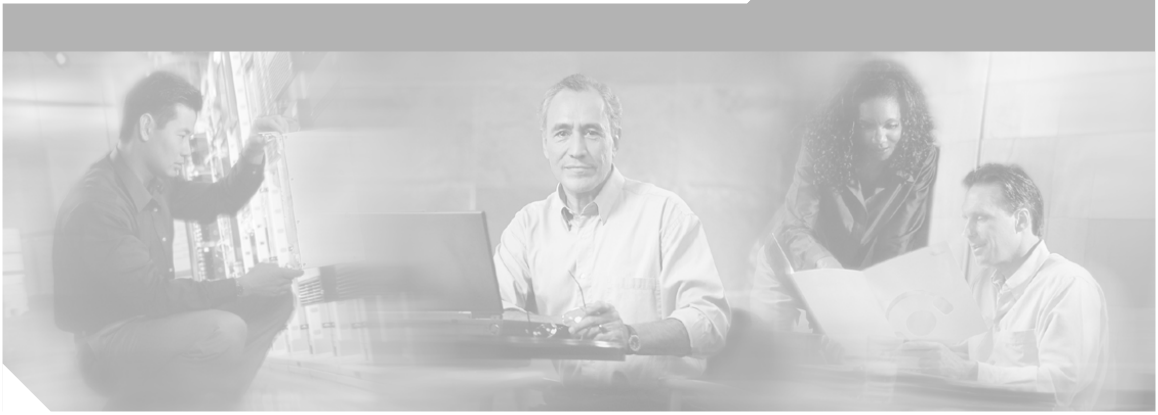
CISCO SYSTEMS



Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine Express

Software Release 2.11
License, Warranty, and Installation Instructions

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-7816779
Text Part Number: 78-16779-01

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.

CCIP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, 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, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, 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. (0206R)

Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine Express
Copyright © 2005 Cisco Systems, Inc. All rights reserved.

CONTENTS

Cisco 90-Day Limited Hardware Warranty Terms ix

Supplemental License Agreement xiii

Preface xv

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

CHAPTER 1 **Product Overview** 1-1

- Software Features 1-1
- Hardware Features—CiscoWorks Wireless LAN Solution Engine 1-2
  - Front Panel Features 1-2

System Indicators and Buttons 1-3
Back Panel Features 1-4
Serial Port 1-5
Ethernet Connector 1-6
Network Cable Requirements 1-7
Equipment Included in the Package 1-7

CHAPTER 2 **Installing WLSE Express Hardware** 2-1

Preparing to Install WLSE Express Hardware 2-1
Maintaining Safety 2-2
Warnings and Cautions 2-2
General Precautions 2-2
Maintaining Safety with Electricity 2-3
Protecting Against Electrostatic Discharge 2-4
Preventing EMI 2-4
Preparing Your Site for Installation 2-5
Environmental 2-5
Choosing a Site for Installation 2-6
Grounding the System 2-6
Creating a Safe Environment 2-6
AC Power 2-6
Cabling 2-7
Precautions for Rack-Mounting 2-8
Precautions for Products with Modems, Telecommunications, or Local Area Network Options 2-9
Tools and Equipment Required for Installation 2-9
Installing WLSE Express Hardware 2-10
Installation Quick Reference 2-10
Installing the WLSE Express in a Rack 2-10
Connecting the WLSE to the AC Power Source 2-12

Connecting Cables 2-12

CHAPTER 3 Configuring WLSE Express Software 3-1

- Factory Defaults 3-1
- Manual Configuration of the WLSE Express 3-2
  - Guidelines for Using the Setup Program 3-3
  - Running the Setup Program 3-3
  - Changing the Configuration After Running Setup 3-6
- Configuring Name Resolution 3-7
  - Using the WLSE Without a DNS Server 3-7
- Verifying the Configuration 3-8
- Configuring the Web Browser on the WLSE 3-9
  - Supported Browsers 3-10
  - Configuring Internet Explorer 3-10
  - Configuring Mozilla 3-12
- Auto-Configuration of the WLSE Express 3-12
  - Prerequisites for Auto-Configuration 3-13
    - Configuring the DHCP Server 3-13
    - Configuring the DNS Server 3-14
    - Requirement for TFTP Server 3-15
  - Auto-Configuration Quick Reference 3-15
  - About the Master Configuration File 3-15
  - Creating the Master Configuration File 3-16
    - Start the Reference WLSE 3-16
    - Manually Change Reference WLSE Defaults 3-17
    - Create the Master Configuration File 3-18
  - Creating the Site-Specific Configuration File 3-23
  - Auto-Configuring the Local WLSEs 3-25
  - Verifying the Configuration 3-25

Reapplying the Configuration File **3-26**
Customizing a WLSE Express After Applying a Configuration File **3-27**

CHAPTER 4 **Setting Up Discovery and Device Management** **4-1**

Device Management Quick Reference **4-1**
Adding Device Credentials to the WLSE **4-2**
  Enter SNMP Community Strings for All Managed Devices **4-3**
  Enter HTTP Credentials for Non-IOS Access Points **4-4**
  Enter Telnet or SSH Credentials for IOS Access Points **4-5**
  Enter HTTP Port Settings for IOS Access Points **4-6**
  Enter WLCCP Credentials for Wireless Domain Services (WDS) **4-6**
Configuring Discovery Options **4-7**
Discovering Devices **4-8**
  Run CDP Discovery **4-8**
    Run CDP Discovery Now **4-9**
    Modify the CDP Discovery Schedule **4-10**
  Import Devices **4-11**
    Import Devices from a File **4-12**
    Import Devices from a CiscoWorks Server **4-12**
Managing Devices **4-14**
Adding AAA Servers to the WLSE **4-15**
Next Step **4-16**

CHAPTER 5 **Setting Up Devices—Overview** **5-1**

Finding Details on Supported Devices **5-1**
About Device Setup Methods **5-1**
  WLSE Deployment Wizard **5-2**
  Basic Device Setup Methods **5-2**
    Overview: Device Setup **5-2**

Configuring Non-IOS Access Points and Bridges **5-3**
Configuring IOS Access Points and Bridges **5-3**
Configuring Routers and Switches **5-3**
Configuring External AAA Servers **5-4**
Configuring the Internal AAA Server **5-4**
Configuring a Wireless LAN Access Module **5-4**

APPENDIX A **Configuration File Reference** **A-1**
Configuration File Components **A-1**
DTD File **A-2**
Example .xml File **A-13**
Tags and Attributes in the .xml File **A-17**

APPENDIX B **Technical Specifications** **B-1**

INDEX

Cisco 90-Day Limited Hardware Warranty Terms

There are special terms applicable to your hardware warranty and various services that you can use during the warranty period. Your formal Warranty Statement, including the warranties and license agreements applicable to Cisco software, is available on Cisco.com. Follow these steps to access and download the *Cisco Information Packet* and your warranty and license agreements from Cisco.com.

1. Launch your browser, and go to this URL:

   http://www.cisco.com/univercd/cc/td/doc/es_inpck/cetrans.htm

   The Warranties and License Agreements page appears.

2. To read the *Cisco Information Packet*, follow these steps:

   a. Click the **Information Packet Number** field, and make sure that the part number 78-5235-03A0 is highlighted.

   b. Select the language in which you would like to read the document.

   c. Click **Go**.

      The Cisco Limited Warranty and Software License page from the Information Packet appears.

   d. Read the document online, or click the **PDF** icon to download and print the document in Adobe Portable Document Format (PDF).

Note You must have Adobe Acrobat Reader to view and print PDF files. You can download the reader from Adobe's website: http://www.adobe.com

3. To read translated and localized warranty information about your product, follow these steps:
   a. Enter this part number in the Warranty Document Number field:

      78-5236-01C0
   b. Select the language in which you would like to read the document.
   c. Click **Go**.

      The Cisco warranty page appears.
   d. Review the document online, or click the **PDF** icon to download and print the document in Adobe Portable Document Format (PDF).

You can also contact the Cisco service and support website for assistance:

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

Duration of Hardware Warranty

Ninety (90) days.

Replacement, Repair, or Refund Policy for Hardware

Cisco or its service center will use commercially reasonable efforts to ship a replacement part within ten (10) working days after receipt of a Return Materials Authorization (RMA) request. Actual delivery times can vary, depending on the customer location.

Cisco reserves the right to refund the purchase price as its exclusive warranty remedy.

To Receive a Return Materials Authorization (RMA) Number

Contact the company from whom you purchased the product. If you purchased the product directly from Cisco, contact your Cisco Sales and Service Representative.

Complete the information below, and keep it for reference:

Company product purchased from	
Company telephone number	
Product model number	
Product serial number	
Maintenance contract number	

Supplemental License Agreement

SUPPLEMENTAL LICENSE AGREEMENT FOR CISCO SYSTEMS NETWORK MANAGEMENT SOFTWARE RUNNING ON THE CISCO 103X HARDWARE PLATFORM

IMPORTANT-READ CAREFULLY: This Supplemental License Agreement ("SLA") contains additional limitations on the license to the Software provided to Customer under the Software License Agreement between Customer and Cisco. Capitalized terms used in this SLA and not otherwise defined herein shall have the meanings assigned to them in the Software License Agreement. To the extent that there is a conflict among any of these terms and conditions applicable to the Software, the terms and conditions in this SLA shall take precedence.

By installing, downloading, accessing or otherwise using the Software, Customer agrees to be bound by the terms of this SLA. If Customer does not agree to the terms of this SLA, Customer may not install, download or otherwise use the Software.

---

1. ADDITIONAL LICENSE RESTRICTIONS

- **Installation and Use**

The CiscoWorks Wireless LAN Solution Engine Express Software component of the Cisco 103X Hardware Platform is preinstalled. CD's containing tools to restore this Software to the 103X hardware are provided to Customer for reinstallation purposes only. Customer may only run the supported CiscoWorks Wireless LAN Solution Engine Express Software on the Cisco 103X Hardware Platform designed for its use. No unsupported Software product or component may be installed on the Cisco 103X Hardware Platform.

- **Software Upgrades, Major and Minor Releases**

Cisco may provide CiscoWorks Wireless LAN Solution Engine Software updates and new version releases for the103X Hardware Platform. If the Software update and new version releases can be purchased through Cisco or a recognized partner or reseller, the Customer should purchase one Software update for each Cisco 103X Hardware Platform. If the Customer is eligible to receive the Software update or new version release through a Cisco extended service program, the Customer should request to receive only one Software update or new version release per valid service contract.

- **Reproduction and Distribution**

Customer may not reproduce nor distribute software.

2. **DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS**

Please refer to the Cisco Systems, Inc. End User License Agreement.

Preface

This guide contains both hardware installation and software setup instructions for the CiscoWorks Wireless LAN Solution Engine (WLSE) Express and contains the following chapters and appendixes:

- Cisco 90-Day Limited Hardware Warranty Terms
- Supplemental License Agreement
- Product Overview
- Installing WLSE Express Hardware
- Configuring WLSE Express Software
- Setting Up Devices—Overview
- Technical Specifications
- Configuration File Reference

Audience

This guide is intended primarily for system administrators who are responsible for installing and configuring internetworking equipment.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**

Conventions

This document uses the following conventions:

Item	**Convention**
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** `font`
Variables you enter	*`italic screen`* 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.

Warning **This symbol means danger. You are in a situation that could cause bodily injury.**

Note Each English warning in this document is followed by a statement number. To read translations into other languages, look up the statement number in *Regulatory Compliance and Safety Information for the CiscoWorks Wireless LAN Solution Engine Express.*

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR

Figyelem **FONTOS BIZTONSÁGI ELOÍRÁSOK**

Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告 重要的安全性说明

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

警告 安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

Product Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should review the online documentation for any updates.

You can access WLSE online help by clicking the **Help** button in the top right corner of the screen or by selecting an option and then clicking the **Help** button. You can access the user guide from the online help by clicking **View PDF**.

Table 1 describes the available product documentation.

Table 1 Product Documentation

Document Title	**Description**
Release Notes for the CiscoWorks Wireless LAN Solution Engine Express	Describes new features, documentation updates, known and resolved problems, information on obtaining documentation, and information on obtaining technical assistance. Available as PDF on the WLSE Recovery CD. www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm
Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine Express	Procedures for configuring access points, routers, switches, AAA servers, and other devices for management by the WLSE. www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm
User Guide for the CiscoWorks Wireless LAN Solution Engine Express	Information about WLSE features and instructions for using WLSE 2.9. Available as PDF on the WLSE recovery CD, from the WLSE online help (click **View PDF**), and on Cisco.com at: www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm
Supported Devices Table for the Wireless LAN Solution Engine Express	Lists devices supported at the time the product was released. www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm
Troubleshooting and FAQs for the CiscoWorks Wireless LAN Solution Engine Express	Contains troubleshooting hints WLSE and FAQs for the WLSE. Available from the WLSE online help (lick **Troubleshooting**) and on Cisco.com at: www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm.
Upgrading CiscoWorks Wireless LAN Solution Engine Software	Upgrading software on a WLSE or WLSE Express to WLSE 2.11. www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm.

Table 1 Product Documentation (continued)

Document Title	Description
Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine Express	Installation and initial configuration of the WLSE. Available as PDF on the WLSE Recovery CD and on Cisco.com at www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm.
Regulatory Compliance and Safety Information for the CiscoWorks 1030 Wireless LAN Solution Engine	Regulatory compliance and safety information for the WLSE. Available as a printed document shipped with the WLSE, as PDF on the WLSE Recovery CD, and on Cisco.com at: www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm.
Developer Guide for the CiscoWorks Wireless LAN Solution Engine	How to use the XML application programming interface. Available on Cisco.com at: www.cisco.com/kobayashi/sw-center/cw2000/crypto/wlan-sol-eng/.

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Documentation DVD

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

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

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

- 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 1 800 553-NETS (6387).

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com

- Nonemergencies—psirt@cisco.com

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

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

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

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

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

Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

Product Overview

The Wireless LAN Solution Engine (WLSE) is a rack-mountable appliance for configuring and managing Cisco wireless devices. This chapter describes the features of WLSE 2.11.

Note For translated safety warnings and regulatory compliance information, see the document titled *Regulatory Compliance and Safety Information for the CiscoWorks 1030 Wireless LAN Solution Engine Express*.

Software Features

The WLSE has the following major software features:

- Configuration—Allows you to apply configuration changes to access points. The WLSE provides templates that you can apply to access points on demand, or you can use auto-managed templates.
- Fault and policy monitoring—Monitors device fault and performance conditions, LEAP server responses, and policy misconfigurations.
- Reporting—Allows you to track device, client and security information. You can email, print, and export reports.
- Firmware—Allows you to upgrade the firmware on access points and bridges.
- AAA server—Built-in RADIUS server.
- Redundancy—Ensuring high availability by using active and standby WLSEs.

- Auto-configuration of the WLSE—When started for the first time, the WLSE Express downloads a configuration file and is ready for use.

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

The WLSE has two user interfaces:

- The Command Line Interface (CLI), which you access by attaching a console to the WLSE or using Telnet. For information on all the CLI commands, see the online help.
- The Web interface provides access to all device management tasks and most of the management tasks for the WLSE system. For information on using the Web interface, see the WLSE online help.

