor node in the device tree in the Assisted Site Survey Wizard?](#)
- [Why don't I see the device that I am looking for in the Assisted Site Survey device tree?](#)
- [When I select devices in the Assisted Site Survey Wizard, why are some shown in red?](#)
- [When I'm using the Assisted Site Survey Wizard, why is the Next button disabled after I complete step one?](#)
- [In the Assisted Site Survey Wizard, why is Use Old Radio Scan Data disabled?](#)
- [In the Assisted Site Survey Wizard, what does None mean in the Last Scan Time field?](#)
- [In the Assisted Site Survey Wizard, why is the Next button disabled on the radio scan step?](#)
- [Why did my radio scan job fail in the Assisted Site Survey Wizard?](#)
- [When I'm using the Assisted Site Survey Wizard, the radio scan progress advances very slowly. How long does it radio scan normally take?](#)

- Can I skip client walkabout in the Assisted Site Survey Wizard even though the number of data shown is zero?
  - In the client walkabout step in the Assisted Site Survey Wizard, what is the Recall button for?
  - What is the difference between the Number of Location Data and Number of New Location Data fields?
  - In the Constraints and Goals step in the Assisted Site Survey Wizard, how do I select multiple channels in the channel list?
  - How long should the Constraints and Goals calculation step take in the Assisted Site Survey Wizard?
  - Where can I see the result of the Constraints and Goals calculation in the Assisted Site Survey Wizard?
  - If I don't like result of the Constraints and Goals calculation in the Assisted Site Survey Wizard, what can I do?
  - When I apply the configuration in the Assisted Site Survey Wizard, where do I see the results?
  - In the last step of the Assisted Site Survey Wizard, why is the Next button disabled?
- Q.** Why don't I see the building or floor node in the device tree in the Assisted Site Survey Wizard?
- A.** Expand the building node to see all floors that belong to the building. If you expand the building node and the floors still do not appear, close the Wizard and make sure the building and floor exist in the Location Manager navigation tree. If the building or floor does not exist in the Location Manager navigation tree, you first need to create them and then restart the Assisted Site Survey Wizard.
- Q.** Why don't I see the device that I am looking for in the Assisted Site Survey device tree?
- A.** Expand the building and floor nodes to see all devices that belong to a building or floor. If the device still does not appear, close the Assisted Site Survey Wizard and make sure the device appears in the Location Manager navigation tree. If the device does not appear in the Location Manager navigation tree, select **Tools > Find Device** to locate it. If you find the device,

move it to the desired location. The device does not appear in Location Manager, it might not have been discovered by the system. After adding the device and specifying its location, restart the Assisted Site Survey Wizard.

- Q.** When I select devices in the Assisted Site Survey Wizard, why are some shown in red?
- A.** The devices might be red if:
- The devices are not in the Managed state. Select **Devices > Discover > Manage/Unmanage** to verify that the devices are Managed.
  - The devices are not in infrastructure mode. Go to the AP configuration for the individual device and verify that it is in “Infrastructure Mode” with the proper WDS assigned.
- Q.** When I’m using the Assisted Site Survey Wizard, why is the **Next** button disabled after I complete step one?
- A.** You have not selected any acceptable devices that are required for the next step. If any of the selected devices are shown in red, you need to deselect them before you can go to the next step.
- Q.** In the Assisted Site Survey Wizard, why is **Use Old Radio Scan Data** disabled?
- A.** You might not have previously run radio scan for the selected devices. You must start a new radio scan.
- Q.** In the Assisted Site Survey Wizard, what does *None* mean in the Last Scan Time field?
- A.** The selected device was not included in a previous radio scan.
- Q.** In the Assisted Site Survey Wizard, why is the **Next** button disabled on the radio scan step?
- A.** You need to run radio scan by clicking **Start**. When the radio scan is complete, you will be able to click **Next**.
- Q.** Why did my radio scan job fail in the Assisted Site Survey Wizard?
- A.** Look at the log window to find out exact failure cause. If radio scan failed:



- Make sure the devices have the correct setup for WDS. Also verify that WDS is authenticated to WLSE and that WDS has an IP address pointing to WLSE.
  - Make sure the devices have the correct SNMP read/write community strings that match the WLSE setting.
- Q.** When I'm using the Assisted Site Survey Wizard, the radio scan progress advances very slowly. How long does it radio scan normally take?
- A.** Radio scan normally takes about 5 to 10 minutes to complete. If you suspect the program has stalled, check its status by selecting **Radio Manager > AP Radio Scan** and viewing the progress of the job.
- Q.** Can I skip client walkabout in the Assisted Site Survey Wizard even though the number of data shown is zero?
- A.** Yes, you can skip client walkabout. However, performing a client walkabout will generate better parameters for your wireless network.
- Q.** In the client walkabout step in the Assisted Site Survey Wizard, what is the **Recall** button for?
- A.** You can click **Recall** to display a list of the last five client MAC addresses that were used for the previous client walkabout. To retrieve a previously used MAC address, click **Recall** and select a MAC address from the list.
- Q.** What is the difference between the **Number of Location Data** and **Number of New Location Data** fields?
- A.** Number of Location Data is the total number of data found by client walkabout for the current session plus any previous sessions. Number of New Location Data is the total number of data found by client walkabout for the current session only. The numbers in these two fields can increase at the same time during a client walkabout.
- Q.** In the Constraints and Goals step in the Assisted Site Survey Wizard, how do I select multiple channels in the channel list?
- A.** For Windows users, control-click on the channels to add them to the selection. The selected channels are highlighted.
- Q.** How long should the Constraints and Goals calculation step take in the Assisted Site Survey Wizard?

- A.** It varies depending on the amount of radio scan and client walkabout data. The more data you have, the longer it will take to calculate.
- Q.** Where can I see the result of the Constraints and Goals calculation in the Assisted Site Survey Wizard?
- A.** If the calculation was successful, you can click **Next** to view the result.
- Q.** If I don't like result of the Constraints and Goals calculation in the Assisted Site Survey Wizard, what can I do?
- A.** Go back and specify different constraints and goals, and then recalculate the constraints and goals.
- Q.** When I apply the configuration in the Assisted Site Survey Wizard, where do I see the results?
- A.** Check Location Manager to view the configuration changes. You might need to refresh the Location Manager window by selecting **View > Refresh Data**. In rare cases, the wizard might have failed to apply the configuration. In that case, check your SNMP settings, particularly the WRITE community string, for the devices.
- Q.** In the last step of the Assisted Site Survey Wizard, why is the **Next** button disabled?
- A.** This is the last step in Assisted Site Survey Wizard. You can close the Wizard unless you want to repeat any previous steps.

## Radio Manager Troubleshooting

- [After completing the Assisted Site Survey, Location Manager did not update to include the applied configurations.](#)

**Symptom** After completing the Assisted Site Survey, Location Manager did not update to include the applied configurations.

**Possible Cause** You did not refresh the Location Manager window.

**Recommended Action** In the Location Manager window, select **View > Refresh Data**.

# Administration FAQs and Troubleshooting

- [Administration FAQs, page 10-39](#)
- [Administration Troubleshooting, page 10-39](#)

## Administration FAQs

- Q.** How can I verify the status of the database?
- A.** You can verify that the WLSE database is running by using the **show process** CLI command. If the command output includes the db2sync process, the database is running.

## Administration Troubleshooting

This section contains the following troubleshooting information:

- [Users cannot log in after failure of the alternative authentication source.](#)
- [Some users are not listed under User Admin > Manage Users.](#)
- [When using Internet Explorer 6.0 to install a new image on a WLSE from a repository located on a Windows XP machine, the progress bar does not appear in the Install Software Updates window. This problem also occurs when you use Internet Explorer 6.0 and a Windows XP system as a client to install a new image on a WLSE.](#)
- [Cannot back up the WLSE configuration to a Windows 2000 or Windows XP Server.](#)
- [Cannot log in with a username and password created in the CLI.](#)

**Symptom** Users cannot log in after failure of the alternative authentication source.

**Possible Cause** The WLSE falls back to the Local authentication module.

**Recommended Action**

- Users can log in using their local passwords.

- The system administrator can log in using the admin log in.
- All users with CLI access can log in using the CLI.
- If you still cannot log in, follow the procedure on recovering from the loss of all admin passwords in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*.

**Symptom** Some users are not listed under User Admin > Manage Users.

**Possible Cause** Only the creator of a user can view that user's name in the list. The admin user, however, can view all users.

**Recommended Action** None.

**Symptom** When using Internet Explorer 6.0 to install a new image on a WLSE from a repository located on a Windows XP machine, the progress bar does not appear in the Install Software Updates window. This problem also occurs when you use Internet Explorer 6.0 and a Windows XP system as a client to install a new image on a WLSE.

**Possible Cause** The Internet Explorer 6.0 browser on Windows XP does not come with the Java plug-in installed.

**Recommended Action** Before using a Windows XP machine as a *remote repository* to update WLSE software, perform the following on the repository:

- Install the JRE version 1.3.1\_08 or later browser plug-in.
- In the browser, select Tools > Internet Options > Privacy. Lower the slider all the way down to achieve the **Accept All Cookies** setting.

Before using a Windows XP machine as a *client* to update WLSE software, install the JRE 1.3.1\_08 or later browser plug-in on the client machine.

You can download the plug-in from third-party sources such as Sun Microsystems or IBM.

**Symptom** Cannot log in with a username and password created in the CLI.

**Possible Cause** The password is too long.

**Recommended Action** Reset the password by using the CLI **username** command, or log in by using the first 8 characters of the password. Passwords should be from 5 to 8 characters long.

**Symptom** Cannot back up the WLSE configuration to a Windows 2000 or Windows XP Server.

**Possible Cause** The backup directory is not writable.

**Recommended Action** Set the directory to UNIX mode and make it write-enabled. For more information, see the backup and restore instructions in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*.





# Naming Guidelines

---

This appendix provides information about:

- [Naming Rules for Users and Roles, page A-1.](#)
- [Naming Rules for Names and Descriptions, page A-2.](#)

## Naming Rules for Users and Roles

[Table A-1](#) lists the rules for usernames, passwords, and roles.

**Table A-1** *Allowable Characters for Users and Roles*

| Type          | Rules                                                                                                                                                                                                             |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Name     | <ul style="list-style-type: none"><li>• No more than 32 characters.</li><li>• Case sensitive.</li><li>• Except for the full stop/period (.) and dash (-), the characters from <a href="#">Table A-2</a></li></ul> |
| User Password | <ul style="list-style-type: none"><li>• 5-8 characters.</li><li>• Case sensitive.</li><li>• Any alphanumeric character and the underscore.</li></ul>                                                              |
| Role          | <ul style="list-style-type: none"><li>• No more than 32 characters.</li><li>• Case sensitive.</li><li>• Any character from <a href="#">Table A-2</a>.</li></ul>                                                   |

Naming Rules for Names and Descriptions

Table A-2 lists the allowable characters for names and descriptions. The number of characters allowed are:

- Names—no more than 64 characters allowed



**Note** Each job name (configuration, firmware, or AP radio scan) must be unique.

- Descriptions—no more than 256 characters allowed



**Note** Do not use the Enter key in any Description fields.

Table A-2    Allowable Characters for Names and Descriptions

| Character Description                                     | Characters   |
|-----------------------------------------------------------|--------------|
| alphanumeric—upper and lower case                         | a123b, A123B |
| space                                                     |              |
| exclamation mark                                          | !            |
| percent sign                                              | %            |
| left and right parenthesis                                | ( )          |
| asterisk                                                  | *            |
| comma                                                     | ,            |
| hyphen, dash, minus                                       | -            |
| <b>Note</b> Not to be used for users and roles usernames  |              |
| full stop (period)                                        | .            |
| <b>Note</b> Not to be used for users and roles usernames. |              |
| solidus (forward slash)                                   | /            |
| colon                                                     | :            |
| semicolon                                                 | ;            |
| equals                                                    | =            |



**Table A-2** Allowable Characters for Names and Descriptions (continued)

| Character Description         | Characters |
|-------------------------------|------------|
| question mark                 | ?          |
| low line (underscore)         | _          |
| left and right square bracket | [ ]        |
| left and right curly bracket  | { }        |
| vertical line                 |            |
| tilde                         | ~          |
| dollar sign                   | \$         |





# Using the Command Line Interface (CLI)

---

This appendix summarizes the Wireless LAN Solution Engine'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 B-2](#)
- [CLI Conventions, page B-2](#)
- [Command Privileges, page B-2](#)
- [Checking Command Syntax, page B-3](#)
- [Command History Feature, page B-3](#)
- [Help for CLI Commands, page B-3](#)
- [Command Summary, page B-4](#)
- [Command Description Conventions, page B-4](#)
- [Privilege Level 0 Commands, page B-10](#)
- [Privilege Level 15 Commands, page B-17](#)
- [Maintenance Image Commands, page B-78](#)

# 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 B-75.

## 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. The command descriptions in this appendix are organized by privilege level.

# 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.

## Help for CLI Commands

You can obtain help using the following methods:

- 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 contains 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 B-1](#) summarizes all commands available on the WLSE. For full descriptions of commands, see the following sections:

- [Privilege Level 0 Commands, page B-10](#)
- [Privilege Level 15 Commands, page B-17](#)
- [Maintenance Image Commands, page B-78](#)

**Table B-1** Command Summary

| Command                      | Privilege Level | Description                                                          | Reference                               |
|------------------------------|-----------------|----------------------------------------------------------------------|-----------------------------------------|
| <a href="#">auth</a>         | 15              | Enables secure remote authentication.                                | <a href="#">auth, page B-17</a>         |
| <a href="#">backup</a>       | 15              | Backs up WLSE configuration.                                         | <a href="#">backup, page B-18</a>       |
| <a href="#">backupconfig</a> | 15              | Sets the backup file location for all backup and restore operations. | <a href="#">backupconfig, page B-19</a> |
| <a href="#">cdp</a>          | 15              | Enables or disables the Cisco Discovery Protocol (CDP).              | <a href="#">cdp, page B-20</a>          |
| <a href="#">clock</a>        | 15              | Sets the system date and time.                                       | <a href="#">show clock, page B-11</a>   |

Table B-1 Command Summary (continued)

| Command                  | Privilege Level  | Description                                                              | Reference                                    |
|--------------------------|------------------|--------------------------------------------------------------------------|----------------------------------------------|
| <b>df</b>                | 15               | Displays the current storage usage on the WLSE.                          | <a href="#">df, page B-22</a>                |
| <b>dumptcp</b>           | 15               | Displays TCP/IP packet content.                                          | <a href="#">dumptcp, page B-23</a>           |
| <b>erase config</b>      | 15 <sup>1</sup>  | Erases the configuration in flash memory and reloads the device.         | <a href="#">erase config, page B-24</a>      |
| <b>exit</b>              | 0                | Logs user out of the WLSE.                                               | <a href="#">exit, page B-10</a>              |
| <b>gethostbyname</b>     | 15               | Displays IP address of a known domain name.                              | <a href="#">gethostbyname, page B-26</a>     |
| <b>fsck</b>              | N/A <sup>2</sup> | Checks and repairs the file system.                                      | <a href="#">fsck, page B-79</a>              |
| <b>firewall</b>          | 15               | Implements port filtering on the WLSE.                                   | <a href="#">firewall, page B-25</a>          |
| <b>hostname</b>          | 15               | Changes the system host name.                                            | <a href="#">hostname, page B-27</a>          |
| <b>import</b>            | 15               | Imports host files or maps IP addresses to host names.                   | <a href="#">import, page B-27</a>            |
| <b>install configure</b> | 15               | Configures the repository for installing software updates on the WLSE.   | <a href="#">install configure, page B-28</a> |
| <b>install list</b>      | 15               | Lists software updates and images currently available on the repository. | <a href="#">install list, page B-29</a>      |
| <b>install update</b>    | 15               | Installs software updates and images from the repository.                | <a href="#">install update, page B-30</a>    |
| <b>interface</b>         | 15               | Configures Ethernet interfaces.                                          | <a href="#">interface, page B-31</a>         |
| <b>ip domain-name</b>    | 15               | Defines the default domain name.                                         | <a href="#">ip domain-name, page B-33</a>    |
| <b>ip name-server</b>    | 15               | Specifies the address of name servers for name and address resolution.   | <a href="#">ip name-server, page B-33</a>    |
| <b>listbackup</b>        | 15               | Lists all current backups at the configured site.                        | <a href="#">listbackup, page B-35</a>        |
| <b>mail</b>              | 15               | Debugs and tests email settings.                                         | <a href="#">mail, page B-35</a>              |

