CISCO SYSTEMS

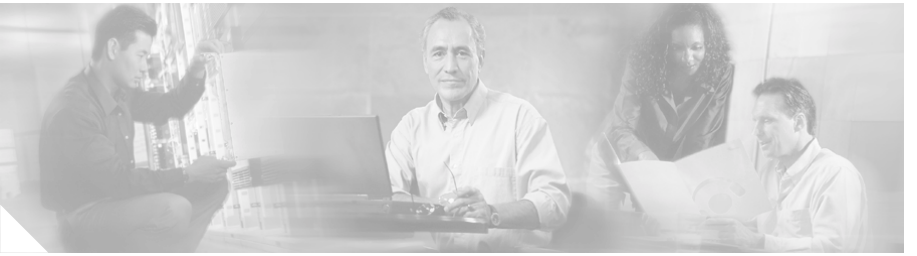
Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine

Software Release 2.5
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-7815903=
Text Part Number: 78-15903-01

Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine



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 warranty applicable to Cisco software, is included on the CD that accompanies your Cisco product. Follow these steps to access and download the *Cisco Information Packet* and your warranty document from the CD or 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 78-5235-02F0 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.

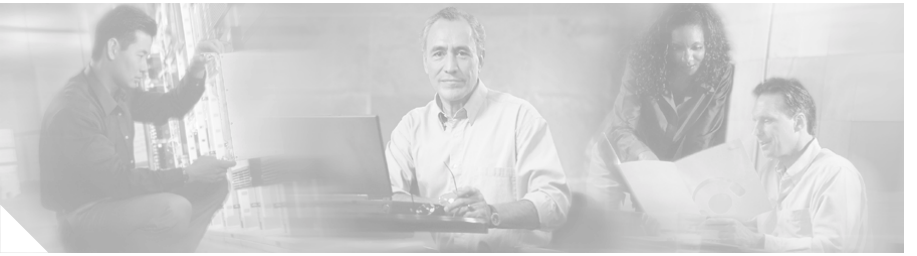
Cisco reserves the right to refund the purchase price as its exclusive warranty remedy.

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	



Preface

This guide describes how to install the CiscoWorks 1130 Wireless LAN Solution Engine (WLSE). It also describes configuration tasks for both CiscoWorks 1105 and CiscoWorks 1130 WLSEs and provides technical specifications for the CiscoWorks 1130 WLSE.

This guide consists of the following chapters and appendixes. Most of these sections apply to both the CiscoWorks 1105 and 1130; sections that apply to only the CiscoWorks 1130 are so titled.

Audience

This guide is intended primarily for system administrators who are responsible for installing and configuring internetworking equipment, and are familiar with Cisco IOS software.

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**

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.

Note The English warnings in this document are followed by a statement number. To see the translations of a warning into other languages, look up its statement number in the *Regulatory Compliance and Safety Information for the CiscoWorks 1130 Wireless LAN Solution Engine.*

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 documentation on Cisco.com for any updates.

On Cisco.com, WLSE documentation is located at **Products and Services > Network Management CiscoWorks > CiscoWorks Wireless LAN Solution Engine**.

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**.

The following product documentation is available for the WLSE:

Document Title	Description
Release Notes for the CiscoWorks Wireless LAN Solution Engine	Describes new features, documentation updates, known and resolved problems, information on obtaining documentation, and information on obtaining technical assistance. Available in the following formats: • On Cisco.com at Products and Services > Network Management CiscoWorks > CiscoWorks Wireless LAN Solution Engine > Technical Documentation. • PDF on the WLSE Recovery CD.
User Guide for the CiscoWorks Wireless LAN Solution Engine	Describes WLSE features and provides instructions for using it. Available in the following formats: • From the WLSE online help. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com at Products and Services > Network Management CiscoWorks > CiscoWorks Wireless LAN Solution Engine > Technical Documentation. • Printed document available by order.

Document Title	Description
Supported Device Table for the Wireless LAN Solution Engine	Lists devices supported at the time the product was released. Available on Cisco.com at Products and Services > Network Management CiscoWorks > CiscoWorks Wireless LAN Solution Engine > Technical Documentation.
Troubleshooting and FAQs for the CiscoWorks Wireless LAN Solution Engine	Contains troubleshooting hints WLSE and FAQs for the WLSE. Available on Cisco.com at Products and Services > Network Management CiscoWorks > CiscoWorks Wireless LAN Solution Engine > Alerts and Troubleshooting.
Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine	Describes how to install and configure the WLSE. Available in the following formats: • PDF on the WLSE Recovery CD-ROM. • On Cisco.com at Products and Services > Network Management CiscoWorks > CiscoWorks Wireless LAN Solution Engine > Technical Documentation. • Printed document available by order.
Regulatory Compliance and Safety Information for the CiscoWorks 1130 Wireless LAN Solution Engine	Provides regulatory compliance and safety information for the WLSE. Available in the following formats: • Printed document shipped with the WLSE. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com at Products and Services > Network Management CiscoWorks > CiscoWorks Wireless LAN Solution Engine > Product Literature.
Integrating Cisco Applications with CiscoWorks Management Connection	Provides information about adding a link to the WLSE from a CiscoWorks server's navigation tree. On Cisco.com at Products and Services > Network Management CiscoWorks > CiscoWorks Wireless LAN Solution Engine > Technical Documentation.
Programmer's Guide	Provides information about using the Software Developer's Kit (SDK). On Cisco.com at Products and Services > Network Management CiscoWorks > CiscoWorks Wireless LAN Solution Engine > Software Center.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

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

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

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

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

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_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 Networking Products MarketPlace:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

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

You can send your comments in e-mail to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco TAC Website

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

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

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

Opening a TAC Case

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

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

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

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

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

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

TAC Case Priority Definitions

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

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

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

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

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

  http://www.ciscopress.com

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips,

configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

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

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

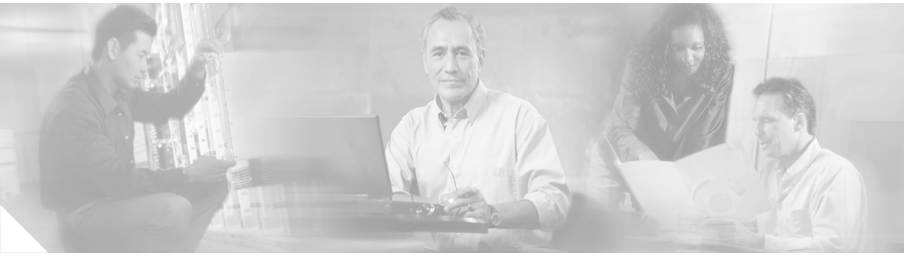
  http://www.cisco.com/go/iqmagazine

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

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

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

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



Supplemental License Agreement

SUPPLEMENTAL LICENSE AGREEMENT FOR CISCO SYSTEMS NETWORK MANAGEMENT SOFTWARE RUNNING ON THE CISCO 11XX 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 Software component of the Cisco 11XX Hardware Platform is preinstalled. CD's containing tools to restore this Software to the 11XX hardware are provided to Customer for reinstallation purposes only. Customer may only run the supported CiscoWorks Wireless LAN Solution Engine Software on the Cisco 11XX Hardware Platform designed for its use. No unsupported Software product or component may be installed on the Cisco 11XX Hardware Platform.

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

Cisco may provide CiscoWorks Wireless LAN Solution Engine Software updates and new version releases for the 11XX 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 11XX 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. Software License Agreement.

Product Overview

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

Note For translated safety warnings and regulatory compliance information, see the document titled *Regulatory Compliance and Safety Information for the CiscoWorks 1130 Wireless LAN Solution Engine.*

Software Features

The WLSE has the following major features:

- Configuration—Allows you to apply configuration changes to access points.
- 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.
- Radio management—Helps you manage your WLAN radio environment.

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

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
- 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 or the *User Guide for the Wireless LAN Solution Engine, Release 2.5*.

Hardware Features—CiscoWorks 1130 Wireless LAN Solution Engine

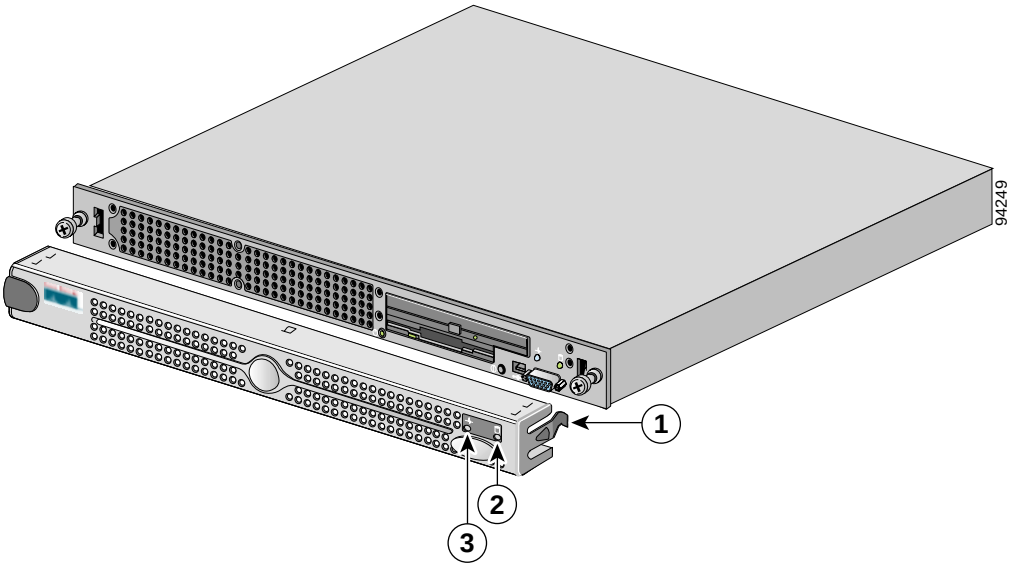
This section describes the WLSE 1130's bezel, front panel, and back panel.