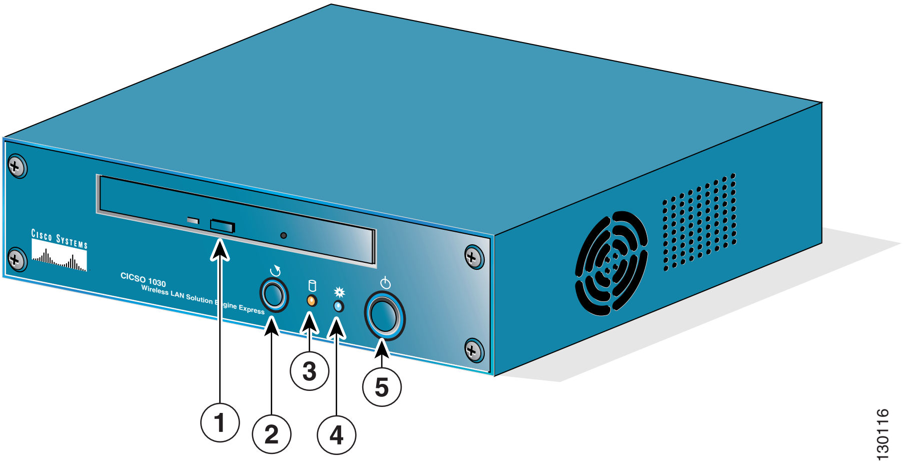
Hardware Features—CiscoWorks Wireless LAN Solution Engine

This section describes the WLSE front panel and back panel.

Front Panel Features

Figure 1-1 shows the front panel features. The front panel features include power button, reset button, system and hard drive status indicators, and two USB connectors.

Figure 1-1 Front Panel Features



1	CD eject button	**4**	System status indicator
2	Reset button	**5**	Power button
3	Hard drive indicator		

System Indicators and Buttons

When troubleshooting your WLSE, you might need to check the status of the indicator lights on the front panel (see Figure 1-1). The appearance and function of these lights are described in Table 1-1.

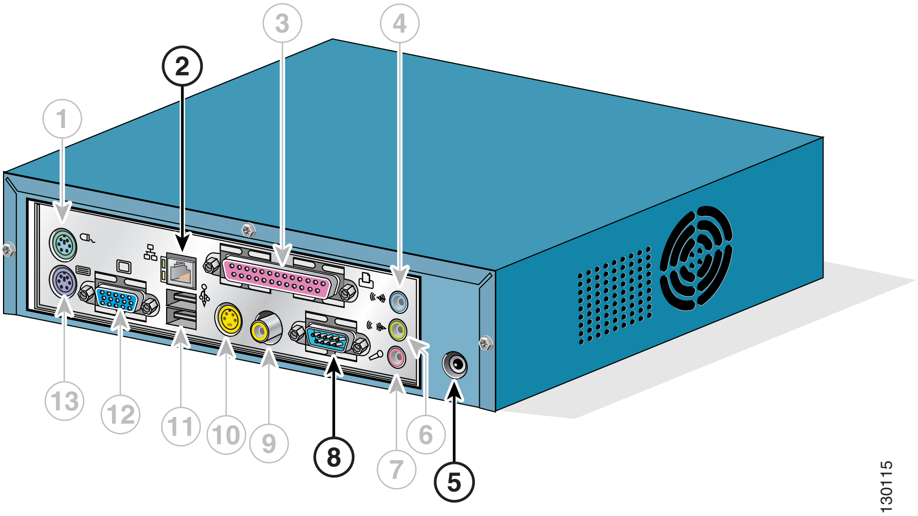
Table 1-1 Front-Panel System Indicators and Buttons

Indicator or Button	**Color**	**Function**
Power button	n/a	The power button controls power input to the power supply.
System status indicator	Blue	Lights up during normal system operation. If the indicator is flashing, the WLSE has a fault.
Hard drive indicator	Amber	Flashes when the hard drive is in use.

Back Panel Features

Figure 1-2 shows the back panel features.

Figure 1-2 Back Panel Features



Caution Do not use any of the ports greyed out in the illustration above. Use only the following ports: Ethernet connector (number 2, above), A/C power receptacle (number 5, above), and the serial/console connector (number 8, above).

1	Mouse connector	**8**	Serial/console connector
2	Ethernet connector	**9**	Video output
3	Parallel port	**10**	S-video output
4	Audio port	**11**	USB connectors (2)

5	A/C power receptacle	**12**	Video output *Do not use this connector for the console.*
6	Audio output port	**13**	Keyboard connector
7	Microphone connector		

Caution Use only the Cisco-specified power supply with this product. If you do not have the correct power supply, please contact Cisco Systems.

Serial Port

The serial port on the back panel uses a 9-pin D-subminiature connector, and is used as the console port. Terminal settings for this port are:

Table 1-2 Serial Port Settings

Parameter	Setting
Baud rate	9600
Data bits	8
Parity	None
Stop bits	1

If you reconfigure your hardware, you may need the serial port pin number and signal information. Figure 1-3 illustrates the pin numbers and Table 1-3 defines the pin assignments and interface signals.

Figure 1-3 Pin Numbers for the Serial Port Connector

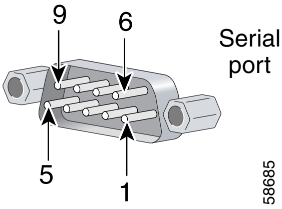


Table 1-3 Serial Port Pin Assignments

Pin	Signal	I/O	Definition
1	DCD	I	Data carrier detect
2	SIN	I	Serial input
3	SOUT	O	Serial output
4	DTR	O	Data terminal ready
5	GND	N/A	Signal ground
6	DSR	I	Data set ready
7	RTS	O	Request to send
8	CTS	I	Clear to send
9	RI	I	Ring indicator
Shell	N/A	N/A	Chassis ground

Ethernet Connector

The WLSE has one integrated 10/100/1000–megabit-per-second (Mbps) Ethernet connector. The Ethernet connector provides all the functions of a network expansion card and supports 10BASE-T, 100BASE-TX, and 1000BASE-T Ethernet standards.

Warning **To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.** Statement 1021

Network Cable Requirements

The Ethernet connector is designed for attaching an unshielded twisted pair (UTP) Ethernet cable equipped with standard RJ-45 compatible plugs. Press one end of the UTP cable into the Ethernet connector until the plug snaps securely into place. Connect the other end of the cable to an RJ-45 jack wall plate or to an RJ-45 port on a UTP concentrator or hub, depending on your network configuration. Observe the following cabling restrictions for 10BASE-T, 100BASE-TX, and 1000BASE-T networks:

- For 10BASE-T networks, use Category 3 or greater wiring and connectors.
- For 100BASE-TX and 1000 BASE-T networks, use Category 5 or greater wiring and connectors.
- The maximum cable run length (from a workstation to a concentrator) is 328 feet (ft) or 100 meters (m).
- For 10BASE-T networks, the maximum number of daisy-chained concentrators on one network segment is four.

Note To avoid line interference, put voice and data lines in separate sheaths.

Equipment Included in the Package

The following equipment is included in the WLSE package:

- CiscoWorks Wireless LAN Solution Engine Express
- Rack mounting shelf (optional component)
- Power cable
- Serial cable (light blue, RJ-45 to RJ-45)
- 10 baseT ethernet cable (yellow)
- 2 DB-9 to RJ-45 Adapters
- 1 DB-25 to RJ-45 Adapter
- WLSE Recovery CD

- WLSE documentation—The following documents are shipped with the WLSE:
  - *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine Express*
  - *Regulatory Compliance and Safety Information for the CiscoWorks 1030 Wireless LAN Solution Engine Express*

Installing WLSE Express Hardware

This chapter contains safety and site preparation information and procedures for installing CiscoWorks Wireless LAN Solution Engine (WLSE) Express hardware. The chapter contains the following major topics:

- Preparing to Install WLSE Express Hardware, page 2-1
- Installing WLSE Express Hardware, page 2-10

Preparing to Install WLSE Express Hardware

This section contains the following topics:

- Maintaining Safety, page 2-2
- Preparing Your Site for Installation, page 2-5
- Precautions for Rack-Mounting, page 2-8
- Precautions for Products with Modems, Telecommunications, or Local Area Network Options, page 2-9
- Tools and Equipment Required for Installation, page 2-9

Maintaining Safety

This section provides safety information for installing this product.

Warnings and Cautions

Read the installation instructions in this document before you connect the system to its power source. Failure to read and follow these guidelines could lead to an unsuccessful installation and possible damage to the system and components.

You should observe the following safety guidelines when working with any equipment that connects to electrical power or telephone wiring. They can help you avoid injuring yourself and damaging the WLSE.

Warnings and cautions are provided to help you prevent damage to the devices or injury to yourself.

General Precautions

Observe the following general precautions when using and working with your system:

- Keep your system components away from radiators and heat sources, and do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the computer gets wet, see the appropriate chapter in your troubleshooting guide or contact the Cisco Technical Assistance Center. For instructions on contacting the Technical Assistance Center, see Obtaining Technical Assistance, page xxvi.
- Do not push any objects into the openings of your system components. Doing so can cause fire or electric shock by shorting out interior components.
- Position system cables and power cables carefully; route system cables and the power cable and plug so that they cannot be stepped on or tripped over. Be sure that nothing rests on your system components' cables or power cable.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.

- To help avoid possible damage to the system board, wait 5 seconds after turning off the system before removing a component from the system board or disconnecting a peripheral device from the computer.

Maintaining Safety with Electricity

Follow these guidelines when working on equipment powered by electricity:

- Contact the Cisco Technical Assistance Center if any of the following conditions occur:
  - The power cable or plug is damaged.
  - An object has fallen into the product.
  - The product has been exposed to water.
  - The product has been dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.
- Use the correct external power source. Operate the product only from the type of power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult the Cisco Technical Assistance Center or a local power company.
- Use only approved power cables. If you have not been provided with a power cable for your computer or storage system or for any AC-powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.
- To help prevent electric shock, plug the WLSE, components, and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable.
- To help protect your system/components from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptable power supply (UPS).

- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.

Warning **There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.** Statement 1015

Protecting Against Electrostatic Discharge

Static electricity can harm delicate components inside your computer. To prevent static damage, discharge static electricity from your body before you touch any of your computer's electronic components, such as the microprocessor. You can do so by touching an unpainted metal surface on the computer chassis.

As you continue to work inside the computer, periodically touch an unpainted metal surface to remove any static charge your body may have accumulated.

You can also take the following steps to prevent damage from electrostatic discharge (ESD):

- When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your computer. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
- When transporting a sensitive component, first place it in an antistatic container or packaging.
- Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads and workbench pads.

Preventing EMI

When you run wires for any significant distance in an electromagnetic field, electromagnetic interference (EMI) can occur between the field and the signals on the wires. Note that:

- Bad plant wiring can result in radio frequency interference (RFI).

- Strong EMI, especially when it is caused by lightning or radio transmitters, can destroy the signal drivers and receivers in the system, and can even create an electrical hazard by conducting power surges through lines and into the system.

To predict and remedy strong EMI, consult RFI experts.

Preparing Your Site for Installation

This section describes the requirements your site must meet for safe installation and operation of your WLSE. Ensure that your site is properly prepared before beginning installation.

Environmental

When planning your site layout and equipment locations, keep in mind the precautions described in this section to help avoid equipment failures and reduce the possibility of environmentally caused shutdowns. If you are currently experiencing shutdowns or unusually high errors with your existing equipment, these precautions will help you isolate the cause of failures and prevent future problems.

Use the following precautions when planning the operating environment for your WLSE.

- Always follow the ESD-prevention procedures described in the Preventing EMI, page 2-4 to avoid damage to equipment. Damage from static discharge can cause immediate or intermittent equipment failure.
- Make sure that the chassis cover is secure. The chassis is designed to allow cooling air to flow effectively within it. An open chassis allows air leaks, which could interrupt and redirect the flow of cooling air from internal components.
- Electrical equipment generates heat. Ambient air temperature might not be adequate to cool equipment to acceptable operating temperatures without adequate circulation. Make sure that the room in which you operate has adequate air circulation.

Choosing a Site for Installation

Warning **This unit is intended for installation in restricted access areas. A restricted access area is where access can only be gained by service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.** Statement 1017

- Choose a site with a dry, clean, well-ventilated and air-conditioned area.
- Choose a site that maintains an ambient temperature of 10° to 35°C (50° to 95°F).

Grounding the System

Warning **Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Creating a Safe Environment

Follow these guidelines to create a safe operating environment:

- Keep tools and chassis components off the floor and away from foot traffic.
- Clear the area of possible hazards, such as moist floors, ungrounded power extension cables, and missing safety grounds.
- Keep the area around the chassis free from dust and foreign conductive material (such as metal flakes from nearby construction activity).

AC Power

Ensure that the plug-socket combination is accessible at all times, because it serves as the main disconnecting device.

Warning **The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.** Statement 1019

Warning **This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.** Statement 1045

Warning **The power supply must be placed indoors.** Statement 331

Warning **Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.** Statement 12

Cabling

Use the cables in the accessory kit to connect the WLSE's console port to a console or computer that is running a console program. In addition to the console cable, you must supply your own standard Ethernet cable to connect the WLSE to your network. For information detailing cable requirements, see Network Cable Requirements, page 1-7.

A structured wiring system provides a standardized way to wire a building for all types of networks for the WLSE to be installed. The main distribution frame links all the building's interior wiring and provides an interface connection to circuits coming from outside sources such as the local telephone company. Wiring hubs (peripherals for cabling installations) provide the connection logic unique to Fast Ethernet cables that the WLSE uses. Unshielded twisted pair (UTP) copper wire is used to connect the WLSE and distributes the network connections to wall jacks near each piece of network equipment.

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

Warning **Before opening the unit, disconnect the telephone-network cables to avoid contact with telephone-network voltages.** Statement 1041

Precautions for Rack-Mounting

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**

This unit should be mounted at the bottom of the rack if it is the only unit in the rack.

When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.

If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack. Statement 1006

Observe the following precautions for rack stability and safety. Also see the rack installation documentation accompanying the rack for specific warning and/or caution statements and procedures.

Servers, storage systems, and appliances are considered to be components in a rack. Thus, "component" refers to any server, storage system, or appliance, as well as to various peripherals or supporting hardware.

- Do not move large racks by yourself. Due to the height and weight of the rack, a minimum of two people are needed to accomplish this task.
- Make sure the rack is level and stable before extending a component from the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Ensure that proper airflow is provided to components in the rack.
- Do not step on or stand on any system/component when servicing other system/components in a rack.

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Precautions for Products with Modems, Telecommunications, or Local Area Network Options

Observe the following guidelines when working with options:

- Do not connect or use a modem or telephone during a lighting storm. There may be a risk of electrical shock from lightning.
- Never connect or use a modem or telephone in a wet environment.
- Do not plug a modem or telephone cable into the Ethernet connector.
- Disconnect the modem cable before opening a product enclosure, touching or installing internal components, or touching an uninsulate4d modem cable or jack.
- Do not use a telephone line to report a gas leak while you are in the vicinity of the leak.

Tools and Equipment Required for Installation

You need the following tools and equipment to install the WLSE:

- Number 2 Phillips screwdriver
- Tape measure and level
- Antistatic mat or antistatic foam
- ESD grounding strap

Installing WLSE Express Hardware

This section provides instructions for installing the WLSE in a rack. The rack must be properly secured to the floor, ceiling, or upper wall, and where applicable, to adjacent racks. The rack should be secured using floor and wall fasteners and bracing specified or approved by the rack manufacturer or by industry standards. See the rack manufacturer's installation documentation for precautionary warnings and information before attempting this installation.

This section contains the following topics:

- Installation Quick Reference, page 2-10
- Installing the WLSE Express in a Rack, page 2-10
- Connecting the WLSE to the AC Power Source, page 2-12
- Connecting Cables, page 2-12

Installation Quick Reference

Table 2-1 provides a high-level overview of hardware installation.

Table 2-1 Installation Quick Reference

Task	References
Use the rack mount shelf to place the WLSE in a rack.	Installing the WLSE Express in a Rack, page 2-10
Connect to an AC power source.	Connecting the WLSE to the AC Power Source, page 2-12
Connect network and console cables.	Connecting Cables, page 2-12

Installing the WLSE Express in a Rack

Before installing the WLSE in a rack, read Preparing Your Site for Installation, page 2-5 to familiarize yourself with the proper site and environmental conditions. Failure to read and follow these guidelines could lead to an unsuccessful installation and possible damage to the system and components.