Table B-1 Command Summary (continued)

| Command                           | Privilege Level | Description                                                                                | Reference                                     |
|-----------------------------------|-----------------|--------------------------------------------------------------------------------------------|-----------------------------------------------|
| <a href="#">mailcntrl clear</a>   | 15              | Deletes the mail log, send queue, or user queue.                                           | <a href="#">mailcntrl clear</a> , page B-36   |
| <a href="#">mailcntrl list</a>    | 15              | Lists the size of the mail log, user queue, or send queue.                                 | <a href="#">mailcntrl list</a> , page B-37    |
| <a href="#">mailroute</a>         | 15              | Forwards email to a specified server.                                                      | <a href="#">mailroute</a> , page B-37         |
| <a href="#">mkcert</a>            | 15              | Generates a Certificate Signed Request (CSR) for HTTPS.                                    | <a href="#">mkcert</a> , page B-38            |
| <a href="#">nslookup</a>          | 15              | Translates a device name to its IP address or an IP address to its device name.            | <a href="#">nslookup</a> , page B-40          |
| <a href="#">ntp server</a>        | 15              | Allows the system clock to be synchronized by a time server.                               | <a href="#">ntp server</a> , page B-40        |
| <a href="#">ping</a>              | 0               | Sends ICMP echo_request packets for diagnosing basic network connectivity.                 | <a href="#">ping</a> , page B-10              |
| <a href="#">reload</a>            | 15 <sup>1</sup> | Reboots the system.                                                                        | <a href="#">reload</a> , page B-42            |
| <a href="#">reinitdb</a>          | 15              | Reinitializes the database.                                                                | <a href="#">reinitdb</a> , page B-43          |
| <a href="#">repository source</a> | 15              | Configures the WLSE to be a repository server.                                             | <a href="#">repository source</a> , page B-46 |
| <a href="#">repository add</a>    | 15              | Transfers software updates and images from a remote server to the WLSE's local repository. | <a href="#">repository add</a> , page B-44    |
| <a href="#">repository delete</a> | 15              | Deletes software updates and images on the local repository.                               | <a href="#">repository delete</a> , page B-44 |
| <a href="#">repository list</a>   | 15              | Lists software updates and images on the local or remote repository.                       | <a href="#">repository list</a> , page B-45   |
| <a href="#">repository server</a> | 15              | Starts, stops, or displays the status of the WLSE's local repository.                      | <a href="#">repository server</a> , page B-47 |



**Table B-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 B-48           |
| <a href="#">route</a>             | 15              | Adds a route.                                                    | <a href="#">route</a> , page B-49             |
| <a href="#">services</a>          | 15              | Lists, starts, or stops management services.                     | <a href="#">services</a> , page B-49          |
| <a href="#">show anilog</a>       | 15              | Displays the WLSE's ANI log.                                     | <a href="#">show anilog</a> , page B-51       |
| <a href="#">show auth-cli</a>     | 15              | Displays the type of authentication used for secure CLI access.  | <a href="#">show auth-cli</a> , page B-52     |
| <a href="#">show auth-http</a>    | 15              | Displays the type of authentication used for secure HTTP access. | <a href="#">show auth-http</a> , page B-52    |
| <a href="#">show backupconfig</a> | 15              | Displays the current backup and restore configuration.           | <a href="#">show backupconfig</a> , page B-53 |
| <a href="#">show bootlog</a>      | 0               | Displays the messages logged during the last system boot.        | <a href="#">show bootlog</a> , page B-53      |
| <a href="#">show cdp neighbor</a> | 15              | Displays the WLSE's nearest neighbor on the network.             | <a href="#">show cdp neighbor</a> , page B-55 |
| <a href="#">show cdp run</a>      | 15              | Displays the Cisco Discovery Protocol (CDP) configuration.       | <a href="#">show cdp run</a> , page B-55      |
| <a href="#">show clock</a>        | 0               | Displays system time in Coordinated Universal Time (UTC).        | <a href="#">show clock</a> , page B-11        |
| <a href="#">show collectorlog</a> | 15              | Displays the WLSE's collector log.                               | <a href="#">show collectorlog</a> , page B-56 |
| <a href="#">show config</a>       | 15              | Displays WLSE configuration.                                     | <a href="#">show config</a> , page B-57       |
| <a href="#">show daemonslog</a>   | 15              | Displays WLSE's daemons log.                                     | <a href="#">show daemonslog</a> , page B-58   |
| <a href="#">show dmgtldlog</a>    | 15              | Displays WLSE's daemon manager log.                              | <a href="#">show dmgtldlog</a> , page B-59    |
| <a href="#">show domain-name</a>  | 0               | Displays WLSE's domain name                                      | <a href="#">show domain-name</a> , page B-12  |

Table B-1 Command Summary (continued)

| Command                           | Privilege Level | Description                                                                           | Reference                                     |
|-----------------------------------|-----------------|---------------------------------------------------------------------------------------|-----------------------------------------------|
| <a href="#">show import</a>       | 15              | Displays imported host files.                                                         | <a href="#">show import</a> , page B-60       |
| <a href="#">show install logs</a> | 15              | Displays software updates and images available on the configured repository.          | <a href="#">show install logs</a> , page B-60 |
| <a href="#">show interfaces</a>   | 0               | Displays information about the WLSE's network interface.                              | <a href="#">show interfaces</a> , page B-13   |
| <a href="#">show ipchains</a>     | 15              | Displays IP chains for the selected interface.                                        | <a href="#">show ipchains</a> , page B-61     |
| <a href="#">show hosts</a>        | 15              | Displays WLSE's host file.                                                            | <a href="#">show hosts</a> , page B-61        |
| <a href="#">show maillog</a>      | 15              | Displays WLSE's mail log.                                                             | <a href="#">show maillog</a> , page B-62      |
| <a href="#">show process</a>      | 0               | Displays information about processes running on the system.                           | <a href="#">show process</a> , page B-14      |
| <a href="#">show repository</a>   | 15              | Displays the status or the access log of a configured repository.                     | <a href="#">show repository</a> , page B-64   |
| <a href="#">show route</a>        | 15              | Displays the routes currently configured.                                             | <a href="#">show route</a> , page B-64        |
| <a href="#">show securitylog</a>  | 15              | Displays WLSE's secure log information.                                               | <a href="#">show securitylog</a> , page B-65  |
| <a href="#">show snmp-server</a>  | 15              | Displays WLSE's SNMP configuration.                                                   | <a href="#">show snmp-server</a> , page B-66  |
| <a href="#">show ssh-version</a>  | 15              | Displays type of SSH enabled.                                                         | <a href="#">show ssh-version</a> , page B-66  |
| <a href="#">show syslog</a>       | 15              | Displays syslog information.                                                          | <a href="#">show syslog</a> , page B-67       |
| <a href="#">show tech</a>         | 15              | Displays information necessary for Cisco's Technical Assistance Center to assist you. | <a href="#">show tech</a> , page B-68         |
| <a href="#">show telnetenable</a> | 15              | Displays WLSE's Telnet status.                                                        | <a href="#">show telnetenable</a> , page B-68 |
| <a href="#">show tomcatlog</a>    | 15              | Displays WLSE's Tomcat log.                                                           | <a href="#">show tomcatlog</a> , page B-69    |

**Table B-1** Command Summary (continued)

| Command                              | Privilege Level | Description                                                        | Reference                                        |
|--------------------------------------|-----------------|--------------------------------------------------------------------|--------------------------------------------------|
| <a href="#">show version</a>         | 0               | Displays information about current software installed on WLSE.     | <a href="#">show version</a> , page B-15         |
| <a href="#">show webaccesslog</a>    | 15              | Displays WLSE's Web access log.                                    | <a href="#">show webaccesslog</a> , page B-70    |
| <a href="#">show weberrorlog</a>     | 15              | Displays WLSE's Web error log.                                     | <a href="#">show weberrorlog</a> , page B-71     |
| <a href="#">show websslaccesslog</a> | 15              | Displays WLSE's Web SSL log.                                       | <a href="#">show websslaccesslog</a> , page B-72 |
| <a href="#">shutdown</a>             | 15              | Shuts down system in preparation for powering it off.              | <a href="#">shutdown</a> , page B-72             |
| <a href="#">snmp-server</a>          | 15              | Configures an SNMP agent.                                          | <a href="#">snmp-server</a> , page B-73          |
| <a href="#">ssh</a>                  | 15              | Connects to an external host by using SSH.                         | <a href="#">ssh</a> , page B-74                  |
| <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 B-74          |
| <a href="#">telnet</a>               | 15              | Telnet to an external host.                                        | <a href="#">telnet</a> , page B-75               |
| <a href="#">telnetenable</a>         | 15              | Configures Telnet access.                                          | <a href="#">telnetenable</a> , page B-75         |
| <a href="#">traceroute</a>           | 0               | Displays route to a specified host and identifies faulty gateways. | <a href="#">traceroute</a> , page B-15           |
| <a href="#">username</a>             | 15              | Creates new user account or changes account properties.            | <a href="#">username</a> , page B-76             |
| <a href="#">webtimeout</a>           | 15              | Changes the session timeout for the Web interface.                 | <a href="#">webtimeout</a> , page B-78           |

1. This command is also available in the maintenance image.
2. This command is available only in the maintenance image.

# Privilege Level 0 Commands

This section describes the privilege level 0 commands.

## exit

To log out of the system, use the following command:

**exit**

### Syntax Description

This command has no arguments or keywords.

### Example

The following command logs you out of the system:

**exit**

## ping

To send ICMP echo\_request packets for diagnosing basic network connectivity, use the following command.

**ping** [ **-c** *count* ] [ **-i** *wait* ] [ **-s** *packetsize* ] [ **-n** ] { *hostname* | *ip-address* }

### Syntax Description

|                   |                                                                                   |
|-------------------|-----------------------------------------------------------------------------------|
| <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. |
| <b>n</b>          | Disables reverse DNS lookup.  |

## 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-sj1.cisco.com (209.165.200.224): icmp_seq=0 ttl=246
time=16.3 ms
64 bytes from dns-sj1.cisco.com (209.165.200.224): icmp_seq=1 ttl=246
time=2.0 ms
64 bytes from dns-sj1.cisco.com (209.165.200.224): icmp_seq=2 ttl=246
time=2.1 ms
64 bytes from dns-sj1.cisco.com (209.165.200.224): icmp_seq=3 ttl=246
time=2.1 ms
```

## show clock

To display the system date and time in Coordinated Universal Time (UTC), use the following command.

```
show clock
```

## Syntax Description

This command has no arguments or keywords.

## Usage Guidelines

or more information about the system time, see the *Configuration and Installation Guide for the Wireless LAN Solution Engine*.

## Example

This command displays the system date and time:

```
show clock
12:43:47 Jun 20 2001
```

## Related Commands

[show clock](#)  
[ntp server](#)

# show domain-name

To display the system domain name, use the following command.

```
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
```

# show interfaces

To display information about the system network interfaces, use the following command.

## 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:febf000-febf038

 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](#)

# show process

To display information about processes running on the system (including the status of the database), use the following command.

**show process [ page ]**



**Note**

If the db2sync process is listed, the database is running.

## Syntax Description

**page** Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.

## Example

This command displays information about processes running on the system:

```
show process page
PID PPID ELAPSED SZ STARTED TTY COMMAND
 1 0 4-20:04:35 277 Fri Jun 15 16:54:03 2001 ? init
 2 1 4-20:04:35 0 Fri Jun 15 16:54:03 2001 ? kflushd
 3 1 4-20:04:35 0 Fri Jun 15 16:54:03 2001 ? kupdate
 4 1 4-20:04:35 0 Fri Jun 15 16:54:03 2001 ? kpiod
 5 1 4-20:04:35 0 Fri Jun 15 16:54:03 2001 ? kswapd
 6 1 4-20:04:28 0 Fri Jun 15 16:54:10 2001 ? kreiserfsd
 81 1 4-20:04:25 0 Fri Jun 15 16:54:13 2001 ? kreiserfsd
 82 1 4-20:04:25 0 Fri Jun 15 16:54:13 2001 ? kreiserfsd
 83 1 4-20:04:25 0 Fri Jun 15 16:54:13 2001 ? kreiserfsd
 84 1 4-20:04:25 0 Fri Jun 15 16:54:13 2001 ? kreiserfsd
 85 1 4-20:04:24 0 Fri Jun 15 16:54:14 2001 ? kreiserfsd
199 1 4-20:04:23 290 Fri Jun 15 16:54:15 2001 ? watchdog
213 1 4-20:04:23 342 Fri Jun 15 16:54:15 2001 ? idled
402 1 4-20:04:17 290 Fri Jun 15 16:54:21 2001 ? syslogd
411 1 4-20:04:17 360 Fri Jun 15 16:54:21 2001 ? klogd
517 1 4-20:04:15 327 Fri Jun 15 16:54:23 2001 ? crond
531 1 4-20:04:15 286 Fri Jun 15 16:54:23 2001 ? inetd
540 1 4-20:04:14 585 Fri Jun 15 16:54:24 2001 ? sshd
585 1 4-20:04:09 842 Fri Jun 15 16:54:29 2001 ? dmgttd.lnx
-----more-----
```



## show version

To display information about the current software on the system, use the following command.

### show version

#### Syntax Description

This command has no arguments or keywords.

#### Example

This command displays the current software on the system:

```
show version
Copyright (c) 1999-2000 by Cisco Systems, Inc.
Build Version (166) Mon Jun 11 16:56:23 PDT 2001
Uptime: 4 days 20 hours 6 mins
Linux/UID32 version 2.2.16-13bipsec.uid32 (gcc version egcs1
```

## traceroute

To display the network route to a specified host and identify faulty gateways, use the following command.

