Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine

Software Release 2.13
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-7817476 =
Text Part Number: 78-17476-01B0

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 78-5235-03B0 is highlighted.

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

   c. Click **Go**.

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

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

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

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

      78-5236-01C0

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

      The Cisco warranty page appears.

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

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

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

Duration of Hardware Warranty

Ninety (90) days.

Replacement, Repair, or Refund Policy for Hardware

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

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

To Receive a Return Materials Authorization (RMA) Number

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

Complete the information below, and keep it for reference:

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

Supplemental License Agreement

SUPPLEMENTAL LICENSE AGREEMENT FOR CISCO SYSTEMS NETWORK MANAGEMENT SOFTWARE RUNNING ON THE CISCO 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 End User 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 End Use 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. When used below, the term "server" refers to central processor unit.

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. End User License Agreement.

Preface

This guyide contains both hardware installationa nd software setup instructions for the Wireless LAN Solution Engine (WLSE) and contains the following chapters and appendixes:

- Cisco 90-Day Limited Hardware Warranty Terms
- Supplemental License Agreement
- Product Overview
- Installing WLSE 1133 Hardware
- Setting Up the WLSE
- Setting Up Devices—Overview
- Setting Up Discovery and Device Management
- Technical Specifications for the WLSE 1133

Audience

This document is for system administrators who are responsible for installing and configuring internetworking equipment.

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

Conventions

This document uses the following conventions:

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

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

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

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

Note 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 1133 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.

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。

주의　중요 안전 지침

이 경고 기호는 위험을 나타냅니다. 작업자가 신체 부상을 일으킬 수 있는 위험한 환경에 있습니다. 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 사고를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾으십시오.

이 지시 사항을 보관하십시오.

تحذير　إرشادات الأمان الهامة

يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات.
قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في أخر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز. قم بحفظ هذه الإرشادات

Upozorenje

VAŽNE SIGURNOSNE NAPOMENE

Ovaj simbol upozorenja predstavlja opasnost. Nalazite se u situaciji koja može prouzročiti tjelesne ozljede. Prije rada s bilo kojim uređajem, morate razumjeti opasnosti vezane uz električne sklopove, te biti upoznati sa standardnim načinima izbjegavanja nesreća. U prevedenim sigurnosnim upozorenjima, priloženima uz uređaj, možete prema broju koji se nalazi uz pojedino upozorenje pronaći i njegov prijevod.

SAČUVAJTE OVE UPUTE

Upozornění

DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY

Tento upozorňující symbol označuje nebezpečí. Jste v situaci, která by mohla způsobit nebezpečí úrazu. Před prací na jakémkoliv vybavení si uvědomte nebezpečí související s elektrickými obvody a seznamte se se standardními opatřeními pro předcházení úrazům. Podle čísla na konci každého upozornění vyhledejte jeho překlad v přeložených bezpečnostních upozorněních, která jsou přiložena k zařízení.

USCHOVEJTE TYTO POKYNY

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

Αυτό το προειδοποιητικό σύμβολο σημαίνει κίνδυνο. Βρίσκεστε σε κατάσταση που μπορεί να προκαλέσει τραυματισμό. Πριν εργαστείτε σε οποιοδήποτε εξοπλισμό, να έχετε υπόψη σας τους κινδύνους που σχετίζονται με τα ηλεκτρικά κυκλώματα και να έχετε εξοικειωθεί με τις συνήθεις πρακτικές για την αποφυγή ατυχημάτων. Χρησιμοποιήστε τον αριθμό δήλωσης που παρέχεται στο τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή.

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

סימן אזהרה זה מסמל סכנה. אתה נמצא במצב העלול לגרום לפציעה. לפני שתעבוד עם ציוד כלשהו, עליך להיות מודע לסכנות הכרוכות במעגלים חשמליים ולהכיר את הנהלים המקובלים למניעת תאונות. השתמש במספר ההוראה המסופק בסופה של כל אזהרה כד לאתר את התרגום באזהרות הבטיחות המתורגמות שמצורפות להתקן.

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА

Симболот за предупредување значи опасност. Се наоѓате во ситуација што може да предизвика телесни повреди. Пред да работите со опремата, бидете свесни за ризикот што постои кај електричните кола и треба да ги познавате стандардните постапки за спречување на несреќни случаи. Искористете го бројот на изјавата што се наоѓа на крајот на секое предупредување за да го најдете неговиот период во преведените безбедносни предупредувања што се испорачани со уредот.

ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie

WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA

Ten symbol ostrzeżenia oznacza niebezpieczeństwo. Zachodzi sytuacja, która może powodować obrażenia ciała. Przed przystąpieniem do prac przy urządzeniach należy zapoznać się z zagrożeniami związanymi z układami elektrycznymi oraz ze standardowymi środkami zapobiegania wypadkom. Na końcu każdego ostrzeżenia podano numer, na podstawie którego można odszukać tłumaczenie tego ostrzeżenia w dołączonym do urządzenia dokumencie z tłumaczeniami ostrzeżeń.

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie **DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY**

Tento varovný symbol označuje nebezpečenstvo. Nachádzate sa v situácii s nebezpečenstvom úrazu. Pred prácou na akomkoľvek vybavení si uvedomte nebezpečenstvo súvisiace s elektrickými obvodmi a oboznámte sa so štandardnými opatreniami na predchádzanie úrazom. Podľa čísla na konci každého upozornenia vyhľadajte jeho preklad v preložených bezpečnostných upozorneniach, ktoré sú priložené k zariadeniu.

USCHOVAJTE SI TENTO NÁVOD

Opozorilo **POMEMBNI VARNOSTNI NAPOTKI**

Ta opozorilni simbol pomeni nevarnost. Nahajate se v situaciji, kjer lahko pride do telesnih poškodb. Preden pričnete z delom na napravi, se morate zavedati nevarnosti udara električnega toka, ter tudi poznati preventivne ukrepe za preprečevanje takšnih nevarnosti. Uporabite obrazložitveno številko na koncu posameznega opozorila, da najdete opis nevarnosti v priloženem varnostnem priročniku.