Bezel Features

The bezel, shown in Figure 1-1, covers the front panel and has two Ethernet indicators, a system status indicator, and a hard drive indicator. For more information about the indicators, see Table 1-1.

To remove the bezel, press the tab on each end and lift it from the chassis.

Figure 1-1 Bezel Features



1	Bezel latches	**3**	Blue/amber status indicator
2	Hard drive indicator		

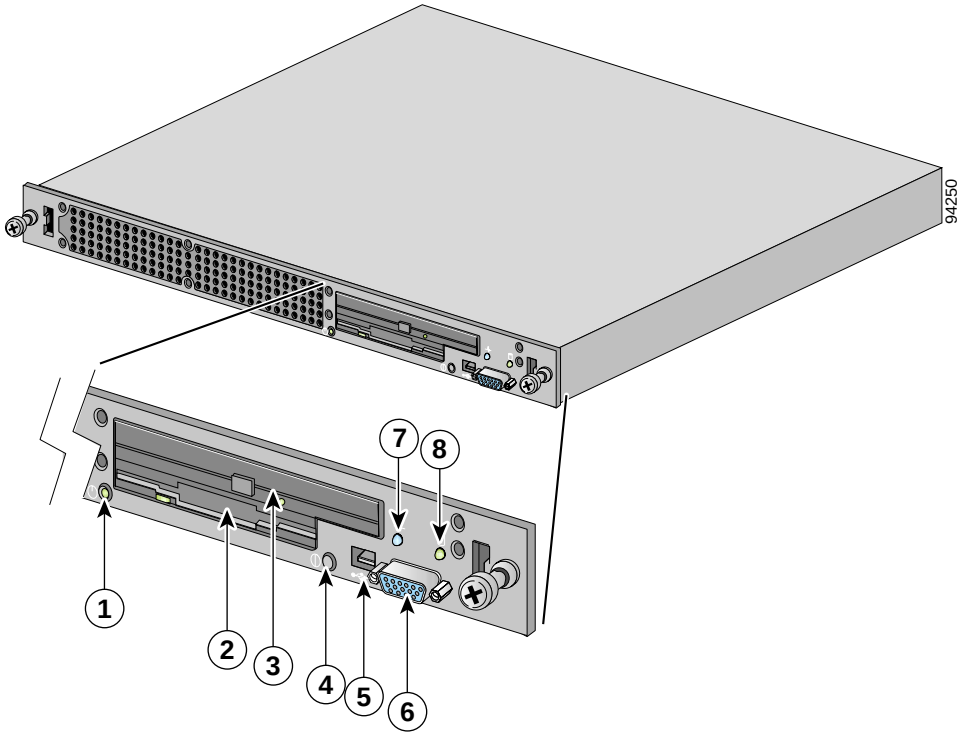
Front Panel Features

Figure 1-2 shows the front-panel features. Some features are not visible when the bezel is attached.

To access the front panel, remove the bezel by pressing the tabs on each end and lifting it from the chassis.

To reinstall the bezel, insert the tabs on each end into the flanges on each side of the chassis.

Figure 1-2 Front Panel Features



1	Power button/indicator	**5**	USB connector
2	Diskette drive	**6**	Video connector
3	CD drive	**7**	Blue/amber system status indicator
4	System identification button	**8**	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 or bezel (see Figure 1-1 and Figure 1-2). The appearance and function of these lights are described in Table 1-1.

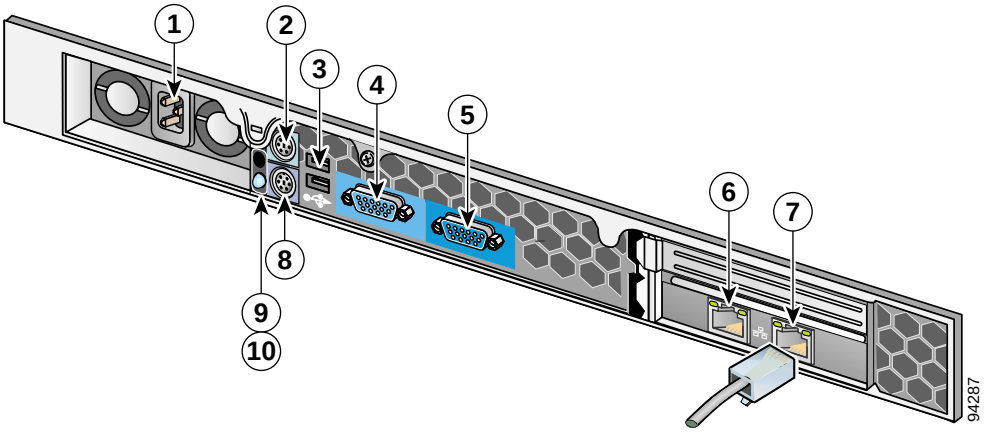
Table 1-1 Front-Panel System Indicators and Buttons

Indicator or Button	Color	Function
Power button and power indicator	Green	The power button controls power input to the power supply. The indicator in the center of the power button indicates whether the WLSE is powered on. If the indicator is flashing, AC power is connected to the WLSE, but the WLSE is not powered on. If the indicator is not on, AC power is not connected. The bezel contains a duplicate of the power indicator.
System identification button(s)	Blue	The system identification button on the front and back panels can be used to locate a particular system in the rack. When you push the system identification button, the blue indicators will flash. This button is not visible with the bezel attached.
System status indicator	Blue or amber	Lights up during normal system operation. If the indicator is amber flashing, the WLSE has a fault. This indicator is not visible with the bezel attached.
Hard drive indicator	Green	Flashes when the hard drives are in use. The bezel contains a duplicate of this indicator.

Back Panel Features

The back panel contains the AC power receptacle, keyboard connector, USB connectors, Ethernet connectors, serial port, video connector, mouse connector, system status indicator, and system identification button. Figure 1-3 shows the back-panel features. The functions of the system status indicator and system identification button are described in Table 1-1.

Figure 1-3 Back Panel Features



1	AC power receptacle	**6**	Ethernet 1 connector (labeled "B")
2	Keyboard connector	**7**	Ethernet 0 connector (labeled "A")
3	USB connectors (2)	**8**	Mouse connector
4	Serial connector	**9**	Blue/amber system status indicator
5	Video connector	**10**	System identification button

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 1-4 illustrates the pin numbers and Table 1-3 defines the pin assignments and interface signals.

Figure 1-4 Pin Numbers for the Serial Port Connector

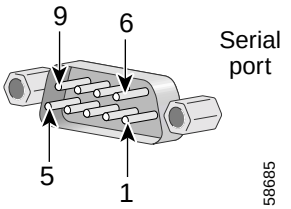


Table 1-3 Serial Port Pin Assignments

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 Connectors

The WLSE has integrated 10/100/1000–megabit-per-second (Mbps) Ethernet connectors. Each Ethernet connector provides all the functions of a network expansion card and supports 10BASE-T, 100BASE-TX, and 1000BASE-T Ethernet standards. The Ethernet connectors are shown in Figure 1-3 on page 1-6.

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.**

Network Cable Requirements

The Ethernet connectors are 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:

- Wireless LAN Solution Engine
- Rack mounting kit
- 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*
  - *Finding Documentation for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*
  - *Regulatory Compliance and Safety Information for the CiscoWorks 1130 Wireless LAN Solution Engine*

Preparing to Install the CiscoWorks 1130 Wireless LAN Solution Engine

This chapter describes the safety instructions and site requirements for installing the CiscoWorks Wireless LAN Solution engine. The chapter contains the following sections:

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.

Note The English warnings in this document are followed by a statement number. To see the translations of a warning into other languages, look up its statement number in the *Regulatory Compliance and Safety Information for the CiscoWorks 1130 Wireless LAN Solution Engine.*

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 **Ha csatlakoztat vagy kihúz bármilyen csatlakozókábelt, elektromos ív jöhet létre, ha a kapcsoló vagy a hálózatban lévő bármely eszköz feszültség alatt van. Ha a készülék veszélyes helyre van telepítve, ez robbanást okozhat. Győződjön meg róla, hogy a kapcsoló nincs feszültség alatt, véletlenül nem kapcsolható be, és mielőtt továbblép, ellenőrizze, hogy a terület nem veszélyes-e.**

Предупреждение Не подключайте и не отключайте кабели к разъемам при поданном на переключатель или какое-либо другое устройство цепи напряжением питания, так как это может привести к возникновению электрической дуги. Это может привести к взрыву во взрывоопасной среде. Перед выполнением каких-либо действий убедитесь в том, что напряжение питания отключено и не может быть случайно включено, или в том, что окружающая среда не является взрывоопасной.

警告 当交换机或网上的任一设备的电源接通时不要在端口插拔电缆，因为这可能产生电弧。如果是在危险的地方安装，就会引发爆炸。应确保交换机已断电且不会意外接通电源，或确定该地区不存在危险，然后再安装。

警告 スイッチまたはネットワーク上の装置が通電状態のときは、ケーブルをポートへ接続したり、ポートから引き抜いたりしないでください。電気アークが発生することがあります。電気アークは、危険な場所での設置の際に爆発を引き起こすことがあります。電源がスイッチから切断されていて偶発的に電源が入らないこと、または作業場所が危険でないことを確認してから作業を進めてください。

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” in the Preface.
- 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.