Perform the following steps when installing and servicing the WLSE:

- Disconnect all power and external cables before installing the system.
- Install the system in compliance with your local and national electrical codes:
  - United States: National Fire Protection Association (NFPA) 70; United States National Electrical Code.
  - Canada: Canadian Electrical Code, Part, I, CSA C22.1.
  - Other countries: If local and national electrical codes are not available, see IEC 364, Part 1 through Part 7.
- Do not work alone under potentially hazardous conditions.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Do not attempt to install the WLSE into a rack that has not been securely anchored in place. Damage to the system and personal injury may result.
- Due to the size and weight of the computer system, never attempt to install the computer system by yourself.

See Precautions for Rack-Mounting, page 2-8 for additional safety information on rack installation.

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**

This unit should be mounted at the bottom of the rack if it is the only unit in the rack.

When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.

If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack. Statement 1006

Connecting the WLSE to the AC Power Source

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Connect the AC power receptacle to the AC power source with the provided power cable.

Connecting Cables

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.**

Use unshielded twisted pair (UTP) copper wire Ethernet cable, with standard RJ-45 compatible plugs, to connect the WLSE to the network.

Plug the network connection into the Ethernet port.

If desired, connect a console to the console/serial port on the back panel using the supplied serial cable and, if necessary, the DB-9-to-RJ-45 console adapter.

Configuring WLSE Express Software

This chapter describes how to set up the WLSE Express. There are two ways in which you can set up the WLSE Express:

- Manually configure the WLSE Express by using the setup script and entering CLI commands.
- Auto-configure the WLSE Express by creating a special configuration file on a “reference” WLSE Express which is then copied to other WLSEs.

This chapter contains the following information about the configuration process:

- Factory Defaults, page 3-1
- Manual Configuration of the WLSE Express, page 3-2
- Configuring the Web Browser on the WLSE, page 3-9
- Auto-Configuration of the WLSE Express, page 3-12

Factory Defaults

A newly manufactured WLSE Express is configured with the following information in flash memory:

- A superuser account name (admin) and password (admin) is included. The name and password are case-sensitive.

  This user can log in through the console, Telnet/SSH, and the Web interface.

Note Telnet access is disabled by default. To enable it, log in as admin and use the **telnetenable enable** CLI command.

- Hostname is set to "localhost."
- The firewall is set to "private."
- The Ethernet interface is set to DHCP mode.

  When powered on, a WLSE in DHCP mode attempts to obtain its network configuration from a DHCP server. This information is then written into the WLSE's flash memory.

  If you do not want to configure a DHCP server with this information, you can log in and configure the network parameters manually after the WLSE starts. For more information, see Manually Change Reference WLSE Defaults, page 3-17.
- An unsigned SSL certificate is generated. This certificate is used by the internal AAA server and for logging in to the Web interface via HTTPS.

Note You can erase a WLSE's flash memory by using the **erase config** CLI command. After flash memory is erased, the WLSE is automatically reset to its newly manufactured state. If the hostname is being set through DHCP, it retains its value. You can use the procedures in this section to reconfigure a WLSE after erasing the configuration.

If you entered a static IP address for the WLSE, but you want to use DHCP for configuration, you must first erase the flash memory.

For more information on the **erase config** command, see the online help.

Manual Configuration of the WLSE Express

By default, the WLSE Express Ethernet interface is set to DHCP mode. When powered on, a WLSE attempts to obtain its network configuration from a DHCP server. If you do not want to configure a DHCP server with this information, you can log in and configure the network parameters manually after the WLSE starts.

Guidelines for Using the Setup Program

When using the setup program:

- Press the **Backspace** or **Delete** key to delete characters when entering a response to a prompt.
- You cannot edit a response after you press the **Enter** key. You can use CLI commands to change some responses after running setup; see Changing the Configuration After Running Setup, page 3-6.
- You can exit the setup program in two ways:
  - Press **Ctrl-c**.

    The login prompt appears. Log in as the user **setup** to rerun the setup program.
  - Enter **no** at the final prompt:

    ```
    Would you like to save this configuration? [yes].
    ```

    The setup program exits without saving the configuration, then restarts.

See Table 3-1 on page 3-4 and Table 3-2 on page 3-5 for the data you will need to enter into the setup prompts.

Running the Setup Program

To configure the WLSE Express network information, perform the following steps:

Procedure

Step 1 Attach a console terminal or PC to the WLSE's serial/console port and log in. Use the admin username and admin password.

To connect a console, use the console/serial port on the back panel. For more information on the port and cabling, see Connecting Cables, page 2-12.

Note If you are using a Windows terminal emulator, it is recommended that you use the Windows Hyper Terminal application.

You can also log in by using SSH and the admin username and admin password. Telnet is disabled by default. To enable it, log in as admin and use the **telnetenable enable** CLI command.

Step 2 Enter **setup**.

Step 3 Enter responses to the first set of prompts to configure the WLSE Express network parameters. Table 3-1 on page 3-4 describes how to respond to the prompts. After each response, press **Enter** to proceed to the next prompt.

Table 3-1 General Configuration

Prompt	Response Description	Sample Response
`host name:`	System hostname	SolutionEngine
`domain name:`	System domain name. **Note** If you reconfigure the WLSE Express, you must specify the domain name again.	cisco.com
`<admin> password:`	Sets the password for the default user **admin**. Characters you type do not appear on screen. **Note** Default user **admin** is reserved and cannot be deleted or changed. You can use the admin password to log into the Web interface and to connect via Telnet/SSH. The admin user has system administrator privileges and can use all CLI commands and all functions in the Web interface. Password length is unlimited, and you can use any characters except the double quote ("), single quote ('), and dollar sign ($). Passwords are case sensitive.	wq1Cvu2pl
`confirm password:`		
`eth0 IP address:`	IP address of Ethernet 0 interface.	209.165.200.224
`eth0 network mask:`	Network mask of Ethernet 0 interface.	255.255.255.224
`default gateway IP address:`	IP address of default router.	209.165.200.224

Table 3-1 General Configuration (continued)

Prompt	Response Description	Sample Response
`DNS server IP address:`	IP address of DNS server for name/address resolution. The setup program does not validate the IP address you enter. If you are not using DNS, see Using the WLSE Without a DNS Server, page 3-7 before proceeding.	209.165.201.1
`Would you like to save this configuration? [yes]:`	• Enter **yes** to save the configuration. The configuration is saved and the system reboots. • Enter **no** to exit without saving the configuration and run the setup program again.	

Step 4 Answer the next set of prompts to create a self-signed SSL certificate. This certificate will allow you to access the WLSE Express securely, using HTTPS, until you are able to obtain a certificate from a certificate authority (CA). Table 3-2 on page 3-5 describes how to respond to the prompts.

To make changes in the certificate after running setup, see Changing the Configuration After Running Setup, page 3-6.

The certificate expires after one year. To obtain a permanent, signed certificate, see the SSL instructions in the online help or in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.11*.

Table 3-2 Self-Signed Certificate Creation

Prompt	Response Description	Sample Response
`Country Name`	2-character code.	US
`State or Province Name`	Full name of a state or province.	Snake Desert
`Locality Name`	City or locality name.	Snake Town
`Organization Name`	Company name.	Snake Oil, LTD.
`Organizational Unit Name`	Unit of the company that is using the WLSE.	Webserver Team
`Common Name`	Fully qualified domain name (FQDN).	www.snakeoil.com
`Email Address`	Email address.	www@snakeoil.com

Step 5 After you finish configuring the WLSE Express, it will reboot.

Step 6 After the WLSE Express reboots, set up your mail server to send mail to external domains by entering the following command:

mailroute {*hostname* | *ip-address*}

where *hostname* is the hostname of the SMTP server and *ip-address* is the IP address of the SMTP server. If you do not set the mail server, email can only be sent to the local domain. For more information about this command, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.11*.

Note You can also set up the mail server after you log in to the Web interface. See the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.11*.

Changing the Configuration After Running Setup

To change the information in the setup configuration, use the following CLI commands at any time. For more information about CLI commands, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.11*.

You can use CLI commands by attaching a console terminal or PC to the WLSE's serial/console port on the back panel and logging in. (For more information on the port and cabling, see Connecting Cables, page 2-12.) Log in initially as the admin user, using the password you created during setup.

Note If you are using a Windows terminal emulator, it is recommended that you use the Windows Hyper Terminal application.

You can also log in by using SSH and the admin username and admin password. Telnet is disabled by default. To enable it, log in as admin and use the **telnetenable enable** CLI command.

- To change from obtaining an IP address via DHCP to using a static IP address, use the following commands:

  interface eth0 *ip_address netmask* **default-gateway** *ip_address* **up**
  ip name-server *ip_address*
  ip domain-name *domain_name*

Enter all of these CLI commands if you are using static addressing for the WLSE Express.

- To change the hostname, use the **hostname** command.
- To change the superuser password, use the **username admin password** command.

Note You must log out before the password change takes affect.

You can also change this password in the Web interface.

Tip To change any other part of the WLSE's initial configuration, use the **erase config** command to erase the previous configuration, and rerun the setup program.

You can further customize the WLSE Express by using its Web interface.

Configuring Name Resolution

The WLSE Express resolves hostnames by using a Domain Name System (DNS) server, or you can use the **import** CLI command to add individual hosts or a UNIX-style hosts file. For information on this command, see *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.11*.

If you are using a DNS server, register the WLSE Express on the DNS server, using the WLSE's hostname as its DNS name.

Using the WLSE Without a DNS Server

The WLSE Express does not require name resolution, but if name resolution is not used, the following problems will occur:

- hostnames will not resolve.
- Discovery will be slow.
- Connecting to the WLSE Express via Telnet will be slow. You will be able to connect to the WLSE only after name resolution on the client times out.

- Ping and traceroute commands will result in 100% packet losses in 4 out of 5 ICMP packets. This occurs because the WLSE Express times out when attempting reverse DNS lookup.
- By default, IP addresses will appear instead of hostnames in WLSE displays.
- You will not be able to download access point firmware directly from Cisco.com to the WLSE Express.

If you are not using a DNS server, perform the steps described in Configuring Name Resolution, page 3-7, with the following exception:

Procedure

Step 1 At the `DNS server ip address` prompt, enter any IP address.

Step 2 After you finish configuring the WLSE, erase the IP address you entered by entering the following command:

no ip name-server *ip-address*

where *ip-address* is the IP address you entered at the `DNS server ip address:` prompt in the setup program. For more information about the **ip name-server** command, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.11*.

Verifying the Configuration

While at the console, verify that the WLSE is correctly configured by performing the following steps.

For more information on the CLI commands used in the following procedure, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.11*.

Procedure

Step 1 At the system console, enter **admin** at the login prompt, and log in with the password you created during setup. You can also use Telnet or SSH to log in as the admin user.

Note For security reasons, Telnet access is disabled by default. To enable it, log in as admin and use the **telnetenable enable** CLI command.

Step 2 If you are using a DNS server, enter the following command to verify that the WLSE can obtain DNS services from the network:

```
# nslookup dns-name
```

where *dns-name* is the DNS name of a host that is registered in DNS. If the system cannot obtain the IP address of the host from DNS, use the **ip name-server** command to specify a working DNS server.

Step 3 Enter the following command to verify that the system can communicate with the network:

```
# ping ip-address
```

where *ip-address* is the IP address of a host that is accessible on the network. A DNS server is a recommended host to ping because it should always be running and accessible.

Step 4 Enter the **show config** command to verify that the configuration is as you expected. For more information on this command, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.11*.

Step 5 Enter the **show clock** command to verify that the system time and date are correct in Coordinated Universal Time (UTC).

- If the time or date is incorrect, set the correct time and date using the **clock** command.
- If your network uses NTP, configure the system to use NTP to set the clock. Use the **ntp server** CLI command.

Step 6 Enter the **exit** command to log out.

Configuring the Web Browser on the WLSE

Before you log in to any WLSE Express Web interface, make sure that:

- You are using a supported browser—See Supported Browsers, page 3-10

- Your browser is properly configured—See:
  - Configuring Internet Explorer, page 3-10
  - Configuring Mozilla, page 3-12

Supported Browsers

The supported browsers for WLSE 2.11 are listed in Table 3-3 on page 3-10.

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

Table 3-3 Supported Browsers

Client Operating System	Supported Browsers
Windows 2000, Windows NT, and Windows XP	Microsoft Internet Explorer 6.0 with Service Pack 1 Mozilla 1.6
Japanese Windows 2000, Windows NT, and Windows XP	Japanese Microsoft Internet Explorer 6.0 with Service Pack 1 Mozilla 1.6
Solaris 8 and 9	Mozilla 1.6
Java Plug-in	1.4.2 (Java Plug-in is required for some WLSE functions).

Configuring Internet Explorer

To configure Internet Explorer 6.0, perform the following steps.

Procedure

Step 1 Select **Tools > Internet Options.**

Step 2 Enable JavaScript:

a. Select **Security**.

b. Make sure that the Internet icon is selected, and click **Custom Level**.

c. Scroll to Scripting and select the following:
  - Select Enable for Active scripting.
  - Select Enable for Allow paste operations via script.
    - Select Enable for **Scripting of Java applets**.

d. Click **OK**.

Step 3 Configure the browser to accept all cookies:

a. Select **Privacy**.

b. Move the slider down to until “Accept all Cookies” appears.

c. Click **OK**.

Step 4 Change the default font to improve readability:

a. Select **General**, then select **Fonts**.

b. Select a sans-serif font (for example, Arial) from the **Web page font** and **Plain text font** lists.

c. Click **OK**, then click **OK** again.

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

Step 5 Disable caching:

a. Select **General**, then select **Settings**.

b. Under “Check for newer versions of stored pages,” select **Every visit to the page**.

c. Click **OK**.

Step 6 Click **OK**.

Note Windows XP does not come with the Java Plug-in installed on Internet Explorer 6.0. This causes problems when upgrading a WLSE’s software. If you plan to use a Windows XP client or server to update WLSE software, configure the browser as described in the procedure for creating a remote repository in the online help.

Configuring Mozilla

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

To configure Mozilla 1.6, perform the following steps:

Procedure

Step 1 Select **Edit > Preferences**.

Step 2 Configure the browser to accept cookies:

- **a.** Under **Privacy & Security > Cookies**, go to “Enable cookies based on privacy settings.”
- **b.** Select **Allow all cookies** or **Allow cookies for the originating web site only**.

Step 3 Disable caching:

- **a.** Select **Advanced > Cache**.
- **b.** Select **Every time I view the page**.

Step 4 Click **OK**.

Auto-Configuration of the WLSE Express

After you have installed your WLSE Expresses, you can arrange for them to be auto-configured. As each WLSE is started up for the first-time, a special configuration file is automatically downloaded, and the WLSE is ready for use.

Normally, a “reference” WLSE is used to create a master configuration file that contains all the necessary settings. This file is sent to each location with WLSEs. At each site, the file is customized as necessary and installed on a TFTP server. As each WLSE Express starts for the first time, this site-specific configuration file is downloaded to the local WLSEs.

This following sections contain procedures for setting up the necessary services and for creating the master and site-specific configuration files.

Prerequisites for Auto-Configuration

Before configuring the WLSE Express, you need to configure the Web browser, which is required for using the WLSE GUI. See Configuring the Web Browser on the WLSE, page 3-9.

To use the auto-configuration feature of the WLSE Express, you need to configure the following:

- Configure the DHCP server—Configuring the DHCP Server, page 3-13.
- Configure the DNS server—Configuring the DNS Server, page 3-14.
- Provide a TFTP server—Requirement for TFTP Server, page 3-15.

