Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine

Software Release 2.7
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-7816345=
Text Part Number: 78-16345-01

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

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

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

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

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

Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine

CONTENTS

Cisco 90-Day Limited Hardware Warranty Terms

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

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

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

   The Warranties and License Agreements page appears.

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

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

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

   c. Click **Go**.

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

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

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

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

      78-5236-01C0

   b. Select the language in which you would like to read the document.
   c. Click **Go**.

      The Cisco warranty page appears.

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

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

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

Duration of Hardware Warranty

Ninety (90) days.

Replacement, Repair, or Refund Policy for Hardware

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

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

To Receive a Return Materials Authorization (RMA) Number

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

Complete the information below, and keep it for reference:

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

Preface

This guide contains both hardware installation and software setup instructions:

- The hardware installation information and technical specifications apply only to the CiscoWorks 1130-19 Wireless LAN Solution Engine.
- The software information applies to any of the following hardware platforms that are running WLSE 2.7 software: CiscoWorks 1105 WLSE, CiscoWorks 1130 WLSE, and CiscoWorks 1130-19 WLSE.

This guide contains the following sections:

Audience

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

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

Conventions

This document uses the following conventions:

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

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

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

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

Note 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 1130-19 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 www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_7/index.htm

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:

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: • On Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_7/index.htm • PDF on the WLSE Recovery CD.
User Guide for the CiscoWorks Wireless LAN Solution Engine	Describes WLSE features and provides instructions for all software features: • From the WLSE online help. Click **View PDF**. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_7/index.htm • Printed document available by order.[1]

Document Title	Description
Supported Devices Table for the Wireless LAN Solution Engine	Lists devices supported at the time the product was released. Available on Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_7/index.htm
Troubleshooting and FAQs for the CiscoWorks Wireless LAN Solution Engine	Troubleshooting hints and FAQs. Available: • From the WLSE online help. Click • On Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_7/index.htm
Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine	Describes how to install and configure the WLSE. Available: • PDF on the WLSE Recovery CD-ROM. • On Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_7/index.htm • Printed document available by order.[2]
Regulatory Compliance and Safety Information for the CiscoWorks 1130-19 Wireless LAN Solution Engine	Regulatory compliance and safety information. Available: • Printed document shipped with the WLSE. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_7/index.htm
Integrating CiscoWorks Wireless LAN Solution Engine with a CiscoWorks Server	Provides information about adding a link to the WLSE from a CiscoWorks server's navigation tree. On Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_7/index.htm
Developer Guide for the CiscoWorks Wireless LAN Solution Engine	Provides information about using XML application programming interface. On Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_upgrades_and_downloads.html

1. For information on ordering, see "Obtaining Documentation" section on page xxii.

2. For information on ordering, see "Obtaining Documentation" section on page xxii.

Obtaining Documentation

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

Cisco.com

You can access the most current Cisco documentation 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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

  http://www.cisco.com/en/US/partner/ordering/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 e-mail comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

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-a-day, 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. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website 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. The Cisco TAC website is located at this URL:

http://www.cisco.com/tac

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

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which 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 the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

http://www.cisco.com/tac/caseopen

For P1 or P2 cases (P1 and P2 cases are those in which 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.

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

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

- 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://cisco.com/univercd/cc/td/doc/pcat/

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

- 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

The WLSE is a rack-mountable appliance for configuring and managing Cisco wireless devices. This chapter describes software features of WLSE 2.7 and hardware features of the WLSE 1130-19.

This chapter contains the following sections:

Note For translated safety warnings and regulatory compliance information, see the document titled *Regulatory Compliance and Safety Information for the CiscoWorks 1130-19 WLSE*.

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 operates 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 or SSH. For information on all the CLI commands, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.
- 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 CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

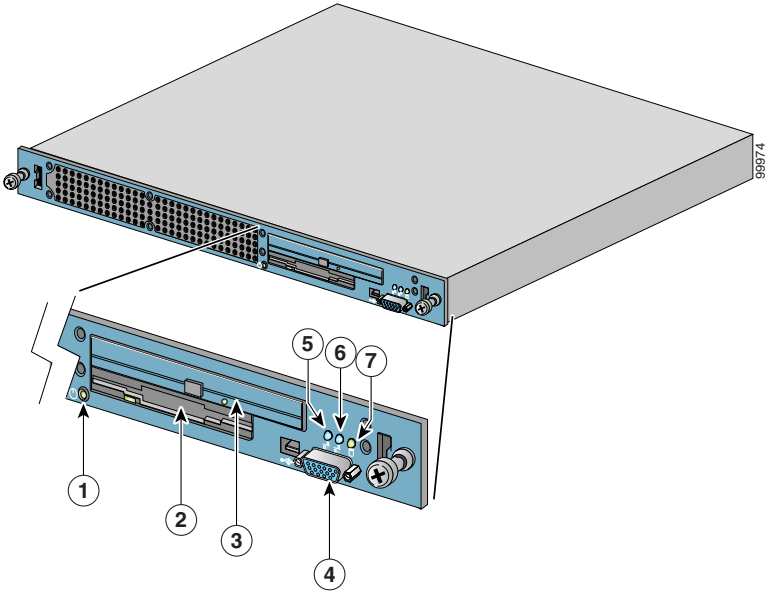
Hardware Features—WLSE 1130-19

This section describes the WLSE 1130-19 front and back panels.

Front Panel Features

Figure 1-1 shows front panel features.

Figure 1-1 Front Panel Features



1	Power switch with built-in power indicator The power switch turns power on or off. To turn system power off, press and hold this switch for at least 4 seconds.	**5**	Ethernet 0 activity/link indicator
2	Floppy disk drive	**6**	Ethernet 1 activity/link indicator
3	CD-ROM drive	**7**	Hard drive indicator
4	Video output or USB port for optional keyboard		

System Indicators

When troubleshooting your WLSE, you might need to check the status of the indicators on the front panel. These lights are described in Table 1-1.

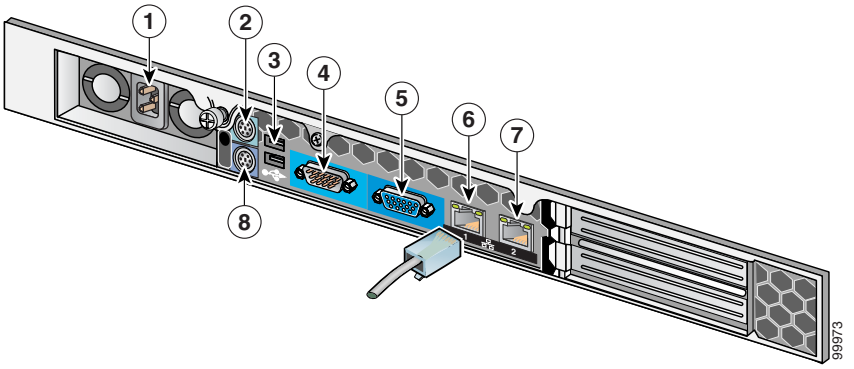
Table 1-1 System Indicators

Indicator	Color	Function
Power	Green	The power indicator lights up when the WLSE is connected to an AC power source.
Hard Drive activity	Blue	The hard drive activity indicator blinks when hard drive activity occurs.
Ethernet 0 activity/link	Blue	The Ethernet 0 activity/link indicator lights up when the Ethernet 0 port is connected to a network and blinks when activity occurs on this channel.
Ethernet 1 activity/link	Blue	The Ethernet 1 activity/link indicator lights up when the Ethernet 1 port is connected to a network and blinks when activity occurs on this channel.

Back Panel Features

Figure 1-2 shows the WLSE back panel.

Figure 1-2 Back Panel Connections



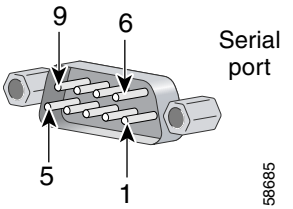
1	AC power receptacle	**5**	Video output
2	Mouse port	**6**	Ethernet 0 connector
3	USB port	**7**	Ethernet 1 connector
4	Console/serial port	**8**	Console keyboard connector

Serial/Console Port

The serial port on the back panel uses a 9-pin D-subminiature connectors.

Figure 1-3 illustrates the pin numbers for the serial port connectors and the following table defines the pin assignments and interface signals for the serial port connector.

Figure 1-3 Pin Numbers for the Serial Port Connectors



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 location of the Ethernet connectors is shown in Figure 1-2 on page 1-5.

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 WLSE package should include the following:

- WLSE 1130-19
- Rack mounting kit. (Your rack mounting kit may be different from the one described in this document.)
- Power cable
- Serial cable (light blue, RJ-45 to RJ-45)
- 10Base-T Ethernet cable (yellow)
- Adapters (DB-9 to RJ-45)
- Adapter (DB-25 to RJ-45)
- WLSE 2.7 Recovery CD
- WLSE documentation:
  - *Installation and Configuration Guide for the CiscoWorks 1130-19 Wireless LAN Solution Engine*
  - *Finding Documentation for the CiscoWorks 1130-19 Wireless LAN Solution Engine*
  - *Regulatory Compliance and Safety Information for the CiscoWorks 1130-19 Wireless LAN Solution Engine*

Preparing to Install WLSE 1130-19 Hardware

This chapter describes the safety instructions and site requirements needed for installing the WLSE 1130-19, and guides you through installation preparation. The chapter contains the following sections:

Safety

This section provides safety information about 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.