SHRANITE TE NAPOTKE!

警告 重要安全性指示
此警告符號代表危險，表示可能造成人身傷害。使用任何設備前，請留心電路相關危險，並熟悉避免意外的標準作法。您可以使用每項警告後的聲明編號，查詢本裝置隨附之安全性警告譯文中的翻譯。
請妥善保留此指示

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_13/index.htm.

Or, from the Cisco.com home page, select **Technical Documentation**. From the Network Management pulldown list, select **CiscoWorks > CiscoWorks WLSE, HSE, and ESSE > Wireless LAN Solution Engine > Wireless LAN Solution Engine 2.13**.

You can access WLSE online help by clicking the **Help** button in the top right corner of the screen. You can access the user guide from the online help by clicking **View PDF**, and access the troubleshooting guide by clicking **Troubleshooting**.

The following product documentation is available:

Document Title	Description and Locations
Release Notes for the CiscoWorks Wireless LAN Solution Engine	New features, documentation updates, known and resolved problems. Available as PDF on the WLSE recovery CD and on Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_release_notes_list.html
User Guide for the CiscoWorks Wireless LAN Solution Engine	Information about WLSE features and instructions for using WLSE 2.13. Available as PDF on the WLSE recovery CD, from the WLSE online help (click **View PDF**), and on Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_list.html
Supported Devices Table for the Wireless LAN Solution Engine	Devices supported by the WLSE. Available on Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_device_support_tables_list.html
Troubleshooting and FAQs for the CiscoWorks Wireless LAN Solution Engine	Troubleshooting hints and FAQs for the WLSE. Available from the WLSE online help (click **Troubleshooting**) and on Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_troubleshooting_guides_list.html

Document Title	Description and Locations
Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine	Installation and initial configuration of the WLSE. Available as PDF on the WLSE Recovery CD and on Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_installation_guides_list.html
Regulatory Compliance and Safety Information for the CiscoWorks 1133 Wireless LAN Solution Engine	Regulatory compliance and safety information for the WLSE. Available as a printed document shipped with the WLSE, as PDF on the WLSE Recovery CD, and on Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_installation_guides_list.html
Upgrading CiscoWorks Wireless LAN Solution Engine Software	Upgrading software on a WLSE or WLSE Express to WLSE 2.13. http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_installation_guides_list.html
Developer Guide for the CiscoWorks Wireless LAN Solution Engine	How to use the XML application programming interface. Available on Cisco.com at www.cisco.com/kobayashi/sw-center/cw2000/crypto/wlan-sol-eng/.

Obtaining Documentation

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

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

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

Ordering Documentation

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

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

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

Documentation Feedback

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

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com

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

- Nonemergencies—psirt@cisco.com

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

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

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

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

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

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

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco

service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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

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

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

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended

solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

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

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

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

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

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

  or view the digital edition at this URL:

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

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

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

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

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

Product Overview

The WLSE is a rack-mountable appliance for configuring and managing Cisco wireless devices. This chapter describes software features of WLSE 2.13 and hardware features of the WLSE 1133.

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 1133 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.
- WLSE administration—Manage WLSE software, including software upgrades, monitoring the WLSE, backing up data, and using two WLSEs as a redundant, highly available WLAN management solution.
- Deployment Wizard—Configures and discovers access points used in a Cisco Structured Wireless-Aware Network (SWAN) framework.

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 2.13*.
- The Web interface, which you access by using a browser, 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 2.13*.

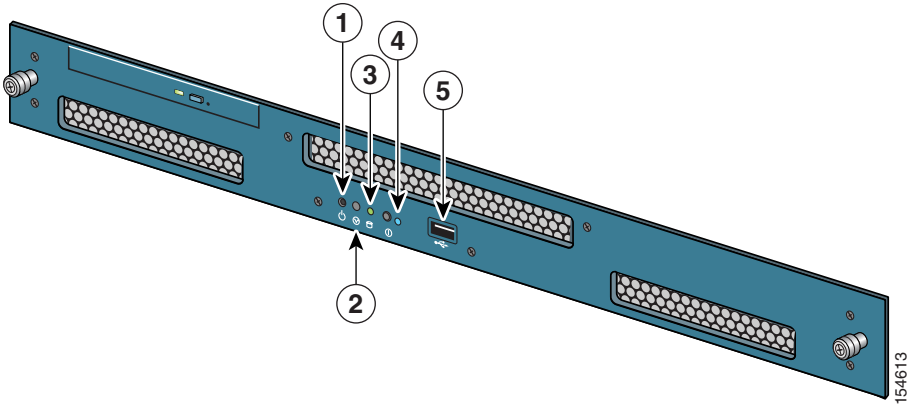
Hardware Features—WLSE 1133

This section describes the WLSE 1133 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.	**4**	Blue light indicator. Blinks if you push it.
2	Not used in this release.	**5**	USB port *Do not use for the console; use the console/serial port on the back panel.*
3	Hard drive indicator		

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.