```
traceroute [-f first_ttl] [-m max_ttl] [-w waittime] host [packetlength]
```

#### Syntax Description

|                  |                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------------|
| <b>-f</b>        | (Optional) Sets the time-to-live used in the first outgoing probe packet.                         |
| <i>first_ttl</i> | Time-to-live value of the first outgoing probe packet. The default is 1 hop.                      |
| <b>-m</b>        | (Optional) Sets the maximum time-to-live (maximum number of hops) used in outgoing probe packets. |
| <i>max_ttl</i>   | Maximum time-to-live for outgoing probe packets. The default is 30 hops.                          |

|                     |                                                                                             |
|---------------------|---------------------------------------------------------------------------------------------|
| <b>-w</b>           | (Optional) Sets the time to wait for a response to a probe, in seconds.                     |
| <i>waittime</i>     | Time to wait for a response to a probe, in seconds. The default is 5.                       |
| <i>host</i>         | Name or IP address of host to which to connect.                                             |
| <i>packetlength</i> | (Optional) The length of the packet to send, in bytes. The default and minimum value is 40. |

## Usage Guidelines

The **tracert** command displays a list of the hosts that receive probe packets as they travel to the destination host, in the order that the receiving hosts receive the packets. Asterisks (\*) appear as the list entry for hosts that do not respond to probing correctly.

## 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:

```
tracert -m 20 -w 10 cisco.com 50
tracert 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](#)

# Privilege Level 15 Commands

This section describes the privilege level 15 commands. Only users with privilege level 15 can run these commands.

## auth

Use the following command to enable secure remote authentication.

```
auth { cli | http } { local | tacacs secret server1 [server2] | radius secret server1 [server2] | nt domain pdc [bdc] }
```

### Syntax Description

|                |                                                                                              |
|----------------|----------------------------------------------------------------------------------------------|
| <b>cli</b>     | Enables authentication using the Command Line Interface (CLI).                               |
| <b>http</b>    | Enables authentication using Hypertext Transfer Protocol (HTTP).                             |
| <b>local</b>   | Enables local authentication.                                                                |
| <b>tacacs</b>  | Enables authentication using the TACACS+ (Terminal Access Controller Access Control System). |
| <b>radius</b>  | Enables authentication using RADIUS (Remote Dial-In User Service).                           |
| <b>nt</b>      | Enables authentication from an NT domain controller.                                         |
| <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>domain</i>  | NT domain name.                                                                              |
| <i>pdc</i>     | Name of the Primary Domain Controller (PDC).                                                 |
| <i>bdc</i>     | Name of the Backup Domain Controller (BDC).                                                  |

## Example

This command enables secure remote authentication from a remote server, using TACACS.

```
auth http tacacs tr5e43 209.165.200.224
```

## backup

Use the following command to back up the WLSE.

**backup [test]**

## Syntax Description

|             |                                                                          |
|-------------|--------------------------------------------------------------------------|
| <b>test</b> | Tests the 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.

## Related Commands

[backupconfig](#)

[listbackup](#)

[restore](#)

[show backupconfig](#)

# backupconfig

Use the **backupconfig** command to specify the location for all backup and restore operations. To clear the backup and restore configuration information, use the **no backupconfig** command.

**backupconfig** { *hostname* } { *username* } { *password* } [ *directory* ]

**no backupconfig**

## Syntax Description

|                  |                                                                                |
|------------------|--------------------------------------------------------------------------------|
| <i>hostname</i>  | Host name or IP address of the host system.                                    |
| <i>username</i>  | Username of host system.                                                       |
| <i>password</i>  | Password of the host system.                                                   |
| <i>directory</i> | Path to specific backup directory, if different from user's default directory. |

## 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](#)

[listbackup](#)

[restore](#)

[show backupconfig](#)

## cdp

Use the **cdp** command to configure the Cisco Discovery Protocol (CDP). CDP allows a Cisco device to recognize, and be recognized by, other Cisco devices.

```
cdp { run [port] | timer seconds | holdtime seconds }
```

```
no cdp { run [port] | timer | holdtime }
```

### Syntax Description

|                 |                                                                                                                                                                                                                                                                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>run</b>      | Start CDP; starts the WLSE sending out signals to other devices.                                                                                                                                                                                                                                                                                  |
| <b>timer</b>    | Set CDP packets retransmission time; sets the amount of time, in seconds, that CDP signals are sent.                                                                                                                                                                                                                                              |
| <b>holdtime</b> | Set CDP packet information hold time; sets 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>port</i>     | Ethernet port on which CDP will be enabled. Acceptable values are eth0-5. 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

If you are using 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
```

## clock

To set the system date and time, use the following command. 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. You can enter full month names or abbreviations that include at least the first 3 characters of the month name (for example, jan, feb, mar). |
| <i>day</i>      | Day of the month (for example, 1 to 31).                                                                                                                    |
| <i>year</i>     | Current year (for example, 2000).                                                                                                                           |

### Usage Guidelines

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:

- 
- |               |                                              |
|---------------|----------------------------------------------|
| <b>Step 1</b> | Stop services:<br><pre>services stop</pre>   |
| <b>Step 2</b> | Change the time.                             |
| <b>Step 3</b> | Start services:<br><pre>services start</pre> |
-

To set the date and time, use the **set** option.

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 *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine*, 2.5.

### 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](#)  
[show clock](#)

## df

To display the current storage usage on the WLSE, use the following command.

**df**

### Usage Guidelines

This command is primarily 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

```

## dumptcp

The following command displays 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]]

```

### 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>               | The 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).                                                                                                                                                                                                                  |

### 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:

```
dump tcp proto snmp interface eth0
```

The following command listens to packets from port 161 only with abc.com as either the source or destination host:

```
dump tcp port 161 host abc.com
```

## erase config

To erase the configuration in flash memory and reload the device, use the following command.

```
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 is erased and the system reboots automatically. The system will not operate until you reconfigure it.

---

When the system reboots, you must reconfigure it with the setup program. For information about using the setup program, see the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine, 2.5*.

### Example

This command erases the system configuration:

```
erase config
```

```
This will erase your configuration, return device t
```

```
o factory defaults, and reload the device
Do you want to continue?[no]:yes
```

## firewall

The following command implements port filtering on the WLSE.

```
firewall eth [0-5] [public | private | none] | [icmp telnet ssh snmp
https 1741 repository tftp traceroute]]
```

### Syntax Description

|                   |                                                                                                                                                                                 |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>eth [0-5]</b>  | 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>public</b>     | Denies access via Internet Control Message Protocol (ICMP), Telnet, SNMP, and the HTTP 1741 port.                                                                               |
| <b>none</b>       | Disables the firewall on an interface.                                                                                                                                          |
| <b>private</b>    | Denies no access.                                                                                                                                                               |
| <b>icmp</b>       | Denies ICMP ping messages.                                                                                                                                                      |
| <b>telnet</b>     | Denies incoming Telnet connections.                                                                                                                                             |
| <b>ssh</b>        | Denies incoming SSH connections.                                                                                                                                                |
| <b>snmp</b>       | Denies incoming SNMP requests.                                                                                                                                                  |
| <b>https</b>      | Denies all connections to the SSL HTTP port.                                                                                                                                    |
| <b>1741</b>       | Denies all connections to the HTTP 1741 port.                                                                                                                                   |
| <b>repository</b> | Disables the local software repository from access from the network.                                                                                                            |
| <b>traceroute</b> | Prevents the WLSE from responding to traceroute commands.                                                                                                                       |
| <b>tftp</b>       | Disables TFTP access.                                                                                                                                                           |

### 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 the following command:

```
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 the following command:

```
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.

## gethostbyname

Use the following command to display the IP address of a known domain name.

```
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
```

# hostname

To change the system host name, use the following command.

**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) and the minus sign (-). |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------|

## Example

The following example changes the hostname to sandbox:

```
hostname sandbox
```

# import

To import host files, or to map IP addresses to hostnames, use the following command:

```
import {host hostname ipaddress} | {hosts ftp-host username password path}
no import {host hostname ipaddress} | {hosts}
```

## Syntax Description

|                  |                                                 |
|------------------|-------------------------------------------------|
| <b>host</b>      | Maps one IP address to a hostname.              |
| <i>hostname</i>  | Hostname to map IP address to.                  |
| <b>hosts</b>     | Imports host files from an FTP-accessible host. |
| <i>ipaddress</i> | IP address to map Hostname to.                  |
| <i>password</i>  | Password used to access an FTP-accessible host. |
| <i>path</i>      | Path to an FTP-accessible host.                 |
| <i>ftp-host</i>  | IP address of an FTP-accessible host.           |

*username* username use to access an FTP-accessible host.

## Usage Guidelines

To map a single hostname to an IP address:

**import host** *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 a 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
```

## install configure

To define the repository that the WLSE uses to install software updates and images, use the following command. A repository is a remote or local server from where a system can download software updates and images. Only HTTP is supported.

**install configure** {*URL URL Value* | **default** | **save**}

## Syntax Description

**URL** Sets the URL of the repository.

|                  |                                                                                                                   |
|------------------|-------------------------------------------------------------------------------------------------------------------|
| <i>URL Value</i> | The URL of the repository. The URL should take the form of http://host:port/path (the path is not a requirement). |
| <b>default</b>   | Configures the Wireless LAN Solution Engine to be its own repository. The URL is http://localhost:9851.           |
| <b>save</b>      | Saves the current configuration in the install.ini file.                                                          |

## Example

The following command configures the WLSE to use http://209.165.200.22, with port 9851, as a repository:

```
install configure URL http://209.165.200.224:9851
```

## Related Commands

[install update](#)

[install list](#)

# install list

To list software updates and images currently available on the configured repository, use the following command. A repository is a remote or local server from where a system can receive software.

```
install list [all | full | page | updates]
```

## Syntax Description

|             |                                                                                                                                                                              |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>all</b>  | Displays all software updates and images on a configured repository. This command displays the name, the version, the requirements, the type, and a summary of the software. |
| <b>full</b> | Displays only the complete images on a configured repository. This command displays the name, the version, the requirements, the type, and a summary of the image.           |
| <b>page</b> | Displays only the names of all software updates and images on a configured repository. All other information is omitted.                                                     |

**updates** Displays only the updates on a configured repository. This command displays the name, the version, the requirements, the type, and a summary of the update.

Example

The following command lists all software updates in the repository:

```
install list all
```

| Name       | Version | Requires | Type     | Summary             |
|------------|---------|----------|----------|---------------------|
| EX-1.02    | 1.02    | HSE-1.0  | UPDATE   | Hosting Solution... |
| EX-1.1aR   | 1.1aR   | HSE-1.1  | UPDATE   | Hosting Solution... |
| EX-1.1a    | 1.1a    | HSE-1.1  | UPDATE   | Hosting Solution... |
| EX-1.0a    | 1.0a    | HSE-1.0  | UPDATE   | Hosting Solution... |
| EX-1.0aR   | 1.0aR   | HSE-1.0  | UPDATE   | Hosting Solution... |
| EX-1.0-ROB | 1.0     | HSE-1.0  | COMPLETE | Hosting Solution... |
| EX-1.0     | 1.0     | HSE-1.0  | COMPLETE | Hosting Solution... |

Related Commands

- [install configure](#)
- [install update](#)

install update

To install a software update or image, use the following command.

**install update** *package name*

Syntax Description

*Package Name* Name of the software update or image to be installed. To see the names of software updates and images available for installation, use the **install list** command. For more information, see [install list](#), page B-29.

Example

The following command installs the update EX-2.0:

```
install update EX-2.0
```



## Related Commands

[install configure](#)

[install list](#)

## interface

To configure an Ethernet interface, use the following command.

```
interface eth[ernet][0-5] { [up | down] | ipaddress netmask
 [default-gateway address] [up | down] }
 [auto | speed [10 | 100 | 1000]] duplex [half | full]
 mtu [46-1500]
```

## Syntax Description

|                        |                                                                                                                                                                                                                                                                                                                                 |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>eth</b> [0-5]       | 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>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.<br><br>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.                                                                                                         |
| <i>ipaddress</i>       | The IP address of the interface.                                                                                                                                                                                                                                                                                                |
| <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- or full-duplex mode.           |
| <b>mtu</b> [46-1500]      | Set the maximum packet size, in bytes.                |

## Default

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.

## Usage Guidelines

If you change the IP address or hostname, follow these steps to make sure that applications can connect to the WLSE:

- 
- Step 1** Stop and restart management services by entering:
 

```
services stop
services start
```
  - Step 2** Verify that management applications can still connect to the WLSE.
  - Step 3** Reconnect any applications that cannot connect to it using the system's new IP address or hostname.
- 

## 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
```

## ip domain-name

To define a default domain name, use the following command. 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

*name* Domain name (for example, cisco.com).

### Example

This command defines the default domain name cisco.com:

```
ip domain-name cisco.com
```

This command removes the default domain name:

```
no ip domain-name
```

### Related Commands

[\*\*ip name-server\*\*](#)

## ip name-server

To specify the addresses of up to three name servers for name and address resolution, use the following command. 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

*ip-address*                      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](#)

# listbackup

Use the following command to list all current backups at the configured site.

## listbackup

### Syntax Description

This command has no arguments or keywords.

### 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](#)

[backupconfig](#)

[restore](#)

[show backupconfig](#)

# mail

To debug and test email settings, use the **mail** command.

```
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:

**to** Sends email to the expressed recipient.

*user@host* Recipient of the email.

To debug email problems, use the **debug** argument.

## 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.

## mailcntrl clear

To delete the mail log, send queue, or user queue, use the following command.

```
mailcntrl clear {log | sendqueue | userqueue}
```

## Syntax Description

|                  |                               |
|------------------|-------------------------------|
| <b>log</b>       | Clears the WLSE's email log.  |
| <b>sendqueue</b> | Clears the WLSE's send queue. |
| <b>userqueue</b> | Clears the WLSE's user queue. |

## Example

The following command clears the WLSE's email log.

```
mailcntrl clear log
```

## Related Commands

[mailcntrl list](#)

## mailcntrl list

To list the size of the mail log, user queue, or the send queue, use the following command.

```
mailcntrl list {logsize | sendqueuesize | userqueuesize}
```

### Syntax Description

|                      |                        |
|----------------------|------------------------|
| <b>logsize</b>       | Size of the mail log.  |
| <b>sendqueuesize</b> | Size of the sendqueue. |
| <b>userqueuesize</b> | Size of the userqueue. |

### Example

The following command displays the size of the WLSE's email log.

```
mailcntrl list logsize
Mail log files total size: 4.0k
```

### Related Commands

[mailcntrl clear](#)

## 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 resolve the correct email server in your local domain. To stop forwarding mail to the SMTP server, use the **no mailroute** command to remove the 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
```

mkcert

Use this command to generate a Certificate Signed Request (CSR) for enabling secure socket layer protocol (SSL), which 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 set up procedure enables SSL.

The unsigned certificate expires in one year; use the **mkcert** command or the Web interface to obtain a permanent, signed certificate.



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**                      Creates a CSR.

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<br>2. State or Province Name<br>3. Locality Name | Country, state or province, and city in which the WLSE is located. Use the 2-character code for the country and the full names of state or province and city. |



| Prompt                      | Response                                                            |
|-----------------------------|---------------------------------------------------------------------|
| 4. Organization Name        | Full name of the organization that owns the WLSE.                   |
| 5. Organizational Unit Name | (Optional) Section of the organization that is using the WLSE.      |
| 6. Common Name              | Fully qualified domain name of the organization that owns the WLSE. |
| 7. Email Address            | Email address of the organization that owns the WLSE.               |

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** Using the WLSE Web interface on the same client, select **Administration > Security > SSL (HTTPS)**.
- Step 3** Enter the path to the certificate or click **Browse** to locate it. Then click **Submit Certificate**.
- Step 4** To use the new certificate, restart the WLSE by running the following commands:
- ```
services stop
services start
```
-

nslookup

To translate a device name to its IP address or an IP address to its device name, use the following command.

```
nslookup {dns-name | ip-address}
```

Syntax Description

dns-name Device name of a host on the network.

ip-address 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

To configure the Network Time Protocol (NTP) and allow the system clock to be synchronized by a time server, use the following command. To disable this function, use the **no** form of this command.

```
ntp server ip-address
```

```
no ntp server ip-address
```

Syntax Description

ip-address IP address of the NTP time server providing clock synchronization.