Configuring the DHCP Server

In most cases, each site has its own DHCP server, and therefore, its own pool of IP addresses.

Note If you do not want to configure a DHCP server with this information, you can log in and configure the network parameters manually after the WLSE starts. For more information, see Manually Change Reference WLSE Defaults, page 3-17.

On the DHCP server, set the following:

- Specify the vendor class ID for the WLSE Express—See Set the Vendor Class ID, page 3-14.
- Create entries for the WLSE Express systems—See Create an Entry for WLSE Express Systems, page 3-14.
- Specify a DNS server for each site—See Configuring the DNS Server, page 3-14.

Set the Vendor Class ID

The vendor class ID tells DHCP what type of device is being configured in the entry. Each type of device has its own vendor class ID. For the WLSE Express, you set the vendor class ID to WLSE_Cisco_Systems_Inc; for example:

```
class "miniWLSE" {
match if substring (option vendor-class-identifier,0,22) = "WLSE_Cisco_Systems_Inc";
vendor class id
}
```

Create an Entry for WLSE Express Systems

Create an entry in which you specify the parameters for the IP address pool for the WLSE Express systems:

```
pool {
    allow members of "miniWLSE";
    range 192.168.0.131 192.168.0.132;
    next-server 192.168.0.7;
    option tftp-server-name "192.168.0.7";
    filename "config_store1.tar";
    option bootfile-name "config_store1.tar;
}
```

In this example, the required parameters are the following:

- *range* is the IP address pool for the WLSE Express systems.
- *next-server* is the TFTP server that will be used to download the master configuration file to the WLSEs.
- *filename* is the name of the site-specific configuration file that you will create in one of the procedures in this chapter. The filename is configurable by the user who creates the site-specific file.

Configuring the DNS Server

The WLSE resolves hostnames to IP addresses by using a Domain Name System (DNS) server.

Configure the DNS server to resolve the hostnames of your WLSEs and make sure there is an entry in the DHCP server's global settings for the DNS server; for example:

```
option domain-name-servers 192.168.0.9;
```

Requirement for TFTP Server

You will need a local TFTP server at each site that is accessible to the WLSEs. The TFTP server stores the site-specific configuration file for the local WLSEs.

Auto-Configuration Quick Reference

The tasks for auto-configuring WLSE Express systems are:

Table 3-4 Configuration Quick Reference

Task	Reference
1. Create the master configuration file: • Start up the reference WLSE. • Log in and create the master configuration file.	About the Master Configuration File, page 3-15
2. Create site-specific configuration files.	Creating the Site-Specific Configuration File, page 3-23
3. Start up the production WLSEs. The WLSEs will be auto-configured by downloading the master configuration file.	Auto-Configuring the Local WLSEs, page 3-25
4. Verify that the production WLSEs are configured as you expect.	Verifying the Configuration, page 3-25

About the Master Configuration File

A WLSE configuration file has 3 components:

- An editable XML file contains all of the WLSE settings that may need to be customized at individual sites.
- A binary file contains the WLSE settings that are the same at all sites.
- An information file contains information used internally during the download and configuration process.

The master configuration file can be copied and then manually edited to create a customized, site-specific configuration file. This site-specific file is then stored on a TFTP server, to be downloaded to the local WLSEs when they start up.

Table 3-6 shows more detail about which information is saved in the XML (.xml) file and which is saved in the binary (.dat) file.

Creating the Master Configuration File

Note The reference WLSE must be running the same software version as the local WLSEs to be configured.

The master configuration file is created on the reference WLSE Express. After creating the file, you can copy it and create a customized, site-specific file. This customized file is then stored on a TFTP server, to be downloaded to the production WLSEs when they start up.

The procedures for creating the master configuration file consist of the following tasks:

1. Start the Reference WLSE, page 3-16
2. Manually Change Reference WLSE Defaults, page 3-17
3. Create the Master Configuration File, page 3-18

Start the Reference WLSE

To turn on the WLSE, press the power button on the front panel. After the WLSE is powered on, it will contain the following information in its flash memory:

- A superuser account with the username admin and password admin. You should change the password as soon as possible; see Manually Change Reference WLSE Defaults, page 3-17.

- The following network information, according to the defaults and the network information you included in the DHCP entry. To change any of this information, you can use CLI commands—See Table 3-5 on page 3-18.
  - Hostname (set to "localhost" by default)
  - Domain name
  - IP address
  - Netmask
  - Default gateway IP address
  - DNS server IP address

Manually Change Reference WLSE Defaults

It is recommended that you change the superuser (admin) password. To change the admin password and other network parameters after starting the WLSE, you can use the CLI commands listed in the following procedure.

Procedure

Step 1 Attach a console terminal or PC to the WLSE's serial/console port and log in. Use the admin username and admin password.

To connect a console, use the console/serial port on the back panel. For more information on the port and cabling, see Connecting Cables, page 2-12.

Note If you are using a Windows terminal emulator, it is recommended that you use the Windows Hyper Terminal application.

You can also log in by using SSH and the admin username and admin password. Telnet is disabled by default. To enable it, log in as admin and use the **telnetenable enable** CLI command.

Step 2 Make changes by setting the parameters show in Table 3-5 on page 3-18, as needed.

Table 3-5 CLI Configuration Commands

Parameter	CLI Commands
Change from obtaining IP address via DHCP to using a static IP address	**interface eth0** *ip_address netmask* **default-gateway** *ip_address* **ip name-server** *ip_address* **ip domain-name** *domain_name* Enter all of these CLI commands if you are using static addressing for the reference WLSE.
Hostname	**hostname** *name*
Change superuser password (recommended)	**username admin password** *password* You can also change this password in the Web interface.
Enable login via Telnet	**telnetenable enable**

Note Reboot the WSLE with the **reload** command after making these changes.

For more details on CLI commands, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.11*.

.

Create the Master Configuration File

To create the master configuration file:

1. Log in to the Web interface of the reference WLSE—See Log into the Reference WLSE Express, page 3-19.
2. Set the parameters you want to save in the master configuration file—See Set Parameters for the Master Configuration File, page 3-19.
3. Save the master configuration file—See Save the Master Configuration File, page 3-22.

Log into the Reference WLSE Express

To log into the Web interface:

Step 1 Access the WLSE through a supported browser by entering the WLSE's IP address or hostname, followed by **:1741** (for example: http://209.165.128:1741).

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

Tip For information on supported browsers, see Configuring Internet Explorer, page 3-10.

Step 2 Enter the admin username and password and click **Login**.

Set Parameters for the Master Configuration File

The master configuration is created by setting parameters on the reference WLSE and saving them into the master configuration files.

Some parameters cannot be saved from the UI into the master configuration; for example:

- AAA server parameters and other parameters under **Administration > Appliance**.
- Settings for NTP servers and the Web timeout for logins.

You can add these parameters to the .xml file in the form of CLI commands. For more information on editing the .xml file, see Save the Master Configuration File, page 3-22. For information on CLI commands, see the online help.

On the reference WLSE, set the parameters to be saved in the master configuration file.

Procedure

Step 1 Using Table 3-6 on page 3-20, set the desired parameters. For details on how to set these parameters in the UI, see the online help.

Table 3-6 Parameters Saved in the Master Configuration File

Category	Navigation Path	Notes
Faults Settings		
Fault Profiles	**Faults > Manage Fault Settings**	Default fault profile.
Fault Notification	**Faults > Notification Settings**	Trap, syslog, and email notifications.
Discover Settings		
Discovery Schedule and Settings	**Devices > Discover > DISCOVER > Discovery Wizard**	Settings for scheduled discoveries, including seed devices and CDP distance.
	Devices > Discover > DISCOVER > Advanced Options	Device name format, reverse DNS lookup, and auto-management.
Device Credentials	**Devices > Discover > Device Credentials > SNMP Communities**	SNMP community strings for all managed devices.
	Devices > Discover > Device Credentials > Telnet/SSH User/Password	Telnet/SSH credentials for IOS access points.
	Devices > Discover > Device Credentials > IOS HTTP/HTTPS Port Settings	HTTP port settings, username, and password for non-IOS access points.
	Devices > Discover > Device Credentials > WLCCP Credentials	WLCCP credentials for communicating with wireless domain services (WDS) devices.
Inventory Polling Parameters	**Devices > Discover > Inventory > Polling**	Polling intervals for client inventory, performance inventory; data aggregation time periods.
AAA Servers	**Devices > Discover > AAA Server**	Credentials for monitoring external AAA servers.
Client Tracking	**Devices > Discover > Client Tracking**	Enable/disable client tracking on all WDS devices.
Rule-Based Groups Settings		
Groups	**Devices > Group Management**	Definitions of user-defined rule-based groups.

Table 3-6 Parameters Saved in the Master Configuration File (continued)

Category	Navigation Path	Notes
Configure Settings		
Templates	**Configure > Templates**	Configuration templates.[1]
	Configure > Auto-Update > Startup Configuration	Startup template assignment.
	Configure > Auto-Update > Auto-Managed Configuration > Assign Templates	Auto-config template assignment.
	Configure > Auto-Update > Auto-Managed Configuration > Auto-Managed Options	Option to email results of auto-configuration jobs.
Administration Settings		
Appliance Settings	**Administration > Appliance > Redundancy > Manage Redundancy**	Redundancy settings.
	Administration > Appliance > Splash Screen	Login message.
User Settings	**Administration > User Admin > Manage Roles**	Definitions of roles.
	Administration > User Admin > Manage Users	User accounts.

[1] Any custom commands in templates are saved in the .xml file. Settings made in the other configuration screens are saved in the .dat file.

Save the Master Configuration File

The master configuration consists of a tar archive that contains an editable .xml file, a binary .dat file, and a .info file. The parameters listed in Table 3-6 on page 3-20 will be saved to the master configuration files—most parameters will appear in the editable .xml file, but some will be in the binary .dat file, as shown in Table 3-7 on page 3-22.

Procedure

Step 1 On the reference WLSE, select **Administration > Appliance > Master Configuration**.

Step 2 Enter a filename, then click **Create Config**.

Result: A list of the information that can be saved in the master configuration file is displayed.

The following table shows which information is saved in the editable .xml file and which is saved in the binary .dat file. For details on the parameters that are saved, see Table 3-6 on page 3-20.

Table 3-7 Data Saved in the .xml and .dat Files

Category	Parameters	In .xml File	In .dat File
Faults	Default fault profile settings		X
	Notification settings	X	
Discover	Discovery schedule and seed devices	X	
	Device credentials	X	
	Advanced options (filtering, device name format)	X	
	Inventory polling parameters	X	
	AAA server monitoring	X	
	Client tracking enable	X	
Rule-Based Groups	User defined rule-based groups		X

Table 3-7 Data Saved in the .xml and .dat Files (continued)

Category	Parameters	In .xml File	In .dat File
Configure	Templates[1]	X	X
	Startup configuration template assignment	X	
	Auto-managed configuration template assignment	X	
Administration	Appliance settings (redundancy, splash screen)	X	
	User role definitions		X
	Users (usernames, passwords, and privileges)	X	

[1] Any custom configuration commands are saved in the .xml file; settings made in the other configuration screens are saved in the .dat file.

Step 3 Select the categories of parameters that you want to save in the master configuration file, then click **Create Config**.

Result: The configuration tar archive and the date it was created appear in the Saved Configurations list.

Step 4 Click **Download** to save the file to your desktop.

Creating the Site-Specific Configuration File

Use the following procedure to create a custom, site-specific configuration file.

Procedure

Step 1 Using a copy of the master configuration tar file that was created on the reference WLSE, extract the .xml file from the archive.

Step 2 Edit the .xml file as needed to:

- Change or add settings to the file, according to the site-specific requirements.
- Add any necessary CLI commands in the CLI block of the .xml file.

CLI commands are used to set parameters that cannot be automatically saved in the master configuration file; for example:

- AAA server parameters and most of the other parameters under **Administration > Appliance**.
- Settings for NTP servers and the Web timeout for logins.

Tip For information on the format of the .xml file, see Appendix A, "Configuration File Reference."

Tip For information on the parameters that can be automatically saved in a master configuration file, see Table 3-6 on page 3-20.

Note You should use caution when editing the site-specific file; however, most errors in the file will be caught and logged in the *dhcp.log* file in the logs directory.

Step 3 After editing the .xml file, retar the archive (.xml, .dat, and .info files). Make sure that:

- All files have read permission for "others."
- All filenames are relative pathnames.
- All filenames match; for example, if the configuration tar filename is *wlse.tar*, the other files must be *wlse.xml*, *wlse.dat* and *wlse.info*.

Step 4 Copy the site-specific configuration tar file to the TFTP server at the local site.

Note The tar file name must be the same as the filename entered on the DHCP server. For more information, see Prerequisites for Auto-Configuration, page 3-13

Auto-Configuring the Local WLSEs

To auto-configure WLSE Express systems, power them on by pressing the power switch on the front panel. When the WLSEs boot up:

- The WLSEs will obtain their IP addresses and other network parameters from DHCP and will download the site-specific configuration file from the TFTP server.
- The WLSE will extract the .dat and .xml files and validate them based on the information from the .info file. Validation ensures that the reference WLSE and WLSEs to be configured are running the same system software version.
- The WLSE will be auto-configured with the settings in the .xml and .dat files.

Verifying the Configuration

You can verify that a production WLSE Express is correctly configured by performing the following steps. Some of the verification is done through the command-line interface (CLI) and some through the Web interface.

Procedure

Step 1 At the system console, or via Telnet or SSH, log in as the admin user.

Note For security reasons, Telnet is disabled on the WLSE by default. To enable it, log in as admin and use the **telnetenable enable** CLI command. For more information on this command and other CLI commands, see the online help.

a. To verify the IP address, enter the following command:

```
# show interface
```

b. To verify that the WLSE can obtain DNS services from the network, enter the following command.

```
# nslookup dns-name
```

where *dns-name* is the DNS name of a host that is registered in DNS. If the system cannot obtain the IP address of the host from DNS, use the **ip name-server** command to specify a working DNS server.

c. To verify that the WLSE can communicate with the network, enter the following command:

```
# ping ip-address
```

where *ip-address* is the IP address of a host that is accessible on the network. The DNS server is a good host to ping because it should always be running and accessible

d. Enter the following command to verify that the system time and date are correct in Coordinated Universal Time (UTC):

```
# show clock
```

If the time or date is incorrect, set the correct time and date using the **clock** command.

If your network uses Network Time Protocol (NTP), use the **ntp server** command to configure the WLSE to use NTP.

e. To log out of the CLI, enter the following command:

```
# exit
```

Step 2 Log in to the Web interface as the admin user and verify that the parameters in the site-specific configuration file are correctly set on the WLSE.

For information on where to look in the UI, use the Navigation Path column in Table 3-6 on page 3-20.

Reapplying the Configuration File

If you change settings in the site-specific configuration file and install a changed file on your TFTP server, the WLSE will automatically download the new file after it reboots and apply the changes to its configuration.

If you need to reapply the configuration file, but the file has not changed, you must first erase the WLSE’s configuration by using the **erase config** CLI command. After you run this command on the WLSE and reboot, the WLSE will download the configuration file and apply settings to its configuration.

For more information on the **erase config** command, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.11*.

Customizing a WLSE Express After Applying a Configuration File

After a WLSE Express starts and loads its configuration from the site-specific configuration file, you can further customize the system by using its Web interface or its CLI command interface.

Caution You might lose your custom settings if the site-specific configuration is reapplied.

Setting Up Discovery and Device Management

After setting up devices, you can discover and manage them. This section describes discovery and management configuration for WLSE 2.11.

Note If you have set up auto-configuration of the WLSE Express and included discovery and management in the auto-configuration process, you do not have to perform the steps in this chapter.