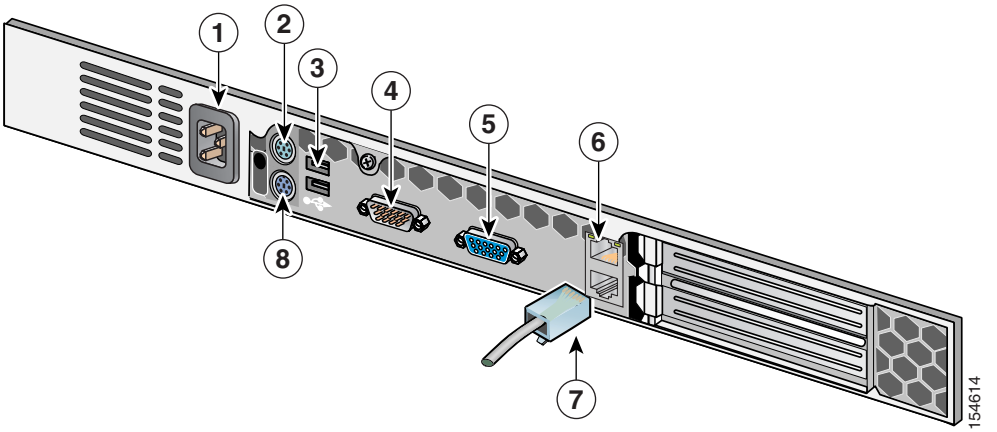
Table 1-1 System Indicators

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.

Back Panel Features

Figure 1-2 shows the WLSE back panel.

Figure 1-2 Back Panel Connections



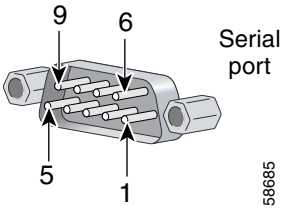
1	AC power receptacle	**5**	Video output *Do not use for the console; use the console/serial port.*
2	Mouse port	**6**	Ethernet 0 connector
3	USB port	**7**	Ethernet 1 connector
4	Console/serial port	**8**	Console keyboard connector. *Do not use.*

Console/Serial Port

The console/serial port on the back panel uses a 9-pin D-subminiature connector.

Figure 1-3 illustrates the pin numbers, and the following table defines the pin assignments and interface signals.

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 1-4.

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

Network Cable Requirements

The Ethernet 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 1133
- 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)
- Ethernet cable (yellow)
- Adapters (DB-9 to RJ-45)
- Adapter (DB-25 to RJ-45)
- WLSE 2.13 Recovery CD
- WLSE documentation:
  - *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine*
  - *Finding Documentation for the CiscoWorks Wireless LAN Solution Engine*
  - *Regulatory Compliance and Safety Information for the CiscoWorks 1133 Wireless LAN Solution Engine*

Installing WLSE 1133 Hardware

This chapter contains safety and site preparation information and procedures procedures for installing CiscoWorks 1133 Wireless LAN Solution Engine (WLSE) hardware. The chapter contains the following major topics:

Preparing to Install WLSE 1133 Hardware

This section describes the safety instructions and site requirements needed for installing the WLSE 1133, and guides you through installation preparation. The section contains the following topics:

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 1133 Wireless LAN Solution Engine.*

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

Warning **The device is designed to work with TN power systems.** Statement 19

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

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

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 **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 unit might have more than one power supply connection. All connections must be removed to de-energize the unit.** Statement 1028

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

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 **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

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

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 xxvii 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 2-8 to avoid damage to equipment. Damage from static discharge can cause immediate or intermittent equipment failure.

- Make sure that the chassis cover is secure. The chassis is designed to allow cooling air to flow effectively within it. An open chassis allows air leaks, which could interrupt and redirect the flow of cooling air from internal components.
- Electrical equipment generates heat. Ambient air temperature might not be adequate to cool equipment to acceptable operating temperatures without adequate circulation. Make sure that the room in which you operate has adequate air circulation.

Choosing a Site for Installation

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

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

Grounding the System

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

Creating a Safe Environment

Follow these guidelines to create a safe operating environment:

- Keep tools and chassis components off the floor and away from foot traffic.
- Clear the area of possible hazards, such as moist floors, ungrounded power extension cables, and missing safety grounds.

- Keep the area around the chassis free from dust and foreign conductive material (such as metal flakes from nearby construction activity).

AC Power

Ensure that the plug-socket combination is accessible at all times, because it serves as the main disconnecting device. For the WLSE's power requirements, see Appendix A, "Technical Specifications for the WLSE 1133."

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).** Statement 1005

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 1-6.

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

- RJ-45 console cable (provided)
- Power cord (provided)
- Number 2 Phillips screwdriver
- Tape measure and level
- Antistatic mat or antistatic foam
- ESD grounding strap
- Ethernet cable

Installing WLSE 1133 Hardware

This section provides instructions for installing the WLSE in a rack. The rack must be properly secured to the floor, ceiling, or upper wall, and where applicable, to adjacent racks. The rack should be secured using floor and wall fasteners and bracing specified by industry standards.

This section contains the following topics:

Installation Quick Reference

Table 2-1 provides a high-level overview of the installation process. After installation is complete, follow the directions in Chapter 3, "Setting Up the WLSE."

Table 2-1 Quick Reference

Task	References
Use the rack mount kit to install the WLSE in a rack.	Installing the WLSE 1133 in a Rack, page 2-13
Connect the WLSE to an AC power source.	Connecting Cables, page 2-25
Connect network and console cables.	Connecting Cables, page 2-25
Power on the WLSE.	Powering On the WLSE, page 2-26

Installing the WLSE 1133 in a Rack

Before installing the WLSE in a rack, read Preparing Your Site for Installation, page 2-8 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.**

The server can be installed in a system 1U rack. The rack rail components are as follows (numbers in parentheses refer to Figure 2-1):

- 2 telescopic rails (1, 2)
- Bag containing:
  - 8 Round head screws with washer (3)
  - 2 Round head screws (4)
  - 10 Cage nuts (5)

Figure 2-1 Rack Rail Components

To install the CiscoWorks 1133 WLSE in a rack, you need to perform these steps as explained in the following sections:

1. Attach the chassis rail mount to the chassis (see Attaching the Chassis Rail Mount, page 2-16).
2. Attach the server rail to the rack assembly (see Attaching the Server Rail, page 2-20).
3. Slide the chassis on to the rack assembly (see , page 2-23).