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 [show clock](#), page B-11.

- 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

[show clock](#)

reload

To reboot the system, use the following command.

```
reload
```

Syntax Description

This command has no arguments or keywords.

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](#)

reinitdb

To reinitialize the database, use the following command. This command erases all information contained within the database and stops and restarts system services.

```
reinitdb
```



Note

This command stops and restarts system services.

Syntax Description

This command has no arguments or keywords.

Example

This command reinitializes the database:

```
reinitdb
```

Related Command

[services](#)

repository add

Use this command to transfer software updates and images from a remote server to the WLSE's local repository.

repository add *package*

Syntax Description

package Name of the software update or image to be transferred.

Usage Guidelines

You will be prompted to enter a username and password if they are needed to access the remote server.

Example

To transfer the update EX_2.0 from an update server to the local repository, enter the following command:

```
repository add ex_2.0
```

Related Commands

[repository source](#)

[repository delete](#)

[repository list](#)

[repository server](#)

repository delete

To delete software updates and images on the WLSE's local repository, use the following command. A repository is a remote or local server from where a system can receive software updates and images.

repository delete [*package* | **all**]

Syntax Description

all	Deletes all software updates and images in the local repository.
<i>package</i>	Name of the software update or image to be deleted.

Example

The following command deletes the update EX_2.0 from the local repository:

```
repository delete EX_2.0
```

Related Commands

[repository source](#)

[repository add](#)

[repository list](#)

[repository server](#)

repository list

To list software updates and images on the configured local or remote repository, use the following command.

```
repository list { local | remote } [ detail ] [ page ]
```

Syntax Description

local	Lists software updates and packages on the local repository.
remote	Lists software updates and packages on a remote repository.
detail	Includes details of the software updates and images displayed.
page	Displays the software updates and packages on page at a time.

Example

To list the software updates and images available on the configured local repository, with details and one page at a time, enter the following command:

```
repository list local detail page
```

Related Commands

[repository source](#)

[repository add](#)

[repository delete](#)

[repository server](#)

repository source

To configure the WLSE to be a repository for software updates, use the following command.

```
repository source URL
```

Syntax Description

source	Sets the location from where the local repository downloads software updates and images.
<i>URL</i>	The IP address of an external server containing software updates and images.

Usage Guidelines

The **repository** command allows the WLSE to be a repository both for itself and for external systems. A repository is a remote or local server from where a system can receive software updates and images.

The **repository** command only configures the WLSE to be a repository. To configure the WLSE to install software updates and images from this repository, see [install configure](#), page B-28.

Example

To configure the WLSE to be a repository, and to download software updates and images from `http:// 209.165.200.224`, enter the following command:

```
repository source ftp://209.165.200.224
```

Related Commands

[repository add](#)

[repository delete](#)

[repository list](#)

[repository server](#)

repository server

To start, stop, or view the status of the WLSE's local repository, use the following command. A repository is a remote or local server from where a system can receive software updates and images.

```
repository server [stop | start | status]
```

Syntax Description

stop	Stops the local repository.
start	Starts the local repository.
Status	Displays the status of the local repository.

Example

The following command stops the local repository:

```
repository server stop
```

Related Commands

[repository source](#)

[repository add](#)

[repository delete](#)

[repository list](#)

restore

Use the following command to restore a backed up configuration of the WLSE.

```
restore -n backup_name
```

Syntax Description

backup_name Name of backup.

-n Restores without overwriting the flash memory, which contains network information (WLSE hostname, IP address, domain name, name servers, NTP server) and users' CLI privileges.

Usage Guidelines

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 8-21](#).

Example

The following command restores the backup called **backup1** from the configured backup location:

```
restore backup1
```

Related Commands

[backup](#)

[backupconfig](#)

[listbackup](#)

[show backupconfig](#)

route

To add a route through a gateway device, use the **route** command. To delete a route, use the no version of the command.

```
route { network address } netmask { network netmask }  
      gateway { gateway address }
```

```
no route { network address } netmask { network netmask }
```

Syntax Description

netmask	Sets value of the network netmask.
gateway	Sets the IP address of the router or gateway.
<i>network address</i>	IP address of the network.
<i>network 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 netmask 255.255.255.224 gateway 209.165.200.224
```

The following command deletes the above route:

```
no route 209.165.201.0 netmask 255.255.255.224
```

services

To list, start, or stop the management services running on the system, use the following command.

```
services [ status | start | stop ]
```

Syntax Description

status	Displays the management services status.
start	Starts the management services.

stop Stops the management services.

Usage Guidelines

Management services are the software installed on the system by network management applications. Use this command to stop and restart the 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= HSECollector
    State = Running but busy flag set
    Pid   = 588
    RC    = 0
    Signo = 0
    Start = 06/15/01 16:54:32
    Stop  = Not applicable
    Core  = Not applicable
    Info  = HSECollector started.

Process= HSEANIServer
    State = Running but busy flag set
    Pid   = 589
    RC    = 0
    Signo = 0
    Start = 06/15/01 16:54:32
-----more-----
```

Related Commands

[show proc](#)

show anilog

To display the WLSE's ANI log, use the following command.

```
show anilog [ page ] | include MatchString1 [ MatchString2 ]
```

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press Ctrl-c to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
<i>matchstring1</i>	String of characters to search for in the command output.
<i>matchstring2</i>	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the WLSE's ANI log, one page at a time:

```
show anilog page
/var/adm/CSCOets/log/ani.log
SNMPThrPool: Instantiated ex.lib.snmp.lib.timer.DynamicThreadPool, min=15, max=48, maxIdleSecs=240
2001/12/20 13:43:12 main ani MESSAGE DBConnection: Created new Database connection
on [hashCode = 45981573]
2001/12/20 13:43:38 main ani MESSAGE ServletServiceModule: Moxie Servlet Engine
is ready to receive requests
2001/12/20 15:43:39 HSEStatusPoll ani MESSAGE DBConnection: Created new Database
connection [hashCode = 85057415]
2001/12/20 17:43:39 HSEStatusPoll ani MESSAGE DBConnection: Created new Database
connection [hashCode = 396959623]
2001/12/20 19:43:39 HSEStatusPoll ani MESSAGE DBConnection: Created new Database
--More--
```

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 the WLSE's local authentication is being used for the CLI:

```
show auth-cli
local
```

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
local
```

show backupconfig

The following command displays 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](#)

[backupconfig](#)

[listbackup](#)

[restore](#)

show bootlog

To display the messages logged during the last system boot, use the following command.

```
show bootlog [ page ]
```

Syntax Description

page Displays command output one screen at a time. Press the **return** key to display the next output screen. Press **Ctrl-c** 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)
PCI: PCI BIOS revision 2.10 entry at 0xfda95
PCI: Using configuration type 1
-----more-----
```

Related Commands

[reload](#)

[show clock](#)

show cdp neighbor

Use this command to display the WLSE's 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

This 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.
```

show collectorlog

To display the WLSE's collector log, use the following command.

```
show collectorlog [page] | include matchstring1 [matchstring2]
```

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press Ctrl-c to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
<i>matchstring1</i>	String of characters to search for in the command output.
<i>matchstring2</i>	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the WLSE's collector log, one page at a time:

```
show collectorlog page
/var/adm/CSCOets/log/collector.log
2001/12/20 13:43:18 main HSECollector MESSAGE CollectorMain: Waiting
for databas
e to be ready
2001/12/20 13:43:21 main HSECollector MESSAGE CollectorMain: Database
is ready
SNMPThrPool: Instantiated ex.lib.snmp.lib.timer.DynamicThreadPool, mi
n=15, max=48, maxIdleSecs=0
2001/12/20 13:43:29 main HSECollector MESSAGE ServletServiceModule:
Moxie Servle
t Engine is ready to receive requests
2001/12/20 13:43:30 PeriodicSchedulerRun:FaultCleanup HSECollector
MESSAGE Colle
ctorDBUtils: DB.TableCleanupCommand=[VACUUM ]
2001/12/20 13:43:30 PeriodicSchedulerRun:FaultCleanup HSECollector
MESSAGE Colle
```

```
ctorDBUtils: DB.TableUpdateStatsCommand=[VACUUM ANALYZE ]
2001/12/21 10:39:52 Moxie Servlet Engine:Pooled Thread:1 HSECollector
MESSAGE Se
rvletContextAdaptor: Collector: init
```

show config

To display the system configuration, use the following command.

show config

Syntax Description

This command has no arguments or keywords.

Example

This command displays the system configuration:

```
show config
hostname ex1
interface ethernet0 209.165.201.0 255.255.255.224 default-gateway
209.165.202.128
interface ethernet1 down
interface ethernet2 down
interface ethernet3 down
interface ethernet4 down
interface ethernet5 down
ip domain-name embu-doc
ip name-server 209.165.202.158
username admin epassword ***** privilege 15
```

show daemonslog

To display the WLSE's daemons log, use the following command.

```
show daemonslog [ page ] | include matchstring1 [ matchstring2 ]
```

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press Ctrl-c to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
<i>matchstring1</i>	String of characters to search for in the command output.
<i>matchstring2</i>	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the WLSE's daemons log, one page at a time:

```
show daemonslog page
/var/adm/CSCOets/log/daemons.log
[dmgrDbg] getenv(PX_DBG)=NULL
[dmgrDbg] getenv(PX_MY_DEBUG)=NULL
[dmgrDbg] getenv(PX_MY_TRACE)=NULL
[dmgrDbg] getenv(PX_DBG_LEVEL)=NULL
[dmgrDbg][Thu Dec 20 13:42:53 2001]##### INFO ##### re-evaluate
DbgLevel=0x0
++>>it(1) = 8077978 <HSECollector>
++>>it(1) = 8077898 <HSEANIServer>
++>>it(1) = 8077428 <PostgreSQL>
++>>it(1) = 8077228 <WebServer>
++>>it(1) = 8077328 <Tomcat>
++>>it(1) = 80770d8 <ExcepReporter>
++>>it(1) = 8076fc8 <CDPbrdcast>
++>>it(1) = 8076e58 <PerfMon>
#!/bin/sh -v
#!/bin/sh -v

if [ "$NMSROOT" = "" ]; then
    NMSROOT=/opt/CSCOets
    export NMSROOT
```

```

fi

cd $NMSROOT
--More--

```

show dmgtldlog

To display the WLSE's daemon manager log, use the following command.

```
show dmgtldlog [ page ] | include matchstring1 [ matchstring2 ]
```

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press Ctrl-c to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
<i>matchstring1</i>	String of characters to search for in the command output.
<i>matchstring2</i>	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the daemon manager log, one page at a time:

```

show dmgtldlog page
/var/adm/CSCOets/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
collector) "/bin/nice -n 19 /opt/CSCOets/bin/collector" pid=715.
Dec 20 13:42:56 ex dmgt[714]: #3007:TYPE=INFO:Started application(HSEA
--More--

```

show import

To display an imported host file, use the following command.

show import *hosts*

Syntax Description

hosts Name of server that host files were imported from.

Example

This command displays the imported host file.

```
show import ftpserver_1
```

show install logs

Displays the software updates and images available on the configured repository.

show install logs [**short** | **long**] [**page**]

Syntax Description

short	Displays only the names of software updates and images on the configured repository
long	Displays the names and descriptions of software updates and images on the configured repository.
page	Displays command output one screen at a time.

Example

The following command displays the software updates and images available on the configured browser, one screen at a time:

```
show install updates page
2
NAME=EX-2.0a
```

show ipchains

This command displays the IP chains for the selected interface.

show ipchains eth[0-5]

Syntax Description

eth[0-5] 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.

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
```

show hosts

This command displays the WLSE's host file.

show hosts [page]

Syntax Description

page Displays command output one screen at a time.

Example

The following command displays the host file one page at a time:

```
show hosts page
```

show maillog

To display the WLSE's mail log, use the following command.

```
show maillog [ page ] | include matchstring1 [ matchstring2 ]
```

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press Ctrl-c to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
<i>matchstring1</i>	String of characters to search for in the command output.
<i>matchstring2</i>	(Optional) Another string of characters to search for in the command output.

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, cla
ss=0, pri=30307, nrcpts=1, msgid=<200112210402.EAA11643@ex.help>, rela
y=root@localhost
Dec 21 04:02:06 ex sendmail[11660]: EAA11643: SYSERR(root): Cannot exe
c /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
```


show proc

To display the WLSE's active process statistics, use the following command.

show proc [page]

Syntax Description

page Displays command output one screen at a time.

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
-----more-----
```

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 command output one screen at a time.

Example

This command displays the status of the configured repository:

```
show repository status
Repository Source: 171.69.212.146:9851
repository is running.
```

show route

To display the routes that are currently configured, use the following command.

```
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
```

show securitylog

To display the WLSE's security log information, use the following command.

```
show securitylog [ page ] | include matchstring1 [ matchstring2 ]
```

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press Ctrl-c to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
<i>matchstring1</i>	String of characters to search for in the command output.
<i>matchstring2</i>	(Optional) Another string of characters to search for in the command output.

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
Dec 20 13:46:39 ex in.tftpd[1430]: connect from 209.165.200.224
Dec 20 13:46:43 ex in.tftpd[1432]: connect from 209.165.200.224
Dec 20 13:46:47 ex in.tftpd[1434]: connect from 209.165.200.224
--More--
```

show snmp-server

The following command displays the WLSE's 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
```

show ssh-version

The following command displays 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
```

show syslog

To display syslog information, use the following command.

```
show syslog [ page ] [ include matchstring1 [ matchstring2 ]]
```

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press Ctrl-c to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
<i>matchstring1</i>	String of characters to search for in the command output.
<i>matchstring2</i>	(Optional) Another string of characters to search for in the command output.

Usage Guidelines

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
-----more-----
```

Related Command

[interface](#)

show tech

Use the following command to display information necessary for Cisco's Technical Assistance Center to assist you:

show tech [page]

Syntax Description

page Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** 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
-----more-----
```

show telnetenable

To display the WLSE's Telnet status, use the following command.

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
```

show tomcatlog

To display the WLSE's Tomcat log, use the **show tomcatlog** command.

```
show tomcatlog [ page ] | include matchstring1 [ matchstring2 ]
```

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press Ctrl-c to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
<i>matchstring1</i>	String of characters to search for in the command output.
<i>matchstring2</i>	(Optional) Another string of characters to search for in the command output.

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)
--More--
```

show webaccesslog

To display the WLSE's Web access log, use the following command.

```
show webaccesslog [ page ] [ include matchstring1 [ matchstring2 ]
```

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press Ctrl-c to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
<i>matchstring1</i>	String of characters to search for in the command output.
<i>matchstring2</i>	(Optional) Another string of characters to search for in the command output.

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-CKK-MCD (Windows NT 5.0; U)"
209.165.200.224 - - [21/Dec/2001:10:38:54 +0000] "GET
/per1/login-form.cgi HTTP/1.0"
0" 200 2268 "-" "Mozilla/4.76 [en]C-CKK-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/per1/login-form.cgi" "Mozilla/4.76
[en]C-CKK-MC
D (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/per1/login-form.cgi"
"Mozilla/4.76 [en]C-CC
K-MCD (Windows NT 5.0; U)"
--More--
```


show weberrorlog

To display the WLSE's Web error log, use the following command.

```
show weberrorlog [ page ] [ include matchstring1 [ matchstring2 ]
```

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press Ctrl-c to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
<i>matchstring1</i>	String of characters to search for in the command output.
<i>matchstring2</i>	(Optional) Another string of characters to search for in the command output.