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 1130-19 Wireless LAN Solution Engine.*

The following warnings and cautions are provided to help you prevent damage to the devices or injury to yourself:

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards.** Statement 117

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

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

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

Warning **This unit might have more than one power cord. To reduce the risk of electrical shock, disconnect all power supply cords before servicing the unit.** Statement 106

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120VAC, 20A U.S. (240VAC, 16 to 20A international) is used on the phase conductors (all current-carrying conductors). The fuse or circuit breaker must have adequate safety approvals recognized by the country of usage.** Statement 119

Warning **This equipment is intended to be grounded to comply with emission and immunity requirements. Ensure that the switch functional ground lug is connected to earth ground during normal use.** Statement 1064

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.** Statement 1029

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

Warning **The power supply circuitry for the equipment can constitute an energy hazard. Before you install or replace the equipment, remove all jewelry (including rings, necklaces, and watches). Metal objects can come into contact with exposed power supply wiring or circuitry inside the DSLAM equipment. This could cause the metal objects to heat up and cause serious burns or weld the metal object to the equipment.** Statement 207

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

Warning **Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord.** Statement 1

Warning **Read the installation instructions before connecting the system to the power source.** Statement 1004

Warning **The ports labeled "Ethernet," "10BaseT," "Token Ring," "Console," and "AUX" are safety extra-low voltage (SELV) circuits. SELV circuits should only be connected to other SELV circuits. Because the BRI circuits are treated like telephone-network voltage, avoid connecting the SELV circuit to the telephone network voltage (TNV) circuits.** Statement 22

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

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 the section Obtaining Technical Assistance, page -xxiii 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:

- If any of the following conditions occur contact the Cisco Technical Assistance Center:
  - 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 cable(s). 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.
- Observe power strip ratings. Make sure that the total ampere rating of all products plugged into the power strip does not exceed 80% of the rating.
- 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" section on page 2-7 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.**

- 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.**

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. For the WLSE's power requirements, see Appendix B, "Technical Specifications— CiscoWorks 1130-19."

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Make sure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. and 240 VAC, 10A international are used on the phase conductors (all current-carrying conductors).**

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 Ethernet Connectors, page 1-7.

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

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

Next Step

Install the WLSE 1130-19 hardware. See Chapter 3, "Installing WLSE 1130-19 Hardware."

Installing WLSE 1130-19 Hardware

This chapter describes how to install the CiscoWorks 1130-19 Wireless LAN Solution Engine in a rack. 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, "Basic Setup—CiscoWorks 1105/1130/1130-19."

Table 3-1 Quick Reference

Task	References
Use the rack mount kit to install the WLSE in a rack.	Installing the WLSE 1130-19 in a Rack, page 3-2
Connect the WLSE to an AC power source.	Connecting Cables, page 3-15
Connect network and console cables.	Connecting Cables, page 3-15
Power on the WLSE.	Powering On the WLSE, page 3-16

Installing the WLSE 1130-19 in a Rack

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 by industry standards.

Before installing the WLSE in a rack, read Preparing Your Site for Installation, page 2-7 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.

The rack must be properly secured to the floor, to the 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.

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 in 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 2-10 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:**

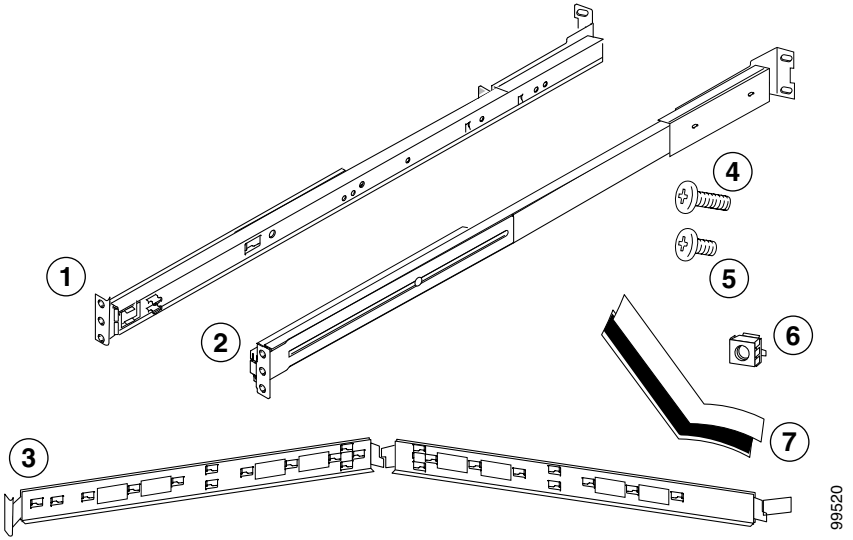
- **This unit should be mounted at the bottom of the rack if it is the only unit in the rack.**
- **When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.**
- **If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.** Statement 1006

The server can be installed in a system 1U rack. The rack rail components are as follows (numbers in parentheses refer to Figure 3-1):

- 2 telescopic rails (1, 2)

- 1 cable management arm (3)
- Bag containing:
  - 9 Round head screws with washer (4)
  - 6 Round head screws (5)
  - 6 Cage nuts (6)
  - Velcro (7)

Figure 3-1 Rack Rail Components



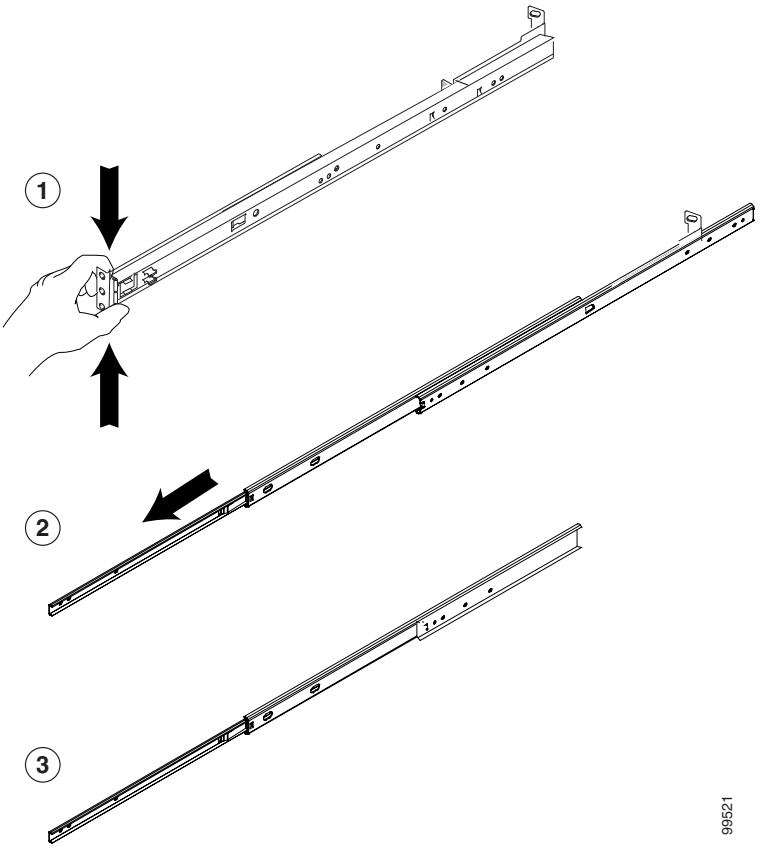
To install the CiscoWorks 1130-19 WLSE in a rack, perform the following steps:

Step 1 Attach the telescopic rails to the rack assembly:

a. See Figure 3-2. Extend the server rail (1) as far as it will go.

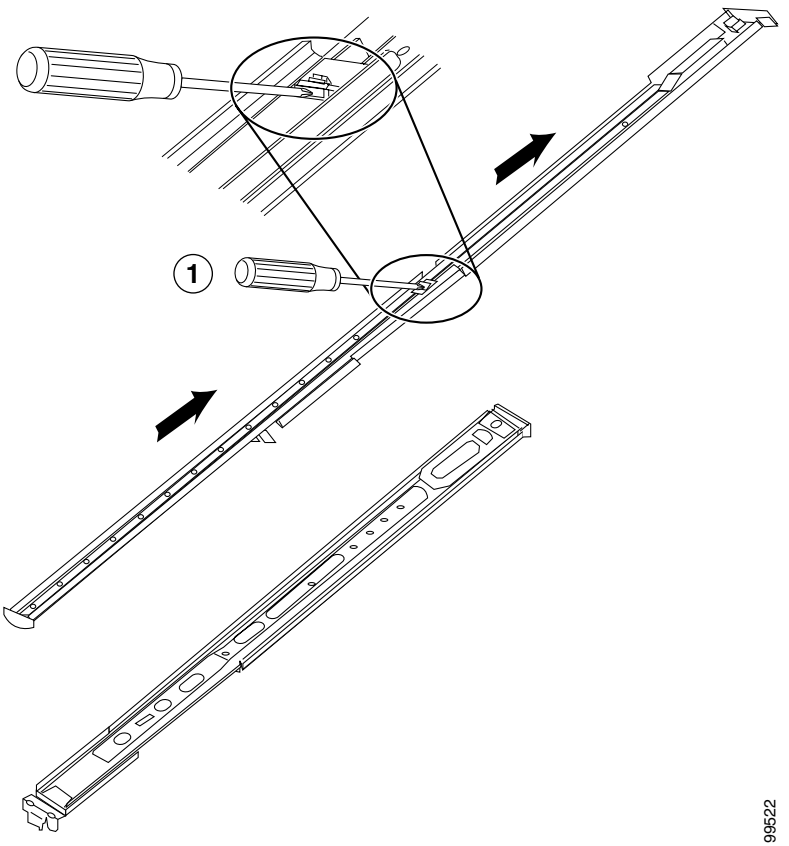
b. Press the green spring plate (2) and slide out that part of the server rail (1). (Set it aside for attaching to the chassis.)

Figure 3-2 Removing the Server Rail



c. See Figure 3-3. Using a screwdriver (1), push the middle rail to the end of the rail.