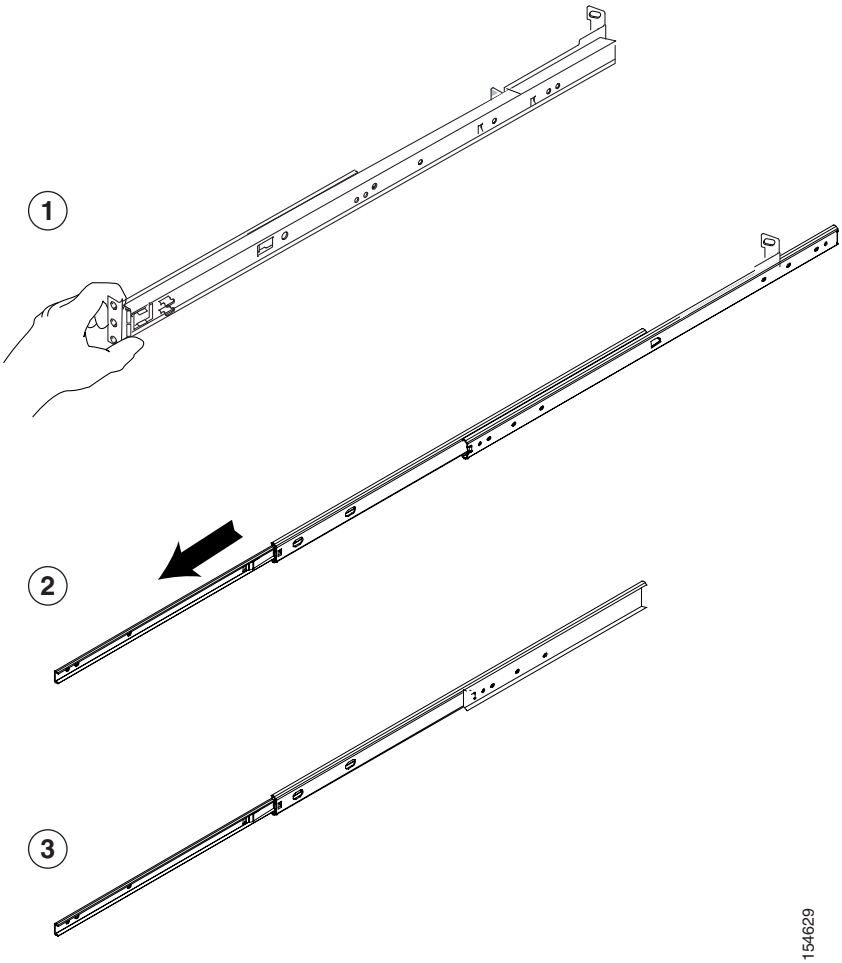
Attaching the Chassis Rail Mount

You must first remove the chassis rail mount section from the server rail and attach it to the chassis as shown in the following steps.

Procedure

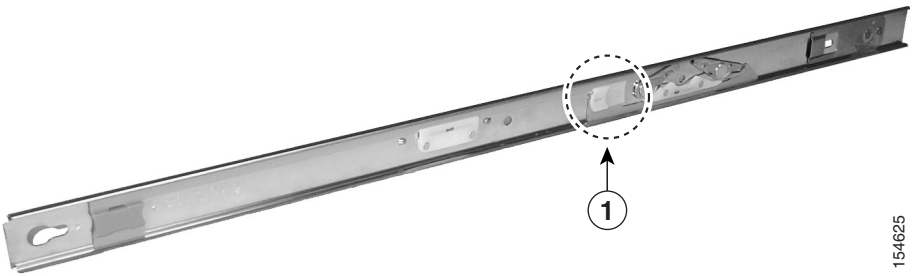
Step 1 See Figure 2-2. Extend the server rail as far as it will go. When fully extended, the server rail locks into the extended position.

Figure 2-2 Removing the Chassis Rail Mount



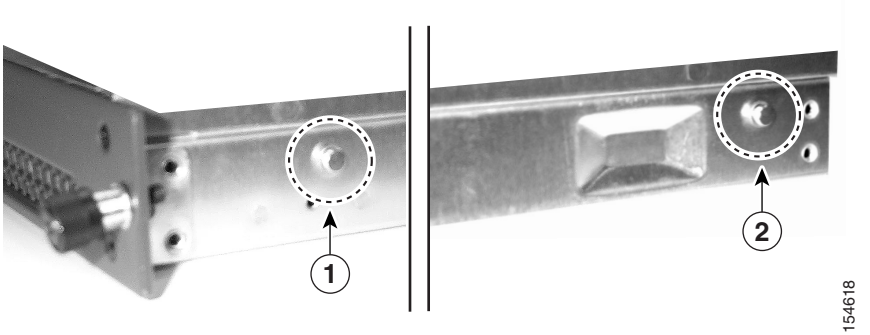
Step 2 See Figure 2-3. Slide the white tab (1) in the direction of its arrow and slide out the chassis rail mount part. (Set it aside for attaching to the chassis in the next step.)

Figure 2-3 Sliding the Chassis Rail Mount Release Tab



Step 3 Align the holes in the chassis rail mount to the pegs on the chassis (1 and 2 in Figure 2-4).

Figure 2-4 Positioning Chassis Rail Mount on Chassis



Step 4 See Figure 2-5. Align the holes (1) and then slide the rail until it locks into place (2).