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 c
onfiguration
[Thu Dec 20 13:43:00 2001] [error] (22)Invalid argument: <Perl>:
```

show websslaccesslog

To display the WLSE's Web SSL log, use the following command.

```
show websslaccesslog [ page ] | include matchstring1 [ matchstring2 ]
```

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press Ctrl-c to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
<i>matchstring1</i>	String of characters to search for in the command output.
<i>matchstring2</i>	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Web SSL log, one page at a time:

```
show websslaccesslog page
```

shutdown

To shut down the system in preparation for powering it off, use the following command.

```
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](#)

snmp-server

To configure an simple network management protocol (SNMP) agent, use the following command.

```
snmp-server { community community-name [ RO | RW ] | location sysLocation-info | contact sysContact-info }
```

```
no snmp-server { community community-name | location | contact }
```

Syntax Description

community	sets the community strings that permit access to the SNMP.
<i>community-name</i>	the community name string.
RO	read only.
RW	read / write.
location	sets the system location string.
<i>sysLocation-info</i>	the location string.
contact	sets the contact string.

sysContact-info the contact string.

Example

This command sets an SNMP contact string:

```
snmp-server contact Dial System Operator at Beeper # 27345
```

ssh

To use SSH to connect to an external host, use the following command.

```
ssh [ options ] host [ command ]
```

Syntax Description

<i>options</i>	Standard SSH options. For a list of these options, enter the ssh command without any arguments.
<i>host</i>	Name or IP address of host to which to connect.
<i>command</i>	Command for the external host to execute.

Example

Enter the following command to connect to an external host using SSH:

```
ssh 209.165.200.224
```

ssh-version

Use this command to enable Secure Shell (SSH) 1, SSH 2, or both SSH 1 and SSH 2.

```
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
```

telnet

To Telnet to an external host, use the telnet command.

```
telnet { hostname | ip-address } [ portnumber ]
```

Syntax Description

<i>hostname</i>	Hostname of the external device.
<i>ip-address</i>	IP address of the external device.
<i>portnumber</i>	portnumber of the external device.

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
```

telnetenable

To configure Telnet access, use the following command.

```
telnetenable { enable [ ip-addresses | domains ] | disable | status }
```

Syntax Description

enable	Enables Telnet access to the system.
disable	Disables Telnet access to the system.
status	Displays current access status.

<i>ip-addresses</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>domains</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.

Default

The default is **disable**.

Usage Guidelines

To enable Telnet access to the system for *all* IP source addresses, use the **telnetenable enable** command alone. To enable *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
```

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 password [ privilege { 0 | 15 } ]
```