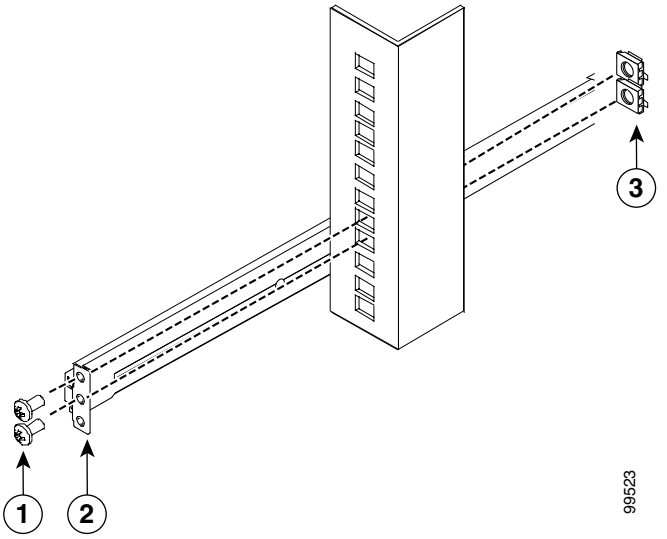
Figure 3-3 Telescoping the Rail



Note To allow for adjustment later in the installation, do not tighten any screws. The outer rail/bracket assembly with extended bracket (1) must be assembled to the left side.

d. See Figure 3-4. Attach the front end of the telescopic outside rail (1) to the rack.

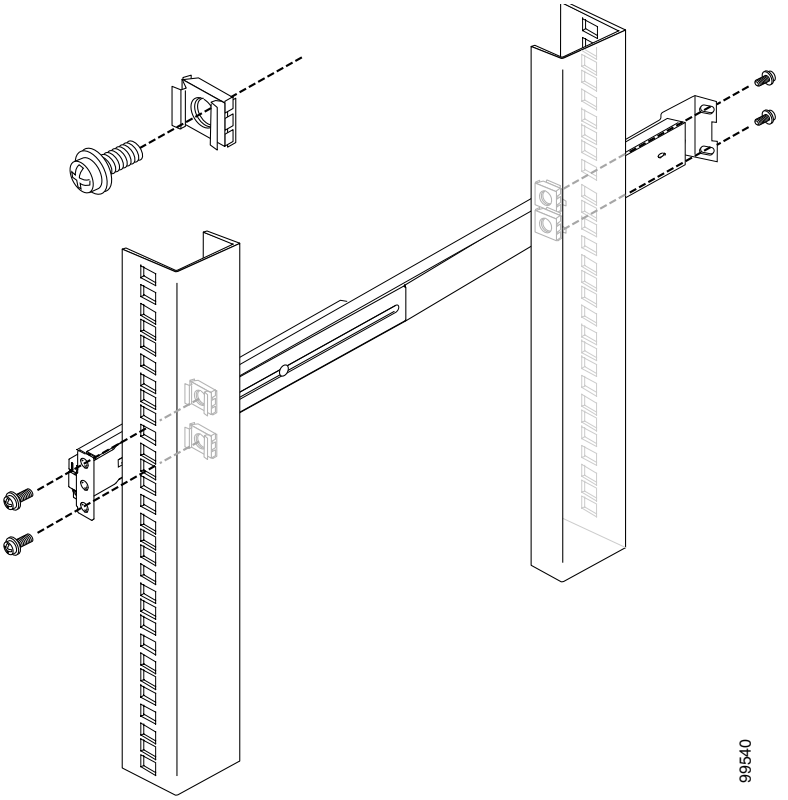
Figure 3-4 Attaching Front Rail to the Rack



Note The left side of the rail is for the cable arm.

e. See Figure 3-5. Attach the back end of the rail to the rack.

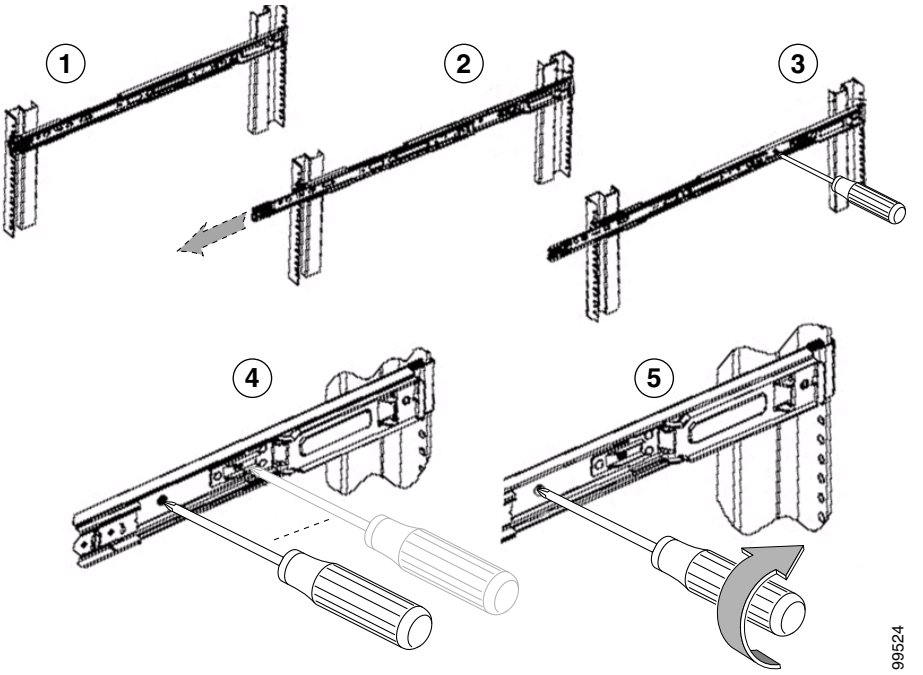
Figure 3-5 Attaching Back Rail to Rack



f. Repeat this process with the other rail and rack assembly.

g. Extend the middle rail about 30 cm and fasten with screws. See Figure 3-6. Then, push the middle rail back into its original position.

Figure 3-6 Attaching Screws to Telescopic Rail

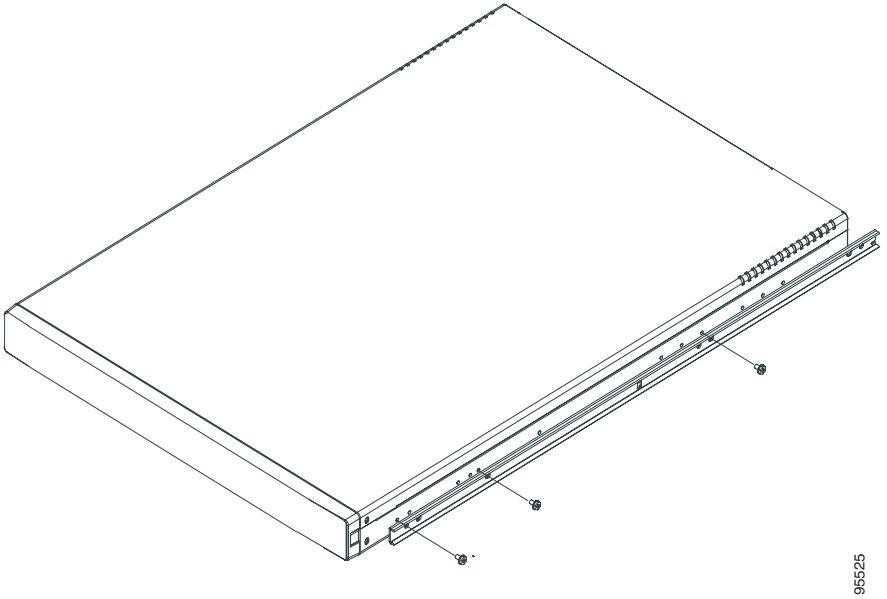


Note Leaving some play between the bracket and the rail until you install the rail into the rack will make affixing the rail to the rack easier. After the rail is attached to the rack, you can tighten the screws.

Step 2 Attach the chassis to the rack:

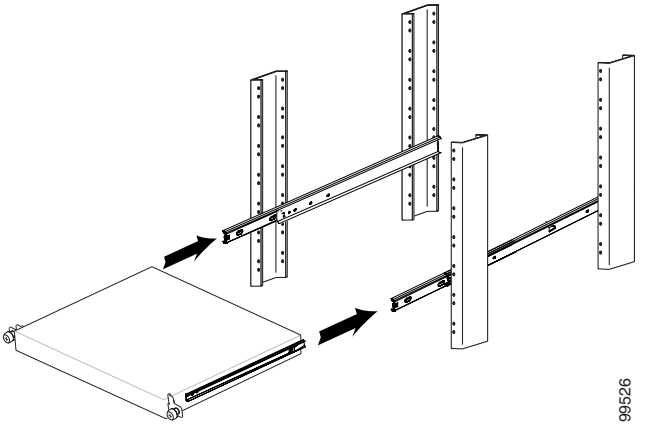
a. See Figure 3-7. Secure chassis to the inner rail using three screws. Repeat this process with the other server rail.

Figure 3-7 Attaching Chassis to Rail



b. See Figure 3-8. Insert the chassis in the rack.

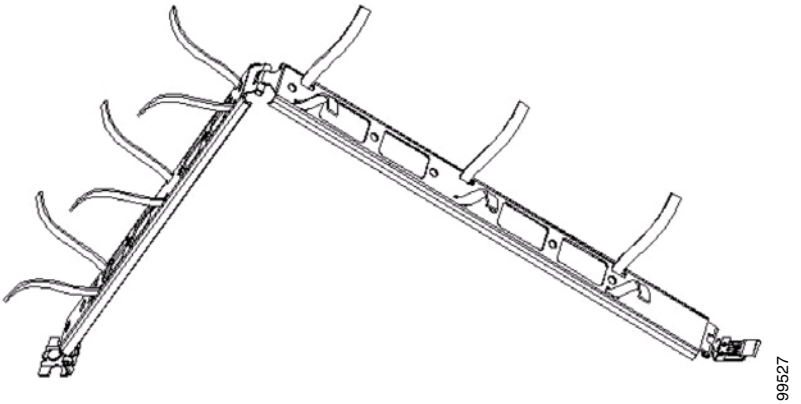
Figure 3-8 Sliding Chassis onto Rack



c. Slide the chassis back and forward several times. Fasten with all the screws described in Step 1d.