Figure 2-5 Attaching Chassis Rail Mount to Chassis

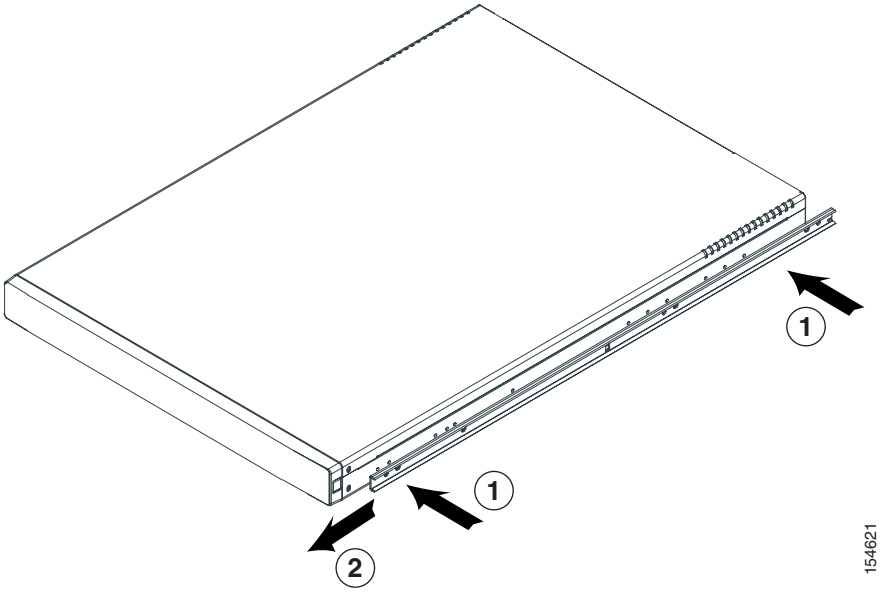
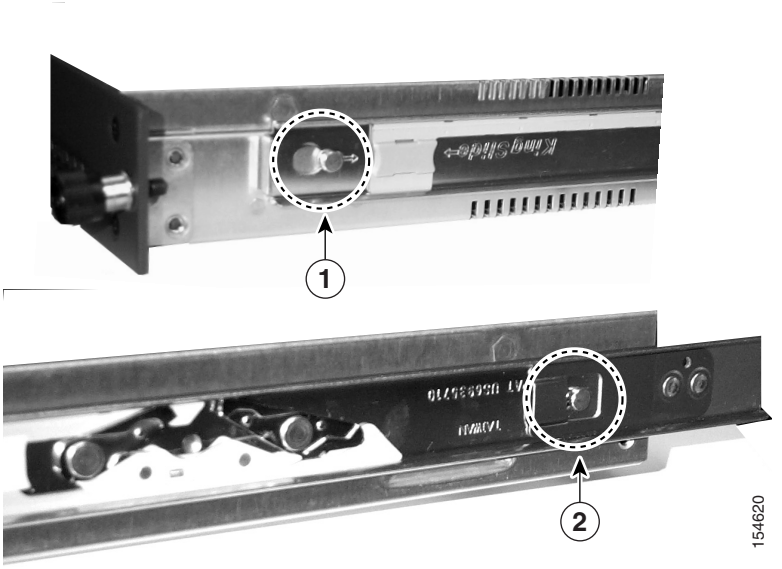


Figure 2-6 shows the chassis rail mount locked into place.

Figure 2-6 Chassis Rail Mount in Locked Position



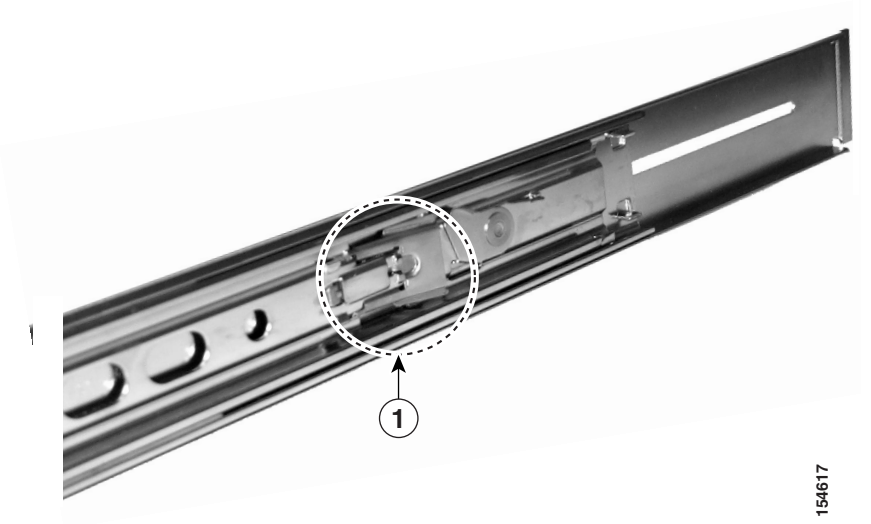
Attaching the Server Rail

Now that you have mounted the chassis rail mount, you need to retract the server rail that you previously extended and then attach it to the rack. If you have already retracted the server rail, go to step 2.

Procedure

Step 1 To retract the arm of the server rail, push the tab shown in Figure 2-7. Then slide the arm back in.

Figure 2-7 Retracting the Server Rail



Step 2 Attach the server rail to the rack as shown in the figure that corresponds to your rack:

- For a square-peg rack, see Figure 2-8.
- For a circular-peg rack, see Figure 2-9.