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 2-8 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

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 1-8.

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.

Precautions for Rack-Mounting

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.
- Ensure that 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.

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

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 the CiscoWorks 1130 Wireless LAN Solution Engine

This chapter describes how to install the CiscoWorks 1130 Wireless LAN Solution Engine (WLSE). The chapter contains the following sections:

Installation Quick Reference

Table 3-1 provides a high-level overview of the installation process. After installation is complete, follow the directions in Chapter 4, “Configuring the CiscoWorks 1105 and 1130 WLSE.”

Table 3-1 Quick Reference

Task	References
Use the rack mount kit to place the WLSE in a rack.	Installing the Wireless LAN Solution Engine in a Rack, page 3-2
Connect to an AC power source.	Connecting the WLSE to the AC Power Source, page 3-9
Connect network and console cables.	Connecting Cables, page 3-9
Power on the WLSE.	Powering On the WLSE, page 3-10

Installing the CiscoWorks 1130 Wireless LAN Solution Engine

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.

Installing the Wireless LAN Solution Engine in a Rack

Before installing the WLSE in a rack, read Preparing Your Site for Installation, page 2-9 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 steps below 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 2-11 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

To install the WLSE in a rack, perform the following steps:

Step 1 In the rack-mounting kit, locate the adapters that best fit your rack. See Table 3-2 on page 3-4.

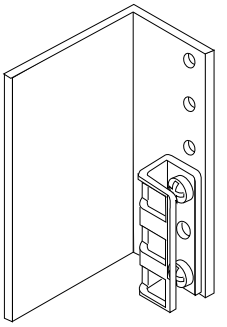
Note The rack-mounting instructions in this document are for a 4-post cabinet (recommended).

Table 3-2 Adapters for Rack Mounting

Rack Depth (inches)	Front Adapter Part Number	Rear Adapter Part Number(s)
22 5/8 to 23 1/2	059	270 and 350
23 1/2 to 24 1/4	059	200 and 350
24 1/4 to 25 1/8	059	200 and 270
25 1/8 to 25 3/8	290	270 and 350
25 3/8 to 26 1/4	059	350
26 1/4 to 27	059	270
27 to 27 3/4	200	200
27 3/4 to 28 1/2	200	270
28 1/2 to 29 1/4	290	270
29 1/4 to 30	270	200

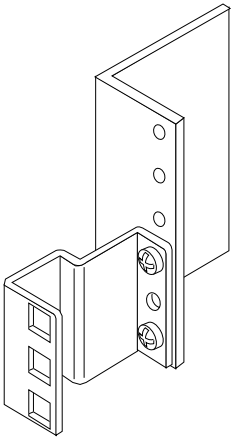
Note In the following illustrations, screws are shown for racks with threaded holes. If your rack has non-threaded holes, install the screw from the front of the rack, and use a nut on the inside against the adapter bracket.

Step 2 Attach the front adapters to the rails of the rack as shown in the following example.

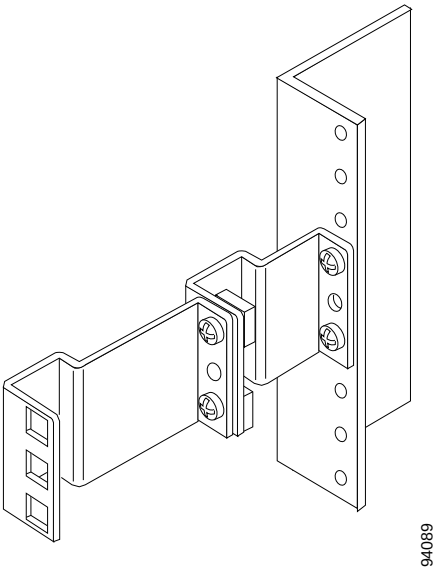


Step 3 Attach one or two rear adapters to the rails of the rack as shown in the following examples.

- Attach one adapter for racks with depths of 25 3/8 to 30 inches. See the following example.



- Attach two adapters for racks with depths of 24 1/4 to 25 3/8 inches. Make sure the longer bracket is at the rear. Attach the two brackets to each other by using two cage nuts and two screws. See the following example.



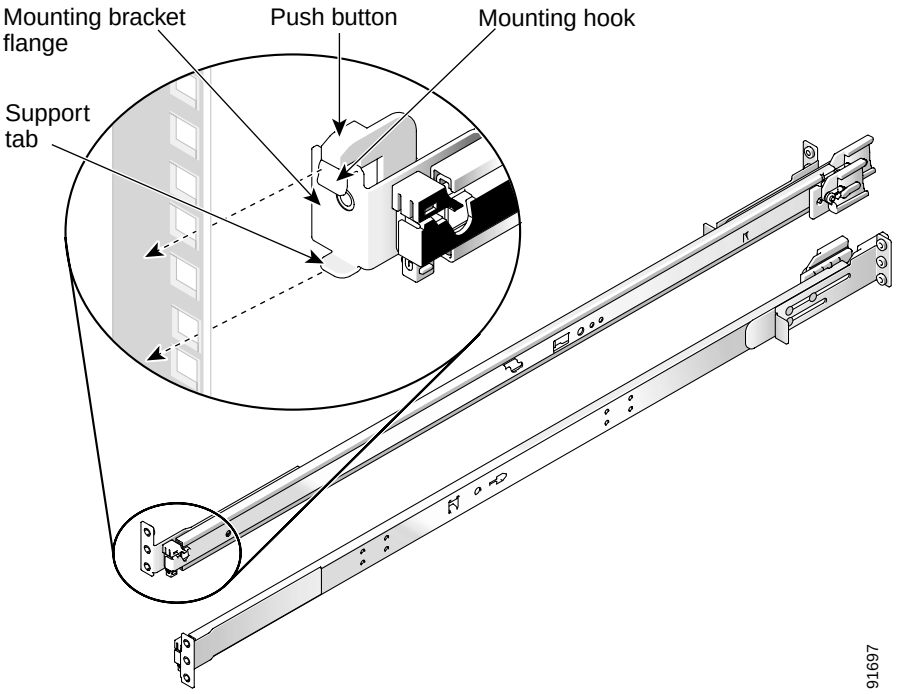
Step 4 Attach a slide assembly to the adapters on each side of the rack:

a. At the front of the cabinet, push the slide assembly forward until the mounting hook enters the square hole on the adapter.

b. Push down the mounting bracket flange until the mounting hook is seated in the square hole and the push button pops out and clicks.

c. At the back of the cabinet, pull back on the mounting flange until the mounting hook is in the square holes on the adapter.

d. Push down on the mounting bracket flange until the mounting hook is seated in the square hole and the push button pops out and clicks.



Step 5 Install the WLSE in the slide assembly.

a. Remove the front bezel.

b. Tilt the back of the WLSE down while aligning the back screws on its sides with the back slide assembly slots.

c. Engage the screws in the slide assembly slots.

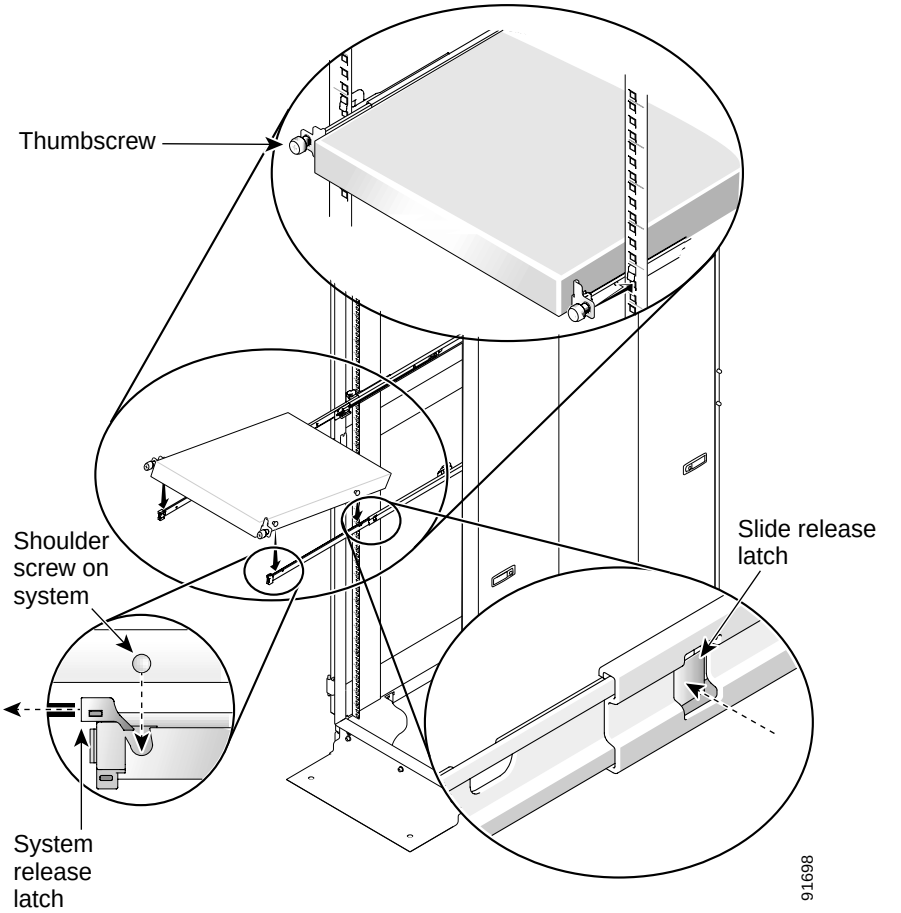
d. Lower the front of the WLSE and engage the front screws on its sides in the front slot behind the system release latch.