Device Management Quick Reference

Table 4-1 on page 4-2 provides a high-level overview of the tasks for discovering and managing devices. Detailed procedures are provided in this chapter.

Note For IOS access points used within a Cisco Structured Wireless-Aware Network (SWAN), you can use Wireless Doman Services (WDS) and the WLSE's Deployment Wizard for device configuration and deployment, instead of performing Tasks 1 through 4 in Table 4-1. The Deployment Wizard is the prefered method for such deployments. The Deployment Wizard displays immediately after you log in to the WLSE's web interface. For more information on the Deployment Wizard, see the WLSE online help and the *User Guide for the*

CiscoWorks Wireless LAN Solution Engine, 2.11 on Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm.

Table 4-1 Quick Reference

Tasks	References
1. Add device credentials to the WLSE.	Adding Device Credentials to the WLSE, page 4-2
2. (Optional) Set discovery and management options.	Configuring Discovery Options, page 4-7
3. Discover or import devices.	Discovering Devices, page 4-8
4. Manage devices.	Managing Devices, page 4-14
5. Add any AAA servers to be monitored.	Adding AAA Servers to the WLSE, page 4-15

Adding Device Credentials to the WLSE

Note If you are importing devices, instead of discovering them, you may not need to manually enter credentials. If you are importing devices from a file, the credentials can be included in the file. If you are importing devices from CiscoWorks RME, the credentials will be imported.

This section provides procedures for entering the following required device credentials on the WLSE:

- For all managed devices, enter SNMP credentials.
- For access points, the following additional credentials are required:
  - For IOS-based access points, enter Telnet or SSH credentials and IOS HTTP port settings.
  - For non-IOS access points, enter HTTP credentials.
- For radio management, enter WLCCP credentials.

Enter SNMP Community Strings for All Managed Devices

SNMP community strings are used for discovery and for enabling WLSE features, such as AP configuration jobs and radio management. The community string must be set on each device, as described in Chapter 5, "Setting Up Devices—Overview." You can enter as many community strings on the WLSE as necessary.

Note If you are importing devices, you do not need to enter their community strings.The community strings will be imported along with the devices and will be listed in WLSE Communities screen, in which you can modify and delete strings as required. For more information, see Import Devices, page 4-11.

To configure community strings on the WLSE, perform the following steps:

Procedure

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

Note This screen contains a default entry which can cover all devices, provided device community strings are set to the default (public).

Step 2 To add an entry:

a. Enter data in the individual text boxes: IP address, Read Community, Timeout, SNMP Retries, and Write Community.

b. Click **Add** to add the community string to the list.

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

Step 3 To modify an entry:

a. Select the entry in the list of entries.

Result: The individual text boxes are populated with the data from the entry.

b. Change the desired fields in the individual text boxes.

c. Click **Modify**.

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

Step 4 To delete an entry:

a. Select the entry in the list of entries. To select a number of entries, use the Ctrl or Shift key.

b. Click **Delete**.

Note The default entry cannot be deleted.

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

Enter HTTP Credentials for Non-IOS Access Points

HTTP credentials are required for downloading configuration files to non-IOS access points and for uploading configurations from such access points. The same password must be set on each access point. You can enter as many usernames and passwords as necessary.

To enter HTTP usernames and passwords:

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.

b. Enter the username.

c. Enter the password.

d. Click **Save**. The IP address and username are added to the Current Entries textbox.

Step 3 Repeat step 2 to add credentials for more devices.

Enter Telnet or SSH Credentials for IOS Access Points

Telnet/SSH credentials are used for downloading configuration files to IOS-based access points and for upgrading firmware on IOS access points.

Note When entering Telnet or SSH credentials, enter data only in the fields that correspond to the login sequence on the access point(s). For example, if the access point does not prompt for a username, do not enter a username.

To enter Telnet or SSH credentials, perform the following steps:

Procedure

Step 1 Select **Devices > Discover > Device Credentials > Telnet/SSH 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 these passwords.
- **b.** Enter the username.
- **c.** Enter the password and confirm it.
- **d.** Enter the enable password and confirm it.
- **e.** Click **Save**. The IP address, username, and passwords are added to the Current Entries textbox.

Step 3 Repeat step 2 to add credentials for more devices.

Enter HTTP Port Settings for IOS Access Points

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

To enter HTTP or HTTPS port settings, perform the following steps:

Procedure

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

Step 2 To add a port:

- **a.** Enter the IP address or range of IP addresses that use this port number.
- **b.** Enter the port number.
- **c.** Click **Save**.

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

Enter WLCCP Credentials for Wireless Domain Services (WDS)

To configure the WLSE to authenticate with WDS devices, perform the following steps:

Procedure

Step 1 Select **Devices > Discover > Device Credentials > WLCCP Credentials**.

Step 2 Enter the Radius User Name and Radius Password.

This is the username and password that you set for the WLSE on the AAA server.

Step 3 Click **Save**.

Configuring Discovery Options

Discovery options allow you to enable automatic management of all discovered devices, specify use of device names in displays, and use MAC address filtering for management of access points.

Note These procedures are optional.

To configure discovery options, perform the following steps:

Procedure

Step 1 Select **Devices > Discover > DISCOVER > Advanced Options**.

- **a.** If you want device names in WLSE displays, instead of their IP addresses, select **Use Reverse DNS lookup**.
- **b.** Configure the name format for devices in WLSE displays in the Name Format field.
- **c.** To enable automatic management for all discovered devices, select **Auto-Manage Devices**. Otherwise, you must manually move devices to the managed state after they have been discovered.
- **d.** To arrange temporary management of access points, configure MAC address filtering. For information, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.11*.
- **e.** Click **Save**.

Step 2 To set up IP filters for limiting discovery to certain devices, select **Devices > Discover > DISCOVER > IP Filter Rules** and follow the instructions in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.11*.

Discovering Devices

Use the procedures in this section to discover devices by using CDP or device import:

- Use the discovery wizard to run a CDP discovery—See Run CDP Discovery, page 4-8.

  Note If you prefer not to use CDP, use the wizard and enter all of your devices as seeds, as indicated in Run CDP Discovery, page 4-8, or import devices.

- Import devices from a file or from a CiscoWorks server—See Import Devices, page 4-11.

Note If WDS is configured on the subnet, CDP discovery proceeds automatically via WLCCP for the infrastructure access points. The access points must be properly configured. All access points will be used as seeds. The WDS must also be configured and in the managed state. For device configuration information, see Chapter 5, “Setting Up Devices—Overview.”

Run CDP Discovery

Before CDP discovery can proceed, you must specify at least one initiating IP address (seed device), from which other devices can be discovered. Neighbors of the seed device are discovered according to the CDP distance that you specify. The seed device and discovered devices must be CDP-enabled.

Note By default, the WLSE runs a CDP discovery every 24 hours.

Use the procedures in this section to run an immediate or scheduled discovery:

- Run an immediate, one-time CDP discovery—See Run CDP Discovery Now, page 4-9.
- Modify the default CDP discovery schedule—See Modify the CDP Discovery Schedule, page 4-10.

Run CDP Discovery Now

To run an immediate discovery, perform the following steps:

Procedure

Step 1 Select **Devices > Discover > DISCOVER > Discovery Wizard.**

Step 2 Select **Automatic Device Discovery based on Cisco Discovery Protocol**, and click **Next**.

Step 3 Select **Run Now** and click **Next**.

Step 4 Add community strings for all of the devices to be discovered if you have not already done so. For details on adding community strings, see Enter SNMP Community Strings for All Managed Devices, page 4-3. After adding community strings, click **Next**.

Step 5 Add one or more initiating IP addresses (seeds) to be used for this one-time discovery only:

> **Note** If CDP is not enabled, you still can discover devices by entering each of their IP addresses as seeds. In that case, however, the connectivity between switches and access points will not be discovered.

a. Enter the IP addresses or device names in the Add Seed Values text box and click **>>**.

b. Set the CDP distance. If the distance is set to 1, only the immediate neighbors of the seed devices are discovered. Set the distance appropriately to discover the entire wireless network. Set the distance to 1 if you are adding all devices as seeds.

> **Note** Routers and switches that do not have access points attached to them are used when computing CDP distance. However, such devices will not appear in the discovered devices list.

c. Click **Next**.

Step 6 (Optional) Enter a name for the discovery job.

Step 7 If the discovery summary is correct, click **Finish** to run the discovery. The discovery will begin within 2 minutes.

If the summary is not correct, click **Back** to make changes in any of your settings.

Step 8 A popup message displays the name of the discovery and the Discovery Run Details window appears. Click **Refresh** to update the Job Run Log.

Modify the CDP Discovery Schedule

To modify the default discovery schedule, perform the following steps:

Procedure

Step 1 Select **Devices** > **Discover > Discover > Discovery Wizard.**

Step 2 Select **Automatic Device Discovery based on Cisco Discovery Protocol,** and click **Next**.

Step 3 Select **Modify Periodic** and click **Next**.

Step 4 To modify the schedule:

- **a.** Select the Start Date and Start Time from the pull-down lists.
- **b.** To repeat discovery at a specified interval, select **Enable**. Then enter a number for the interval and select Minutes, Hours, Days, Weeks or Months from the pull-down list.
- **c.** Click **Next**.

Step 5 If you already added community strings, click **Next**.

If you have not added community strings, you must add them now. For details on adding community strings, see Enter SNMP Community Strings for All Managed Devices, page 4-3. After adding community strings, click **Next**.

Step 6 Add one or more initiating IP addresses (seeds):

Note If CDP is not enabled, you still can discover devices by entering each of their IP addresses as seeds in this window, however the connectivity between switches and access points will not be discovered.

a. Enter the IP addresses or device names in the Add Seed Values text box and click **>>**.

b. Set the CDP distance. If the distance is set to 1, only the immediate neighbors of the seed devices are discovered. Set the distance appropriately to discover the entire wireless network.

Note Routers and switches that do not have access points attached to them are used when computing CDP distance. However, such devices will not appear in the discovered devices list.

Step 7 Click **Next**.

Step 8 Click **Finish** to submit your changes. Discovery will begin at the scheduled time.

Click **Back** to make changes before submitting, or click **Cancel** to cancel all changes.

For more information about scheduled discoveries, see the WLSE online help.

Import Devices

After you import devices, a one-time discovery job starts immediately. All of the WLSE-supported devices in the file or found on the CiscoWorks server are used as seed devices with a CDP distance of 1. After importing devices, ensure that they are managed.

Note If CDP is not enabled and you import devices, only the imported access points and wireless bridges will be discovered. Routers and switches will not be discovered.

Import Devices from a File

Devices can be imported from a comma-separated values (CSV) file. You can create the file by exporting devices from CiscoWorks RME or by creating a file with a text editor. After you import the file, a one-time discovery begins immediately.

Procedure

Step 1 Select **Devices > Discover > Discover > Discovery Wizard**.

Step 2 Select **Import From File** and click **Next**.

Step 3 Enter the pathname of the file or click **Browse** to find it. If you do not have a file, click **See sample CSV file** for the correct format.

Step 4 Only the hostnames, IP addresses, and read and write community strings are imported automatically.

- If you want to specify timeout and retry values, enter them in the SNMP Timeout and SNMP Retry fields. Otherwise, the default values of a 10-second timeout and 1 retry will be assigned to the imported devices.
- Click **Next,** or click **Cancel** to cancel the import.
- Click **Check Last Status** to see the results of the last discovery.

Step 5 Click **Finish** to import the devices listed in the file. A one-time discovery begins immediately.

Step 6 Click **Check Last Status** to see the results of the import.

See the online help for more detailed information on importing devices from a file.

Import Devices from a CiscoWorks Server

You can import devices from a CiscoWorks server that is running Resource Manager Essentials. This import can be immediate or scheduled, and you can schedule repeat imports. A discovery runs after the import.

Procedure

Step 1 Select **Devices > Discover > Discover > Discovery Wizard.**

Step 2 Select **Import From CiscoWorks** and click **Next**.

Step 3 Complete the Schedule Import from CiscoWorks dialog.

a. Enter the following data. All fields are required.

Text Box	Description
Host	The CiscoWorks server's IP address.
Server Port	The port number on which the CiscoWorks server listens for HTTP requests. You may have to contact the administrator of the CiscoWorks server for this information.
Username	Any user who has the authority to export and import device credentials on the CiscoWorks server.
Password	

b. For an immediate, one-time import, select **Run Now**.

c. To schedule a one-time import for a later time or schedule repeated imports:

- Select the start date and start time from the pulldown lists.
- To schedule repeated imports, select Enable Repeat. Then set the interval by entering a number after Every and selecting Minutes, hours, Days, Weeks, or Months.

d. Click **Cancel** to cancel the import.

e. Click **Check Last Status** to see the results of the last discovery.

Step 4 Click **Finish** to import devices.

- If you selected Run Now, discovery begins immediately.
- If you scheduled the discovery for a later time, the list of scheduled and completed discoveries appears.

Managing Devices

After discovering or importing devices and verifying the results, make sure that all the devices you want to manage or monitor are in the Managed folder.

Note If you specified auto-management when configuring advanced options, the newly discovered devices will be in the Managed folder. For information on setting the auto-manage option, see Configuring Discovery Options, page 4-7.

To move devices to the Managed folder (if necessary):

Procedure

Step 1 Select **Devices > Discover > Managed Devices**.

The Discovered Devices tree appears.

If you specified auto-manage, all discovered devices will already be in the Managed folder. An inventory will automatically run for these devices

Step 2 If you did not specify auto-manage, you must move the newly discovered devices to the managed state:

a. Expand the New folder. All of the devices in the folder will be listed in the New Devices box in the Group Change Status pane.

b. Select one or more devices in the New Devices box, and click **Manage**.

The selected devices move to the appropriate group in the Managed folder. For example, if you select a switch and click **Manage**, it will move to the Switch folder.

Note Inventory will run automatically after you move devices to the managed state.

Step 3 To view information about a device, select the device from the Discovered Devices tree. The Device Details pane displays details about the device.

From the Device Details pane, you can change a device's management status or delete the device from Discovered Devices.

Adding AAA Servers to the WLSE

Use the following procedure to add information about all AAA servers to be monitored by the WLSE. For information about configuring an ACS server for monitoring, see Adding AAA Servers to the WLSE, page 4-15.

Procedure

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

Step 2 Select the server type: EAP-MD5, LEAP, PEAP, RADIUS, or EAP-FAST.

Step 3 Complete the following:

Text Box	Description
Server Name	Hostname or IP address of an AAA server to be added. **Note** Depending on how your network is set up, the AAA server can be a Cisco Secure Access Control Server, a Cisco Access Registrar RADIUS server, or an access point configured as an AAA server.
Server Port	Port on the server used for authentication; use port 1812.
Username	Client username that you entered on the AAA server.
Password	Client password that you entered on the AAA server.
Secret	Shared secret key that you entered on the AAA server.

Step 4 Click **Save**.

Step 5 Repeat Steps 2-4 for each AAA server you want to add.

For more information on AAA servers, see the WLSE online help.

Next Step

For information on advanced configuration and day-to-day operation of the WLSE, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.11* or the WLSE online help.

CHAPTER 5

Setting Up Devices—Overview

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, firmware upgrade, and radio management.

Note This chapter provides an overview of device setup and information on where to find detailed instructions and information on the devices are supported by the WLSE.

Finding Details on Supported Devices

For information about device models and versions supported by the WLSE, see the *Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine, 2.11* on Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm.

About Device Setup Methods

There are two ways to set up devices:

- Configure devices manually or use basic WLSE configuration methods—See Basic Device Setup Methods, page 5-2.

- Use the WLSE Deployment Wizard. This method is for IOS access points using Wireless Doman Services (WDS) within a Cisco Structured Wireless-Aware Network (SWAN)—See WLSE Deployment Wizard, page 5-2.