Figure 2-8 Attaching Rail to a Square-Peg Rack

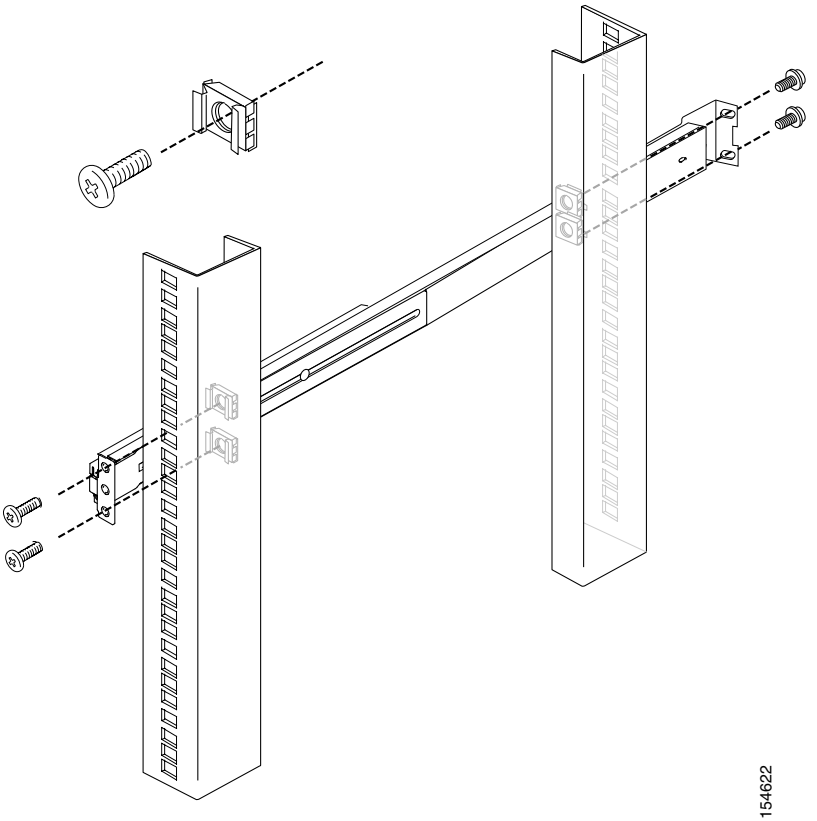
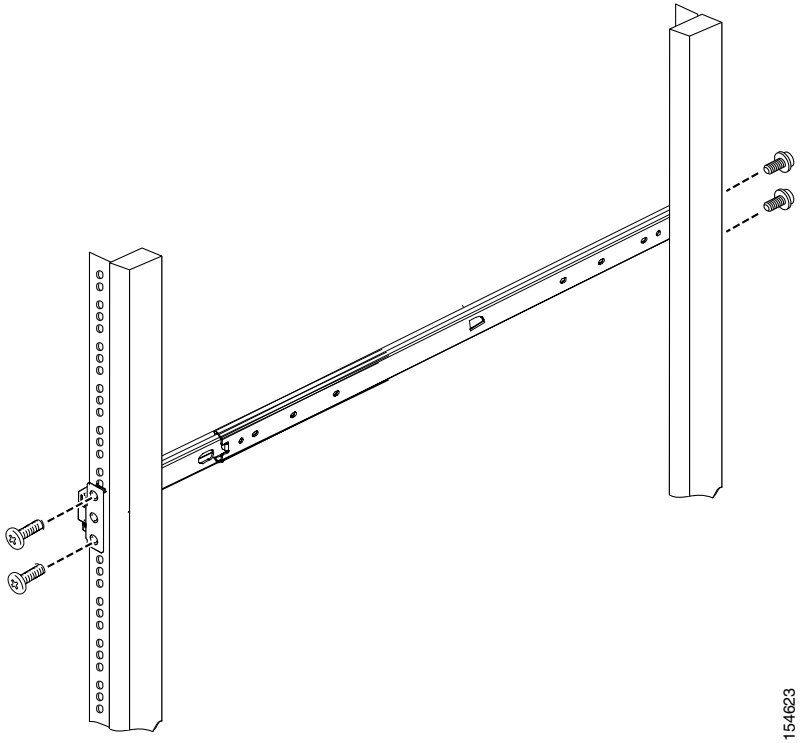


Figure 2-9 Attaching Rail to a Circular-Peg Rack



Step 3 Repeat this process with the other rail and rack assembly.

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.

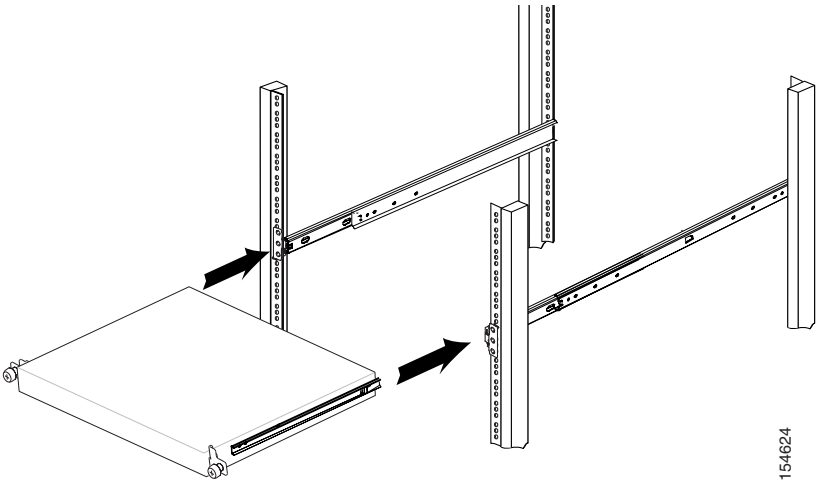
Sliding Chassis On the Rack

Step 1 See Figure 2-10. On the chassis rail mount, slide and hold the purple-colored tab in the direction of the arrow. This allows the chassis rail mount to slide on to the rail.

Figure 2-10 Sliding the Chassis Rail Mount Extended Tab

Step 2 Insert the chassis in the rack. See Figure 2-11.

Figure 2-11 Sliding Chassis onto Rack



Slide the chassis back and forward several times. Fasten with all the screws.

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, follow these steps:

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

Step 1 Plug the network connection into the Ethernet 0 port. See Figure 1-2 on page 1-4 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 1-4 for the location of the serial port.

Powering On the WLSE

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 equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals. (43)**

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 3, "Setting Up the WLSE."

Setting Up the WLSE

This chapter describes how to run the setup program and perform basic configuration for WLSE 2.13 software.