- The system release latch will move forward and then snap back.
- Use this latch when removing the WLSE from the slide assembly.

e. Press the slide release latch at the side of each slide to move the WLSE completely into the rack.

f. Push in and turn the thumbscrews on each side of the WLSE's front panel to secure it to the rack.

g. Reinstall the front bezel.



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

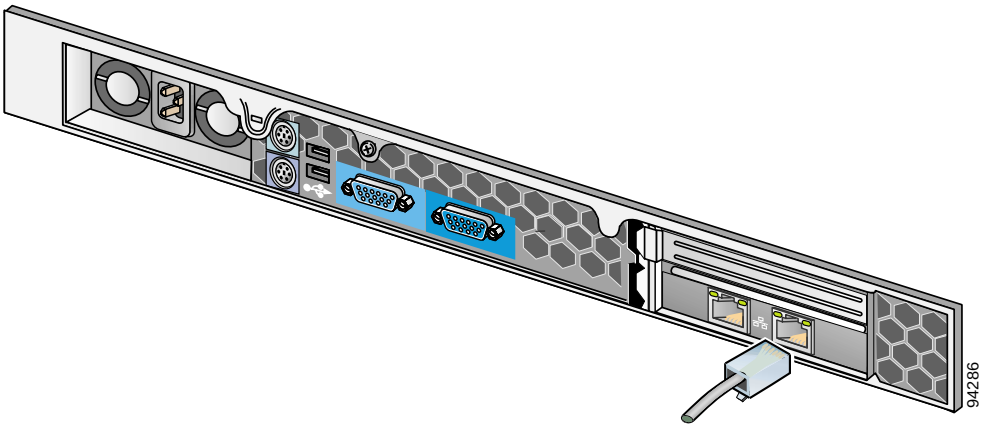
Connect the AC power receptacle to the AC power source with the provided power cable.

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.

Step 1 Plug the network connection into the Ethernet port labeled "A." This port corresponds to the Ethernet 0 interface.



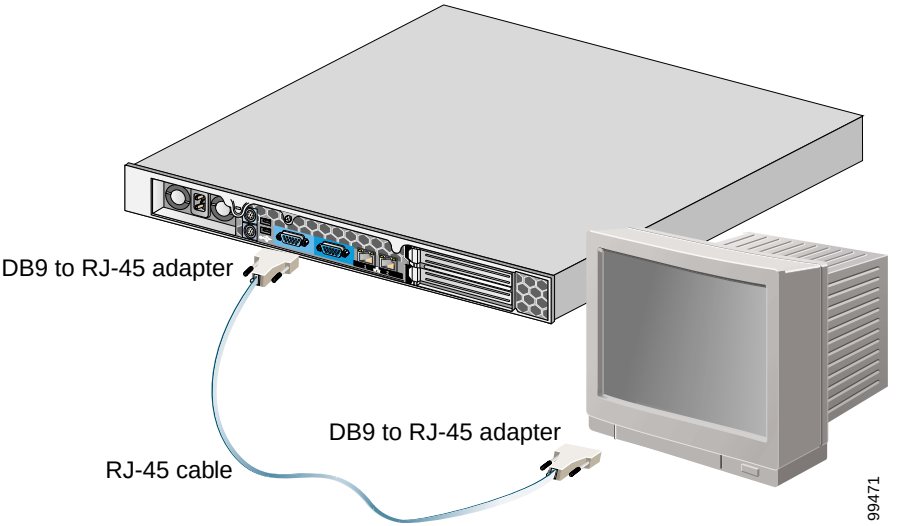
Step 2 Connect a console to the serial port:

a. Attach a DB-9 to RJ-45 adapter (provided) to the serial port of the console.

b. Attach a DB-9 to RJ-45 adapter (provided) to the serial port of the WLSE.

c. Connect the console to the WLSE using an RJ-45 cable (provided).

Note You will need the console to run the setup program. See Chapter 4, "Configuring the CiscoWorks 1105 and 1130 WLSE."



Powering On the WLSE

To turn the power on or off, press the power button on the front panel. When you turn the power off, after 30 seconds the WLSE will shut down gracefully.

The system begins booting and sending messages to the console window. When the login prompt appears, you can configure the system; see the instructions in Chapter 4, "Configuring the CiscoWorks 1105 and 1130 WLSE."

Next Steps—Configuration

Configure the WLSE and the devices to be managed. See Chapter 4, “Configuring the CiscoWorks 1105 and 1130 WLSE.”

Configuring the CiscoWorks 1105 and 1130 WLSE

This chapter describes how to configure the CiscoWorks 1105 and CiscoWorks 1130 WLSEs and how to set up devices for management.

Configuration Quick Reference

Table 4-1 provides a high-level overview of the initial configuration process. Detailed procedures are provided in this chapter. After configuration is complete, see the *User Guide for the Wireless LAN Solution Engine* or the WLSE online help for information on day-to-day operations.

Table 4-1 Quick Reference

Task	Steps	References
Configure the WLSE's network information.	1. Boot the WLSE and log in at the system console. 2. Run the setup program.	Configuring the WLSE's Network Information, page 4-3
Configure name resolution.	If you are not using a DNS server, remove the name server address from the configuration	Configuring Name Resolution, page 4-6
Verify the configuration.	While at the system console. verify configuration.	Verifying the Configuration, page 4-7

Table 4-1 Quick Reference (continued)

Task	Steps	References
Configure the Web browser on the client.	1. Verify that client system is using a supported browser. 2. Configure the browser.	Configuring the Web Browser, page 4-9
Log in and verify HTTP and HTTPS connectivity.	1. Log in to the Web interface. 2. Verify that you can connect to the WLSE via HTTP and HTTPS.	Logging into the Web Interface and Verifying Connectivity, page 4-13
Prepare devices and the WLSE for device management.	1. Set up devices. 2. Add device credentials to the WLSE (including credentials for Wireless Domain Services). 3. Add any AAA servers to be monitored. 4. Set options for discovery and management. 5. Discover or import devices. 6. Manage devices.	Setting Up Device Management, page 4-13
Add additional users.	Add Web interface users.	Adding Users, page 4-36

Configuring the WLSE's Network Information

Use the setup program to configure the WLSE when you boot it for the first time, and if you ever have to erase the configuration.

- 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 4-6.
- 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 4-2 on page 4-4 and Table 4-3 on page 4-5 for the data you will need to enter into the setup prompts.

Running the Setup Program

To configure WLSE network information, perform the following steps:

Step 1 Connect a console to the console port:

- For the WLSE 1105, use the serial port on the front panel; do not use the serial port on the back panel as a console port.
- For the WLSE 1130, the serial/console port is on the back panel.

  For more information about connecting a console to the WLSE 1130, see Connecting Cables, page 3-9.

Step 2 Power on the WLSE.

When the system finishes booting, a login prompt appears on the console.

Step 3 At the login prompt, enter **setup**.

When you boot the system for the first time, it is not configured. Logging in as **setup** allows you to configure the system.

Step 4 Enter responses to the first set of prompts to configure the WLSE's connectivity. Table 4-2 describes how to respond to the prompts. After each response, press **Enter** to proceed to the next prompt.

Table 4-2 General Configuration

Prompt	Response Description	Sample Response
`host name:`	System host name.	SolutionEngine
`domain name:`	System domain name.	cisco.com
`<username> password:`	Sets the password for the default user **admin**.	wq1Cvu2pl
`confirm password:`	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 use CLI commands.	wq1Cvu2pl
`eth0 IP address:`	IP address of Ethernet 0 interface.[1]	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 that connects WLSE to network.	209.165.200.224
`DNS server IP address:`	IP address of DNS server that WLSE uses for name/address resolution.The setup program does not validate the IP address you enter. If you are not using a DNS server, see the Configuring the WLSE Without a DNS Server, page 4-6 for instructions before proceeding.	209.165.201.1
`Would you like to save this configuration? [yes]:`	• Type **yes** to save the configuration. The configuration is saved and system reboots. • Type **no** to exit without saving configuration and run setup program again.	

1. Corresponds to the Ethernet port labeled "A" on the WLSE 1130.

Step 5 Answer the next set of prompts to create a self-signed certificate. This certificate will allow you to access the WLSE securely, using HTTPS, until you are able to obtain a certificate from a certificate authority (CA). Table 4-3 describes how to respond to the prompts. To make changes in the certificate after running setup, see Changing the Configuration After Running Setup, page 4-6.

Table 4-3 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`	Section of the company that is using the WLSE.	Webserver Team
`Common Name`	Fully qualified domain name (FQDN).	www.snakeoil.dom
`Email Address`	Email address.	www@snakeoil.dom

Step 6 After you finish configuring the Wireless LAN Solution Engine, it will reboot. After it finishes rebooting, 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 Wireless LAN Solution Engine, Release 2.5*.

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, 2.5*.

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 Wireless LAN Solution Engine, Release 2.5*.

You can use CLI commands by connecting to the WLSE through the console or by using Telnet or SSH. Log in initially as the admin user, using the password you created during setup.

- To change the host name, use the **hostname** command.
- To change the domain name, use the **ip-domain-name** command.
- To change the DNS server, or add up to 2 additional DNS servers, use the **ip name-server** command.
- To configure or reconfigure an Ethernet port, use the **interface** command.
- To make changes in the HTTPS certificate, use the **mkcert** command.

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.

Configuring Name Resolution

The WLSE resolves host names 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 Wireless LAN Solution Engine, Release 2.5*.

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

Configuring the WLSE Without a DNS Server

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

- Host names will not resolve.