WLSE Deployment Wizard

If you are using the WLSE Deployment Wizard to deploy IOS access points or a Wireless LAN Services Module (WLSM) used within a Cisco SWAN framework, the Wizard will set up those devices for you. In that case, for those devices, you do not need to perform the manual setup procedures described in the rest of this chapter.

The Deployment Wizard displays immediately after you log in to the WLSE's web interface.

For information on using the Deployment Wizard, see the WLSE online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.11* on Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm.

Basic Device Setup Methods

For details on setting up external devices, see the document *Configuring Devices for Management by the Wireless LAN Solution Engine, 2.11*.

Overview: Device Setup

This section briefly describes the required configuration for the following devices managed or monitored by the WLSE:

- Configuring Non-IOS Access Points and Bridges, page 5-3
- Configuring IOS Access Points and Bridges, page 5-3
- Configuring Routers and Switches, page 5-3
- Configuring External AAA Servers, page 5-4
- Configuring the Internal AAA Server, page 5-4

- Configuring a Wireless LAN Access Module, page 5-4

Configuring Non-IOS Access Points and Bridges

You can use the device Web interface or a WLSE configuration template to configure non-IOS devices.

Device configuration consists of:

- Normally, enabling Cisco Discovery Protocol (CDP)
- Configuring SNMP
- Adding an HTTP user and enabling the User Manager
- Normally, selecting TFTP as the transfer protocol between APs and the WLSE

Configuring IOS Access Points and Bridges

You can use the device Web interface, the device CLI, or WLSE configuration templates to configure IOS devices.

Device configuration consists of:

- Normally, enabling Cisco Discovery Protocol (CDP)
- Configuring SNMP
- Configure Telnet or SSH for pushing configuration templates to APs

Configuring Routers and Switches

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

Router and switch configuration consists of:

- Enabling Cisco Discovery Protocol (CDP)
- Configuring SNMP

Configuring External AAA Servers

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

AAA server configuration consists of:

- Configuring the server to recognize the WLSE
- Configuring the WLSE to monitor and report on the AAA servers

Configuring the Internal AAA Server

To configure the internal AAA server, use the AAA Administration option under the Administration tab. For more information, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.11*.

To set up monitoring and reporting for the internal AAA server, use the AAA Server option under the Devices tab and Discover subtab. For more information, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.11*.

Configuring a Wireless LAN Access Module

You can use a Wireless LAN Services Module (WLSM) to provide Wireless Domain Services (WDS) to access points. See *Configuring Devices for Management by the Wireless LAN Solution Engine, 2.11*.

Configuration File Reference

This appendix provides information on WLSE configuration files.

- Components of the configuration file—See Configuration File Components, page A-1
- Parameters that can be saved in the .xml file—See Tags and Attributes in the .xml File, page A-17

Configuration File Components

The WLSE configuration file consists of the following files:

- A binary .dat file, which contains the AP configuration template settings (except for custom commands)
- An editable .xml file, which contains most of the saved parameters—See Example .xml File, page A-13
- A .info file

Also included in this appendix is the DTD file—See DTD File, page A-2.

DTD File

The following DTD file defines the parameters that can appear in the .xml file. Special characters after names indicate how many instances are permitted:

none	1 time
?	0 or 1 times
*	0 to many times
+	1 or more times

```
<?xml version="1.0" encoding="UTF-8"?>

<!ELEMENT StartupConfig (Faults?, Devices?, APConfiguration?, Administration?,
APLocations?, RMConfiguration?) >
<!ATTLIST StartupConfig
    version CDATA "3.0"
    model (1030|1130) "1030"
    configId CDATA "0"
>

<!ELEMENT Faults (NotificationSettings?, FaultPolicy*, FaultThreshold*, AAAServerInfo*) >
<!ELEMENT NotificationSettings (TrapNotification*, SyslogNotification*,
EmailNotification*) >
<!ATTLIST NotificationSettings
    format (PlainText|XML) "XML"
>

<!ELEMENT TrapNotification EMPTY >
<!ATTLIST TrapNotification
    host CDATA #REQUIRED
    port CDATA "162"
    community CDATA #REQUIRED
    isEncrypted (YES|NO) "YES"
>

<!ELEMENT SyslogNotification EMPTY >
<!ATTLIST SyslogNotification
    host CDATA #REQUIRED
>

<!ELEMENT EmailNotification EMPTY >
<!ATTLIST EmailNotification
    address CDATA #REQUIRED
    priority (P1|P2|P3|P4|P5|OK) #REQUIRED
```

```
>

<!ELEMENT FaultPolicy (FSMState+, FSMStateTransition*)>
<!ATTLIST FaultPolicy
    name CDATA #REQUIRED
    type CDATA #REQUIRED
    enabled (YES|NO) "YES"
    pollFrequencyInSeconds CDATA #REQUIRED
>
<!ELEMENT FSMState EMPTY>
<!ATTLIST FSMState
    name CDATA #REQUIRED
    severity (P1|P2|P3|P4|P5|OK) #REQUIRED
>
<!ELEMENT FSMStateTransition EMPTY>
<!ATTLIST FSMStateTransition
    fromState CDATA #REQUIRED
    toState CDATA #REQUIRED
    parameters CDATA #REQUIRED
    formula CDATA #REQUIRED
    formulaType (numeric|string-in|string-equals|string-like) #REQUIRED
>

<!ELEMENT FaultThreshold (FSMRange+)>
<!ATTLIST FaultThreshold
    name CDATA #REQUIRED
    type CDATA #REQUIRED
    enabled (YES|NO) "YES"
    pollFrequencyInSeconds CDATA #REQUIRED
>
<!ELEMENT FSMRange EMPTY>
<!ATTLIST FSMRange
    stateName CDATA #REQUIRED
    fromRange CDATA #REQUIRED
    toRange CDATA #REQUIRED
    fromComparator CDATA #REQUIRED
    toComparator CDATA #REQUIRED
    count CDATA #REQUIRED
    severity (P1|P2|P3|P4|P5|OK) #REQUIRED
>

<!ELEMENT AAAServerInfo EMPTY >
<!ATTLIST AAAServerInfo
    hostNameOrIP CDATA #REQUIRED
    port CDATA #REQUIRED
    protocol (EAPMD5|LEAP|PEAP|RADIUS) #REQUIRED
    user CDATA #REQUIRED
    password CDATA #REQUIRED
    secret CDATA #REQUIRED
    isEncrypted (YES|NO) "YES"
>

<!ELEMENT Devices (DeviceCredentials?, Discovery?, Inventory?, Groups?) >


<!ELEMENT DeviceCredentials
(SNMPCredentials*,HTTPCredentials*,HTTPPort*,CLICredentials*,WLCCPCredentials?) >

<!ELEMENT SNMPCredentials EMPTY >
<!ATTLIST SNMPCredentials
    ipAddressRange CDATA #REQUIRED
    readCommunity CDATA #REQUIRED
    writeCommunity CDATA #REQUIRED
    isEncrypted (YES|NO) "YES"
    timeoutSeconds CDATA "10"
    retries CDATA "1"
>

<!ELEMENT HTTPCredentials EMPTY >
<!ATTLIST HTTPCredentials
    ipAddressRange CDATA #REQUIRED
    user CDATA #REQUIRED
    password CDATA #REQUIRED
    isEncrypted (YES|NO) "YES"
>

<!ELEMENT HTTPPort EMPTY >
<!ATTLIST HTTPPort
    ipAddressRange CDATA #REQUIRED
    port CDATA "80"
>

<!ELEMENT CLICredentials EMPTY >
<!ATTLIST CLICredentials
    ipAddressRange CDATA #REQUIRED
    user CDATA #REQUIRED
    password CDATA #REQUIRED
    enableUser CDATA #REQUIRED
    enablePassword CDATA #REQUIRED
    isEncrypted (YES|NO) "YES"
>

<!ELEMENT WLCCPCredentials EMPTY >
<!ATTLIST WLCCPCredentials
    user CDATA #REQUIRED
    password CDATA #REQUIRED
    isEncrypted (YES|NO) "YES"
>

<!ELEMENT Schedule EMPTY >
<!ATTLIST Schedule
    enabled (YES|NO) "YES"
    repeatIntervalInMinutes CDATA #REQUIRED
>

<!ELEMENT Discovery (Schedule, CDPDiscovery?) >
<!ATTLIST Discovery
    displayNameFormat CDATA "%dns%"
    reverseDNSLookup (YES|NO) "NO"
    autoManage (YES|NO) "YES"
>

<!ELEMENT CDPDiscovery (CDPSeed*) >
<!ATTLIST CDPDiscovery
    cdpDistance CDATA "1"
>

<!ELEMENT CDPSeed EMPTY >
<!ATTLIST CDPSeed
    ipAddress CDATA #REQUIRED
>

<!ELEMENT Inventory (FullInventory?, ClientInventory?, PerformanceInventory?,
APRebootDetection?, AggregationSettings?, SystemSettings?, ClientTrackingSettings?)>

<!ELEMENT FullInventory (Schedule) >

<!ELEMENT ClientInventory (Schedule) >

<!ELEMENT PerformanceInventory (Schedule) >

<!ELEMENT APRebootDetection EMPTY >
<!ATTLIST APRebootDetection
    repeatIntervalInMinutes CDATA #REQUIRED
>

<!ELEMENT AggregationSettings EMPTY >
<!ATTLIST AggregationSettings
    daysToKeepHourlyData CDATA "7"
    daysToKeepDailyData CDATA "30"
    daysToKeepWeeklyData CDATA "180"
    daysToKeepMonthlyData CDATA "365"
>
```

```
<!ELEMENT SystemSettings EMPTY >
<!ATTLIST SystemSettings
    daysToKeepJobHistoryData CDATA "30"
    daysToKeepFaultHistoryData CDATA "30"
>


<!ELEMENT ClientTrackingSettings EMPTY >
<!ATTLIST ClientTrackingSettings
    enabled (YES|NO) "YES"
>

<!ELEMENT APConfiguration (ConfigTemplate*, StartupTemplate*, AutoTemplates?)>

<!ELEMENT ConfigTemplate (SupportedDevice*, IOS*) >
<!ATTLIST ConfigTemplate
    name CDATA #REQUIRED
    description CDATA #IMPLIED
    type CDATA "IOS"
    configFile CDATA #IMPLIED
    customConfigFile CDATA #IMPLIED
>
<!ELEMENT SupportedDevice EMPTY>
<!ATTLIST SupportedDevice
    deviceType CDATA #REQUIRED
    versions CDATA #REQUIRED
>

<!ELEMENT IOS EMPTY >
<!ATTLIST IOS
    command CDATA #REQUIRED
>

<!ELEMENT StartupTemplate EMPTY >
<!ATTLIST StartupTemplate
    name CDATA #REQUIRED
    configTemplateName CDATA #REQUIRED
    description CDATA #IMPLIED
    writeToNVRAM (YES|NO) "NO"
>

<!ELEMENT AutoTemplates (AutoTemplate*, AutoTemplateOptions?) >
<!ELEMENT AutoTemplate
(DeviceSerialNumberRule?|DeviceMACRule?|(DeviceTypeRule?,DeviceSubnetRule?,DeviceVersionRu
le?))>
<!ATTLIST AutoTemplate
    name CDATA #REQUIRED
    configTemplateName CDATA #REQUIRED
    description CDATA #IMPLIED
    enabled (YES|NO) "YES"
    writeToNVRAM (YES|NO) "NO"
>

<!ELEMENT DeviceSerialNumberRule (DeviceSerialNumber+) >
<!ELEMENT DeviceMACRule (DeviceMAC+) >
<!ELEMENT DeviceTypeRule (DeviceType+) >
<!ELEMENT DeviceSubnetRule (DeviceSubnet+) >
<!ELEMENT DeviceVersionRule (DeviceVersion+) >
<!ELEMENT DeviceSerialNumber (#PCDATA) >
<!ELEMENT DeviceMAC (#PCDATA) >
<!ELEMENT DeviceType (#PCDATA) >
<!-- DeviceType ("AP 1100"|"AP 1200"|"AP 1210"|"AP 340"|"AP 350"|"AP 350-IOS"|"BR
1310"|"BR 1410"|"AP 1210-SR")-->
<!ELEMENT DeviceSubnet (#PCDATA) >
<!ELEMENT DeviceVersion (#PCDATA) >

<!ELEMENT AutoTemplateOptions (SendEmailList?) >
<!ATTLIST AutoTemplateOptions
    IOSProtocol (SSH|TELNET) "TELNET"
>
<!ELEMENT SendEmailList EMPTY >
<!ATTLIST SendEmailList
    enabled (YES|NO) "YES"
    emailList CDATA #IMPLIED
>

<!ELEMENT Groups (RuleBasedGroup+) >
<!ELEMENT RuleBasedGroup (GroupRule+) >
<!ATTLIST RuleBasedGroup
    name CDATA #REQUIRED
    path CDATA #REQUIRED
    description CDATA #IMPLIED
>
<!ELEMENT GroupRule EMPTY >
<!ATTLIST GroupRule
    name CDATA #REQUIRED
    op CDATA #REQUIRED
    value CDATA #IMPLIED
>

<!ELEMENT Administration (Role*, User*, Redundancy?,  AAAServerConfig?,
ApplianceSettings?, CLIBlock?, SplashScreenMessage?) >

<!ELEMENT Role (Task*) >
<!ATTLIST Role
    name CDATA #REQUIRED
    creator CDATA "admin"
>
<!ELEMENT Task EMPTY >
<!ATTLIST Task
    tab CDATA #REQUIRED
    subtab CDATA #REQUIRED
>

<!ELEMENT User (Role+) >
<!ATTLIST User
    name CDATA #REQUIRED
    password CDATA #REQUIRED
    isEncrypted (YES|NO) "YES"
    cliAccess (None|0|15) "None"
    creator CDATA "admin"
    email CDATA #IMPLIED
>

<!ELEMENT Redundancy EMPTY >
<!ATTLIST Redundancy
    enabled (YES|NO) "NO"
    httpPort (1741|80) #REQUIRED
    adminPassword CDATA #REQUIRED
    isEncrypted (YES|NO) "YES"
    notificationEmail CDATA #REQUIRED
    virtualIPeth0 CDATA #REQUIRED
    primaryIP CDATA #REQUIRED
    secondaryIP CDATA #REQUIRED
    minutesBetweenSync CDATA #REQUIRED
    secondsBetweenCheck CDATA #REQUIRED
>

<!ELEMENT AAAServerConfig (AAAClient*, AAAUser*) >
<!ELEMENT AAAClient EMPTY >
<!ATTLIST AAAClient
    name CDATA #REQUIRED
    ipAddress CDATA #REQUIRED
    secret CDATA #REQUIRED
    isEncrypted (YES|NO) "YES"
>
<!ELEMENT AAAUser EMPTY >
<!ATTLIST AAAUser
    name CDATA #REQUIRED
    password CDATA #REQUIRED
    isEncrypted (YES|NO) "YES"
>

<!ELEMENT ApplianceSettings (WLSEManager?, NTPServer*, NameServer*) >
```

```
<!ATTLIST ApplianceSettings
    telnetEnabled (YES|NO) "NO"
    sshProtocol (SSH1|SSH2|SSH1_SSH2) "SSH1"
    httpServerPort (1741|80) #REQUIRED
    webTimeoutInSeconds CDATA #REQUIRED
    mailServer CDATA #REQUIRED
>
<!ELEMENT WLSEManager (#PCDATA)>
<!ATTLIST WLSEManager
    protocol (HTTP|HTTPS) "HTTPS"
    httpPort CDATA "1741"
>
<!ELEMENT NTPServer EMPTY>
<!ATTLIST NTPServer
    server CDATA #REQUIRED
>
<!ELEMENT NameServer EMPTY>
<!ATTLIST NameServer
    server CDATA #REQUIRED
>
<!ELEMENT CLIBlock (CLI*)>
<!ELEMENT CLI EMPTY >
<!ATTLIST CLI
    command CDATA #REQUIRED
>

<!ELEMENT SplashScreenMessage EMPTY >
<!ATTLIST SplashScreenMessage
    enabled (YES|NO) "NO"
    message CDATA #REQUIRED
>
<!ELEMENT APLocations (Site+)>
<!ELEMENT RMConfiguration (RadioMonitoring?, SelfHealing?, AutoReSiteSurvey?,
RogueAPDetection?, AdHocNetworkDetection?, UnregisteredClientMonitoring?, RMJobList?,
InitialRMSetup?)>
<!ELEMENT FloorSelection EMPTY>
<!ATTLIST FloorSelection
    siteName CDATA #REQUIRED
    buildingName CDATA #REQUIRED
    floorName CDATA #REQUIRED
>
<!ELEMENT ARSSFloorSelection EMPTY>
<!ATTLIST ARSSFloorSelection
    siteName CDATA #REQUIRED
    buildingName CDATA #REQUIRED
    floorName CDATA #REQUIRED
    select11a NMTOKEN "false"
    select11b11g NMTOKEN "false"
```

```
>
<!ELEMENT DeviceSelection EMPTY>
<!ATTLIST DeviceSelection
    identifier CDATA #REQUIRED
    identifierType (NAME | DESCRIPTION | IP_ADDRESS | MAC_ADDRESS) #IMPLIED
>
<!ELEMENT DeviceSelectionList (DeviceSelection*)>
<!ATTLIST DeviceSelectionList
    includeAllAccessPoints NMTOKEN "false"
>
<!ELEMENT RadioInterfaceSelection EMPTY>
<!ATTLIST RadioInterfaceSelection
    select11a NMTOKEN "true"
    select11b11g NMTOKEN "true"
>
<!ELEMENT RMJob (RadioScan | ClientWalkAbout | RadioParameterGeneration)>
<!ATTLIST RMJob
    name CDATA #REQUIRED
    description CDATA #IMPLIED
    startDate CDATA #IMPLIED
    startTime CDATA #IMPLIED
    repeatIntervalInMinutes NMTOKEN #IMPLIED
>
<!ELEMENT RadioScan (DeviceSelectionList?, RadioInterfaceSelection?)>
<!ATTLIST RadioScan
    maximumTransmitPower NMTOKEN #IMPLIED
>
<!ELEMENT ClientWalkAbout (DeviceSelectionList?, RadioInterfaceSelection?,
ClientMACAddressSelection)>
<!ATTLIST ClientWalkAbout
    useAPMaximumPowerSetting NMTOKEN "true"
    maximumTransmitPower NMTOKEN #IMPLIED
>
<!ELEMENT RadioParameterGeneration (DeviceSelectionList?)>
<!ATTLIST RadioParameterGeneration
    radioInterfaceType (11a | 11bg) #REQUIRED
    channelSet CDATA #IMPLIED
    minimumTransmitPower NMTOKEN #IMPLIED
    maximumTransmitPower NMTOKEN #IMPLIED
    ignoreRogueAccessPoints NMTOKEN "false"
    enableBlackHoleMitigation NMTOKEN "true"
    writeToNVRAMOnApply NMTOKEN "true"
>

<!ELEMENT ClientMACAddressSelection EMPTY>
<!ATTLIST ClientMACAddressSelection
    macAddress1 CDATA #REQUIRED
    macAddress2 CDATA #IMPLIED
    macAddress3 CDATA #IMPLIED
    macAddress4 CDATA #IMPLIED
    macAddress5 CDATA #IMPLIED
>
<!ELEMENT Site (Building+)>
<!ATTLIST Site
    name CDATA #REQUIRED
>
<!ELEMENT RadioMonitoring (ServingChannelMonitoring?, NonServingChannelMonitoring?,
RadioInterfaceSelection?, DeviceSelectionList?)>
<!ATTLIST RadioMonitoring
    enabled (YES | NO) "YES"
    enabledForNewAccessPoints (YES | NO) "YES"
>
<!ELEMENT SelfHealing (FloorSelectionList?)>
<!ATTLIST SelfHealing
    enabled (YES | NO) "NO"
    faultPriority (P1 | P2 | P3 | P4 | P5) "P2"
    changeNeighborAPs NMTOKEN "true"
    minimumTimeToWait NMTOKEN #IMPLIED
>
<!ELEMENT AutoReSiteSurvey (ARSSFloorSelectionList?)>
<!ATTLIST AutoReSiteSurvey
    enabled (YES | NO) "NO"
    faultPriority (P1 | P2 | P3 | P4 | P5) "P1"
    threshold NMTOKEN "20"
>
<!ELEMENT RogueAPDetection (SwitchPortSuppression?)>
<!ATTLIST RogueAPDetection
    enabled (YES | NO) "YES"
    faultPriority (P1 | P2 | P3 | P4 | P5) "P1"
    rssiThreshold NMTOKEN "-95"
>
<!ELEMENT AdHocNetworkDetection EMPTY>
<!ATTLIST AdHocNetworkDetection
    enabled (YES | NO) "YES"
    faultPriority (P1 | P2 | P3 | P4 | P5) "P2"
>
<!ELEMENT UnregisteredClientMonitoring EMPTY>
<!ATTLIST UnregisteredClientMonitoring
    enabled (YES | NO) "YES"
    faultPriority (P1 | P2 | P3 | P4 | P5) "P2"
    requestCountThreshold (100 | 200 | 300 | 400 | 500) "100"
>
<!ELEMENT RMJobList (RMJob+)>
<!ELEMENT InitialRMSetup (RadioScan, (RadioParameterGeneration, RadioParameterGeneration,
RadioParameterGeneration?))>
<!ELEMENT Building (Floor+)>
```

```
<!ATTLIST Building
    name CDATA #REQUIRED
    contact CDATA #IMPLIED
    address CDATA #IMPLIED
>
<!ELEMENT Floor (Device+)>
<!ATTLIST Floor
    name CDATA #REQUIRED
    width NMTOKEN #REQUIRED
    length NMTOKEN #REQUIRED
    metric (FEET | METERS) "FEET"
    imageURL CDATA #IMPLIED
>
<!ELEMENT Device ((Antenna, Antenna, Antenna?, Antenna?))>
<!ATTLIST Device
    identifier CDATA #REQUIRED
    identifierType (NAME | DESCRIPTION | IP_ADDRESS | MAC_ADDRESS) "NAME"
    x NMTOKEN #REQUIRED
    y NMTOKEN #REQUIRED
    z NMTOKEN #IMPLIED
>
<!ELEMENT Antenna EMPTY>
<!ATTLIST Antenna
    radioInterfaceType (2.4GHZ | 5GHZ) #REQUIRED
    type (AJAX-2.4GHZ | AJAX-5GHZ | AIR-ANT1728 | AIR-ANT1729 | AIR-ANT2012 |
AIR-ANT2410Y-R | AIR-ANT3351 | AIR-ANT3549 | AIR-ANT4941 | AIR-ANT570-R | AIR-ANT5959 |
AP1100 | BR1310 | KODIAK-DIRECTIONAL | KODIAK-OMNI | OSPREY-DIRECTIONAL | OSPREY-OMNI |
Unspecified-2.4GHz | Unspecified-5GHz) #REQUIRED
    azimuth NMTOKEN #REQUIRED
    downtilt NMTOKEN #REQUIRED
    height NMTOKEN #IMPLIED
    cableLoss NMTOKEN #IMPLIED
>
<!ELEMENT ServingChannelMonitoring EMPTY>
<!ATTLIST ServingChannelMonitoring
    enableForAccessPoints (YES | NO) "NO"
    enableForClients (YES | NO) "NO"
>
<!ELEMENT NonServingChannelMonitoring EMPTY>
<!ATTLIST NonServingChannelMonitoring
    enableForAccessPoints (YES | NO) "NO"
    enableForClients (YES | NO) "NO"
>
<!ELEMENT FloorSelectionList (FloorSelection*)>
<!ATTLIST FloorSelectionList
    includeAllFloors NMTOKEN "false"
>
<!ELEMENT ARSSFloorSelectionList (ARSSFloorSelection*)>
```

```
<!ATTLIST ARSSFloorSelectionList
    includeAllFloors NMTOKEN "false"
>
<!ELEMENT SwitchPortSuppression EMPTY>
<!ATTLIST SwitchPortSuppression
    enabled (YES | NO) "NO"
    cdpHopCount NMTOKEN "1"
    skipGigabitEthernetPort NMTOKEN "false"
    skipManagedAPPort NMTOKEN "false"
    skipPortChannelingPort NMTOKEN "false"
    skipPortGroupingPort NMTOKEN "false"
    skipNonAccessPointCDPNeighbor NMTOKEN "false"
>
```