Initial Setup Quick Reference

Table 3-1 provides a high-level overview of the basic initial setup of the WLSE.

Table 3-1 Initial Setup Quick Reference

Task	References
1. Run the setup program.	Configuring the WLSE's Network Information, page 3-2
2. Configure DNS, if necessary.	Configuring Name Resolution, page 3-6
3. Verify the configuration.	Verifying the Configuration, page 3-7
4. Configure the web browser.	Configuring the Web Browser, page 3-8
5. Log in and verify connectivity.	Logging into the Web Interface and Verifying Connectivity, page 3-12
6. Add additional users.	Adding Users, page 3-13

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 3-5.
- You can exit the setup program in two ways:
  - Press **Ctrl-c**.

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

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

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

See Table 3-2 on page 3-3 and Table 3-3 on page 3-4 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 terminal or PC to the serial/console port on the back panel. *Do not use the video port for this purpose*.

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 network parameters. Table 3-2 describes how to respond to the prompts. After each response, press **Enter** to proceed to the next prompt.

Table 3-2 General Configuration

Prompt	Response Description	Sample Response
`host name:`	System host name.	SolutionEngine
`domain name:`	System domain name.	cisco.com
`<admin> 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 to connect via Telnet/SSH. The admin user has system administrator privileges and can use all CLI commands and all functions in the Web interface. Password length is unlimited, and you can use any characters except the double quote ("), single quote (’), and dollar sign ($). Passwords are case sensitive.	wq1Cvu2pl
`eth0 IP address:`	IP address of Ethernet 0 interface.	209.165.200.224
`eth0 network mask:`	Network mask of Ethernet 0 interface.	255.255.255.224
`default gateway IP address:`	IP address of default router.	209.165.200.224

Table 3-2 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 DNS, see Using the WLSE Without a DNS Server, page 3-6 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 SSL certificate. This certificate will allow you to access the WLSE securely, using HTTPS, until you are able to obtain a certificate from a certificate authority (CA). Table 3-3 on page 3-4 describes how to respond to the prompts.

If you are already running a self-signed certificate, WLSE will recognize it and ask you if you want to regenerate it.

To make changes in the certificate after running setup, see Changing the Configuration After Running Setup, page 3-5.

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 2.13*.

Table 3-3 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

Table 3-3 Self-Signed Certificate Creation (continued)

Prompt	Response Description	Sample Response
`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.

Step 7 After the WLSE reboots, set up your mail server to send mail to external domains by entering the following command:

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

where *hostname* is the hostname of the SMTP server and *ip-address* is the IP address of the SMTP server. If you do not set the mail server, email can only be sent to the local domain. For more information about this command, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13*.

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 2.13*.

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 2.13*.

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 2.13*.

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

Using 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.
- By default, IP addresses will appear instead of hostnames in WLSE displays.
- You will not be able to download access point firmware directly from Cisco.com to the WLSE.

If you are not using a DNS server, perform the steps described in Configuring the WLSE's Network Information, page 3-2, 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 the **ip name-server** command, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13*.

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 2.13*.

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 2.13*.

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

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

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

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 3-9
- Configuring Internet Explorer, page 3-9
- Configuring Firefox, page 3-11

Supported Browsers

Before connecting to the WLSE web interface, make sure you are using a supported browser and the browser is properly configured. The supported browsers for WLSE 2.13 are listed in Table 3-4 on page 3-9. Use the procedures in Configuring Internet Explorer, page 3-9 or Configuring Firefox, page 3-11 to configure your browser.

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

Table 3-4 Supported Browsers

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

Configuring Internet Explorer

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

To configure Internet Explorer 6.0, perform the following steps:

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

Step 2 Enable JavaScript:

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 select **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 2.13 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 2.13*.

Configuring Firefox

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

To configure Firefox 1.0.6, perform the following steps:

Procedure

Step 1 Select **Tools > Options**.

Step 2 Configure the browser to accept cookies:

a. Under **Privacy > Cookies**.

b. Select **Allow sites to set cookies**.

c. Select **until they expire**.

Step 3 Enable Java:

a. Select the **Web Features** panel.

b. Select **Enable Java** and **Enable Javascript**.

Step 4 Click **OK**.

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 in the URL.

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 2.13*.

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 privileges of such roles.

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 4, "Setting Up Devices—Overview."
- Configure device management on the WLSE—see Chapter 5, "Setting Up Discovery and Device Management."

Setting Up Devices—Overview

You must set up devices before the WLSE can discover and manage them and before you can use the WLSE for the following tasks: discovery, monitoring, reporting, configuration, firmware upgrade, and radio management.

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

Finding Details on Supported Devices

For information about device models and versions supported by the WLSE, see the *Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine,* 2.13 on Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_13/index.htm.

About Device Setup Methods

There are two ways to set up devices:

- Configure devices manually or create and apply WLSE configuration templates—See Basic Device Setup Methods, page 4-3.
- Use the WLSE Deployment Wizard. This method is for IOS access points using Wireless Domain Services (WDS) within a Cisco Structured Wireless-Aware Network (SWAN)—See WLSE Deployment Wizard, page 4-2.

WLSE Deployment Wizard

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

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

For information on using the Deployment Wizard, see the WLSE online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13* on Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_13/index.htm.

Basic Device Setup Methods

For details on setting up external devices, see the document *Configuring Devices for Management by the Wireless LAN Solution Engine, 2.13* on Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_13/index.htm.