- Discovery will be slow.
- Connecting to the WLSE 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 times out when attempting reverse DNS lookup.
- 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.

If you are not using a DNS server, perform the steps described in Configuring the WLSE's Network Information, page 4-3, with the following exception:

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 this command, see the *User Guide for the Wireless LAN Solution Engine, Release 2.5*.

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 Wireless LAN Solution Engine, Release 2.5*.

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 is disabled on the WLSE by default. If you want to connect to the CLI interface using Telnet, you can enable it by using the **telnetenable enable** CLI command.

- For the WLSE 1105, use the serial port on the front panel; do not use the serial port on the back panel as a console port.
- For the WLSE 1130, the serial/console port is on the back panel.

Step 2 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, 2.5*.

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.

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

You are now finished using the console. The remaining steps take place at the client system.

Configuring the Web Browser

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

Supported Browsers

Before connecting to the WLSE web interface, make sure you are using a supported browser and the browser is properly configured. The supported browsers for CD One 2.0 are listed in Table 4-4 on page 4-9. Use the procedures in Configuring Internet Explorer, page 4-10 or Configuring Netscape Navigator, page 4-11 to configure the browser.

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

Table 4-4 Supported Browsers

Client Operating System	Supported Browsers
Windows 2000, Windows NT, and Windows XP	Microsoft Internet Explorer 6.0 with Service Pack 1 Netscape Navigator 7.02
Japanese Windows 2000 and Windows NT	Japanese Microsoft Internet Explorer 6.0 with Service Pack 1 Japanese Netscape Navigator 7.02
Solaris 8 and 9	Netscape Navigator 7.01

Configuring Internet Explorer

To configure Internet Explorer 6.0, perform the following steps:

Step 1 Enable JavaScript:

a. Select **Tools > Internet Options > 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 2 Configure the browser to accept all cookies:

a. Select **Tools > Internet Options > Privacy**.

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

c. Click **OK**.

Step 3 Change the default font to improve readability:

a. Select **Tools > Internet Options > General**. Then elect **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 4 Configure temporary Internet files:

a. Select **Tools > Internet Options > General**. Then s elect **Temporary Internet files > Settings**.

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

Note Windows XP does not come with the Java Plugin installed on Internet Explorer 6.0. This causes problems when upgrading a WLSE to 2.5 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 or in the *User Guide for the Wireless LAN Solution Engine, Release 2.5*.

Configuring Netscape Navigator

To configure Netscape Navigator 7.01 or 7.02, perform the following steps:

Step 1 Select **Edit** > **Preferences**.

Step 2 Enable JavaScript:

a. Expand Advanced and select **Scripts & Plugins**.

b. Under "Enable JavaScript for," select **Navigator**.

c. Click **OK**.

Step 3 Configure Netscape Navigator to accept all cookies:

a. Expand Privacy & Security and select **Cookies**.

b. Select **Enable all cookies**.

c. Click **OK**.

Step 4 Change the default font for improved readability:

a. Expand Appearance and select **Fonts**.

b. From the Proportional list, select Sans Serif and a font size.

c. From the Sans-serif list, select the desired font.

d. Click **OK**.

Some fonts do not change after you use this option.

Next Steps—Finish Initial Configuration

For the remainder of the configuration, you use the WLSE's Web interface.

Table 4-5 Quick Reference for WLSE Configuration and Device Setup

Task	Steps	References
Log in and verify connectivity.	Verify that you can connect to the WLSE via HTTP and HTTPS.	Logging into the Web Interface and Verifying Connectivity, page 4-13
Configure devices to be managed or monitored by the WLSE.	• Configure IOS access points.	Set Up IOS Access Points, page 4-16
	• Configure non-IOS access points.	Set Up Non-IOS Access Points and Wireless Bridges, page 4-14
	• Configure routers and switches.	Set Up Routers and Switches, page 4-21
	• Configure AAA servers.	Set Up AAA Servers, page 4-22
Enter device credentials on the WLSE.	Enter SNMP credentials for all devices and other credentials, depending on device type and WLSE features you will be using.	Adding Device Credentials to the WLSE, page 4-24
Enter information about AAA servers.	Enter information about all AAA servers to be monitored.	Adding AAA Servers to the WLSE, page 4-28
Discover and manage devices.	• Discover devices by using the discovery wizard or importing devices. • Make sure all devices to be managed are in the managed state.	Discovering and Managing Devices, page 4-29
(Optional) Add additional users.	You can add additional users and specify their privileges by assigning roles to them.	Adding Users, page 4-36

Logging into the Web Interface and Verifying Connectivity

To verify HTTP and HTTPS connectivity, connect to the WLSE using a supported, properly configured Web browser and perform the following steps:

Step 1 To verify HTTP connectivity, enter the system IP address, followed by **:1741** (the default port number).

For example, if the system IP address is 209.165.202.128, enter **http://209.165.202.128:1741**.

If a login dialog box appears, you have connectivity.

Step 2 To verify HTTPS connectivity, enter the system IP address, prefixed by https. Do not use a port number.

For example, if the system IP address is 209.165.202.128, enter **https://209.165.202.128**.

If a login dialog box appears, you have connectivity.

Step 3 Enter the user name **admin** and the password you created during setup in the login dialog box. The WLSE home page appears.

Setting Up Device Management

The tasks in preparing the devices and the WLSE for use are:

- Setting Up Devices, page 4-14
- Adding Device Credentials to the WLSE, page 4-24
- Adding AAA Servers to the WLSE, page 4-28
- Discovering and Managing Devices, page 4-29

Setting Up Devices

You must set up network devices so the WLSE can discover and manage them. This section describes both required and optional setup tasks for:

- Non-IOS access points—see Set Up Non-IOS Access Points and Wireless Bridges, page 4-14
- IOS access points—see Set Up IOS Access Points, page 4-16
- Routers and switches—see Set Up Routers and Switches, page 4-21
- AAA servers—see Set Up AAA Servers, page 4-22

Set Up Non-IOS Access Points and Wireless Bridges

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

- By using the WLSE's automatic configuration option for first-time device configuration (select **Configuration > Auto Update > Startup Configuration**). For more information, see the online help or the *User Guide for the Wireless LAN Solution Engine, Release 2.5*.
- By opening a web browser session on each device and performing the tasks in the following table. To use this method, you must first configure each access point or bridge for web browsing.

Table 4-6 Setup Procedures for Non-IOS Access Points and Bridges

Tasks	Procedure	Notes
1. Enable Cisco Discovery Protocol (CDP).	**1.** In the Summary Status page, click **Setup**. **2.** Under Services: Cisco Services, click **Cisco Discovery Protocol**. **3.** Select Enabled. Click **Apply** or **OK**.	CDP is used by the WLSE to discover devices on the network. [1]

Table 4-6 Setup Procedures for Non-IOS Access Points and Bridges (continued)

Tasks	Procedure	Notes
2. Enable SNMP. (Optional) Set the location. (Optional) Set the system name and system contact.	1. In the Summary Status page, click **Setup**. 2. Under Services, click **SNMP**. 3. Select Enabled. 4. Enter a System Name, System Location, and System Contact. 5. Click **Apply** or **OK**.	SNMP is required for the WLSE to discover devices, populate reports, transfer configuration information to devices, and upgrade device firmware. Setting the system name and system location provides this information when you display device details.
3. Set the read community string.	1. In the Summary Status page, click **Setup**. 2. Under Services, click **Security**. 3. Click **User Information**; then click **Add New User**. 4. Create a user with all privileges, including SNMP, Firmware, Write, and Admin privileges. 5. In addition, for access points that are running a firmware version earlier than 12.01(T), assign Ident privileges. 6. Click **Apply** or **OK**.	The read community string is required for device discovery and populating reports.
4. Set the read-write community string.	1. In the Summary Status page, click **Setup**. 2. Under Services, click **Security**. 3. Click **User Information**; then click **Add New User**. 4. To create an user with SNMP read/write privileges, enter a username and password and select the Write, SNMP, Firmware, and Admin privileges. 5. Click **Apply** or **OK**.	The read-write community string is required for configuration and firmware jobs.

Table 4-6 Setup Procedures for Non-IOS Access Points and Bridges (continued)

Tasks	Procedure	Notes
5. Add an HTTP user with the ability to modify firmware, and enable the User Manager. You can use the same user that you created in Task 4, if the user has firmware privileges.	1. In the Summary Status page, click **Setup**. 2. Click **Security**. 3. Click **User Information**; then click **Add New User**. 4. Enter a username and password and select Firmware; then click **Apply**. 5. Navigate back to the Security Setup page and click **User Manager**. 6. Select Enabled; then click **Apply** or **OK**.	This allows configuration uploads from the WLSE to access points. You must also enter HTTP users and passwords on the WLSE (see Enter HTTP Credentials for Non-IOS Access Points, page 4-24).
6. Set up TFTP as the transfer protocol between the WLSE and access points.	1. In the Summary Status page, click **Setup**. 2. Under Services, click **FTP**. 3. Use the pulldown menu to select TFTP as the file transfer protocol. 4. In the Default File Server text box, enter the IP address of the WLSE. 5. Click **Apply** or **OK**.	TFTP is used for transferring configuration changes to access points.

1. If you do not want to enable CDP, see the Discovering and Managing Devices, page 4-29 for alternative methods of discovering devices.

Set Up IOS Access Points

You can set up IOS-based access points (Cisco Aironet 1100 and 1210 access points) in three ways:

- Use the WLSE's automatic configuration option for first-time device configuration (select **Configuration > Auto Update > Startup Configuration**). For more information, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.5*.
- Log in to each device by using Telnet or SSH and using the device's CLI commands. See Set Up IOS Access Points by Using the Device CLI, page 4-17.

