



Upgrading the CiscoWorks Wireless LAN Solution Engine, 2.12

This document provides general information about upgrading WLSE system software to Release 2.12 and provides a pointer to the software images and accompanying Readme files on Cisco.com. The Readme files provide detailed upgrade procedures.

This document contains the following sections:

- [Other Relevant Documentation, page 1](#)
- [Before Upgrading, page 2](#)
- [Upgrade Methods, page 2](#)
- [Overview: Repository Method, page 3](#)
- [Overview: Recovery CD Method, page 3](#)
- [Upgrading a Redundant Cluster, page 4](#)
- [Software and Hardware that Can Be Upgraded, page 5](#)
- [Backing Up the WLSE Before Upgrade, page 5](#)
- [Viewing the Installation Log, page 6](#)

Other Relevant Documentation

Use this document along with the following documents:

- The Readme files located along with the software images in the download area on Cisco.com.
- The instructions for backing up and restoring the WLSE database in the online help and the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.12*.



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2005 Cisco Systems, Inc. All rights reserved.

Before Upgrading

Please review the following notes and cautions before upgrading.

- WLSE images are subject to import/export regulations respecting strong encryption. Before you are allowed to download the image, you might need to establish a Cisco.com profile or edit your Cisco.com profile to confirm that you are allowed to download such images. You will also need to respond to the Encryption Software Export Distribution Authorization query.
- You cannot upgrade a WLSE 1105 to WLSE 2.12. If you attempt to do so, the installation will fail. Messages in the install.log file will include the following:

```
Error: Hardware type 1105 not supported for this upgrade.
Error: Aborting upgrade installation.
Daemon Manager could not start. The port is in use.
```

For information on the install.log file, see [Viewing the Installation Log, page 6](#).

- Non-IOS access points are not supported by WLSE 2.12. You must convert all non-IOS access points to IOS before proceeding with the upgrade. For instructions on converting access points, see the following document on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/convert/index.htm

- Always review the Readme.txt file that accompanies the upgrade image on Cisco.com before attempting to install the upgrade.
- If you are upgrading from Release 2.9 or 2.9.1a, you must first install a patch. (See the Readme for instructions.)
- You can downgrade to an earlier software version by using the recovery CD method. The database is not preserved when you use the recovery CD, so make sure you have a backup from the earlier version before downgrading. For example, if you downgrade from 2.12 to 2.11, you would need to restore a 2.11 backup.
- You cannot upgrade from pre-release, non-FCS, or beta software to the released version. Also, you cannot back up data from pre-release, non-FCS, or beta software and restore it to a WLSE running the released version.
- Upgrading a redundant WLSE cluster requires special procedures. See [Upgrading a Redundant Cluster, page 4](#).

Upgrade Methods

There are two basic methods of upgrading a WLSE to 2.12:

- **Repository method:** Download the upgrade files and install them from a repository. You can use the WLSE itself or a Microsoft Windows server as the repository. *This method is easier and faster and is the recommended method.*
- **Recovery CD method:** Download files and create a recovery CD. Then use this CD to upgrade the WLSE.

The database is not preserved when you use this method. You must restore the database after upgrading.

Overview: Repository Method

This section gives an overview of the upgrade procedure for downloading. For details, see the relevant Readme file.

1. Navigate to the software download area on Cisco.com:
<http://www.cisco.com/cgi-bin/tablebuild.pl/wlan-sol-eng>
 Here you will find the Readme files and software images.
2. Read the following image Readme: WLSE-2.12-K9.readme-V1.txt
3. (Strongly recommended) Back up the WLSE database. The upgrade attempts to preserve the WLSE database, but a new backup is needed in case of errors during the upgrade. For information on backing up and restoring the WLSE database, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.12*.
4. Install the WLSE 2.12 upgrade image on a repository.
5. Install the upgrade image on the WLSE.
6. If necessary, restore the backup from Step 3.
7. Run a manual inventory on all managed devices. This ensures that radio management functionality will work correctly. For information on running inventories, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.12*.

Overview: Recovery CD Method

This section gives an overview of the upgrade procedure for downloading and installing the patch and creating a recovery CD. For details, see the relevant Readme file.