```
no username name
```

Syntax Description

<i>name</i>	Name of the user account to create or remove. User names can be up to 32 characters long.
password	Specifies a password for the account.

<i>password</i>	The password for the account. Passwords can be 5 to 8 characters long.
privilege	(Optional) Specifies the account privilege level.
0	Gives the account level 0 privileges. This is the default.
15	Gives the account level 15 privileges.

Usage Guidelines

The default privilege level is 0 if you do not provide the privilege option.

For information on the allowable characters in user names and passwords, see [Appendix A, “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 with system administrator privileges.
 - 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 the *User Guide for the Wireless LAN Solution Engine*.

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

This command sets 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 the 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 the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine, 2.5*.

erase config

This command is identical to the level-15 **erase config** command. For a description, see [erase config, page B-24](#).

fsck

To check and repair the filesystem, use the following command.

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 B-42](#).



A

AAA Authentication, Authorization, and Accounting. The WLSE monitors LEAP, PEAP, EAP-MD5 and RADIUS AAA services provided by AAA servers running CiscoSecure ACS Server software.

See also [EAP-MD5 server](#), [LEAP server](#), [PEAP server](#), and [RADIUS](#).

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.

ANI Asynchronous Network Interface. A mediation layer between the network devices and client applications. ANI provides discovery, inventory, and topological computations of networks and their devices

B

BDPU Bridge Protocol Data Unit. *See* [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	See wireless bridge .
BSS	Basic Service Set—a set of 802.11 stations associated with a single AP.

C

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 1105 Wireless LAN Solution Engine</i> —from the online help, click PDF .
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

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 <code>http://www.website.com</code> might actually point to the IP address <code>http://123.456.789.0</code> . 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.
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.

E

EAP-MD5 server	Servers running extensible authentication protocol to provide 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. <i>See also</i> AAA .
exception	A group of related faults.

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](#).

H

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). *See also* [SSL](#).

I

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.

L

LEAP server Light EAP server, which combines centralized two-way authentication with dynamically generated wireless equivalent privacy keys or WEP keys.

See also [AAA](#) and [WEP keys](#).

M

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 Media Interface Connector. FDDI de facto standard connector.

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).

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.

P

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 proxyMobile 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

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. <i>See also AAA.</i>
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.
RSA	Rivest, Shamir, and Adelman (RSA), the inventors of the technique. Public-key cryptographic system that can be used for encryption and authentication.

S

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.
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	Spanning tree algorithm. Algorithm used by the Spanning-Tree Protocol to create a spanning tree.
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.
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.

tracert 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

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.

UTC Coordinated Universal Time. Time zone at zero degrees longitude. Formerly called Greenwich Mean Time (GMT) and Zulu time.

V

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

WDS	Wireless Domain Services. An access point 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, the WDS access point forwards the client's credentials to the new access point with the multicast key. <i>See also</i> WLCCP .
WISPr	Wi-Fi Service Provider Roaming.
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.
wireless bridge	Designed to connect two or more networks (typically located in different buildings). Bridges connect hard-to-wire sites, noncontiguous 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.
WGB	Workgroup bridges (WGB) 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.
WLCCP	Wireless LAN Context Control Protocol. Protocol used by the WLSE to authenticate with an access point that provides WDS to the wireless LAN network. <i>See also</i> WDS .



Numerics

11a radio (non-IOS), configuring [4-175](#)

advanced [4-185](#)

data encryption [4-195](#)

filters [4-179](#)

hardware [4-180](#)

identification [4-176](#)

module service sets [4-199](#)

primary module service set [4-204](#)

QoS [4-206](#)

searched channels [4-192](#)

11b radio (non-IOS), configuring [4-157](#)

advanced [4-167](#)

filters [4-160](#)

hardware [4-161](#)

identification [4-158](#)

searched channels [4-173](#)

802.11a radio (IOS), configuring [4-19](#)

802.11b radio (IOS), configuring [4-11](#)

A

AAA

ACS failed login report [8-48](#)

definition [GL-1](#)

server

adding [3-37](#)

deleting [3-37](#)

setting up [3-25](#)

services supported [3-38](#)

access point

accessing through WLSE,
troubleshooting [10-4](#)

AP and bridge connected to router report,
displaying [6-68](#)

AP and bridge connected to switch report,
displaying [6-66](#)

AP associations report, displaying [6-48](#)

channel loading report (11b) [6-11](#)

configured radio parameters report (11b) [6-9](#)

configuring [4-1](#)

converting from non-IOS to IOS [5-35](#)

definition [GL-1](#)

detailed report, displaying [6-43](#)

Ethernet transmission statistics,
displaying [6-79](#)

Ethertype protocol filters report,
displaying [6-51](#)

faults, displaying [2-6](#)

fault thresholds, setting [2-18](#)

firmware, updating [5-5](#)

- firmware versions, support for [8-38](#)
- group client association report,
 - displaying [6-22](#)
- group performance report
 - Ethernet utilization, displaying [6-74](#)
 - RF utilization, displaying [6-73](#)
- group policy report, displaying [6-38](#)
- group security report, displaying [6-26](#)
- group SSID report, displaying [6-29](#)
- group VLAN report, displaying [6-32](#)
- hot standby report, displaying [6-64](#)
- HTTP username and password,
 - specifying [3-32](#)
- interface
 - adding, results of [10-15](#)
 - removing, results of [10-15](#)
- IOS, converting to [5-20](#)
- IOS reports [6-21](#)
- IP port filters report, displaying [6-53](#)
- IP protocol filters report, displaying [6-52](#)
- limitation on number of [3-80](#)
- non-IOS reports [6-21](#)
- path loss between managed APs report (11b) [6-10](#)
- performance graph, displaying [6-80](#)
- performance table, displaying [6-81](#)
- per VLAN client (group) report,
 - displaying [6-35](#)
- per VLAN client (individual) report,
 - displaying [6-62](#)
- policy report, displaying [6-55](#)
- policy settings [2-18](#)
- QoS report, displaying [6-56](#)
- radio monitoring [7-6](#)
- radio scans [7-9](#)
 - changing job choices [7-19](#)
 - checking status [7-16](#)
 - copying [7-21](#)
 - creating [7-11](#)
 - deleting [7-20](#)
 - filtering [7-18](#)
 - naming [7-12](#)
 - overview [7-9](#)
 - refresh job list [7-23](#)
 - running [7-11](#)
 - scheduling [7-14](#)
 - stopping [7-20](#)
 - viewing run log [7-21](#)
- RF transmission statistics, displaying [6-78](#)
- setting up
 - IOS [3-8](#)
 - non-IOS [3-6](#)
- SSH passwords, specifying [3-33](#)
- SSID report, displaying [6-58](#)
- summary report, displaying [6-40](#)
- system-defined groups for [3-98](#)
- Telnet passwords, specifying [3-33](#)
- template, creating [4-253](#)
- top n busiest clients, displaying [6-82](#)
- top n client bit error rate report,
 - displaying [6-85](#)

- top n client MIC error rate report, displaying [6-84](#)
- top n number of associations report, displaying [6-75](#)
- top n percentage errors report, displaying [6-77](#)
- VLAN report, displaying [6-60](#)
- WDS, configuring for [3-37](#)
- wireless services, configuring for [4-95](#)
- accounting (non-IOS), configuring [4-238](#)
- ACS Failed Login report [8-49](#)
- address filters, configuring [4-110](#)
- admin access
 - (IOS) setting [4-26](#)
 - local (non-IOS), setting [4-209](#)
- advanced
 - associations (non-IOS), configuring [4-142](#)
 - security (IOS), configuring [4-46](#)
 - settings, Ethernet port (non-IOS) [4-154](#)
- aggregation data
 - parameters for [3-90](#)
 - understanding [3-90](#)
- aggregation intervals
 - about [3-90](#)
 - parameters for [3-90](#)
 - resetting [3-87](#)
- ANI
 - definition [GL-1](#)
 - log, displaying [B-51](#)
- AP Ethertype protocol filters report, displaying [6-51](#)
- AP IP port filters report, displaying [6-53](#)
- AP IP protocol filters report, displaying [6-52](#)
- AP policy report, displaying [6-55](#)
- AP QoS report, displaying [6-56](#)
- AP SSID report, displaying [6-58](#)
- AP summary report, displaying [6-40](#)
- AP usage report, displaying [6-70](#)
- AP VLAN report, displaying [6-60](#)
- archives
 - managing, configuration [4-261](#)
- ARP cache
 - configuring
 - IOS template [4-90](#)
- assisted configuration [7-60](#)
- assisted site survey wizard [7-55](#)
- associations (non IOS), setting up
 - address filters [4-110](#)
 - Ethertype filters [4-112](#)
- associations (non-IOS), setting up
 - advanced [4-142](#)
 - DSCP to CoS [4-148](#)
 - IP port filters [4-120](#)
 - IP protocol filters [4-116](#)
 - policy groups [4-124](#)
 - port assignments [4-147](#)
 - primary service set [4-139](#)
 - quality of service [4-133](#)
 - service sets [4-134](#)
 - VLANs [4-126](#)

audience for this document [xix](#)

auth command [9-4, B-17](#)

authentication

- displaying [B-52](#)
- enabling [B-17](#)
- modules supported [8-16](#)
- overview [8-16](#)
- setting up [8-17, 9-4](#)

auto-managed configuration [4-306](#)

- assigning [4-306](#)
- options for email [4-308](#)

auto-managing devices [3-65](#)

automatic configurations, creating [4-300](#)

B

backing up and restoring WLSE configuration

- backing up
 - using CLI commands [9-7](#)
 - using Web interface [8-24](#)
- backup and restore log [8-4](#)
- backup CLI command [B-18](#)
- backupconfig CLI command [B-19](#)
- backup location, configuration
 - using the CLI [9-6](#)
- backup location, configuring
 - on Windows server [8-24](#)
 - using the Web interface [8-22](#)
- listbackup CLI command [B-35](#)

- restore CLI command [B-48](#)
- restoring
 - using the CLI [9-7](#)
 - using Web interface [8-26](#)
- restoring data from one WLSE to another [9-10](#)
- show backupconfig CLI command [B-53](#)
- troubleshooting
 - Windows 2000 or Windows XP server [10-41](#)
- backup command [B-18](#)
- backupconfig command [B-19](#)
- basic template, configuring
 - IOS template [4-4](#)
 - non-IOS template [4-102](#)
- booting, WLSE
 - boot messages, displaying [B-53](#)
 - from the maintenance image [9-20](#)
 - from Web interface [8-5](#)
 - reload command [B-42](#)
 - troubleshooting [10-9](#)
- bridge
 - AP and bridge connected to router report, displaying [6-68](#)
 - AP and bridge connected to switch report, displaying [6-66](#)
 - AP associations report, displaying [6-48](#)
 - configuring [4-1](#)
 - definition [GL-2](#)
 - detailed report, displaying [6-43](#)
 - Ethernet transmission statistics [6-79](#)

- firmware, updating [5-5](#)
- group client association report, displaying [6-22](#)
- group performance report
 - Ethernet utilization, displaying [6-74](#)
 - RF utilization, displaying [6-73](#)
- group policy report, displaying [6-38](#)
- group security report, displaying [6-26](#)
- group SSID report, displaying [6-29](#)
- group VLAN report, displaying [6-32](#)
- limitation on number of [3-80](#)
- performance graph, displaying [6-80](#)
- per VLAN client (group) report, displaying [6-35](#)
- per VLAN client (individual) report, displaying [6-62](#)
- RF transmission statistics, displaying [6-78](#)
- setting up [3-6](#)
- template, creating [4-253](#)
- top n number associations report, displaying [6-75](#)
- top n percentage errors report, displaying [6-77](#)
- browser
 - configuring [1-3](#)
 - date and time display [1-8](#)
 - supported browsers [1-3](#)
 - troubleshooting
 - cannot connect to WLSE [10-7](#)
 - IE, installing software updates [10-40](#)
- building, adding to Location Manager [7-47](#)

C

- cautions
 - conversion from non-IOS to IOS [5-35](#)
 - erase config command [B-24](#)
 - losing data
 - jobs, configuration [4-271](#)
 - jobs, firmware [5-16](#)
 - reload command [B-42](#)
 - shutdown command, failure to run [B-73](#)
 - significance of [xx](#)
- CDP (Cisco Discovery Protocol)
 - alternatives to [3-46](#)
 - configuring
 - displaying configuration [B-55](#)
 - template (IOS) [4-60](#)
 - template (non-IOS) [4-230](#)
 - definition [GL-2](#)
 - enabling on devices [3-5](#)
 - enabling on WLSE [B-20](#)
 - individual device seeding [3-46](#)
 - neighbors of WLSE, displaying [B-55](#)
 - understanding [3-44](#)
- cdp command [B-20](#)
- CDP distance
 - definition of [GL-2](#)
 - specifying [3-58](#)
- channel color key [7-41](#)
- channel loading report (11b), displaying [6-11](#)

- character set, allowable [A-1](#)
- Cisco Access Registrar (CAR) [3-25](#)
- CiscoSecure ACS Server, configuring [3-25](#)
- CiscoWorks server
 - exporting devices to [3-94](#)
 - importing devices from
 - procedure for [3-61](#)
 - understanding [3-51](#)
 - linking to CiscoWorks server [8-48](#)
- CLI
 - access, configuring [8-42](#)
 - command history feature [B-3](#)
 - command privileges [B-2](#)
 - commands [B-1](#)
 - command summary (table) [B-4](#)
 - conventions [B-2](#)
 - definition [GL-2](#)
 - help for commands [B-3](#)
 - maintenance image commands [B-78](#)
 - erase config [B-78](#)
 - fsock [B-79](#)
 - reload [B-79](#)
 - Privilege Level 0 commands [B-10](#)
 - exit [B-10](#)
 - ping [B-10](#)
 - show clock [B-11](#)
 - show domain-name [B-12](#)
 - show interfaces [B-13](#)
 - show process [B-14](#)
 - show version [B-15](#)
 - traceroute [B-15](#)
 - Privilege Level 15 commands [B-17](#)
 - auth [B-17](#)
 - backup [B-18](#)
 - backupconfig [B-19](#)
 - cdp [B-20](#)
 - clock [B-21](#)
 - dumptept [B-23](#)
 - erase config [B-24](#)
 - firewall [B-25](#)
 - gethostbyname [B-26](#)
 - hostname [B-27](#)
 - import [B-27](#)
 - interface [B-31](#)
 - ip domain-name [B-33](#)
 - ip name-server [B-33](#)
 - listbackup [B-35](#)
 - mail [B-35](#)
 - mailcntrl clear [B-36](#)
 - mailcntrl list [B-37](#)
 - mailroute [B-37](#)
 - mkcert [B-38](#)
 - nslookup [B-40](#)
 - ntp server [B-40](#)
 - reload [B-42](#)
 - restore [B-48](#)
 - route [B-49](#)
 - services [B-49](#)

- show auth-cli [B-52](#)
- show auth-http [B-52](#)
- show backupconfig [B-53](#)
- show bootlog [B-53](#)
- show cdp-neighbor [B-55](#)
- show cdp-run [B-55](#)
- show config [B-57](#)
- show import [B-60](#)
- show route [B-64](#)
- show ssh-version [B-66](#)
- show syslog [B-67](#)
- show tech [B-68](#)
- shutdown [B-72](#)
- snmp-server [B-73](#)
- ssh-version [B-74](#)
- telnetenable [B-75](#)
- username [B-76](#)
- webtimeout [B-78](#)
- syntax, checking [B-3](#)
- typographical conventions [B-4](#)
- use of quotes in commands [B-2](#)
- using [B-2](#)
- client
 - detail report, displaying [6-14](#)
 - group association report [6-22](#)
 - historical association report, displaying [6-18](#)
 - inventory, troubleshooting [10-18](#)
 - inventory of associations [3-81](#)
 - per VLAN (group) report, displaying [6-35](#)
 - per VLAN (individual) report, displaying [6-62](#)
 - statistics report, displaying [6-16](#)
 - top n bit error rate, displaying [6-85](#)
 - top n busiest report, displaying [6-82](#)
 - top n MIC error rate, displaying [6-84](#)
 - client polling interval, setting [3-89](#)
 - client walkabout [7-24](#)
 - checking status [7-33](#)
 - creating [7-26](#)
 - deleting [7-34](#)
 - editing [7-34](#)
 - guidelines [7-25](#)
 - naming [7-28](#)
 - options [7-30](#)
 - refresh walkabout list [7-38](#)
 - running [7-31](#)
 - starting [7-35](#)
 - stopping [7-35](#)
 - viewing AP location details [7-37](#)
 - viewing details [7-36](#)
- clock command [B-21](#)
- collector log, displaying [B-56](#)
- command reference [B-1](#)
- community strings
 - definition [GL-2](#)
 - guidelines [3-30](#)
 - recommendations [3-31](#)
 - requirement for [3-28](#)
 - setting on devices [3-5](#)

- specifying [3-28](#)
- configuration, WLSE
 - backing up
 - by using the CLI [9-6](#)
 - using Web interface [8-21](#)
 - copying to another WLSE [9-10](#)
 - Ethernet interfaces [9-14](#)
 - restoring
 - by using the CLI [9-7](#)
 - using Web interface [8-21](#)
- configuration archives
 - recommendations for using [4-286](#)
- configuration history, viewing device's [6-2](#)
- configured radio parameters report (11b), displaying [6-9](#)
- configuring devices
 - configuration jobs [4-267](#)
 - FAQs [10-19](#)
 - firmware, updating [5-1](#)
 - radio management assisted configuration [7-60](#)