- Log in to each device's Web interface. See Set Up IOS Access Points by Using the Web Interface, page 4-19.

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

About Configuration for VLANs

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

About Configuration for WDS

If you are using Wireless Domain Service (WDS), you must configure one or more access points to provide WDS. Currently, WDS is supported on Cisco Aironet 1100 and 1200 access points. For information on configuring access points and the WLSE for WDS, see Enter WLCCP Credentials for Wireless Domain Services (WDS), page 4-27.

Set Up IOS Access Points by Using the Device CLI

Step 1 Use Telnet or SSH (secure shell protocol) to log into the AP 1100 or AP 1210.

Step 2 Enter enable mode.

Step 3 Enter global configuration mode.

Step 4 To use Cisco Discovery Protocol (CDP) for discovery, enable CDP by entering the following command:

```
cdp run
```

Note To find out whether CDP is enabled, use the **show cdp** command in enable mode.

Note For information on alternatives to using CDP for discovery, see Discovering Devices, page 4-30.

Step 5 To set up SNMP community strings, enter the following commands in the sequence shown.

- The first two commands create an ISO view and set the read-only community string for discovery, faults, and reports. IOS access points that do not have an ISO view will be placed in the Misconfigured Devices group after discovery and faults will be generated. The fault messages refer to a "dot11 MIB" problem.
- The third command sets a read/write community string for updating access point firmware and configuring access points.

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

Note These community strings must also be entered on the WLSE before the device can be discovered and managed. See Enter SNMP Community Strings for All Managed Devices, page 4-25.

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

Step 7 To enable and configure SSH, enter the following commands. After the prompt for the number of bits in the modules, press **Return** to accept the default or enter a value.

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

In the preceding commands, *hostname* is the hostname of the access point, and *domain_name* is your domain name (for example, cisco.com).

The following commands are optional, but are recommended:

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

Step 8 To configure Telnet, enter the following commands. Telnet is enabled by default.

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

The following optional commands are recommended:

```
width 80
length 24
```

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

```
write memory
```

Set Up IOS Access Points by Using the Web Interface

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

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

a. After Cisco Discovery Protocol (CDP), select **Enabled**.

b. Click **Apply**.

Note If you do not want to use CDP for discovery, see Discovering Devices, page 4-30, for alternative methods.

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

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

a. Select **SERVICES** > **Telnet/SSH**.

b. Enable **Secure Shell**.

c. Enter a System Name.

d. Enter a Domain Name (for example, cisco.com).

e. (Optional) Enter the RSA key size

f. (Optional) Enter the Authentication Timeout.

g. (Optional) Enter Authentication Retries.

h. Click **Apply**.

Step 5 To enable and configure Telnet:

a. Select **SERVICES** > **Telnet/SSH**.

b. Enable **Telnet**.

c. (Optional) Enable **Teletype**.

d. Enter the number of Columns.

e. Enter the number of Lines

f. Click **Apply**.

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

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

b. Click **Apply**.

Step 7 In the SNMP Request Communities section, enter a community string for the ISO view:

Note This community string is required for the access point to be discovered and managed by the WLSE. Devices that do not have an ISO view will be placed in the Misconfigured Devices group after discovery, and faults will be generated. The fault messages refer to a "dot 11 MIB" problem.

a. Enter the community string in the SNMP Community field.

b. Enter `iso` in the Object Identifier (optional) field.

c. Click **Read-Only.**

d. Click **Apply**.

Step 8 In the SNMP Request Communities section, enter a read/write community string.

Note This community string is required to enable firmware updates and configuration downloads on the access point.

a. Enter the community string in the SNMP Community field.

b. Click **Read-Write**.

c. Click **Apply**.

Step 9 The community strings created in Steps 7 and 8 must be entered on the WLSE before the device can be discovered and managed. For more information, see Enter SNMP Community Strings for All Managed Devices, page 4-25.

Set Up Routers and Switches

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

Configure each router and switch as shown in Table 4-7 on page 4-21.

Table 4-7 Set Up Procedures for Routers and Switches

Task	Procedure	Notes
1. Enable CDP and verify that access points and bridges are visible from the router or switch.	Enter enable mode and use the following commands to verify that CDP is running on the switch or router: • IOS-based devices—**show cdp run** • Hybrid OS-based Catalyst switches—**show cdp** If CDP is not running, enter global configuration mode and enter **cdp run**. To verify that access points or bridges are visible in the device's CDP table, enter **show cdp neighbors**.	CDP is required for the WLSE to discover the device.
2. Enable SNMP and set up community strings.	On IOS-based devices, enter configuration mode and use the **snmp community** *community_string* **ro** command. On Hybrid OS-based Catalyst devices, enter enable mode and use the **set snmp community read-only** *community_string* command.	SNMP is required for the WLSE to discover and manage the device.

Table 4-7 Set Up Procedures for Routers and Switches (continued)

Task	Procedure	Notes
3. (Optional) Set the system name, contact, and location variables.	On IOS-based devices, enter configuration mode and use the following commands: • Set system name—**hostname** *name*. • Set system contact—**snmp contact** *contact*. • Set location—**snmp location** *location*. On Hybrid OS-based Catalyst switches, enter enable mode and use the following commands: • Set system name—**set system name** *name*. • Set system contact—**set system contact** *contact*. • Set location—**set system location** *location*.	These variables make the device more manageable. The system name, system contact, and location will appear in the device detail displays.

Set Up AAA Servers

The WLSE can monitor the performance of AAA (Authentication, Authorization, and Accounting) services provided by:

- CiscoSecure ACS Server.
- Cisco Access Registrar (CAR) (RADIUS services only).

The WLSE supports LEAP, RADIUS, EAP-MD5, and PEAP servers. For information on supported versions of CiscoSecure ACS, see the Supported Devices Table for WLSE 2.5 on Cisco.com.

An AAA server is required for using Wireless Domain Service (WDS). For more information about configuring for WDS, see Enter WLCCP Credentials for Wireless Domain Services (WDS), page 4-27.

Note For PEAP, in addition to the procedures in this section, you must also do the following on the ACS server: set up a certificate and private key and enable PEAP. For more information, see the Cisco Secure ACS documentation.

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

Note When you set up the WLSE (see Adding AAA Servers to the WLSE, page 4-28), you will need the IP address or name of the system that is running CiscoSecure ACS Server.

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

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

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

Note When you set up the WLSE (see Adding AAA Servers to the WLSE, page 4-28), you will need this name and password.

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

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

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

Note You will need this key when you add AAA servers to the WLSE. Adding AAA Servers to the WLSE, page 4-28

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

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

Adding Device Credentials to the WLSE

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

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

Enter HTTP Credentials for Non-IOS Access Points

HTTP credentials are required for downloading configuration files to non-IOS access points and for uploading configuration from such access points. The same password must be set on each access point, as described in Table 4-6 on page 4-14. You can enter as many usernames and passwords as necessary.

To enter HTTP usernames and passwords:

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 SNMP Community Strings for All Managed Devices

SNMP community strings are used for discovering and communicating with network devices. The community string must be set on each device, as described in Setting Up Devices, page 4-14. You an enter as many community strings as necessary.

Note If you are importing devices, you do not need to enter their community strings. For more information, see Import Devices, page 4-33.

To enter community strings:

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

Initially, the dialog box contains a default entry which covers all devices, provided device community strings are set to the default (public).

Step 2 Add new entries using one of these methods:

- Using the text boxes and lists for individual parameters. After you have specified all the parameters, click **Add** to add the community string to the list.
- Entering data directly in the list of community strings by using the following syntax:

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

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

Step 3 Click **Save** to apply your changes.

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 user name, do not enter a user name.

To enter Telnet or SSH credentials:

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

d. Enter the confirm password.

e. Enter the enable password.

f. Enter the confirm enable password.

g. 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 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 port settings:

Step 1 Select **Devices > Discover > Device Credentials > IOS HTTP 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)

If you are using WDS on your wireless LAN, you must set up an AAA server (if you don't already have an AAA server set up), add WLCCP credentials, and configure the access point that is providing WDS.

Configure an AAA Server

To set up the AAA server, see Set Up AAA Servers, page 4-22.

Configure the WLSE for WDS

To configure the WLSE to authenticate with the access point providing WDS:

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

Step 2 Enter the Radius User Name and Radius Password.

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

Step 3 Click **Save**.

Configure the WDS Access Point

WDS is currently supported by on the Cisco Aironet 1100 and 1200 IOS-based access points.

To configure the access point that will provide Wireless Domain Services:

Step 1 Log in to the CLI interface.

Step 2 In configure mode, enter the following command:

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

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

Step 3 To verify that authentication is configured properly, enter the following command

```
# show wlccp wnm status
```

The command returns a status of SECURITY KEYS SETUP if the authentication is successful.

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 AAA server for monitoring, see Set Up AAA Servers, page 4-22.

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

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

Step 3 Select **Add Server**. and complete the following:

Text Box	Description
Server Name	Hostname or IP address of the AAA server.
Server Port	Port on the server that is used for authentication; use port 1645.
Username	Client username that you entered on the AAA server.
Password	Client password that you entered on the AAA server.
Secret	Shared secret key that you entered on the AAA server.

Step 4 Click **Add**.

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.

Discovering and Managing Devices

Before the WLSE can manage devices, the devices must first be discovered. After devices are discovered, they must be managed.

The major tasks in discovering and managing devices are listed in the following table. Detailed procedures follow.

Table 4-8 Device Management Quick Reference.