Example .xml File

An example .xml file follows.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE StartupConfig SYSTEM "startup.dtd">

<StartupConfig>

<Faults>
      <NotificationSettings format="PlainText">
      <SyslogNotification host="sysloghost"/>
      <EmailNotification address="jim@cisco.com" priority="P2"/></Faults>

<DeviceCredentials>

      <SNMPCredentials retries="1" timeoutSeconds="9" readCommunity="public"
             writeCommunity="public">
            <IPAddressRange>*.*.*.*</IPAddressRange>
      </SNMPCredentials>

      <HTTPCredentials user="httpuser" password="httppassword">
            <IPAddressRange>10.223.3.[4-8]</IPAddressRange>
      </HTTPCredentials>
      <HTTPCredentials user="httpuser9" password="httppassword9">
            <IPAddressRange>10.2.3.[9-11]</IPAddressRange>
      </HTTPCredentials>
      <HTTPCredentials user="httpuserold" password="httppassword">
            <IPAddressRange>10.2.3.[200-220]</IPAddressRange>
      </HTTPCredentials>

      <HTTPPort port="898">
            <IPAddressRange>10.*.[11-55].*</IPAddressRange>
      </HTTPPort>

      <CLICredentials enablePassword="enablepP" user="cliP" password="userpP"
                 enableUser="enable">
            <IPAddressRange>*.*.*.*</IPAddressRange>
      </CLICredentials>
      <CLICredentials enablePassword="enableP" user="cli1O" password="userpK"
                 enableUser="enable1">
            <IPAddressRange>172.16.[7-11].*</IPAddressRange>
      </CLICredentials>

      <WLCCPCredentials user="WLCCPUSER" password="WLCCPPASSWORD"/>
</DeviceCredentials>

<Discovery displayNameFormat="%dns%(%ip%)" reverseDNSLookup="YES" autoManage="NO">
        <Schedule enabled="YES" repeatIntervalInMinutes="120"/>
        <CDPDiscovery cdpDistance="1">
            <CDPSeed ipAddress="172.20.11.101"/>
            <CDPSeed ipAddress="172.20.13.102"/>
            <CDPSeed ipAddress="172.20.13.103"/>
        </CDPDiscovery>
</Discovery>

<Inventory>

        <FullInventory>
            <Schedule enabled="YES" repeatIntervalInMinutes="720"/>
        </FullInventory>

        <ClientInventory>
            <Schedule enabled="YES" repeatIntervalInMinutes="51"/>
        </ClientInventory>

        <PerformanceInventory>
            <Schedule enabled="YES" repeatIntervalInMinutes="13"/>
        </PerformanceInventory>

        <APRebootDetection>
            <Schedule enabled="NO" repeatIntervalInMinutes="0"/>
        </APRebootDetection>

        <AggregationSettings daysToKeepMonthlyData="360" daysToKeepWeeklyData="180"
                 daysToKeepDailyData="30" daysToKeepHourlyData="7"/>
</Inventory>

<SystemSettings daysToKeepJobHistoryData="15" daysToKeepFaultHistoryData="45"/>

<AAAServerMonitoring>
```

```
        <AAAServerInfo secret="leapsecret" user="leap" port="0" password="leappassword"
               hostNameOrIP="10.2.2.2" protocol="LEAP"/>
        <AAAServerInfo secret="777S" user="777" port="0" password="777P"
               hostNameOrIP="10.7.7.7" protocol="LEAP"/>
        <AAAServerInfo secret="peapsecret" user="peap" port="0" password="peappassword"
               hostNameOrIP="10.3.3.3" protocol="PEAP"/>
        <AAAServerInfo secret="secret" user="user" port="0" password="password"
               hostNameOrIP="10.2.3.4" protocol="EAPMD5"/>
        <AAAServerInfo secret="radiussecret" user="radius" port="0"
               password="radisupassword" hostNameOrIP="10.4.4.4" protocol="RADIUS"/>
</AAAServerMonitoring>

<ClientTrackingSettings enabled="NO"/>

<ConfigurationSettings>

      <ConfigTemplate name="startup-ios" description="This is a startup template">
            <IOS>cdp run</IOS>
      </ConfigTemplate>

      <ConfigTemplate name="custom" description="this is custom template">
         <IOS>line 0 16no access-class 111 interminal-type teletypewidth 80length 40</IOS>
      </ConfigTemplate>

      <StartupTemplate name="iostartup.cfg" description="Startup file for ios APs"
                configTemplateName="startup-ios" writeToNVRAM="NO"/>
      <StartupTemplate name="forthd" description="" configTemplateName="bldg1-ap1200"
                writeToNVRAM="NO"/>

      <AutoTemplate enabled="YES" name="custom" description="MAC Address Serial Number"
                configTemplateName="ios1" writeToNVRAM="NO">
            <DeviceMACRule>
                <DeviceMAC>111213141516</DeviceMAC>
                <DeviceMAC>111213141517</DeviceMAC>
            </DeviceMACRule>
            <DeviceSerialNumberRule>
                <DeviceSerialNumber>abcdef34343</DeviceSerialNumber>
                <DeviceSerialNumber>abcdef34346</DeviceSerialNumber>
       </AutoTemplate>

      <AutoTemplate enabled="NO" name="auto4" description="Various"
                     configTemplateName="startup-ios" writeToNVRAM="YES">
            <DeviceTypeRule>
                <DeviceType>AP 350</DeviceType>
                <DeviceType>BR 1310</DeviceType>
            </DeviceTypeRule>
            <DeviceSubnetRule>
                <DeviceSubnet>192.168.98.0</DeviceSubnet>
                <DeviceSubnet>172.20.110.64</DeviceSubnet>
            </DeviceSubnetRule>
            <DeviceVersionRule>
                <DeviceVersion>12.02T1</DeviceVersion>
                <DeviceVersion>12.2(13)JA1</DeviceVersion>
            </DeviceVersionRule>
       </AutoTemplate>

       <AutoTemplateOptions>
            <SendEmailList enabled="YES">arora@abc.com, viking@thor.net</SendEmailList>
       </AutoTemplateOptions>
</ConfigurationSettings>


<Redundancy secondsBetweenCheck="16" adminPassword="admin" httpPort="1741" enabled="YES"
    primaryIP="192.168.98.107" notificationEmail="yushu@cisco.com"
    virtualIPeth0="192.168.98.109" minutesBetweenSync="15" secondaryIP="192.168.98.108" />

<Appliance>
    <SplashScreenMessage enabled="YES">Welcome to WLSE Express</SplashScreenMessage>
</Appliance>

<Users>
    <User isEncrypted="YES" email="admin@abc.com"
           password="$1$d3niWPWT$DVQKhU40t09s2qRqhACf21" name="admin" creator="admin"
           cliAccess="15">
    <Role name="System Admin" />
    </User>

    <User isEncrypted="YES" email="kim@jungle.com"
           password="$1$Gg9oWPWT$hyC5V99JbIOUpgW/Tk9uI1" name="kim" creator="admin"
           cliAccess="0" />
    <Role name="Help Desk" />