 - setting up for discovery [3-5](#)
 - templates, using [4-1](#)
 - troubleshooting [10-22](#)
- connectivity, testing [8-35](#)
- console/Telnet services (non-IOS), configuring [4-225](#)
- conventions
 - CLI [B-2](#)
 - in command descriptions [B-4](#)
 - conversion
 - access points, from non-IOS to IOS [5-38](#)
 - templates, non-IOS to IOS [4-256](#)
 - CoS (class of service), configuring from DSCP [4-148](#)
 - credentials, devices
 - entering on WLSE [3-27](#)
 - HTTP [3-32](#)
 - HTTP port [3-35](#)
 - SNMP [3-28](#)
 - Telnet/SSH [3-33](#)
 - WLCCP [3-36](#)
 - CSV files, about [3-49](#)
 - current reports, displaying [6-19](#)
 - AP and bridge connected to router report [6-68](#)
 - AP and bridge connected to switch report [6-66](#)
 - AP associations [6-48](#)
 - AP Ethertype protocol filters report [6-51](#)
 - AP IP port filters report [6-53](#)
 - AP IP protocol filters report [6-52](#)
 - AP policy report [6-55](#)
 - AP QoS report [6-56](#)
 - AP SSID report [6-58](#)
 - AP summary [6-40](#)
 - AP usage report [6-70](#)
 - AP VLAN report [6-60](#)
 - detailed [6-43](#)
 - EAP authentication [6-50](#)

- group client association [6-22](#)
- group policy report [6-38](#)
- group security [6-26](#)
- group SSID [6-29](#)
- group VLAN [6-32](#)
- hot standby report [6-64](#)
- per VLAN (group) client report [6-35](#)
- per VLAN client (individual) report [6-62](#)
- router summary [6-67](#)
- server summary report [6-69](#)
- switch summary [6-65](#)
- custom values, configuring
 - IOS template [4-99](#)
 - non-IOS template [4-251](#)

D

- daemon log, displaying [8-4, B-58](#)
- daemon manager log, displaying [8-4, B-59](#)
- database
 - backing up [8-21](#)
 - checking database status [10-39](#)
 - purging [9-19](#)
 - reinitializing [B-43](#)
 - restoring [8-21](#)
- date and time
 - displaying
 - current local time setting [8-33](#)
 - system time [B-11](#)

- incorrect, troubleshooting [10-9](#)
- in WLSE displays [1-8](#)
- setting
 - browser time [8-33](#)
 - current local time [8-33](#)
 - system time (UTC) [9-12, B-21](#)
 - system time, by using Web interface [8-33](#)
 - synchronizing to a time server [8-34, B-40](#)
- deleting
 - devices [3-77](#)
 - groups [3-113](#)
 - users [8-45, B-76](#)
- detailed report, displaying [6-43](#)
- device center [6-2](#)
- Device Credentials option [3-27](#)
- devices
 - configuring
 - archive jobs [4-293](#)
 - configuration jobs [4-271](#)
 - setting up for discovery [3-5](#)
 - templates [4-1](#)
 - connectivity, testing [8-35](#)
 - credentials, setting [3-27](#)
 - deleting [3-77](#)
 - device name, display of [1-8](#)
 - exporting
 - to a file [3-96](#)
 - to CiscoWorks server [3-94](#)
 - fault summary, viewing [6-2](#)

- firmware, updating [5-1](#)
- getting started with device management [3-3](#)
- grouping [3-98](#)
- history viewing [6-2](#)
- limitation on number of access points [3-80](#)
- location manager [7-42](#)
- managing
 - auto-management filtering [3-65](#)
 - auto-management, all devices [3-65](#)
 - management state, changing [3-76](#)
 - understanding [3-42](#)
- new versions, supporting [8-38](#)
- setting up [3-5](#)
- unmanaged [3-76](#)
- device selector, using [1-9](#)
- diagnostics, WLSE
 - processes, viewing [8-32](#)
 - self-test [8-29](#)
 - status reports [8-28](#)
- discovery
 - advanced options [3-63](#)
 - CDP, enabling
 - on access points and bridges [3-6](#)
 - on routers and switches [3-24](#)
 - CDP discovery, running [3-54](#)
 - device import
 - running [3-59](#)
 - understanding [3-47](#)
 - device setup for [3-5](#)
 - discovery logs [3-69](#)
 - Discovery Run Details window [3-69](#)
 - FAQs [10-39](#)
 - filtering
 - by IP address [3-68](#)
 - by MAC address (access points) [3-65](#)
 - history [3-91](#)
 - individual device seeding [3-46](#)
 - logs [3-69](#)
 - messages [3-71](#)
 - troubleshooting [10-15](#)
 - common problems [3-74](#)
 - devices discovered, but not displayed [10-15](#)
 - Misconfigured Devices group [10-16](#)
 - seed devices [10-14](#)
 - SNMP Authorization Exception in discovery log [10-18](#)
 - time discrepancy in jobs [10-16](#)
 - understanding [3-42](#)
 - wizard [3-54](#)
- Discovery Run Details window [3-69](#)
- disk
 - checking and repairing [B-79](#)
 - usage, viewing [B-22](#)
- DNS
 - configuring (IOS) [4-62](#)
 - configuring (non-IOS) [4-231](#)
 - definition [GL-3](#)
 - name servers, specifying [8-34](#), [B-33](#)
 - reverse lookup

- effect on device name display [3-64](#)
- enabling [3-64](#)
- documentation [xx](#)
 - audience for this [xix](#)
 - obtaining [xxii](#)
 - typographical conventions in [xx](#)
- domain name
 - default, defining [B-33](#)
 - displaying [B-12](#)
- dot11 mib fault
 - Misconfigured group, devices in [3-10](#)
 - troubleshooting [10-16](#)
- DSCP to CoS (non-IOS), configuring [4-148](#)
- dump tcp command [B-23](#)

E

- EAP-MD5 server
 - AP usage report, displaying [6-70](#)
 - authentication report, displaying [6-50](#)
 - definition [GL-3](#)
 - setting up [3-25](#)
 - summary report, displaying [6-69](#)
- email
 - automatic configuration results [4-308](#)
 - faults [2-55](#)
 - forwarding [B-37](#)
 - logs and queues [8-3, B-36, B-62](#)
 - mail server, specifying by using the CLI [9-16](#)
 - mail server, specifying by using Web interface [8-35](#)
 - notification settings [2-55](#)
 - report [6-88](#)
 - scheduling [6-90](#)
 - testing and debugging [B-35](#)
- erase config command [B-24](#)
- erasing system configuration [9-19, B-24](#)
- Ethernet, configuring fast (IOS) [4-9](#)
- Ethernet, WLSE
 - connectors, labeling on WLSE 1130 [9-14](#)
 - firewall CLI command [B-25](#)
 - interface CLI command [B-31](#)
 - ports, configuring [9-14](#)
- Ethernet filters (non-IOS), configuring [4-152](#)
- Ethernet port (non-IOS), configuring [4-149](#)
 - advanced settings [4-154](#)
 - filters [4-152](#)
 - hardware [4-153](#)
 - identification [4-150](#)
- Ethertype filters, configuring
 - IOS template [4-72](#)
 - non IOS template [4-112](#)
- event
 - handling (non-IOS), configuring [4-245](#)
 - log (IOS), configuring [4-91](#)
 - notification (non-IOS), configuring [4-250](#)
- exception, definition [GL-3](#)
- exit command [B-10](#)
- exporting

devices [3-94](#)
 reports
 GUI-based, using [6-88](#)
 URL-based, using [6-94](#)
 templates [4-261](#)

F

FAQs

administration [10-39](#)
 configuration [10-19](#)
 faults [10-12](#)
 firmware [10-23](#)
 general [10-2](#)
 radio manager [10-35](#)
 reports [10-30](#)

fastEthernet (IOS), configuring [4-9](#)

faults

defined [2-3](#)
 displaying [2-1](#)
 emailing [2-55](#)
 exception, definition of [GL-3](#)
 FAQs [10-12](#)
 fault history truncation interval, setting [8-38](#)
 faults log (WLSE), displaying [8-4](#)
 network-wide settings [2-49](#)
 notification settings [2-51](#)
 emailing faults [2-55](#)
 syslog [2-54](#)

 trap notification [2-51](#)
 parameters for fault reporting [8-38](#)
 security policy, specifying [2-18](#)
 states, understanding [2-3](#)
 threshold-related, understanding [2-4](#)
 thresholds, specifying [2-18](#)
 troubleshooting [10-13](#)
 understanding [2-2](#)

filters

AP Ethertype protocol report,
 displaying [6-51](#)
 AP IP port report, displaying [6-53](#)
 AP IP protocol report, displaying [6-52](#)
 discovery
 by IP Address [3-68](#)
 by MAC address (access points) [3-65](#)
 Ethernet (non-IOS), configuring [4-152](#)
 Ethertype (IOS), configuring [4-72](#)
 Ethertype (non-IOS), configuring [4-112](#)
 IP (IOS), configuring [4-66](#)
 IP port (non-IOS), configuring [4-120](#)
 IP protocol (non-IOS), configuring [4-116](#)
 MAC address (IOS), configuring [4-63](#)

firewall command [9-14](#), [B-25](#)

firmware

"not verified" status [5-33](#)
 converting non-IOS device to IOS [5-20](#)
 estimating change window [5-3](#)
 FAQs [10-23](#)
 history, viewing device's [6-2](#)

how firmware upgrades work [5-2](#)

images

deleting [5-8](#)

editing on WLSE [5-6](#)

importing [5-8](#)

storing on remote TFTP server [5-13](#)

viewing [5-6](#)

jobs

copying [5-32](#)

creating [5-16](#)

deleting [5-31](#)

details, displaying [5-32](#)

displaying [5-30](#)

editing [5-31](#)

failures [5-33](#)

job choices [5-16](#)

number of devices in [10-25](#)

protocol, changing [5-32](#)

scheduling [5-19](#)

status [5-28, 5-33](#)

status, checking [5-28](#)

time discrepancy in schedule [10-25](#)

validating [5-20](#)

new versions, support for [8-38](#)

supported versions, displaying [8-39](#)

troubleshooting [10-23](#)

cryptography permissions, message
about [10-28](#)

email fails to arrive [10-26](#)

job not verified [10-27](#)

slow links [10-28](#)

SNMP job fails [10-26](#)

some devices not updated [10-26](#)

Telnet/SSH credentials [10-29](#)

upgrading

about [5-2](#)

procedures [5-5](#)

versions supported by WLSE

updating [8-39](#)

viewing [8-38](#)

floor information, Location Manager [7-49](#)

fsck command [B-79](#)

FTP, configuring [4-233](#)

G

gethostbyname command [B-26](#)

getting started

with device management [3-3](#)

with WLSE [1-1](#)

group client association report, displaying [6-22](#)

group performance report

Ethernet utilization [6-74](#)

RF utilization [6-73](#)

groups

client association report, displaying [6-22](#)

copying

rule-based [3-108](#)

static [3-107](#)

- creating
 - rules-based [3-105](#)
 - static [3-103](#)
 - deleting [3-113](#)
 - editing
 - rule-based [3-111](#)
 - static [3-110](#)
 - IOS reports [6-20](#)
 - Misconfigured Devices group [10-16](#)
 - non-IOS reports [6-20](#)
 - overview [3-98](#)
 - performance report for Ethernet utilization, displaying [6-74](#)
 - performance report for RF utilization, displaying [6-73](#)
 - per VLAN client report, displaying [6-35](#)
 - policy report, displaying [6-38](#)
 - rule-based
 - copying [3-108](#)
 - creating [3-105](#)
 - deleting [3-113](#)
 - editing [3-111](#)
 - security report, displaying [6-26](#)
 - SSID report, displaying [6-29](#)
 - static
 - creating [3-103](#)
 - creating by copying [3-107](#)
 - deleting [3-113](#)
 - editing [3-110](#)
 - system-defined [3-98](#)
 - top number of associations report, displaying [6-75](#)
 - top percentage errors report, displaying [6-77](#)
 - understanding [3-98](#)
 - user-defined [3-100](#)
 - VLAN report, displaying [6-32](#)
 - GUI
 - About button [1-7](#)
 - dashboard [1-5](#)
 - device name display [1-8](#)
 - Help button [1-7](#)
 - Logout button [1-7](#)
 - tabs and subtabs [1-5](#)
 - time display [1-8](#)
 - timeout period [1-11](#)
-
- ## H
- hardware configuration, Ethernet port [4-153](#)
 - help
 - CLI, displaying [B-3](#)
 - Web interface [1-7](#)
 - host file
 - displaying [B-60](#), [B-61](#)
 - importing [B-27](#)
 - hostname
 - changing system hostname [B-27](#)
 - translating to IP addresses [B-40](#)
 - hostname command [B-27](#)
 - hot standby

- configuring
 - IOS template [4-58](#)
 - non-IOS template [4-227](#)
 - report, displaying [6-64](#)
 - HTTP
 - configuring
 - IOS template [4-74](#)
 - non-IOS template [4-234](#)
 - credentials for non-IOS access points [3-32](#)
 - definition [GL-4](#)
 - setting on access points [3-6](#)
 - HTTPS
 - certificate signed request, obtaining
 - using the Web interface [8-18](#)
 - definition [GL-4](#)
 - log, viewing [8-3](#)
 - using to export devices [3-96](#)
-
- images
 - access point firmware [5-1](#)
 - WLSE software [8-5](#)
 - import command [B-27](#)
 - importing
 - device firmware [5-8](#)
 - devices
 - about CSV files [3-49](#)
 - from CiscoWorks server [3-61](#)
 - from file [3-59](#)
 - understanding [3-47](#)
 - firmware versions, support for [8-38](#)
 - image for Location Manager [7-48](#)
 - templates [4-257](#)
 - installing a replacement WLSE
 - installing the new WLSE [9-9](#)
 - removing the old WLSE [9-8](#)
 - installing software updates, WLSE
 - from the CLI [9-10](#)
 - from the Web interface [8-12](#)
 - interface command [B-31](#)
 - interference, setting network-wide fault detection [2-50](#)
 - inventory
 - automatic
 - polling interval [3-82](#)
 - understanding [3-81](#)
 - client associations inventory [3-81](#)
 - FAQs [10-14](#)
 - history [3-91](#)
 - immediate [3-84](#)
 - logs [3-91](#)
 - performance inventory [3-81](#)
 - polling intervals
 - guidelines for [3-83](#)
 - setting [3-87](#)
 - run by Radio Manager [3-92](#)
 - running [3-84](#)
 - scheduled [3-80](#)

- troubleshooting
 - common problems [3-93](#)
 - effects on traffic and performance [10-18](#)
 - length of time required [10-18](#)
 - IOS
 - access point reports [6-21](#)
 - converting APs from non-IOS to IOS [5-35](#)
 - group reports [6-20](#)
 - templates, configuration [4-3](#)
 - templates, converting from non-IOS [4-256](#)
 - trend report [6-84](#)
 - IP addresses
 - displaying [3-64](#), [B-26](#)
 - in UI, display of [1-8](#)
 - translating to hostnames [B-40](#)
 - IP chains, displaying [B-61](#)
 - ip domain-name command [B-33](#)
 - IP filters (IOS), configuring [4-66](#)
 - ip name-server command [B-33](#)
 - IP port filters (non-IOS), configuring [4-120](#)
 - IP protocol filters (non-IOS), configuring [4-116](#)
-
- ## J
- Java Plugin
 - requirement for Windows XP repository [8-10](#)
 - job history truncation interval, setting [3-89](#)
 - jobs, archive
 - copying [4-297](#)
 - creating [4-293](#)
 - deleting [4-297](#)
 - editing [4-296](#)
 - filtering [4-296](#)
 - job run details, viewing [4-298](#)
 - managing [4-261](#)
 - overview [4-286](#)
 - recommendations [4-286](#)
 - running again [4-297](#)
 - viewing status [4-293](#)
 - jobs, configuration
 - copying [4-283](#)
 - creating [4-277](#)
 - deleting [4-282](#)
 - editing [4-281](#)
 - filtering [4-281](#)
 - managing [4-267](#)
 - naming guidelines [A-1](#)
 - overview [4-268](#)
 - recommendations [4-269](#)
 - running again [4-282](#)
 - undoing [4-283](#)
 - viewing status [4-278](#)
 - jobs, email [6-90](#)
 - jobs, firmware
 - copying [5-32](#)
 - creating [5-15](#)
 - deleting [5-31](#)
 - duration [5-25](#)

- editing [5-31](#)
 - FAQs [10-23](#)
 - filtering [5-30](#)
 - for converting access points to IOS [5-43](#)
 - job run details [5-32](#)
 - managing [5-14](#)
 - naming guidelines [A-1](#)
 - troubleshooting [10-23](#)
 - viewing [5-28](#)
 - jobs log, displaying [8-4](#)
-
- ## L
- LEAP server
 - AP usage report, displaying [6-70](#)
 - definition [GL-4](#)
 - EAP authentication report, displaying [6-50](#)
 - setting response time [2-18](#)
 - setting up [3-25](#)
 - summary report, displaying [6-69](#)
 - Links subtab [8-48](#)
 - listbackup command [B-35](#)
 - local
 - admin access (non-IOS), configuring [4-209](#)
 - AP/client security (non-IOS), configuring [4-213](#)
 - location manager [7-39](#)
 - channel color key [7-41](#)
 - measuring tool [7-40](#)
 - logging in
 - from Web interface [1-11](#)
 - procedure [9-2](#)
 - splash screen, adding a message [8-32](#)
 - troubleshooting
 - cannot log in [10-5](#)
 - cannot log in as system administrator [10-5](#)
 - failure of authentication source [10-39](#)
 - password created in CLI [10-41](#)
 - logging out
 - from the CLI [9-2](#)
 - from the WLSE [1-11](#)
 - logs, WLSE
 - collector log [B-56](#)
 - daemon manager log [8-3, B-59](#)
 - daemons log [8-3, B-58](#)
 - discovery logs [3-69](#)
 - displaying, using Web interface [8-3](#)
 - displaying from the CLI [9-17](#)
 - downloading [8-3](#)
 - emailing [8-3](#)
 - install logs [B-60](#)
 - inventory logs [3-91](#)
 - searching [8-3](#)
 - syslog [B-67](#)
 - system log [8-32](#)
 - Tomcat log [8-3, B-69](#)
 - View Log File option [8-3](#)
 - Web access log [8-3, B-70](#)
 - Web error log [8-3, B-71](#)

Web SSL access log [B-72](#)

M

MAC address, displaying [B-13](#)

MAC address filters (discovery) [3-65](#)

MAC address filters (IOS), configuring [4-63](#)

mailctrl clear command [B-36](#)

mailctrl list command [B-37](#)

mail command [B-35](#)

mailroute command [B-37](#)

mail server

specifying, by using the CLI [9-16, B-37](#)

specifying, using Web interface [8-35](#)

maintenance image, WLSE

booting from [9-20](#)

CLI commands for [B-78](#)

using [9-19](#)

management services (WLSE) [9-16](#)

Manage Roles option [8-40](#)

Manage Users option [8-42](#)

managing devices

auto-manage filtering [3-65](#)

auto-management [3-65](#)

changing device state [3-76](#)

device detail display [3-79](#)

limitation on number of [3-79](#)

understanding [3-42](#)

Misconfigured Devices system group

description [3-100](#)

moving devices from [10-16](#)

mkcert command [B-38](#)

N

name servers, specifying [8-34, B-33](#)

naming guidelines [A-1](#)

neighbors (of WLSE), displaying [B-55](#)

network

connection failure, troubleshooting [10-6](#)

connectivity testing [8-35](#)

setting up [3-5](#)

network interfaces

configuring

fastEthernet (IOS) [4-9](#)

radio-802.11a (IOS) [4-19](#)

radio-802.11b (IOS) [4-11](#)

on WLSE

configuring [9-14, B-31](#)

information about, displaying [B-13](#)

IP chains, displaying [B-61](#)

using both interfaces [9-15](#)

template [4-9](#)

network management systems, integrating with
WLSE [1-2](#)

non-IOS

access point reports [6-21](#)

converting to IOS [5-35](#)

group reports [6-20](#)

- templates, configuration [4-100](#)
- templates, converting to IOS [4-256](#)
- trend report [6-85](#)
- notification settings, faults [2-51](#)
- nslookup
 - definition [GL-5](#)
 - NSlookup tool [8-35](#)
- nslookup command [B-40](#)
- NTP (Network Time Protocol)
 - configuring IOS template [4-87](#)
 - configuring time servers on WLSE [8-34](#), [B-40](#)
 - definition [GL-5](#)
 - setting current date and time [8-34](#)
 - setting system date and time [9-12](#)
- ntp server command [B-40](#)

P