Task		Reference
1. (Optional) Configure discovery options.		Configuring Discovery Options, page 4-29.
2. Discover devices by one of these methods:	Use CDP Discovery.	Run CDP Discovery, page 4-30.
	Import devices.	Import Devices, page 4-33.
3. Manage devices.		Managing Devices, page 4-35.

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. This step is optional.

To configure discovery options, perform the following steps:

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. To enable automatic management for all discovered devices, select **Auto-Manage Devices**. Otherwise, you must move devices to the managed state after they have been discovered.

c. To arrange temporary management of access points, you can configure MAC filtering. For information, see the online help or the *User Guide for the Wireless LAN Solution Engine, Release 2.5*.

d. Click **Save**.

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

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 4-30.

Note If you prefer not to use CDP, use the wizard, but enter all of your devices as seeds as indicated in the procedure.

- Import devices from a file or from a CiscoWorks server—See Import Devices, page 4-33.

Run CDP Discovery

Before 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 4-31.
- Modify the default CDP discovery schedule by scheduling a one-time job or repeated jobs—See Modify the CDP Discovery Schedule, page 4-32.

Run CDP Discovery Now

To run an immediate discovery, perform the following steps:

Step 1 Select **Devices** > **Discover** > **DISCOVER** > **CDP Discovery** and click Next.

Step 2 Select **Run Now** and click **Next**.

Step 3 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 4-25. After adding community strings, click **Next**.

Step 4 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, 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.

c. Click **Next**.

Step 5 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 6 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:

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

Step 2 In the Discovery Wizard, select **CDP Discovery** 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 and select the interval 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 4-25. 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 Resource Manager Essentials or by creating a file with a text editor. After you import the file, a one-time discovery begins immediately.

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

Step 2 In the Discovery Wizard, select **Import From File** and click **Next**.

Step 3 Enter the pathname of the file or click **Browse** to find it. If you have not created 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.

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.

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.

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

Step 2 In the Discovery Wizard, select **Import From CiscoWorks** and click **Next**.

Step 3 Enter the following information. 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	

Step 4 For a one-time import, select Run Now.

Step 5 To schedule a one-time import or repeated imports:

a. Select the start date and start time from the pulldown lists.

b. 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.

Step 6 Click **Finish** to import devices or click **Cancel** to cancel the import.

Step 7 Click **Check Last Status** to see the results of the import.

Managing Devices

After discovering or importing devices and verifying the results, ensure that all devices 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, and an inventory will be run. For information on setting the auto-manage option, see Configuring Discovery Options, page 4-29.

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

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

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.

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 Users

You can add users and configure their access to the WLSE Web interface and their access to the CLI. User access to the Web interface is determined by the roles assign to each user account. Users can only perform WLSE functions that are allowed by their logins.

Note For information about using alternative sources of authentication, see the online help or the *User Guide for the Wireless LAN Solution Engine, Release 2.5*.

To create users:

Step 1 Select **Administration > User Admin > Manage Users**.

Step 2 Enter a user name, password, and email address in the appropriate fields.

Step 3 Select the user's CLI access level.

Step 4 Select the user's role. A user's role determines which WLSE features that user is allowed to access. The WLSE provides the following default user roles and you can create others and assign access to tabs and subtabs to your roles.

- System Admin
- Network Admin
- Network Operator
- Help Desk

Note The System Administrator role cannot be modified or deleted. You cannot delete the other default roles, but you can modify the tabs and subtabs to which they have access.

Step 5 Click **Add** to create the user.

Next Steps

For more information on using the WLSE to manage devices, customizing WLSE operations, and maintaining the WLSE system, see the online help or the *User Guide for the Wireless LAN Solution Engine, Release 2.5*. You can access the user guide:

- In PDF in the Documentation directory on the Recovery CD-ROM.
- From the WLSE desktop. Click **Help**, then click the **View PDF** button.
- On Cisco.com.

Installing Software on the CiscoWorks 1105 and 1130 WLSE

This section describes the process for updating the system software on a CiscoWorks 1105 or CiscoWorks 1130 Wireless LAN Solution Engine.

Caution Always review the readme file that accompanies the upgrade image on Cisco.com before attempting to install the upgrade. The procedure for upgrading might have changed after this document was printed and might not be accurate for some upgrades. Some upgrades require a specific installation method. In addition, the readme file contains information about caveats (such as data that is not preserved during the upgrade) and the new features and fixes in the release.

This section contains the following topics:

Upgrade Versions

You can upgrade directly to WLSE 2.5 as follows:

- From WLSE 2.0 to WLSE 2.5
- From WLSE 2.0.2 to WLSE 2.5

Note Upgrading from the Web interface might fail for upgrading WLSE 2.0 or 2.0.2 to WLSE 2.5. For the latest information see the readme file included with the upgrade image on Cisco.com.

Backing Up the WLSE

Before upgrading WLSE software, back up the configuration. The upgrade attempts to preserve the WLSE database, but a backup is needed in case of errors during the upgrade. See the online help or the *User Guide for the Wireless LAN Solution Engine, Release 2.5*.

Downloading the Upgrade Image

Unless you are upgrading from the recovery CD, you must download the upgrade files from Cisco.com.

Procedure

Step 1 Locate the files by using the following URLs:

- http://www.cisco.com/kobayashi/sw-center/cw2000/crypto/wlan-sol-eng
- ftp://ftp.cisco.com/cisco/crypto/3DES/cw2000/wlan-sol-eng
- Or, follow this navigation path on Cisco.com: **Products and Services > Network Management CiscoWorks > CiscoWorks Wireless LAN Solution Engine > Software Center**.

Note WLSE images are subject to import/export regulations respecting strong encryption. Before you are allowed to download the image, you might be directed to edit your Cisco.com profile to confirm that you are allowed to download such images.

Step 2 The files to download depend on whether you are using the WLSE as a local repository or you are using a Windows server as a remote repository:

- If you are using the WLSE as the repository, download the ZIP file, the info file and the readme file to an FTP server. The upgrade zip file and the info file must be in the same directory on the FTP server. *Do not extract the zip file.*
- If you are using a Windows system (Windows XP, Windows 2000, or Windows NT) as a remote repository:
  a. Download the ZIP file and readme file into a directory on the Windows system.
  b. Extract the ZIP file to any empty directory.

Upgrade Methods

WLSE offers the following upgrade methods:

- Upgrading by using the Web interface—see Upgrading by Using the Web Interface, page 5-4.
- Upgrading by using the command line interface (CLI)—see Upgrading by Using the CLI, page 5-8.
- Upgrading by using the recovery CD—see Upgrading from the Recovery CD, page 5-12.

Upgrading by Using the Web Interface

Caution Before upgrading, read the readme.txt file that accompanies the software. This method might fail for upgrading from WLSE 2.0 to WLSE 2.5; use the CLI method instead.

This section contains the following topics:

- Upgrade quick reference.
- Alternative upgrade procedures:
  - Installing from the Local Repository, page 5-4
  - Installing from a Windows Server, page 5-6

Upgrade Quick Reference

The basic tasks in installing software upgrades by using the Web interface are listed in below. See the referenced sections for details about these tasks.

Task	Reference
1. Back up WLSE.	Backing Up the WLSE, page 5-2
1. Download software from Cisco.com.	Downloading the Upgrade Image, page 5-2
2. Install software.	To install from the local repository, see Installing from the Local Repository, page 5-4.
	To install from the remote repository, see Installing from a Windows Server, page 5-6.

Installing from the Local Repository

Use this procedure to install from a local repository on the WLSE.

Procedure

Step 1 Log in via Telnet or SSH as the admin user on a WLSE.

Step 2 Specify the FTP site that will be the source of the software updates by entering the following command:

```
repository source ftp://source/path
```

where *source* is the hostname or IP address of the FTP server on which the image resides and *path* is the path to the image files.

Step 3 To list the contents of the source, enter the following command. This command requires a valid username and password on the remote FTP server.

```
repository list remote
```

Step 4 Download the software to the repository by entering the following command. This command requires a valid username and password on the remote FTP server.

```
repository add package
```

where *package* is the name of the software image to be transferred. For example, if the zip file is named WLSE-2.5-K9.zip, the package would be WLSE-2.5-K9.

Step 5 To verify the contents of the repository, enter the following command. This command requires a valid username and password on the remote FTP server.

```
repository list
```

Step 6 Log in to the WLSE Web interface as a user with system administration privileges.

Step 7 Define the repository:

a. Select **Administration > Appliance > Software > Define Repository**.

b. Enter the following data:

Field	Data to Enter
Host Name	`localhost`
Port Number	`9851`
Description	(optional)

c. Click **Connect to Repository**.

Step 8 Select **Administration > Appliance > Software > Install Software Updates**.

The Install Software Updates window displays information about the WLSE, the currently defined repository, and the compatible software available for updating.

a. Select a software update to install. To view details, click **README** in the Details field.

b. Click **Install**.

c. Click **Confirm**.

Note When the installation is complete, the WLSE will be unavailable for a few minutes while it restarts. The Login screen will appear when the update is complete.

Step 9 To view details after the installation is complete, select **Administration > Appliance > Software > Status > View Log**.

Installing from a Windows Server

Use this procedure to install from a remote repository on a Windows 2000, Windows XP, or Windows NT server.

Procedure

Step 1 If you are using a Windows XP or Windows NT server as the repository and you are using Internet Explorer 6.0 on the client, configure the browser *on the repository* as follows. This ensures that the display works properly during installation.

a. Install Java Plugin 1.3.1_08 or later on the repository.

b. Start Internet Explorer 6.0 and select **Tools > Internet Options > Privacy**.

c. Lower the slider all the way down to achieve the **Accept All Cookies** setting.