    <User isEncrypted="YES" email="hedwig@hogwarts.com"
           password="$1$eNfyAFGH$mTPJ10ervL3Z/9jhHU.hf." name="hedwig" creator="admin"
           cliAccess="None">
    <Role name="familiar"/>
    </User>
</Users>

<CLIBlock>
    <CLI>http-server port 1741</CLI>
    <CLI>hostname thishostname</CLI>
    <CLI>mailroute mailer.abc.com</CLI>
    <CLI>snmp-server location london</CLI>
    <CLI>snmp-server contact snape</CLI>
    <CLI>import host wlseexpress 198.71.131.209</CLI>
```

```
</CLIBlock>

</StartupConfig>
```

Tags and Attributes in the .xml File

This section provides information about all of the tags that are permitted in a configuration .xml file. See the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.11* for details on these parameters.

Use this information along with the example .xml file and DTD file.

Table A-1 Configuration File Tags

Tag	Attributes	Description and UI Reference	
StartupConfig		Container for configuration parameters	
Faults		Container for fault notification settings	
NotificationSettings	format	Message format: plainText or XML	**Faults > Notification Settings**
TrapNotification	host	SNMP trap receiver	
	port	Port on trap receiver	
	community	Community string	
SyslogNotification	host	Syslog server(s)	
EmailNotification	address	User(s) receiving fault notifications	
	priority	Priority of faults to be mailed	

Table A-1 Configuration File Tags (continued)

Tag	Attributes	Description and UI Reference	
Discovery		Container for discovery settings	
Discovery (Schedule)	enabled	Enable/disable repeat discoveries	**Devices > Discover > Discovery Wizard**
	repeatInvervalInMinutes	Repeat interval for scheduled discoveries	
CDPDiscovery	cdpDistance	CDP distance	
CDPSeed	ipAddress	Address of discovery seed device	
DeviceCredentials		Container for credentials	
SNMPCredentials (IPAddressRange	(IP address)	IP addresses of devices using this community	**Devices > Discover > Device Credentials > SNMP Communities**
SNMPCredentials	readCommunity	Read-only community	
	writeCommunity	Read/write community	
	timeoutSeconds	SNMP timeout	
HTTPCredentials (IPAddressRange)	(IP address or range)	IP addresses of devices using this user and password.	For configuring non-IOS APs **Devices > Discover > Device Credentials > HTTP User/Password**
HTTPCredentials	user	Username	
	password	User password	
HTTPPort (IPAddressRange)	(IP address or range)	IP address of devices using this port	**Devices > Discover > Device Credentials > IOS HTTP Port Settings**
HTTPPort	port	Port for links to IOS APs from reports	

Table A-1 Configuration File Tags (continued)

Tag	Attributes	Description and UI Reference	
DeviceCredentials (continued)		Container for credentials	
CLICredentials (IPAddressRange)	(IP address or range)	IP addresses of devices with these credentials	Credentials for uploading configuration and firmware to IOS APs **Devices > Discover > Device Credentials > Telnet/SSH User/Password**
CLICredentials	user	Telnet/SSH username	
	password	Telnet/SSH password	
	enableUser	Telnet/SSH enable username	
	enablePassword	Telnet/SSH enable password	
WLCCPCredentials	user	RADIUS username for WDS	**Devices > Discover > Device Credentials > WLCCP Credentials**
	password	RADIUS password	
Inventory		Container for inventory settings	
FullInventory (Schedule)	enabled	Enable/disable repeat polling	**Devices > Inventory > Polling**
	repeatIntervalInMinutes	Polling interval	
ClientInventory (Schedule)	enabled	Enable/disable repeat polling	**Devices > Inventory > Polling**
	repeatIntervalInMinutes	Polling interval	
PerformanceInventory (Schedule)	enabled	Enable/disable repeat polling	**Devices > Inventory > Polling**
	repeatIntervalInMinutes	Polling interval	
APRebootDetection	repeatIntervalInMinutes	Polling interval for AP reboot detection	Not in the UI

Table A-1 Configuration File Tags (continued)

Tag	Attributes	Description and UI Reference	
Inventory (continued)		Container for inventory settings	
AggregationSettings	daysToKeepHourlyData	How long to keep data for reports	**Devices > Inventory > Polling**
	daysToKeepDailyData		
	daysToKeepWeeklyData		
	daysToKeepMonthlyData		
SystemSettings	daysToKeepJobHistoryData	How long to keep job and fault history	**Devices > Inventory > Polling**
	daysToKeepFaultHistoryData		
AAAServerMonitoring		Container for AAA server monitoring	
AAAServerInfo	hostNameOrIP	AAA server	AAA servers to be monitored by the WLSE **Devices > Discover > AAA Server-**
	port	Port used for authentication	
	protocol	Authentication protocol	
	user	Client username	
	password	Client password	
	secret	Shared secret	
ClientTracking Settings	enabled	Enable/disable advanced client tracking for all WDS devices	**Devices > Discover > Client Tracking**
ConfigurationSettings		Container for AP configuration	
ConfigTemplate	name	Template name	**Configure > Templates**
	description	Template description	
ConfigTemplate (IOS)	IOS commands	Custom commands in the template	

Table A-1 Configuration File Tags (continued)

Tag	Attributes	Description and UI Reference	
ConfigurationSettings (continued)		Container for AP configuration	
Startup Template	name	Name of bootfile associated with the startup template	Configuration template for newly installed APs **Configuration > Templates > Auto Update > Startup Configuration**
	configTemplateName	Name of template	
	description	Description of template	
	writeToNVRAM	Whether to write configuration to NVRAM	
AutoTemplate		Container for assigning templates for auto-managed configuration	
AutoTemplate	name	Name of auto-managed configuration	**Configure > Templates > Auto-Update > Auto-Managed Configuration > Assign Templates**
	configTemplateName	Name of template	
	description	Description of template	
	enabled	Enable/disable application of template to matching devices	
	writeToNVRAM	Write configuration to NVRAM	

Table A-1 Configuration File Tags (continued)

Tag	Attributes	Description and UI Reference	
AutoTemplate (continued)		Container for assigning templates for auto-managed configuration	
DeviceMACRule (DeviceMAC)	Container for MAC addresses	Matching rules for apply templates to auto-managed APs	**Configure > Templates > Auto-Update > Auto-Managed Configuration > Assign Templates**
DeviceTypeRule (DeviceType)	Container for device types		
DeviceSubnetRule (DeviceSubnet)	Container for subnets		
DeviceVersionRule (Device Version)	Container for firmware version		
DeviceSerialNumberRule (DeviceSerialNumber)	Container for serial number		
AutoTemplateOptions		Container for auto-managed configuration options	
	IOSProtocol	Use SSH or Telnet	Not in the UI
SendEmailList	enabled	Enable/disable email on results of auto-configuration	**Configure > Templates > Auto-Update > Auto-Managed Configuration > Auto-Managed Options**

Table A-1 Configuration File Tags (continued)

Tag	Attributes	Description and UI Reference	
Redundancy	enabled	Enable/disable redundancy	Settings for redundant WLSEs **Administration > Appliance > Redundancy**
	httpPort	HTTP port on both systems	
	adminPassword	Admin password on both systems	
	notificationEmail	Address for notifications	
	virtualIPeth0	Virtual IP address of ethernet port	
	primaryIP	Static IP address of primary system	
	secondaryIP	Static IP address of secondary system	
	minutesBetweenSync	Synchronization interval	
	secondsBetweenCheck	How often standby checks status of primary system	
Appliance		Container for **Administration > Appliance** settings	
SplashScreenMessage	enabled	Enable/disable logon message	**Administration > Appliance > Splash Screen**

Table A-1 Configuration File Tags (continued)

Tag	Attributes	Description and UI Reference	
Users		Container for users	
User (Role)	name	Name(s) of role(s) assigned to user	User accounts on WLSE **Administration > User Admin > Manage Users**
User	name	Username	
	password	Password	
	cliAccess	CLI access privileges	
	creator	User who created this account	
	email	Email address of user	
CLIBlock		Container for WLSE CLI commands	
CLIBlock(CLI)	(WLSE CLI commands)	Any CLI command for setting appliance parameters. You can use this section to set parameters that cannot be saved in the configuration files from the UI.	

APPENDIX B

Technical Specifications

Table B-1 provides the specifications for the CiscoWorks Wireless LAN Solution Engine Express.

Table B-1 Technical Specifications

Component	Specifications
Serial ports	One 9-pin serial/console connector
RJ-45 port	One RJ-45 connector for connection to integrated 10/100 Ethernet controller
USB ports	Two USB connectors
Keyboard/mouse	One PS2 keyboard connector and one mouse connector
Parallel port	One parallel port
AC power supply wattage	60W
AC power supply voltage	100 - 240 VAC, 50/60 Hz
System battery	CR2032, 3V Lithium
Height	6.5 cm (2.56 inches)
Width	21 cm (8.27 inches)
Depth	25.8 cm (10.16 inches)
Weight	2.49 kg (5.49 pounds)
Operating temperature	10° to 40°C (50° to 104°F)
Storage temperature	-40° to 65°C (-40° to 149°F)

Table B-1 Technical Specifications (continued)

Component	**Specifications**
Operating relative humidity	90% non-condensing relative humidity at 40°C
Storage relative humidity	90% non-condensing relative humidity at 60°C
Operating maximum vibration	1.146g (peak swept sine) at a sweep of 5 to 200 Hz RMS random vibration
Storage maximum vibration	0.5 g (peak swept sine) at 5 to 200 Hz
Operating maximum shock	31 g (half sine), 2 ms, bottom side only
Storage (non-operational) maximum shock	71 g (half sine), 2 ms, for all six sides
Operating altitude	0 - 2000m
Storage altitude	No constraints

INDEX

A

AAA server, internal
  monitoring 5-4
  setting up 5-4
AAA servers
  adding to WLSE 4-15
  for WDS authentication 4-6
AAA servers, external
  monitoring 5-4
  setting up 5-4
access point, configuring for management 5-1
AC power, connecting to 2-12
admin user
  default password 3-16
audience for this document xv
auto-configuration 3-12

B

back panel features 1-4
  Ethernet connector 1-6
  serial port 1-5
bridge, configuring for management 5-3
browser
  configuring 3-10
  supported browsers 3-10

C

cabling
  connecting a console 2-12
  considerations 2-7
  Ethernet connector 1-7
  network cable requirements 1-7
cautions
  power supply 1-5
  significance of xvi
CDP, running 4-8
Cisco Access Registrar (CAR) 5-4
Cisco Discovery Protocol (CDP)
  alternatives to
    all devices as seeds 4-8
    device import 4-11
  using for discovery 4-8
CiscoSecure ACS Server, configuring 5-4
CiscoWorks server, importing devices from 4-12
community strings
  adding to WLSE 4-3

configuration
  default 3-1
configuration, WLSE
  configuration file
    .dat file, data saved in 3-22
    .xml file
      data saved in 3-22
      example A-13
      tags and attributes A-17
    creating 3-18
    DTD file A-2
    tags and attributes in A-17
    uploading 3-22
    using 3-25
  customizing 3-27
  defaults 3-15
  erasing 3-2
  manual configuration 3-17
  reapplying configuration file 3-26
  reference WLSE 3-15
  site-specific file 3-23
  verifying 3-25
configuration file
  .xml file, example of A-13
  components of A-1
  creating 3-18
  downloading to WLSEs 3-25
  DTD file A-2
  reference information for A-1
  uploading to TFTP server 3-22
  using 3-25
configuring
  credentials
    on WLSE 4-2
  verifying the configuration 3-8
  WDS
    on WLSE 4-6
configuring devices for management 5-1
console port 1-5
creating a safe environment 2-6
credentials, on WLSE
  HTTP credentials for non-IOS access points 4-4
  HTTP port settings for IOS access points 4-6
  SNMP credentials for all managed devices 4-3
  Telnet/SSH credentials for IOS access points 4-5
  WLCCP credentials for Wireless Domain Services 4-6

D

Developer Guide xxiii
devices
  configuring 5-1
  credentials, adding to WLSE 4-2
  discovering 4-8
  discovery options 4-7
  importing 4-11

- managing **4-14**
- setting up **5-1**
- supported **xxii**

discovery
- CDP
  - configuring on WLSE **4-8**
- entering all devices as seeds **4-9**
- importing devices **4-11**
- options for **4-7**

DNS
- consequences of not using **3-7**

DNS, requirement for **3-14**

documentation **xxi**
- audience for this **xv**
- product **xxi**
- typographical conventions in **xvi**

E

EAP-MD5 server
- adding to WLSE **4-15**

Ethernet connector
- location of **1-4**
- network cable requirements **1-7**

F

factory defaults **3-1**

features **1-1**

front panel features **1-2**
- system buttons **1-4**
- system indicators **1-3**

I

importing devices **4-11**

indicators and buttons **1-3**

installation
- basic WLSE configuration **3-22**
- cables, connecting **2-12**
- configuring the WLSE **4-2**
  - verifying the configuration **3-8**
- installing WLSE in a rack **2-10**
- powering on WLSE **2-12**
- power source, connecting to **2-12**
- preparing for
  - creating a safe environment **2-6**
  - LAN options, precautions for **2-9**
  - modems, precautions for **2-9**
  - rack-mounting, precautions for **2-8**
  - safety **2-2**
  - site preparation **2-5**
  - telecommunications, precautions for **2-9**
  - tools and equipment required **2-9, 2-10**
- quick reference **2-10**
- rack mounting **2-10**

Internet Explorer, configuring **3-10**

L

LAN options, precautions for 2-9

LEAP server

- adding to WLSE 4-15

license agreement, supplemental xiii

logging in

- console 3-8, 3-25
- Telnet/SSH 3-8, 3-25
- Web interface 3-19

M

managing devices 4-14

modems, precautions for 2-9

Mozilla, configuring 3-12

O

overview of WLSE 1-1

P

PEAP server

- adding to WLSE 4-15

pop-up blocker software 3-12

powering on the WLSE 2-12

R

rack-mounting

- instructions for 2-10
- precautions for 2-8

radio management

- configuring WLSE for 4-6

RADIUS server

- adding to WLSE 4-15

recovery CD 1-7

reference WLSE, configuring 3-15

release notes xxii

router, configuring for management 5-3

S

safety 2-2

- electrostatic discharge 2-4
- environmental
  - creating save environment 2-6
- general precautions 2-2
- preventing EMI 2-4
- warnings and cautions 2-2
- with electricity 2-3

serial port 1-5

servers, AAA

- entering on WLSE 4-15

site preparation 2-5

- AC power 2-6

  cabling 2-7
  environmental 2-5
    choosing a site for installation 2-6
    grounding the system 2-6
specifications, WLSE Express B-1
superuser, WLSE 3-16
supplemental license agreement xiii
switch, configuring for management 5-3

T

technical specifications B-1
telecommunications, precautions for 2-9
Telnet/SSH
  credentials for IOS access points 4-5
  enabling Telnet on WLSE 3-9
  using to log in 3-3, 3-17
TFTP server, requirement for 3-15
Troubleshooting Guide xxii
turning on the WLSE 2-12
typographical conventions
  in this document xvi

U

User Guide xxii
users
  adding to WLSE 3-21
  admin user 3-16

W

warnings
  grounding 2-12
  grounding the system 2-6
  lightning 2-12
  plug and socket 2-7
  rack-mounting equipment 2-11
  regarding
    installation area 2-6
    rack-mounting equipment 2-8
    shock danger 1-6
  significance of xvi, 2-2
  translations of xvi
warranty ix
Web interface
  browsers, supported 3-10
  logging in 3-19
Wireless Domain Services (WDS)
  configuring WLSE for 4-6