- packet content, command for displaying [B-23](#)
- parameters, system [8-38](#)
- passwords
 - changing your password [8-46](#)
 - HTTP [3-32](#)
 - LEAP server [3-37](#)
 - loss of, recovering from [9-23](#)
 - Telnet [3-33](#)
 - WLSE users [8-42](#)
- path loss between managed APs report
 - (11b) [6-10](#)
- path loss data, collecting [7-9](#)

- PEAP server
 - ACS failed login report [8-49](#)
 - entering on WLSE [3-37](#)
 - setting up [3-25](#)
- performance
 - inventory [3-81](#)
 - parameters for data collection [8-38](#)
 - problems caused by frequent client inventory [10-18](#)
- performance graph, displaying for access points and bridges [6-80](#)
- performance polling interval, setting [3-89](#)
- performance table, displaying for access points and bridges [6-81](#)
- per VLAN client (group) report, displaying [6-35](#)
- ping
 - CLI command [B-10](#)
 - definition [GL-6](#)
 - Ping tool [8-35](#)
- policy
 - AP report, displaying [6-55](#)
 - group report, displaying [6-38](#)
 - groups, configuring [4-124](#)
- polling
 - aggregation parameters [3-90](#)
 - fault and job data truncation parameters [3-89](#)
 - inventory parameters [3-88](#)
- port
 - assignments, configuring [4-147](#)
- port filtering (WLSE), configuring [B-25](#)

primary service set

- association service set, configuring [4-139](#)
- radio11a service set, configuring [4-204](#)

processes, WLSE

- active statistics, displaying [B-63](#)
- displaying [8-29](#), [B-14](#)
- starting and stopping [8-29](#)

protocols, on WLSE [9-14](#)proxy mobile IP (IOS), configuring [4-75](#)proxy server, for firmware import [5-11](#)

Q

quality of service (QoS)

- configuring
 - associations (non-IOS) [4-133](#)
 - policies (IOS) [4-78](#)
 - radio 11a (non-IOS) [4-206](#)
 - radio traffic (IOS) [4-82](#)
- report, displaying [6-56](#)

R

radio

- 11a (non-IOS), configuring [4-175](#)
 - advanced [4-185](#)
 - data encryption [4-195](#)
 - filters [4-179](#)
 - hardware [4-180](#)

identification [4-176](#)module service sets [4-199](#)primary module service set [4-204](#)QoS [4-206](#)searched channels [4-192](#)11b (non-IOS), configuring [4-157](#)advanced [4-167](#)filters [4-160](#)hardware [4-161](#)identification [4-158](#)searched channels [4-173](#)802.11a (IOS), configuring [4-19](#)802.11b (IOS), configuring [4-11](#)monitoring [7-6](#)

radio manager

access points, configuring for [3-13](#)AP radio scans [7-9](#)assisted configuration [7-60](#)FAQs [10-35](#)overview [7-2](#)radio monitoring [7-6](#)reports, displaying [6-8](#)troubleshooting [10-35](#)radio measurements, collecting [7-4](#)radio measurements, deleting [7-71](#)radio monitoring [7-6](#)

RADIUS

authentication module [8-17](#)definition [GL-7](#)

RADIUS server

- AP usage report, displaying [6-70](#)
- EAP authentication report, displaying [6-50](#)
- setting response time [2-18](#)
- setting up [3-25](#)
- summary report, displaying [6-69](#)

rebooting, WLSE

- using the CLI [9-11](#), [B-42](#)
- using Web interface [8-5](#)

recovery (WLSE)

- maintenance image [9-19](#)
- recovery CD [9-21](#)
- resetting WLSE to factory defaults [9-19](#)

recovery CD (WLSE)

- reimaging the WLSE [9-21](#)
- rescue image, using [9-22](#)

reimaging the WLSE [9-21](#)

reload command [B-42](#)

replacement WLSE, installing

- installing the new WLSE [9-9](#)
- removing the old WLSE [9-8](#)

reports

- ACS failed login report [8-49](#)
- current, displaying [6-19](#)
- device center, using [6-2](#)
- emailing [6-88](#)
- exporting [6-88](#)
- FAQs [10-30](#)
- parameters for [8-38](#)

radio manager, displaying [6-8](#)

- scheduling email [6-90](#)
- trend, using for capacity planning [6-72](#)
- trends, displaying [6-71](#)
- troubleshooting [10-30](#)
- wireless client, displaying [6-13](#)

repository

- browsing [8-13](#)
- defining
 - using Web interface [8-11](#)
- definition [GL-7](#)
- install configure CLI command [B-28](#)
- install list CLI command [B-29](#)
- repository add CLI command [B-44](#)
- repository delete CLI command [B-44](#)
- repository list CLI command [B-45](#)
- repository server CLI command [B-47](#)
- repository source CLI command [B-46](#)
- show repository CLI command [B-64](#)

rescue image, WLSE [9-22](#)

resetting WLSE to factory defaults [9-19](#)

restarting (rebooting) WLSE

- bootlog, displaying [B-53](#)
- from Web interface [8-5](#)
- reload command [B-23](#)

restore command [B-48](#)

restoring data from backups

- restoring from one WLSE to another [9-10](#)
- using the CLI [9-7](#), [B-48](#)

- using Web interface [8-26](#)
- reverse DNS lookup [3-64](#)
- rogue AP
 - displaying location of [7-52](#)
 - setting network-wide fault detection [2-49](#)
- roles
 - creating and modifying [8-41](#)
 - deleting [8-40](#)
 - for users created by using the CLI [9-3](#)
 - naming guidelines [A-1](#)
 - predefined [8-40](#)
 - XML API privileges [8-40](#)
- route command [B-49](#)
- router
 - AP and Bridge connected to, displaying [6-68](#)
 - fault thresholds, setting [2-18](#)
 - setting up [3-24](#)
 - summary report, displaying [6-67](#)
 - system-defined group for [3-98](#)
- routes (WLSE)
 - adding [B-49](#)
 - displaying [B-15, B-64](#)
- routing (non-IOS), configuring [4-229](#)

S

- scheduling
 - archive jobs [4-291](#)
 - backups [8-24](#)
- configuration jobs [4-275](#)
- discovery [3-54](#)
- email [6-90](#)
- firmware jobs [5-15](#)
- inventory [3-82](#)
- search, for devices
 - troubleshooting [10-4](#)
 - using [1-10](#)
- security
 - advanced (IOS), configuring [4-46](#)
 - authentication (WLSE)
 - enabling [B-17](#)
 - failure of authentication source [10-39](#)
 - modules [8-16](#)
 - troubleshooting [10-39](#)
- HTTPS (WLSE) [8-18](#)
- IOS templates [4-26](#)
 - admin access [4-26](#)
 - advanced [4-46](#)
 - local RADIUS server [4-51](#)
 - server manager [4-41](#)
 - SSID manager [4-29](#)
 - WEP key manager [4-37](#)
- last 10 logged in users, viewing [8-20](#)
- log, displaying [B-65](#)
- non-IOS templates [4-208](#)
 - authentication server [4-216](#)
 - local admin access [4-209](#)
 - local AP/client [4-213](#)

- SSH [8-20](#)
- SSL
 - certificate signed request, obtaining
 - by using Web interface [8-18](#)
 - Telnet, enabling or disabling [8-20](#)
- security policy
 - monitoring, understanding [2-2](#)
- seed
 - CDP-based discovery [3-44](#)
 - definition [GL-7](#)
 - individual device seeding [3-46](#)
 - invalid [10-14](#)
- server
 - AAA
 - managing [3-37](#)
 - setting up [3-25](#)
 - AP usage report, displaying [6-70](#)
 - local RADIUS server (IOS),
 - configuring [4-51](#)
 - manager (IOS), configuring [4-41](#)
 - response time graph, displaying [6-86](#)
 - security (non-IOS), configuring [4-216](#)
 - setting response time [2-18](#)
 - summary report, displaying [6-69](#)
- server, SMTP [9-16](#)
- services (IOS), configuring [4-55](#)
 - ARP cache [4-90](#)
 - CDP [4-60](#)
 - DNS [4-62](#)
 - Ethertype filters [4-72](#)
 - hot standby [4-58](#)
 - HTTP [4-74](#)
 - IP filters [4-66](#)
 - MAC address filters [4-63](#)
 - NTP [4-87](#)
 - proxy mobile IP [4-75](#)
 - QoS policies [4-78](#)
 - QoS radio traffic [4-82](#)
 - SNMP [4-83](#), [4-208](#)
 - Telnet/SSH [4-56](#)
 - VLAN [4-88](#)
- services (non-IOS), configuring
 - accounting [4-238](#)
 - CDP [4-230](#)
 - console/Telnet [4-225](#)
 - DNS [4-231](#)
 - FTP [4-233](#)
 - hot standby [4-227](#)
 - HTTP [4-234](#)
 - routing [4-229](#)
 - SNMP [4-235](#)
 - SNTP [4-236](#)
 - start-up [4-222](#)
- services (WLSE)
 - managing [9-16](#), [B-49](#)
 - reintdb command, effect on [B-43](#)
 - stopping and starting [9-16](#)
 - time reset, requirement for stopping
 - services [B-21](#)
- services command [B-49](#)

service sets (non-IOS)

configuring

primary service set [4-139](#)

service sets [4-134](#)

settings

assigning to devices [2-23](#)

copying for device faults [2-20](#)

creating for device faults [2-19](#)

deleting for device faults [2-22](#)

device fault, understanding [2-18](#)

device faults, managing [2-18](#)

editing for device faults [2-22](#)

local time [8-33](#)

network-wide fault [2-49](#)

renaming for device faults [2-21](#)

system date and time [9-12](#)

viewing summary for device fault [2-23](#)

setting system date and time

using the CLI [9-12](#)

using the Web interface [8-33](#)

short term trending inventory truncation

interval, setting [8-38](#)

show auth-cli command [B-52](#)

show auth-http [B-52](#)

show backupconfig command [B-53](#)

show bootlog command [B-53](#)

show cdp-neighbor [B-55](#)

show cdp-run command [B-55](#)

show clock command [B-11](#)

show config command [B-57](#)

show domain-name command [B-12](#)

show import command [B-60](#)

show interfaces command [B-13](#)

show process command [B-14](#)

show route command [B-64](#)

show ssh-version command [B-66](#)

show syslog command [B-67](#)

show tech command [B-68](#)

show version command [B-15](#)

shutdown command [B-72](#)

shutting down (WLSE) [9-11, B-72](#)

SMTP

definition [GL-7](#)

server, specifying [8-35](#)

server, specifying by using the CLI [9-16](#)

SNMP

agent, configuring [B-73](#)

agent log, displaying [8-4](#)

community strings

guidelines for [3-30](#)

recommendations [3-31](#)

setting on devices [3-5](#)

specifying [3-28](#)

configuration, displaying [B-66](#)

configuring

IOS template [4-83, 4-208](#)

non-IOS template [4-235](#)

definition [GL-7](#)

reachability, testing [8-35](#)

- retries, recommendations for [3-31](#)
- timeouts, recommendations for [3-31](#)
- trap notification
 - MIB [2-51](#)
 - setting [2-51](#)
- traps supported [1-2](#)
- variables, querying [8-37](#)
- snmp-server command [B-73](#)
- SNTP, configuring [4-236](#)
- software, on devices
 - converting to IOS [5-35](#)
 - firmware, managing [5-1](#)
 - groups for [3-98](#)
- software, on WLSE
 - installation logs, displaying [8-4](#)
 - maintenance image [B-78](#)
 - overview [8-5](#)
 - recovery CD [9-21](#)
 - reimaging the WLSE [9-21](#)
 - repository, browsing [8-13](#)
 - status, viewing [8-6](#)
 - update history, viewing
 - using Web interface [8-14](#)
- updates
 - history, viewing [8-14](#)
 - installing, by using Web interface [8-12](#)
 - Internet Explorer, problems using [10-40](#)
 - transferring to WLSE [B-44](#)
- version, viewing [1-7, B-15](#)
- splash screen, adding a message [8-32](#)
- SSH
 - credentials for access points, entering [3-33](#)
 - definition [GL-7](#)
 - disabling [10-3](#)
 - enabling [B-74](#)
 - type, displaying [B-66](#)
 - type, selecting [8-20](#)
- ssh-version command [B-74](#)
- SSID
 - definition [GL-7](#)
 - manager (IOS), configuring [4-29](#)
 - report, displaying [6-58](#)
 - system-defined groups for [3-98](#)
- SSL
 - certificate, obtaining [8-18](#)
 - certificate signed request, obtaining
 - CLI command for [B-38](#)
 - definition [GL-8](#)
 - log, displaying [8-4](#)
- startup configuration
 - assigning [4-300](#)
 - creating a template for [4-302](#)
- start-up settings (non-IOS), configuring [4-222](#)
- subnet, system-defined group for [3-98](#)
- summary report
 - access point [6-40](#)
 - router [6-67](#)
 - server [6-69](#)

- switch [6-65](#)
- switch
 - AP and bridge connected to report, displaying [6-66](#)
 - fault thresholds, setting [2-18](#)
 - setting up [3-24](#)
 - summary report, displaying [6-65](#)
 - system-defined group for [3-98](#)
- syntax of commands, checking [B-3](#)
- sysContact information, updates to [10-14](#)
- sysLocation information
 - not updated in WLSE [10-14](#)
- syslog
 - displaying [B-67](#)
 - notification, setting [2-54](#)
- sysName, display of [1-8, 3-64](#)
- system
 - configuration
 - displaying [B-57](#)
 - erasing [B-24](#)
 - hostname, changing [B-27](#)
 - information, viewing [9-17](#)
 - logs, displaying [9-17](#)
 - processes, managing [8-29](#)
 - rebooting
 - from the Web interface [8-5](#)
 - using the CLI [9-11](#)
 - shutting down [9-11, B-72](#)
 - status, displaying [8-29](#)
 - storage usage, displaying [B-22](#)

- system log, using [8-32](#)
- system parameters, setting [8-38](#)

T

- TAC (Technical Assistance Center)
 - case priorities [xxv](#)
 - information for, displaying [B-68](#)
 - opening a case [xxv](#)
 - website [xxiv](#)
- TACACS+
 - authentication module [8-16](#)
 - definition [GL-8](#)
- TCP/IP packet content, displaying [B-23](#)
- TCP Port Scan tool [8-35](#)
- Telnet
 - credentials for IOS access points, entering [3-33](#)
 - disabling [B-75](#)
 - enabling [8-20, B-75](#)
 - status, displaying [B-68](#)
- Telnet/console services (non-IOS), configuring [4-225](#)
- Telnet/SSH services (IOS) , configuring [4-56](#)
- Telnet connection, troubleshooting [10-10](#)
- telnetenable command [B-75](#)
- templates
 - automatic configurations [4-300](#)
 - configuration, defined [4-2](#)
 - converting from non-IOS to IOS [4-256](#)

- copying [4-254](#)
- creating, for configuration [4-253](#)
- deleting [4-257](#)
- editing [4-255](#)
- exporting [4-261](#)
- for converting access points to IOS [5-41](#)
- importing [4-257](#)
- IOS choices [4-3](#)
- non-IOS choices [4-100](#)
- using [4-1](#)
- TFTP
 - definition [GL-8](#)
 - setting up on access points [3-8](#)
- threshold
 - definition [GL-8](#)
 - specifying fault threshold [2-18](#)
- time
 - browser time, setting [8-33](#)
 - display of, on WLSE [1-8](#)
 - incorrect, troubleshooting [10-9](#)
 - synchronizing to an NTP server [8-34](#)
 - system time, setting
 - using CLI command [9-12](#)
- UTC
 - definition [GL-9](#)
 - display of [1-8](#)
- timeout period
 - webtimeout command [B-78](#)
 - WLSE Web interface [1-11](#)
- tomcat log, displaying [8-4](#), [B-69](#)
- top n number of associations report,
 - displaying [6-75](#)
- top n percentage errors report, displaying [6-77](#)
- traceroute
 - command [B-15](#)
 - definition [GL-9](#)
 - Traceroute tool [8-35](#)
- transmission statistics
 - displaying Ethernet for AP and bridge [6-79](#)
 - displaying RF for AP and bridge [6-78](#)
- traps
 - MIB to define [2-51](#)
 - setting for notification [2-51](#)
 - version supported, on WLSE [1-2](#)
- trending data
 - aggregation of [3-90](#)
 - data retention parameters [3-90](#)
- trend reports, using for capacity planning [6-72](#)
- trends, displaying [6-71](#)
 - AP and bridge Ethernet transmission statistics [6-79](#)
 - AP and bridge performance graph [6-80](#)
 - AP and bridge performance table [6-81](#)
 - AP and bridge RF transmission statistics [6-78](#)
 - group performance report, Ethernet utilization [6-74](#)
 - group performance report, RF utilization [6-73](#)
 - server response time graph [6-86](#)
 - top n busiest clients [6-82](#)

- top n client bit error rate [6-85](#)
- top n client MIC error rate [6-84](#)
- top n number of associations report [6-75](#)
- top n percentage errors report [6-77](#)
- troubleshooting
 - administration [10-39](#)
 - AP web page, accessing [10-4](#)
 - configuration [10-22](#)
 - diagnostics for WLSE appliance [8-28](#)
 - faults [10-13](#)
 - firmware [10-25](#)
 - passwords, loss of [9-23](#)
 - process management for WLSE appliance [8-29](#)
 - radio manager [10-35](#)
 - reports [10-30](#)
 - searching for devices [10-3](#)
 - WLSE, recovery of [9-18](#)
- typographical conventions
 - in command descriptions [B-4](#)
 - in this document [xx](#)

U

- undoing a job [4-283](#)
- unknown radio, displaying [7-52](#)
- unmanaged devices [3-76](#)
- upgrade
 - access point firmware [5-1](#)
 - WLSE software (by using the CLI) [9-10](#)
 - WLSE software (by using Web interface) [8-5](#)
- usage report, AP [6-70](#)
- usage report, displaying [6-70](#)
- user-defined
 - groups [3-100](#)
 - roles [8-40](#)
- username command [B-76](#)
- users
 - authentication servers [8-17](#)
 - CLI access [8-42](#)
 - creating
 - using the CLI [9-3](#), [B-76](#)
 - using Web interface [8-42](#)
 - deleting [8-45](#), [B-76](#)
 - home page, modifying [8-47](#)
 - last 10 logged in users. viewing [8-20](#)
 - modifying [8-42](#), [B-76](#)
 - naming guidelines [A-1](#)
 - roles
 - assigning to users [8-43](#)
 - managing [8-40](#)
- troubleshooting
 - authentication failure [10-39](#)
 - password created in CLI not accepted [10-41](#)
 - users not listed [10-40](#)
 - username CLI command [B-76](#)
- UTC
 - definition [GL-9](#)
 - on WLSE [1-8](#)

V
VLAN

- AP report, displaying [6-60](#)
- configuring
 - IOS template [4-88](#)
 - non-IOS template [4-126](#)
- group report, displaying [6-32](#)
- per client report (group), displaying [6-35](#)
- per client report (individual), displaying [6-35](#)
- system-defined groups for [3-100](#)

W

- Web access log, displaying [8-4, B-70](#)
- Web error log, displaying [8-4, B-71](#)
- Web interface, WLSE [1-3](#)
- Web session timeout [1-11, B-78](#)
- Web SSL log, displaying [B-72](#)
- webtimeout command [B-78](#)
- WEP key manager (IOS), configuring [4-37](#)
- WEP keys, definition [GL-10](#)
- Windows server
 - as backup location [8-24](#)
 - as repository [8-10](#)
- wireless client polling interval, setting [3-89](#)
- wireless client reports, displaying [6-13](#)
 - client detail [6-14](#)
 - client historical association [6-18](#)

- client statistics [6-16](#)

Wireless Domain Services (WDS)

- access points, configuring for [3-13](#)
- configuring [4-96](#)
- credentials for [3-36](#)
- definition [GL-10](#)
- system-defined groups for [3-100](#)
- wireless services, configuring [4-95](#)

WLCCP

- credentials, entering on WLSE [3-36](#)
- definition [GL-10](#)

WLSE 1105, limitation on number of managed devices [3-79](#)**WLSE 1130**

- Ethernet port labelling [9-14](#)
- limitation on number of managed devices [3-79](#)

X
XML API

- documentation for [xxii](#)
- privileges in roles [8-40](#)