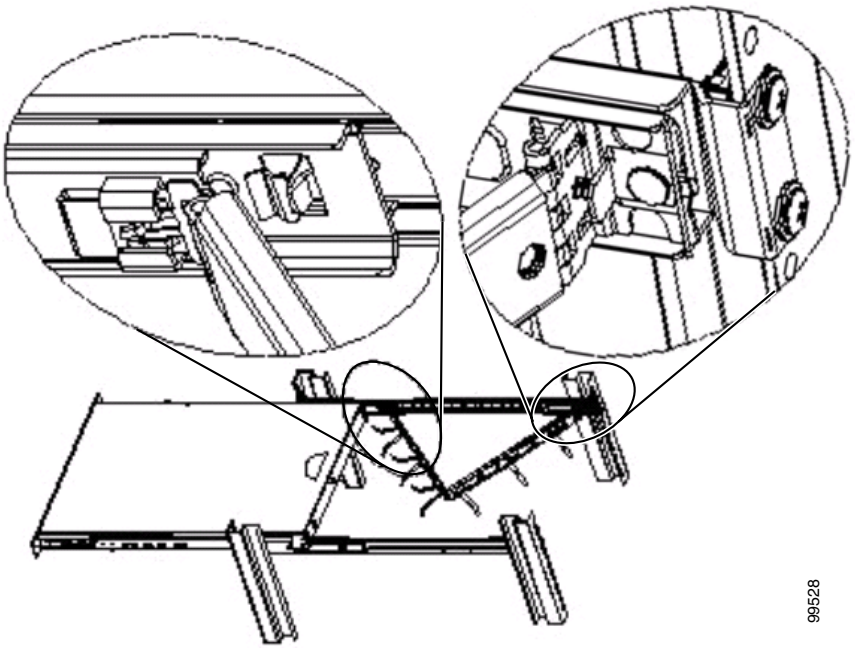
d. See Figure 3-9. Slide six Velcro strips into the holes of the management arm.

Figure 3-9 Attaching Velcro to Management Arm



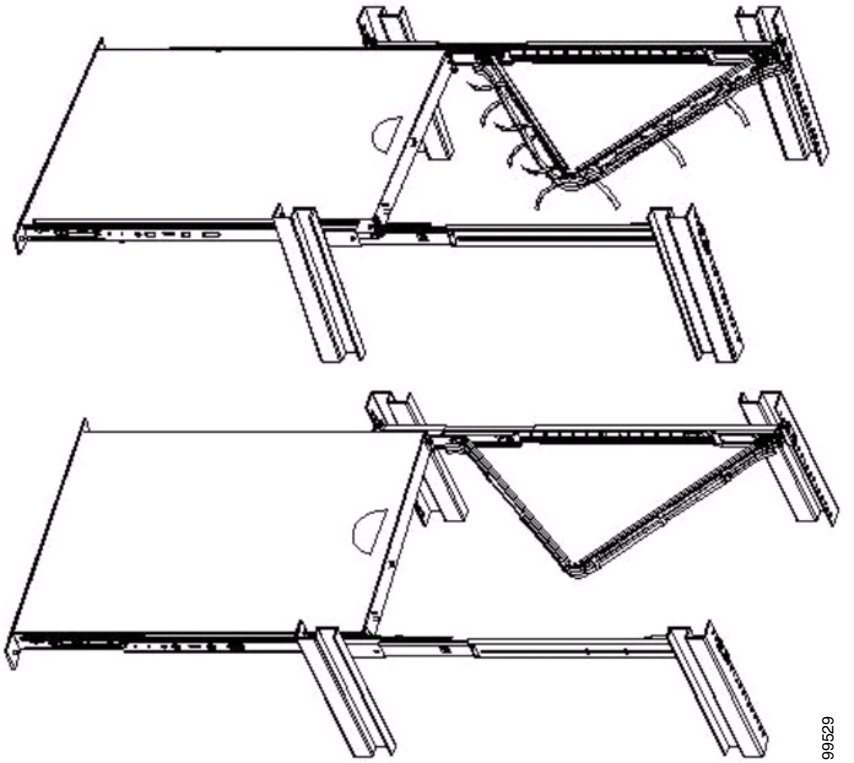
e. See Figure 3-10. Install the rear side of the cable management arm into the back rail until it snaps in the clip. Then install the front cable management arm into the inner rail until it snaps into the clip.

Figure 3-10 Attaching Management Arm



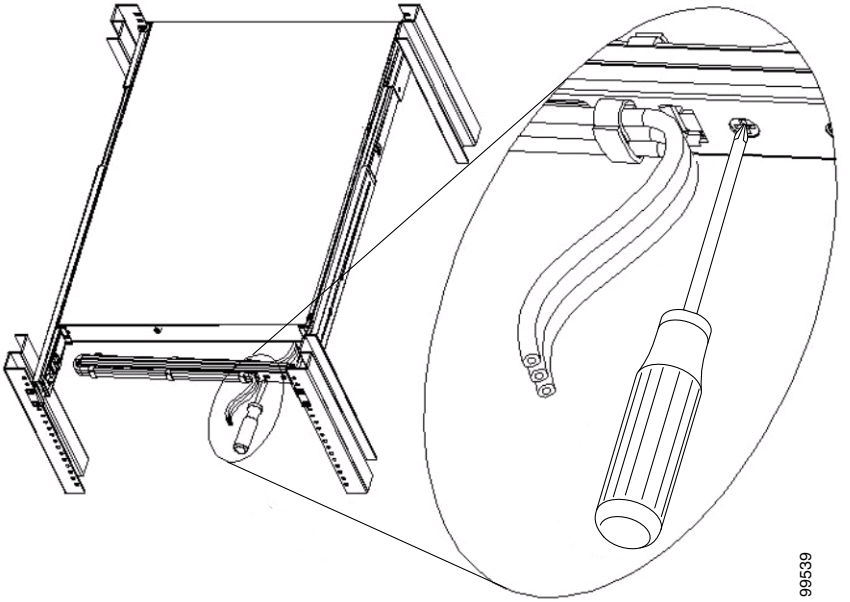
f. See Figure 3-11. Put cables into the cable management arm and use the Velcro to tighten the cable into the arm.

Figure 3-11 Installing Cable in Management Arm



g. See Figure 3-12. Push the server to the closed position. If the cable is too heavy to carry the server, use a screwdriver to adjust the cam so that the cable management arm is horizontal.

Figure 3-12 Fastening the Server into the Rack



Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A (U.S./CAN); 240 VAC, 10A (INTERNATIONAL).** Statement 1005

Connecting 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

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

To connect the cables:

Step 1 Plug the network connection into the Ethernet 0 port. See Figure 1-2 on page 1-5 for the location of the Ethernet 0 port

Step 2 Connect a console to the console/serial port using the supplied serial cable and, if necessary, the DB-9-to-RJ-45 console adapter. See Figure 1-2 on page 1-5 for the location of the serial port.

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

Powering On the WLSE

To turn the WLSE's power on, press the power switch. To turn its power off, press and hold the power switch for at least four seconds. See Figure 1-1 on page 1-3 for the location of the power switch.

The system begins booting and sending messages to the console window. When the login prompt appears, you can configure the system.

Next Step—Configuration

Run the setup program and perform basic configuration—See Chapter 4, "Basic Setup—CiscoWorks 1105/1130/1130-19."

Basic Setup—CiscoWorks 1105/1130/1130-19

This chapter describes how to run the setup program and perform basic configuration for WLSE 2.7 software.

Initial Setup Quick Reference

Table 4-1 provides a high-level overview of the basic initial setup of the WLSE.

Table 4-1 Initial Setup Quick Reference

Task	References
1. Run the setup program.	Configuring the WLSE's Network Information, page 4-2
2. Configure DNS, if necessary.	Configuring Name Resolution, page 4-6
3. Verify the configuration.	Verifying the Configuration, page 4-7
4. Configure the web browser.	Configuring the Web Browser, page 4-8
5. Log in and verify connectivity.	Logging into the Web Interface and Verifying Connectivity, page 4-11
6. Add additional users.	Adding Users, page 4-12

Configuring the WLSE's Network Information

Use the setup program to configure the WLSE when you boot it for the first time, and after erasing the configuration.

Guidelines for Using the Setup Program

When using the setup program:

- Press the **Backspace** or **Delete** key to delete characters when entering a response to a prompt.
- You cannot edit a response after you press the **Enter** key. You can use CLI commands to change some responses after running setup; see Changing the Configuration After Running Setup, page 4-5.
- 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 4-3 and Table 4-3 on page 4-4 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 serial/console port on the back panel.

- For the CiscoWorks 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 CiscoWorks 1130 or 1130-19, use the serial port on the back panel.

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

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:` `confirm password:`	Sets the password for the default user **admin**. Characters you type do not appear on screen. **Note** Default user **admin** is reserved and cannot be deleted or changed. You can use the admin password to log into the Web interface and and to connect via Telnet/SSH. Password length is unlimited, and you can use the alphanumeric characters (A-Z, a-z, 0-9) plus the underscore(_). Passwords are case sensitive.	wq1Cvu2pl
`eth0 IP address:`	IP address of Ethernet 0 interface.	209.165.200.224
`eth0 network mask:`	Network mask of Ethernet 0 interface.	255.255.255.224
`default gateway IP address:`	IP address of default router.	209.165.200.224

Table 4-2 General Configuration (continued)

Prompt	Response Description	Sample Response
`DNS server IP address:`	IP address of DNS server for name/address resolution. The setup program does not validate the IP address you enter. If you are not using a DNS server, see Configuring the WLSE Without a DNS Server, page 4-6 before proceeding.	209.165.201.1
`Would you like to save this configuration? [yes]:`	• Enter **yes** to save the configuration. The configuration is saved and system reboots. • Enter **no** to exit without saving configuration and run setup program again.	