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

Configuring IOS Access Points and Bridges

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

Device configuration consists of:

- Basic network configuration:
  - Normally, enabling Cisco Discovery Protocol (CDP)
  - Configuring SNMP
  - Configuring Telnet or SSH for pushing configuration to APs
- Radio management configuration:
  - Configuring Wireless Domain Services (WDS) devices—either APs or Wireless LAN Services Modules (WLSMs)
  - Configuring infrastructure APs to authenticate to WDS

Configuring Routers and Switches

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

Router and switch configuration consists of:

- Enabling Cisco Discovery Protocol (CDP)
- Configuring SNMP

Configuring AAA Servers

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

AAA server configuration consists of:

- Configuring the server to recognize the WLSE
- Configuring the WLSE to add information about the servers to be monitored

Configuring a Wireless LAN Services Module

You can use a Wireless LAN Services Module (WLSM) to provide Wireless Domain Services (WDS) to access points. See the WLSM documentation for details.

Setting Up Discovery and Device Management

After setting up devices, you can discover and manage them. This section describes discovery and management configuration for WLSE 2.13.

Device Management Quick Reference

Table 5-1 on page 5-2 provides a high-level overview of the tasks for discovering and managing devices. Detailed procedures are provided in this chapter.

Note For IOS access points used within a Cisco Structured Wireless-Aware Network (SWAN), you can use Wireless Domain Services (WDS) and the WLSE's Deployment Wizard for device configuration and deployment, instead of performing Tasks 1 through 4 in Table 5-1. The Deployment Wizard is the preferred method for such deployments. The Deployment Wizard displays immediately after you log in to the WLSE's web interface. For more information on the Deployment Wizard, see the WLSE online help and the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.13* on Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_13/index.htm.

Table 5-1 Quick Reference

Tasks	References
1. Add device credentials to the WLSE.	Adding Device Credentials to the WLSE, page 5-2
2. (Optional) Set discovery and management options.	Configuring Discovery Options, page 5-6
3. Discover or import devices.	Discovering Devices, page 5-7
4. Manage devices.	Managing Devices, page 5-12
5. Add any AAA servers to be monitored.	Adding AAA Servers to the WLSE, page 5-14

Adding Device Credentials to the WLSE

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

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

- For all managed devices, enter SNMP credentials.
- For access points, you must enter Telnet or SSH credentials and IOS HTTP port settings.
- For radio management, enter WLCCP credentials.

Enter SNMP Community Strings for All Managed Devices

SNMP community strings are used for discovery and for enabling WLSE features, such as AP configuration jobs and radio management. The community string must be set on each device, as described in Chapter 4, "Setting Up Devices—Overview." You can enter as many community strings on the WLSE as necessary.

Note If you are importing devices, you do not need to enter their community strings.The community strings will be imported along with the devices and will be listed in WLSE Communities screen, in which you can modify and delete strings as required. For more information, see Import Devices, page 5-10.

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

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

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

Step 2 To add an entry:

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

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

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

Step 3 To modify an entry:

a. Select the entry in the list of entries.

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

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

c. Click **Modify**.

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

Step 4 To delete an entry:

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

b. Click **Delete**.

Note The default entry cannot be deleted.

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

Enter 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, perform the following steps:

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

Step 2 To add a username and password:

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

b. Enter the username.

c. Enter the password and confirm it.

d. Enter the enable password and confirm it.

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

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

Enter HTTP Port Settings for IOS Access Points

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

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

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

Step 2 To add a port:

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

b. Enter the port number.

c. Click **Save**.

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

Enter WLCCP Credentials for Wireless Domain Services (WDS)

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

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**.

Configuring Discovery Options

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

Note These procedures are optional.

To configure discovery options, perform the following steps:

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

a. If you want device names in WLSE displays, instead of their IP addresses, select **Use Reverse DNS lookup**.

b. Configure the name format for devices in WLSE displays in the Name Format field.

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

d. To arrange temporary management of access points, configure MAC address filtering. For information, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13*.

e. Click **Save**.

Step 2 To set up IP filters for limiting discovery to certain devices, select **Devices > Discover > DISCOVER > IP Filter Rules** and follow the instructions in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13*.

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 5-7.

  Note If you prefer not to use CDP, use the wizard and enter all of your devices as seeds, as indicated in Run CDP Discovery, page 5-7, or import devices.

- Import devices from a file or from a CiscoWorks server—See Import Devices, page 5-10.

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 4, "Setting Up Devices—Overview."

Run CDP Discovery

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

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

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

- Run an immediate, one-time CDP discovery—See Run CDP Discovery Now, page 5-8.
- Modify the default CDP discovery schedule—See Modify the CDP Discovery Schedule, page 5-9.

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 5-3. After adding community strings, click **Next**.

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

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

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

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

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

c. Click **Next**.

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

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

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

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

Modify the CDP Discovery Schedule

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

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 5-3. After adding community strings, click **Next**.

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

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

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

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

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

Step 7 Click **Next**.

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

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

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

Import Devices

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

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

Import Devices from a File

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

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

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

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

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

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

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

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

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

Import Devices from a CiscoWorks Server

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

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

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

Step 3 Complete the Schedule Import from CiscoWorks dialog.

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

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

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

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

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

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

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

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

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

Managing Devices

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

Note If you specified auto-management when configuring advanced options, the newly discovered devices will be in the Managed folder. For information on setting the auto-manage option, see Configuring Discovery Options, page 5-6.

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.

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

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

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

Adding AAA Servers to the WLSE

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

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

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

Step 3 Complete the following:

Text Box	Description
Server Name	Hostname or IP address of an AAA server to be added. **Note** Depending on how your network is set up, the AAA server can be a Cisco Secure Access Control Server, a Cisco Access Registrar RADIUS server, or an access point configured as an AAA server.
Server Port	Port on the server used for authentication; use port 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.

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 2.13* or the WLSE online help.

Technical Specifications for the WLSE 1133

Table A-1 provides the specifications for the CiscoWorks 1133 Wireless LAN Solution Engine.

Table A-1 Technical Specifications

Component	Specifications
Serial ports	Two 9-pin connectors
RJ-45 ports	RJ-45 connectors for connection to integrated 10/100/1000 Ethernet controllers
AC power supply wattage	280 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 A-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