Step 2 Open a command window, create a virtual drive, and map the virtual drive to the drive containing the update files; for example:

```
subst f: d:\WLSE_repository
```

Note The virtual drive (f: in this example) will be removed after you reboot the Windows server.

Step 3 Double-click the virtual drive icon. Then, double-click the autorun.bat file if it does not automatically run.

Result: A browser window opens and displays the Appliance Update screen.

Step 4 Enter the hostname or IP address of the WLSE in the Appliance Update screen.

Step 5 Log in to the WLSE Web interface as a user with system administration privileges.

Result: The Install Software Update window opens.

Step 6 Install the new software:

a. Select a software update to install. To view details, click **README** in the Details field.

b. Click **Install**.

c. Click **Confirm**.

Step 7 After the software installation finishes, the Appliance Update screen reappears. Click **Cancel** to close the screen.

Note When the installation is complete, the WLSE will be unavailable for a few minutes while it restarts.

Step 8 To view details after the installation is complete, select **Administration > Appliance > Software > Status > View Log**.

Upgrading by Using the CLI

Caution Before upgrading, read the readme.txt file that accompanies the software.

This section contains:

- Upgrade quick reference.

- Procedures for using CLI commands to upgrade WLSE software:
  - Create the Repository, page 5-8
  - Install the Software, page 5-11
- Related CLI commands.

Upgrade Quick Reference

The basic tasks in installing software upgrades by using the CLI are listed in below. See the referenced sections for details about these tasks.

Task	Reference
1. Back up WLSE.	Backing Up the WLSE, page 5-2
2. Download image to an FTP server.	Downloading the Upgrade Image, page 5-2
3. Create repository.	Create the Repository, page 5-8
4. Install upgrade.	Install the Software, page 5-11

Create the Repository

Upgrades are normally installed from a repository, which can be located on the WLSE to be upgraded or on a remote Windows FTP server. This section contains the following topics:

- Create a Local Repository, page 5-9
- Create a Repository on a Windows Server, page 5-10

Create a Local Repository

Use this procedure to create a repository on the WLSE to be upgraded.

Procedure

Step 1 Log in using Telnet or SSH to the WLSE to be upgraded.

Step 2 Specify the FTP site that will be the source of the software updates by using the following command:

```
repository source ftp://source/path
```

where *source* is the hostname or IP address of the FTP server on which the image resides and *path* is the path to the image files.

If the message “unable to obtain file” appears, you have entered the wrong password.

Step 3 List the contents of the source by using the following command. This command requires a valid username and password on the remote FTP server.

```
repository list remote
```

Step 4 Download the software to the repository by using the following command. This command requires a valid username and password on the remote FTP server.

```
repository add package
```

where *package* is the name of the software image to be transferred. For example, if the zip file is named WLSE-2.5-K9.zip, the package would be WLSE-2.5-K9.

Step 5 To verify the contents of the repository, use the following command. This command requires a valid username and password on the remote FTP server.

```
repository list
```

Step 6 Go to Install the Software, page 5-11

Create a Repository on a Windows Server

The remote repository created on a Windows server is temporary; it will no longer exist after the server reboots.

To use a Windows NT, Windows 2000, or Windows XP server as a remote repository:

Procedure

Step 1 If you are using a Windows XP or Windows NT server as the repository and you are using Internet Explorer 6.0 on the client, configure the browser *on the repository* as follows. This ensures that the display works properly during installation.

a. Install Java Plugin 1.3.1_08 or later on the repository.

b. Start Internet Explorer 6.0 and select **Tools > Internet Options > Privacy**.

c. Lower the slider all the way down to achieve the **Accept All Cookies** setting.

Step 2 Open a command window, create a virtual drive, and map the virtual drive to the drive containing the update file; for example:

```
subst f: d:\WLSE_repository
```

Note The virtual drive (f: in this example) will be removed after you reboot the Windows 2000, Windows NT, or Windows XP server.

Step 3 Double-click the virtual drive icon. Then, double-click the autorun.bat file if it does not automatically run.

A browser window opens and displays the Appliance Update screen. Minimize this window.

Step 4 Go to Install the Software, page 5-11.

Install the Software

In this procedure, you define the repository and install the software.

Procedure

Step 1 Log in as the admin user via Telnet or SSH on the WLSE to be upgraded.

Step 2 Enter install mode:

```
install
install:
```

Step 3 Define the repository.

- To define a local repository, enter the following command:

  `install:`**`configure default`**

- To define a remote repository, enter the following command:

  `install:`**`configure URL`** *`URL_value`*

  where *URL_value* is the HTTP URL of the remote repository. For example:

  `install:`**`configure URL http://209.165.200.224:9851`**

Step 4 To view a list of the software images and updates available for installation, enter the following command:

`install:`**`install list`**

Step 5 Enter the following command to install the software:

`install:`**`install update`** *`package`*

where *package* is the name of the software image to be installed. For example, if the ZIP file is called WLSE-2.5-K9.zip, the package name is WLSE-2.5-K9.

Result: The WLSE is reimaged and reboots.

Related CLI Commands

To delete images from the WLSE's local repository, use the following command:

`repository delete` [*`package`* | **`all`**]

where **all** deletes all images in the local repository, and *package* deletes the named image only.

To change the status of the WLSE's local repository, use the following command:

`repository server` [**`stop`** | **`start`** | **`status`**]

to stop, start, or display the status of the local repository. You can stop the repository if you are not using it or if you have security concerns. The repository will automatically restart if you reboot the WLSE.

Upgrading from the Recovery CD

If you have a recovery CD with the release of the WLSE software you want to install, you can use the CD to upgrade your WLSE.

Note Although every effort has been made to validate the accuracy of the software version on the recovery CD, you must review WLSE software versions on Cisco.com and download and install any required earlier updates. For information on installing such updates, see the readme files that accompany software updates on Cisco.com.

Caution This procedure will destroy all data and install a new image. You will need to replace the data by restoring a backup. For information on backups, see the online help or the *User Guide for the Wireless LAN Solution Engine, Release 2.5*.

To reimage the WLSE, use the following procedure.

Procedure

Step 1 Connect a console to the WLSE's console port.

- For the WLSE 1105, use the serial port on the front panel; do not use the serial port on the back panel as a console port.
- For the WLSE 1130, the serial/console port is on the back panel.

Step 2 Log in as the admin user.

Step 3 Put the recovery CD in the CD drive.

Step 4 Enter the following command; the WLSE will reboot.

```
reload
```

Step 5 At the following prompt, enter **yes**:

Caution If you decide not to reimage the WLSE, enter rescue. For more information about the rescue image, see the *User Guide for the Wireless LAN Solution Engine, Release 2.5*.

```
Do you wish to continue (Yes/No)/Rescue) yes
```

Step 6 When the WLSE ejects the recovery CD, remove it.

Step 7 Restore the backup.

For information about restoring backups, see the *User Guide for the Wireless LAN Solution Engine, Release 2.5* or the online help.

Technical Specifications for the CiscoWorks 1130 WLSE

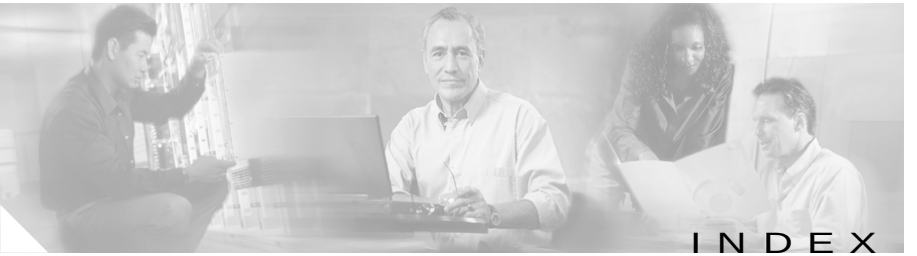
Table A-1 provides the Wireless LAN Solution Engine's (WLSE) specifications.

Table A-1 WLSE Technical Specifications

Component	Specifications
Serial port	One 9-pin connector
RJ-45 ports	Two RJ-45 connectors for connection to integrated 10/100 Ethernet controllers
AC power supply wattage	230 W
AC power supply voltage	100 to 120 VAC / 200 to 240 VAC, 50 / 60 Hz
System battery	CR2032 3-V lithium coin cell
Height	4.3 cm (1.7 inches)
Width	42.5 cm (16.7 inches)
Depth	55 cm (22 inches)
Weight	10 kg (23 lb) maximum
Operating temperature	10° to 35°C (50° to 95°F)
Storage temperature	–40° to 65°C (–40° to 149°F)
Operating relative humidity	8% to 80% (noncondensing) with a humidity gradation of 10% per hour

Table A-1 WLSE Technical Specifications (continued)

Component	Specifications
Storage relative humidity	5% to 95% (noncondensing)
Operating maximum vibration	0.25 G (half-sine wave) at a sweep of 3 to 200 Hz for 15 minutes
Storage maximum vibration	0.5 G at 3 to 200 Hz for 15 minutes
Operating maximum shock	Six consecutively executed shock pulses in the positive and negative x, y, and z axes (one pulse on each side of the system) of 41 G for up to 2 ms
Storage (non-operational) maximum shock	Six consecutively executed shock pulses in the positive and negative x, y, and z axes (one pulse on each side of the system) of 71 G for 2 ms
Operating altitude	–16 to 2000 m (–50 to 6500 ft)
Storage altitude	–16 to 10,600 m (–50 to 35,000 ft)



A

B

C

D

E

F

H

I

K

L

M

N

O

P

R

S

T

U

V

W