Step 5 Answer the next set of prompts to create a self-signed certificate as described in Table 4-3. 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). To make changes in the certificate after running setup, see Changing the Configuration After Running Setup, page 4-5.

The certificate expires after one year. To obtain a permanent, signed certificate, see the SSL instructions in the online help or in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

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`	Unit of the company that is using the WLSE.	Webserver Team
`Common Name`	Fully qualified domain name (FQDN).	www.snakeoil.com
`Email Address`	Email address.	www@snakeoil.com

Step 6 After you finish configuring the WLSE, 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 CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

Note You can also set up the mail server after you log in to the Web interface. See the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

Changing the Configuration After Running Setup

To change the information in the setup configuration, use the following CLI commands at any time. For more information about CLI commands, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

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 CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

If you are using a DNS server, register the WLSE 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 4-2, 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 CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

Verifying the Configuration

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

For more information on the CLI commands used in the following procedure, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

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 selecting **Administration > Appliance > Security > SSH and Telnet**. Then select **enable** and click **Configure** to save the change.

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

nslookup *dns-name*

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

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

ping *ip-address*

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

Step 4 Enter the **show config** command to verify that the configuration is as you expected. For more information on this command, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

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, page 4-8
- Configuring Internet Explorer, page 4-9
- Configuring Netscape Navigator, page 4-10

Supported Browsers

Before connecting to the WLSE web interface, make sure you are using a supported browser and the browser is properly configured. The supported browsers for WLSE 2.7 are listed in Table 4-4 on page 4-9. Use the procedures in Configuring Internet Explorer, page 4-9 or Configuring Netscape Navigator, page 4-10 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, Windows NT, and Windows XP	Japanese Microsoft Internet Explorer 6.0 with Service Pack 1 Japanese Netscape Navigator 7.02
Solaris 8 and 9	Netscape Navigator 7.01
Java Plug-in	1.4.1 **Note** Java Plug-in is required for some WLSE functions.

Configuring Internet Explorer

To configure Internet Explorer 6.0, perform the following steps:

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

Step 2 Enable JavaScript:

a. Select **Security.**

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

c. Scroll to Scripting and select the following:

- Select Enable for Active scripting.
- Select Enable for Allow paste operations via script.
- Select Enable for **Scripting of Java applets**.

d. Click **OK**.

Step 3 Configure the browser to accept all cookies:

a. Select **Privacy**.

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

c. Click **OK**.

Step 4 Change the default font to improve readability:

a. Select **General**. Then 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 5 Disable caching:

a. Select **General**. Then s elect **Settings**.

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

Step 6 Click **OK**.

Note Windows XP does not come with the Java Plug-in installed on Internet Explorer 6.0. This causes problems when upgrading a WLSE 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 CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

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**.

Note Some fonts do not change after you use this option.

Step 5 Disable caching:

a. Expand Advanced and click Cache. If no subcategories are listed, double-click Advanced to expand the list.

b. Under "Compare the page in the cache to the page on the network," select "Every time I view the page."

Logging into the Web Interface and Verifying Connectivity

Note Disable pop-up blocker software while using the WLSE web interface.

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.

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 CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

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—Set Up Devices and Configure Device Management

The next steps are to:

- Prepare devices for management—see Chapter Chapter 5, "Setting Up Devices—CiscoWorks 1105/1130/1130-19."
- Configure device management on the WLSE—Chapter 6, "Setting Up Discovery and Device Management—CiscoWorks 1105/1130/1130-19."

Setting Up Devices—CiscoWorks 1105/1130/1130-19

You must set up devices before the WLSE can discover and manage them and before you can use WLSE features such as monitoring, reporting, configuration, firmware upgrade, and radio management. This section describes initial setup tasks for the following devices:

- Non-IOS access points and bridges—See Setting Up Non-IOS Access Points and Bridges, page 5-1
- IOS access points and bridges—See Setting Up IOS Access Points, page 5-4
- Routers and switches—See Setting Up Routers and Switches, page 5-24
- AAA servers—Setting Up AAA Servers, page 5-25

Setting Up Non-IOS Access Points and Bridges

This section provides setup procedures to prepare non-IOS access points for basic network management by the WLSE. You can perform initial setup in two ways:

- Open a web browser session on each access point—See Set Up Using the Web Interface, page 5-2.
- Use the WLSE startup configuration option for first-time device configuration and apply a configuration template to a number of access points—See Set Up Using a WLSE Configuration Template, page 5-4.

After discovering and managing devices, you can use WLSE configuration templates for configuration changes—See the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

Set Up Using the Web Interface

To use this method, you must first configure each access point or bridge for web browsing.

Log in to the Web interface of the AP to be configured and set the following parameters.

Table 5-1 Set Up Procedures for Non-IOS Access Points and Bridges

Tasks	Procedure	Notes
1. Enable Cisco Discovery Protocol (CDP).[1]	1. In the Summary Status page, click **Setup**. 2. Under Services: Cisco Services, click **Cisco Discovery Protocol** and select Enabled. 3. Click **Apply** or **OK**.	Required for the WLSE to use CDP to discover the device. If you are not using CDP, add all APs as seed devices or import devices. See Discovering Devices, page 6-7.
2. Enable SNMP.	1. In the Summary Status page, click **Setup**. 2. Under Services, click **SNMP**. 3. Select Enabled. 4. (Optional) Enter a System Name, System Location, and System Contact. 5. Click **Apply** or **OK**.	SNMP is required for the WLSE to discover devices, populate reports, transfer configuration information to devices, and upgrade device firmware. Setting the system name, system contact, and system location ensures that this information is included in device detail displays.

Table 5-1 Set Up Procedures for Non-IOS Access Points and Bridges (continued)

Tasks	Procedure	Notes
3. 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** or select an existing user. 4. Check all capabilities. **Note** Ident privileges are required only for APs that are running a firmware version earlier than 12.01(T). 5. Click **Apply** or **OK**.	The username is the AP's read/write community, which is required for discovery, reports, and configuration and firmware jobs.[2] You must also enter all AP community strings on the WLSE. See Enter SNMP Community Strings for All Managed Devices, page 6-2.
4. Add an HTTP user and enable the User Manager.[3] You can use the same user that you created in Task 3, if the user has write, firmware, admin, and ident capabilities.	1. In the Summary Status page, click **Setup**. 2. Click **Security**. 3. Click **User Information**; then click **Add New User** or select an existing user. 4. Enter a username and password and select Firmware; then click **Apply**. 5. Return to the Security Setup page and click **User Manager**. 6. Select **Enabled**; then click **Apply** or **OK**.	Allows configuration uploads from the WLSE to access points. You must also enter all AP HTTP users and passwords on the WLSE. See Enter HTTP Credentials for Non-IOS Access Points, page 6-3.
5. If you will use HTTP to initiate configuration or firmware downloads, select TFTP as the transfer protocol between the WLSE and APs.	1. In the Summary Status page, click **Setup**. 2. Under Services, click **FTP**. 3. 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 and firmware changes to access points. Selecting the WLSE as the TFTP server is not required if you only use SNMP for configuration and firmware.

1. Do not run CDP on radio ports.
2. For example, if the AP has a user "lab" with password "cisco", its SNMP credential is lab::10:1:::lab. Its HTTP username and password are lab/cisco. If the SNMP credential is set incorrectly, jobs will fail.
3. You can use a non-standard HTTP port. If HTTP browsing is not enabled, you must enable it. Enter the console and navigate to Security > Web Server. Enable Allow Non-Console Browsing.

Set Up Using a WLSE Configuration Template

You can perform initial configuration on access points by using the WLSE's startup template feature. Startup configuration works in conjunction with a DHCP server. The access points get their IP addresses from the DHCP server. If you prefer static IP addressing, you can either configure the DHCP server like a BOOTP server (using MAC address-to-IP address mapping) or configure the static IP address individually on each access point afterwards.

For information on using a startup template, see the online help or the "Managing Device Configuration" chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

Setting Up IOS Access Points

This section provides:

- Procedures to prepare IOS access points for basic network management by the WLSE—See Basic Network Management Setup—IOS Devices, page 5-4.
- Procedures to prepare IOS access points and the WLSE for participation in the Cisco Structured Wireless-Aware Network (SWAN)—See Radio Management Setup—IOS Devices, page 5-10.

Basic Network Management Setup—IOS Devices

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

- Log into each device by using Telnet or SSH and use the device's CLI commands—See Using the AP CLI for Network Management Setup, page 5-5.
- Log into each device's Web interface—See Using the AP Web Interface for Network Management Set Up, page 5-7.
- Use the WLSE's automatic configuration option for first-time device configuration and applying a configuration template to a number of access points—See Chapter 7, Managing Device Configuration, in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

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

After discovering and managing devices, you can use WLSE configuration templates for configuration changes—See the online help or the "Using IOS Templates" chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

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

Using the AP CLI for Network Management Setup

To configure IOS devices by using the device CLI:

Procedure

Step 1 Access the device CLI via Telnet, SSH, or the console.

Step 2 Enter configuration mode.

Step 3 Enable Cisco Discovery Protocol (CDP) by entering the following commands for each interface that will participate in CDP. Do not enable CDP on radio interfaces.

```
configure terminal
interface interface
cdp run
```

where *interface* is the name of the interface; for example FastEthernet0.

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

Note If you do not want to use CDP, you can add all access points as seeds or import devices. For more information, see Discovering Devices, page 6-7.

Step 4 To configure SNMP, enter the following commands in the sequence shown. The first command includes the ISO view. The read-only community string, is required for discovery and the fault and report features on the WLSE. The read/write community string is required for AP firmware management, AP configuration, and all radio-management functions (client walkabout, radio scanning, and so on).

a. Include the ISO view:

```
snmp-server view iso iso included
```

a. Configure the read-only community:

```
snmp-server community ro_ommunity_string view iso ro
```

b. Configure the read/write community:

```
snmp-server community rw_community_string view iso rw
```

Note The community strings must also be entered on the WLSE. See Enter SNMP Community Strings for All Managed Devices, page 6-2.

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

Step 5 (Optional) It is useful to set the system name, contact, and location SNMP variables to make the device more manageable. Use the following commands:

```
configuration terminal
hostname access_point
snmp-server location AP_location
snmp-server contact AP_contact
```

where *access_point* is the system name, *AP_location* is its location, and *AP_contact* is the name of the contact person.

Step 6 You can use either Telnet or SSH to push configuration templates to IOS access points. To use templates to configure IOS access points, you must configure either Telnet or SSH or both, as follows.

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

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

  The following commands are recommended, but optional:

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

- To configure Telnet, enter the following commands:

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

  The following commands are recommended, but optional:

  ```
  width 80
  length 24
  ```

Step 7 Exit global configuration mode, then enter the following command:

```
write memory
```

Using the AP Web Interface for Network Management Set Up

To configure IOS devices by using the device Web interface:

Procedure

Step 1 Log into the Web interface of the access point.

Step 2 To enable CDP, select **SERVICES** from the menu, then click **CDP**:

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

b. Click **Apply**.

Note If you do not wish to use CDP, you can add all access points as seeds or import devices. For more information, see Discovering Devices, page 6-7.

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

- To enable and configure SSH (secure shell protocol), enter the following:
  1. Select **SERVICES > Telnet/SSH**.
  2. Enable **Secure Shell**.
  3. Enter a System Name.
  4. Enter a Domain Name (for example, cisco.com).
  5. (Optional) Enter the RSA key size.
  6. (Optional) Enter the Authentication Timeout.
  7. (Optional) Enter Authentication Retries.
  8. Click **Apply**.
- To enable and configure Telnet:
  1. Select **SERVICES > Telnet/SSH**.
  2. Enable **Telnet**.
  3. (Optional) Enable **Teletype**.
  4. Enter the number of Columns.
  5. Enter the number of Lines.
  6. Click **Apply**.

Step 4 To enable SNMP:

a. Select **Services > SNMP**.

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

c. Enter the System Name (sysName), System Location (sysLocation), and System Contact (sysContact).

d. Click **Apply**.

Step 5 In the SNMP Request Communities section, enter a read-only community string. This community string is required for discovery and the fault and report features.

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

b. Enter `iso` in the Object Identifier field.

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

c. Select **Read-Only.**

d. Click **Apply**.

Step 6 In the SNMP Request Communities section, enter a read/write community string. This community string is required for all radio-management features.

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

b. Select **Read-Write**.

c. Enter `iso` in the Object Identifier field.

d. Click **Apply**.

Step 7 The community strings created in Steps 5 and 6 must be entered on the WLSE before the device can be discovered and the other WLSE features can be used. For more information, see Enter SNMP Community Strings for All Managed Devices, page 6-2.

Using WLSE Configuration Templates for Network Management Set Up

You can perform initial configuration by using the WLSE's startup template feature. For information on using a startup template, see the online help or the "Managing Device Configuration" chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

Radio Management Setup—IOS Devices

Note Make sure you also configure all access points for basic network management. See Basic Network Management Setup—IOS Devices, page 5-4.

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

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

This section contains the following information:

About WDS Devices

The device that supplies WDS can be either one of the following:

- A Cisco Aironet 1100 or 1200 series access point

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

- A Wireless LAN Services Module (WSM)

  Each WSM can support multiple AP subnets, as long as all of the subnets are served by the switch in which the WSM is installed.

About Configuring Authentication

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

- Local authentication on a WDS device. See Using Access Points as WDS Devices, page 5-12.
- AAA servers that you have already configured, or you can configure servers as described in Setting Up AAA Servers, page 5-25.

In addition, server groups must be created on the WDS access points for:

- Infrastructure authentication

  For information on creating server groups for infrastructure APs, see Using Access Points as WDS Devices, page 5-12.

- Client authentication

  For information on creating server groups for client authentication, see the AP documentation.

Radio Management Setup Quick Reference

Table 5-2 lists the high-level setup tasks and sections in this document where you can find detailed instructions.

Table 5-2 Radio Management Setup Tasks Quick Reference

Task	References
Configure WDS devices	Using Access Points as WDS Devices, page 5-12 Using a Wireless LAN Services Module (WSM) as the WDS Device, page 5-18
Configure infrastructure access points to authenticate to a WDS device	Configuring Infrastructure Access Points to Register with WDS Access Points, page 5-18 Configuring Infrastructure Access Points to Register with a Wireless LAN Services Module (WSM), page 5-20
Configure access points to be scanning-only APs	Configuring Scanning APs, page 5-20
Configure the WLSE with WLCCP credentials	Configuring the WLSE, page 5-22
Define authentication servers	About Configuring Authentication, page 5-11
Confirm the configuration	Confirming the Configuration, page 5-22

Using Access Points as WDS Devices

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

WDS must be active on an access point in each subnet in which APs are placed; you can also define backup WDS access points in each AP subnet. Configuring WDS requires:

- Defining the AAA servers and server groups that the WDS will use to LEAP authenticate infrastructure access points and the WLSE.
- Enabling WDS and set WDS priorities.
- Entering the WNM IP address.

There are three ways to configure WDS access points:

- Use the access point web interface—See Using the Web Interface to Configure WDS Points, page 5-13.
- Use the access point CLI interface—See Using the CLI Interface to Configure WDS Access Points, page 5-14.
- Use a WLSE configuration template—Using a WLSE Configuration Template to Configure WDS Access Points, page 5-16.

Note If you are using redundant WLSEs for high availability, use the VIP address as the IP address of the WLSE when configuring WDS. For more information on redundancy, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

Using the Web Interface to Configure WDS Points

To configure WDS access points by using the web interface:

Step 1 Log in to an AP that will serve as a WDS device.

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

Step 3 Select the General Set-Up tab.

Step 4 To enable WDS, select **Use this AP as Wireless Domain Services**.

Step 5 Enter a value between 1 and 255 in the **Wireless Domain Services** Priority field.

The priority value is used to determine which AP will be the active WDS AP when multiple APs are configured to run WDS. The highest priority is 255.

Step 6 Configure the Wireless Network Manager (WNM) options:

a. Select **Configure Wireless Network Manager.**

b. Enter the IP address of your WLSE in the **Wireless Network Manager IP Address** field.

c. Click **Apply**.

Step 7 Define the AAA server group(s) for LEAP authenticating the WLSE and the infrastructure access points participating in SWAN:

a. Select the Server Groups tab.

b. Enter a server group name.

c. From the **Priority** lists, select the appropriate AAA servers.

   If no AAA servers have been entered, click **Define Servers** to add the servers, then select the appropriate servers. Consult the AP online help for assistance in entering AAA servers into the AP.

d. Under **Use Group For**, select **Infrastructure Authentication**.

Step 8 Configure the WDS AP to authenticate itself to the WDS so that it can participate in the SWAN hierarchy:

a. Select **Wireless Services > AP**.

b. Select **Enable**.

c. Enter a username and password that can be LEAP authenticated by the AAA servers in the infrastructure server group.

Step 9 To commit the configuration, click **Apply**.

Note To configure authentication for wireless clients, see the AP documentation.

Using the CLI Interface to Configure WDS Access Points

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

The key steps in configuring the WDS are:

- Configure AAA servers to authenticate SWAN infrastructure access points and the WLSE.
- Configure WDS.
- Configure the WNM.

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

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

Step 2 Turn on AAA services:

```
aaa new-model
```

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

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

Step 4 Define a server group for infrastructure authentication:

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

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

Step 6 Configure the AP to run WDS:

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

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

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

```
wlccp wnm ip address wlse_ip_address
```

where *wlse_ip_address* is the address of the WLSE.

Step 8 Configure the server group the WDS will use to LEAP authenticate SWAN infrastructure access points. Use the server group name that you created in Step 4.

```
aaa authentication login named_authentication_list group
server_group_name

wlccp authentication-server infrastructure named_authentication_list
```

Step 9 The WDS access point must also register and authenticate itself to the WDS to participate in the SWAN hierarchy; therefore, the WDS AP is also an infrastructure AP. To configure the WDS access point as an infrastructure access point:

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

Note To configure authentication for wireless clients, see the relevant AP documentation.

Using a WLSE Configuration Template to Configure WDS Access Points

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

The major configuration steps are:

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

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

Step 1 Log in to the WLSE web interface.

Step 2 Select **Configure > Templates.**

a. Enter a template name, selecting IOS as the template type.

b. Click **Create New**.

Step 3 Enter the AAA servers for LEAP authenticating the infrastructure access points and the WLSE to the WDS, and the AAA servers for authenticating wireless client devices:

a. Select **Security > Server Manager**.

b. In the Corporate Servers section, for each server, enter the IP address, select RADIUS, and enter the shared secret.

c. Click **Save**.

Step 4 Select **Wireless Services > WDS** to configure the WDS parameters.

In the Global Properties section:

a. Select **Enable**.

b. Enter the Wireless Domain Services priority. This value determines which access point will serve as the active WDS when multiple access points are configured to run WDS on the same subnet. Valid priority values are 1-255, with 255 being the highest.

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

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

In the Server Groups section:

a. Enter one or more server names or server IP addresses.

b. Under Use Group For, select Infrastructure Authentication.

c. Click **Save**.

Step 6 The WDS access point must also register and authenticate itself to the WDS to participate in the SWAN hierarchy, so the WDS AP is also an infrastructure AP. To authenticate and register the WDS AP as an infrastructure AP:

a. Select **Wireless Services > AP Configuration**.

b. Select **Enabled** as the Wireless Services option.

c. Enter a username and password that can be LEAP authenticated by the AAA servers in the infrastructure server group.

Step 7 (Optional) Select **Preview** to see a preview of the configuration template.

Step 8 Select **Save**, then click the **Save** button.

Step 9 Select **Yes** to apply the template immediately or select **No** to save the template. For information on configuration jobs, see the "Managing Device Configuration" chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

Note To configure authentication for wireless clients, see the relevant AP documentation.

Using a Wireless LAN Services Module (WSM) as the WDS Device

If you are using a WSM to provide WDS, instead of using APs for WDS, follow the procedures in the WSM documentation to configure it for WDS. Use the IP address of the WLSE as the WNM IP address.

Configuring Infrastructure Access Points to Register with WDS Access Points

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

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

There are three ways to configure infrastructure access points to register with WDS:

- Using the access point web interface—See Using the Web Interface to Configure Infrastructure APs, page 5-18.
- Using the access point CLI interface—See Using the Command Line Interface to Configure Infrastructure APs, page 5-19.
- Using a WLSE configuration template—See Using a WLSE Configuration Job to Configure Infrastructure APs, page 5-19.

Using the Web Interface to Configure Infrastructure APs

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

Step 1 Log in to the AP's web interface.

Step 2 Select **Wireless Services > AP**.

Step 3 Select **Enabled**.

Step 4 Enter the username and password for authenticating the infrastructure AP to the WDS.

Step 5 Click **Apply**.

Using the Command Line Interface to Configure Infrastructure APs

To use the command line interface to configure infrastructure APs:

Step 1 Log in to the AP's CLI.

Step 2 Enter the following command:

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

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

Using a WLSE Configuration Job to Configure Infrastructure APs

The WLSE can configure multiple infrastructure APs in a single job. To configure infrastructure APs using the WLSE, create a configuration template using the template creation wizard, then apply the template in a configuration job. For more information about using the template creation wizard and the configuration job interface, see the online help or the "Using IOS Templates" chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

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

Step 1 Log in to the WLSE web interface.

Step 2 Select **Configure > Templates**.

Step 3 Select **Wireless Services > AP Configuration**.

Step 4 Select **Enabled**.

Step 5 Enter the username and password for LEAP authenticating infrastructure APs to the WDS.

Step 6 Create a configuration job to apply the template to the appropriate devices. For information on configuration jobs, see the online help or the "Managing Device Configuration" chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

Configuring Infrastructure Access Points to Register with a Wireless LAN Services Module (WSM)

To configure infrastructure access points to register with a Wireless LAN Services Module, see the relevant AP and WSM documentation on Cisco.com.

Configuring Scanning APs

This section describes how to configure an AP as a scanning-only AP. After you have performed the basic network management configuration and radio management configuration described in this chapter, perform the additional configuration described in this section to make the AP into a scanning AP. Scanning APs can detect and report "bug-lighted" clients (clients associated to unauthorized access points). Scanning APs do not accept client associations.

For more information on scanning APs and other requirements for using scanning APs with a WLSE, see the online help "Radio Management" chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

Note Radio scanning requires a read/write SNMP community string on APs. For more information, see Radio Management Setup—IOS Devices, page 5-10,

Table 5-3 on page 5-20 lists the high level tasks for setting up scanning APs.

Table 5-3 Setting Up Scanning APs Quick Reference

Task	References
1. Configure the scanning APs for basic management and radio management. • *Do not* configure VLAN/SSID on the scanning AP. • *Do not* configure the scanning AP as a WDS device.	Setting Up IOS Access Points, page 5-4
2. Configure the specific scanning AP parameters.	Configuring a Scanning AP—Using the AP CLI, page 5-21 Configuring a Scanning AP—Using a WLSE Configuration Template, page 5-21

Table 5-3 Setting Up Scanning APs Quick Reference

Task	References
3. Run inventory on the WLSE.	Run Inventory, page 5-21
4. Enable client registration scanning on the WLSE.	Enable Client Registration Scanning, page 5-21

Configuring a Scanning AP—Using the AP CLI

To configure an access point for scanning only, enter the following commands:

```
config t
int dot11 0 (for interface 0)
station-role scanner
```

Configuring a Scanning AP—Using a WLSE Configuration Template

To configure an access point for scanning only from a WLSE configuration template:

1. Select **Configuration > Templates > IOS > Basic Settings,** then select **Scanner Access Point**.
2. Select **Configuration > Templates > IOS > Network Interfaces**. Select a radio and select **Scanner Access Point**.

Run Inventory

Select **Administration > Devices > Discover > Inventory** and run inventory so the WLSE can update the role of the AP. The scanning APs will be listed in the WLSE's Scanning AP system group.

For more information, see the online help or the "Managing Devices" chapter of the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

Enable Client Registration Scanning

Select **Radio Management > Radio Monitoring** and enable Client Registration Scanning to detect bug-lighted clients.

For more information, see the online help or the "Radio Management" chapter of the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

Configuring the WLSE

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

- SWAN components communicate via a Cisco proprietary technology called WLCCP. You must enter the WLCCP username and password in the WLSE. This username and password is used to LEAP authenticate the WLSE to the WDS APs in the network. See Enter WLCCP Credentials for Wireless Domain Services (WDS), page 6-5.
- Enter the SNMP read-only and read/write communities for all managed IOS access points. See Enter SNMP Community Strings for All Managed Devices, page 6-2.
- Enter Telnet/SSH credentials for IOS access points. See Enter Telnet or SSH Credentials for IOS Access Points, page 6-4.

Confirming the Configuration

After you complete all the configuration procedures, you should confirm that the configuration is correct and that the SWAN components are communicating properly. Perform the following confirmation steps on the *active* WDS APs. There are two ways to confirm configuration:

- Using the Web interface—See Using the Web-based Interface to Validate the Configuration, page 5-23.
- Using the command-line interface—See Using the Command-Line Interface to Validate the Configuration, page 5-23.

Note To determine which WDS APs are actively providing WDS services, you can use the WDS Summary Report on the WLSE. For more information, see the online help or the "Reports" chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

Using the Web-based Interface to Validate the Configuration

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

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

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

Check for the following:

- The WDS Information section should display the device WDS state as ACTIVE.
- The WDS Registration and AP Information sections should show the correct number of APs (all of the infrastructure APs and the WDS AP).
- The Mobile Node Information section should display the wireless clients participating in SWAN.
- The Wireless Network Manager section should contain the WLSE IP address. If the WLSE authentication status is SECURITY KEYS SETUP, the WLSE is properly registered.

Using the Command-Line Interface to Validate the Configuration

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

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

Step 2 To validate the WDS configuration, enter:

```
show wlccp wds ap
```

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

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

```
show wlccp wnm status
```

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

Setting Up Routers and Switches

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

Configure each router and switch as shown in Table 5-4 on page 5-24.

Table 5-4 Setup Procedures for Routers and Switches

Task	Procedure	Notes
1. Enable CDP and verify that access points and bridges are visible from the router or switch.	1. In enable mode, verify that CDP is running on the device by using one of the following commands: • On IOS-based devices—**show cdp run**. • On Hybrid OS-based Catalyst switches—**show cdp**. 2. If CDP is not running, in global configuration mode, enter **cdp run** to enable CDP. 3. 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 5-4 Setup Procedures for Routers and Switches (continued)

Task	Procedure	Notes
3. (Optional) Set system name, contact, and location variables.	On IOS-based devices, enter configuration mode and use the following commands to set the system name, system contact, and system location: • **hostname** *name* • **snmp contact** *contact* • **snmp location** *location* On Hybrid OS-based Catalyst switches, enter enable mode and use the following commands to set the system name, system contact, and system location: • **set system name** *name* command. • **set system contact** *contact* • **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.

Setting Up AAA Servers

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

Note This section covers setting up an ACS server. To set up a CAR server, see the CAR documentation on Cisco.com.

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

To enable monitoring of an ACS server, you must:

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

Note If two Ethernet interfaces are configured with IP addresses on the WLSE, both addresses must be configured as clients on ACS server.

- Configure the WLSE to add information about servers. For more information, see Adding AAA Servers to the WLSE, page 6-6.

In addition to monitoring AAA servers, you can use an AAA server to authenticate to Wireless Domain Services (WDS) access points. To enable this authentication, make sure an AAA server is configured as described in this section, and configure WDS as described in Radio Management Setup—IOS Devices, page 5-10.

Procedure

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

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

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

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

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

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

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

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

Note If two Ethernet interfaces are configured with IP addresses on the WLSE, both addresses must be configured as clients on ACS server.

Field	Description
Client Hostname	WLSE hostname.
Client IP	WLSE IP address.[1]
Key	Secret key.[2]

1. If you are using redundant WLSEs, enter the VIP address. For more information about WLSE redundancy, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.
2. You will need this key when configuring the WLSE.

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

Step 8 If you are using this server for Wireless Domain Services (WDS) authentication, configure the server for simultaneous login sessions. See the ACS server documentation for details.

Step 9 Click **Submit** or **Submit+Restart**. A restart is required for the changes to take effect.

Setting Up Discovery and Device Management—CiscoWorks 1105/1130/1130-19

After setting up devices, you can discover and manage them. This section describes discovery and management configuration for WLSE 2.7.

Device Management Quick Reference

Table 6-1 provides a high-level overview of the tasks for discovering and managing devices. Detailed procedures are provided in this chapter.

Table 6-1 Quick Reference

Tasks	References
1. Add device credentials to the WLSE.	Adding Device Credentials to the WLSE, page 6-2
2. Add any AAA servers to be monitored.	Adding AAA Servers to the WLSE, page 6-6
3. (Optional) Set options for discovery and management.	Configuring Discovery Options, page 6-7
4. Discover or import devices.	Discovering Devices, page 6-7
5. Manage devices.	Managing Devices, page 6-13

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.
- For radio management, you must enter WLCCP credentials.

Enter SNMP Community Strings for All Managed Devices

SNMP community strings are used for discovery and for enabling WLSE features, such as AP configuration jobs and radio management. The community string must be set on each device, as described in Chapter 5, "Setting Up Devices—CiscoWorks 1105/1130/1130-19.". You can enter as many community strings on the WLSE as necessary.

Note If you are importing devices, you do not need to enter their community strings.The community strings will be imported along with the devices and will be listed in WLSE Communities screen, in which you can modify and delete strings as required. For more information, see Import Devices, page 6-11.

To configure community strings on the WLSE:

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

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

Step 2 To add an entry:

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

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

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

Step 3 To modify an entry:

a. Select the entry in the list of entries.

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

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

c. Click **Modify**.

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

Step 4 To delete an entry:

a. Select the entry in the list of entries.

b. Click **Delete**.

Note The default entry cannot be deleted.

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

Enter HTTP Credentials for Non-IOS Access Points

HTTP credentials are required for downloading configuration files to non-IOS access points and for uploading configuration from such access points. The same password must be set on each access point, as described in Table 5-1 on page 5-2. 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 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/SSH User/Password**.

Step 2 To add a username and password:

a. Enter the access point IP address or range of IP addresses that will use this username and these passwords.

b. Enter the username.

c. Enter the password and confirm it.

d. Enter the enable password and confirm it.

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

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

Enter HTTP Port Settings for IOS Access Points

HTTP 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)

To configure the WLSE to authenticate with WDS devices:

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**.

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 Setting Up AAA Servers, page 5-25.

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

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

Step 3 Complete the following:

Text Box	Description
Server Name	Hostname or IP address of an AAA server to be added. **Note** Depending on how your network is set up, the AAA server can be a Cisco Secure Access Control Server or a Cisco Access Registrar RADIUS server.
Server Port	Port on the server 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 **Save**.

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

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

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 CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

d. Click **Save**.

Step 2 To set up IP filters for limiting discovery to certain devices, select **Devices > Discover > DISCOVER > IP Filter Rules** and follow the instructions in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

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 6-8.

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

- Import devices from a file or from a CiscoWorks server—See Import Devices, page 6-11.

Note If WDS is configured on the subnet, CDP discovery proceeds automatically via WLCCP for the infrastructure access points. The access points must be properly configured. All access points will be used as seeds. The WDS must also be configured and in the managed state. For device configuration information, see Chapter 5, "Setting Up Devices—CiscoWorks 1105/1130/1130-19."

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 6-8.
- Modify the default CDP discovery schedule by scheduling a one-time job or repeated jobs—See Modify the CDP Discovery Schedule, page 6-10.

Run CDP Discovery Now

To run an immediate discovery, perform the following steps:

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

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

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

Step 4 Add community strings for all of the devices to be discovered if you have not already done so. For details on adding community strings, see Enter SNMP Community Strings for All Managed Devices, page 6-2. After adding community strings, click **Next**.

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

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

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

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

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

c. Click **Next**.

Step 6 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 7 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 > Discovery Wizard.**

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

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

Step 4 To modify the schedule:

a. Select the Start Date and Start Time from the pull-down lists.

b. To repeat discovery at a specified interval, select **Enable**. Then enter a number for the interval and select Minutes, Hours, Days, Weeks or Months from the pull-down list.

c. Click **Next**.

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

If you have not added community strings, you must add them now. For details on adding community strings, see Enter SNMP Community Strings for All Managed Devices, page 6-2. 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.

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

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

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

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

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

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

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

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

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 > Discovery Wizard.**

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

Step 3 Complete the Schedule Import from CiscoWorks dialog.

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

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

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

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

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

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

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

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

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

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

Managing Devices

After discovering or importing devices and verifying the results, 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. For information on setting the auto-manage option, see Configuring Discovery Options, page 6-7.

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

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

The Discovered Devices tree appears.

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

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

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

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

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

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.

Next Step

For information on advanced configuration and day-to-day operation of the WLSE, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7* or the WLSE online help.

Installing Software—CiscoWorks 1105/1130/1130-19

This section describes the options for updating the system software to WLSE 2.7.

Caution Always review the readme file that accompanies the upgrade image on Cisco.com before attempting to install the upgrade. The procedures might have changed after this document was printed. Some upgrades require different installation methods. 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:

Note You can downgrade to an earlier software version by using the recovery CD. See Upgrading from the Recovery CD, page A-11.

Note You cannot upgrade from pre-release software to the released version.

Upgrade Versions

You can upgrade directly to WLSE 2.7 as follows:

- From WLSE 2.0 to WLSE 2.7
- From WLSE 2.0.2 to WLSE 2.7
- From WLSE 2.5 to WLSE 2.7

If you are using an earlier version, such as 1.x or 1.3.x, and you want to upgrade directly to 2.7, see Upgrading from the Recovery CD, page A-11.

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 CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

Note You cannot restore a backup from a WLSE 1130-19 or WLSE 1130 to a WLSE 1105.

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 URL:

www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_upgrades_and_downloads.html

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

Normally, you can use any of the following upgrade methods:

- Upgrading by using the Web interface—see Upgrading by Using the Web Interface, page A-4.
- Upgrading by using the command line interface (CLI)—see Upgrading by Using the CLI, page A-7.
- Upgrading by using the recovery CD—see Upgrading from the Recovery CD, page A-11.

Upgrading by Using the Web Interface

This section contains the following topics:

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

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 A-2
2. Download software from Cisco.com.	Downloading the Upgrade Image, page A-2
3. Install software.	To install from the local repository, see Installing from the Local Repository, page A-4.
	To install from the remote repository, see Installing from a Windows Server, page A-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-2.7-K9.zip, the package name is WLSE-2.7-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 Plug-in 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 or if you log out from 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 A-8
  - Install the Software, page A-10
- Related CLI commands.

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 A-2
2. Download image to an FTP server.	Downloading the Upgrade Image, page A-2
3. Create repository.	Create the Repository, page A-8
4. Install upgrade.	Install the Software, page A-10

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 A-8
- Create a Repository on a Windows Server, page A-9

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-2.7-K9.zip, the package name is WLSE-2.7-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 A-10

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 A-10.

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

You can use this method to upgrade from 1.x versions or 2.0.x versions to 2.7.

You can also use the recovery CD to downgrade to an earlier version

Note You cannot restore a backup from a WLSE 1130-19 or WLSE 1130 to a WLSE 1105.

You can create a recovery CD by downloading the image from cisco.com at the following URL:

www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_upgrades_and_downloads.html

If you already have a recovery CD with the release of the WLSE software you want to install, you can use the CD to upgrade your WLSE. Two methods for upgrading from the Recovery CD are provided in this section:

- Reimaging the WLSE—Local Installation Method, page A-12
- Reimaging the WLSE—Remote Installation Method, page A-14

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, and you will have to replace the data by restoring a backup. For information on backups, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

Reimaging the WLSE—Local Installation Method

Note Although every effort has been made to validate the accuracy of the software version on the Recovery CD, you must review the WLSE's software versions on http://www.cisco.com and download any necessary software updates. See the Readme files included with the updates to perform the update procedure.

Caution This procedure will destroy all data and install a new image. You will need to replace the data by restoring a backup. For more information, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

To reimage your WLSE, perform the following steps:

Step 1 Connect a console to the WLSE's serial/console port:

- For the WLSE 1105, use the serial port on the front panel; do not use the serial port on the back panel for a console.
- For the WLSE 1130 or WLSE 1130-19, use the serial port on the back panel.

Step 2 Log in as the **admin** user, and enter the password created when the WLSE was configured.

Step 3 Put the Recovery CD in the WLSE's CD drive (on the front panel).

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

```
reload
```

Step 5 At the following prompt, enter **yes** to start the Recovery CD:

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

Caution If you do not want to re-image the WLSE, enter **rescue**. For more information about the rescue image, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

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

Step 7 At the following prompt, enter **yes**:

```
Do you wish to reload and start the install?(yes/[no]) yes
```

Result: The WLSE is re-imaged and reboots.

Step 8 When the Recovery CD ejects from the CD drive, remove it.

When the installation completes, the login prompt appears on the console.

Step 9 Restore the backup.

For information about restoring backups, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7* or the online help.

Reimaging the WLSE—Remote Installation Method

Note Although every effort has been made to validate the accuracy of the software version on the Recovery CD, you must review the WLSE's software versions on http://www.cisco.com and download any necessary software updates. See the Readme files included with the updates to perform the update procedure.

Caution This procedure will destroy all data and install a new image. You will need to replace the data by restoring a backup. For information on backups, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

To reimage your WLSE, perform the following steps:

Step 1 Insert the Recovery CD into the CD drive of a system running Microsoft Windows 2000.

Step 2 Double-click on the CD drive to display the contents of the Recovery CD.

Step 3 Double-click on the autorun.bat file.

A command prompt window appears and as well as a pop-up window displaying instructions for installing the Recovery CD.

Step 4 Follow the installation instructions in the pop-up window.

Note Make sure you keep both the command prompt window and pop-up window open until the installation finishes.

Step 5 Restore the backup.

For information about restoring backups, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

Technical Specifications—CiscoWorks 1130-19

Table B-1 provides the specifications for the CiscoWorks 1130-19 Wireless LAN Solution Engine.

Table B-1 Technical Specifications

Component	Specifications
Serial ports	Two 9-pin connectors
RJ-45 ports	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)

Table B-1 Technical Specifications (continued)

Component	Specifications
Operating relative humidity	8% to 80% (noncondensing) with a humidity gradation of 10% per hour
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

J

K

L

M

N

O

P

R

S

T

U

W