Caution

Performing a database backup as described below is essential. Data is not preserved during this method of upgrading, and the database must be restored after upgrading.

1. Navigate to the software download area on Cisco.com:
<http://www.cisco.com/cgi-bin/tablebuild.pl/wlan-sol-eng>
 Here you will find the Readme files and software images.
2. Read the following image Readme: WLSE-2.12-ISO-ReadmeV1.txt
3. Back up the WLSE database. For information on backing up and restoring the WLSE database, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.12*.
4. Use the instructions in the ISO Readme file to create the recovery CD.
5. Install the recovery CD.
6. Restore the backup from Step 3.

Upgrading a Redundant Cluster

There are two ways to upgrade software on redundant WLSEs:

- [Using Manual WLSE Upgrade Procedures, page 4](#)
- [Using Cisco Works Resource Manager Essentials \(RME\) Software Image Management \(SWIM\) and the Redundancy CLI Command, page 4](#)

Using Manual WLSE Upgrade Procedures

Use the normal WLSE upgrade procedures in the Readme files. This requires that you:

1. Disable redundancy.
2. Upgrade both nodes.
3. Re-enable redundancy.

With this method, the virtual IP addresses are not bound, causing a temporary outage. Also, this might cause issues with connectivity to the remote network.

For information on disabling and re-enabling redundancy, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.12* on Cisco.com.

Using Cisco Works Resource Manager Essentials (RME) Software Image Management (SWIM) and the Redundancy CLI Command

You can use CiscoWorks Resource Manager Essentials (RME) Software Image Management (SWIM) to download the image and then use the **redundancy** CLI command to accomplish the upgrade.

**Note**

The minimum version required to use this procedure is RME 4.0.2 and Common Services (CS) 3.0 with Service Pack 2.

This method is preferable because:

- You do not have to disable redundancy.
- The virtual IP addresses (VIPs) remain bound to the WLSE systems.
- Connectivity issues with remote networks are avoided.

During this method of upgrading, synchronization between the two servers is briefly halted and restarted; and the WLSE node that was standby before the upgrade becomes the new active node.

**Caution**

Do not change the admin password on either node while the upgrade is in progress or the upgrade will fail on one of the nodes.

The procedure to upgrade by using this method is:

1. Use SWIM to download the image to the local repository on the active node. For details on downloading the image via SWIM, see the CiscoWorks Resource Manager Essentials documentation on Cisco.com at the following URL:
http://www.cisco.com/en/US/products/sw/cscowork/ps2073/tsd_products_support_series_home.html, or the CiscoWorks server's online help.
2. Make sure the upgrade image is in the WLSE's local repository.
3. Log in to the WLSE CLI as a the user admin.
4. Run the **redundancy upgrade** CLI command on either the active or standby node, although it is preferable run the command on the active node. During upgrade, the redundancy status of the node is shown as Active Upgrade or Standby Upgrade.
5. The upgrade proceeds automatically as follows:
 - a. The standby node is upgraded first.
 - b. The standby node reboots and becomes active, while the original active node is upgraded.
 - c. The original active node becomes the standby node.

Software and Hardware that Can Be Upgraded

You can upgrade a WLSE 1030 Express with WLSE 2.11 to WLSE 2.12.

You can upgrade a WLSE 1130 or 1130-19 to WLSE 2.12 as follows:

- From WLSE 2.9 to WLSE 2.12
- From WLSE 2.9.1a to WLSE 2.12
- From WLSE 2.11 to WLSE 2.12



Note

If you are upgrading from Release 2.9 or 2.9.1a , you must first install a patch. (See the Readme for instructions.)

WLSE 2.12 software is supported on the WLSE 1030, WLSE 1130, and WLSE 1130-19 hardware. You cannot upgrade a WLSE 1105 to WLSE 2.12. If you attempt to do so, the installation will fail.

Backing Up the WLSE Before Upgrade

Before upgrading WLSE software, back up the database. The upgrade attempts to preserve the WLSE database, but a backup is recommended in case of errors during the upgrade. For information on backing up the WLSE database, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.12*.



Caution

Backup is essential if you are upgrading via the recovery CD. Data is not preserved during this method of upgrade. After upgrading, you must restore the WLSE's database.

Viewing the Installation Log

The install.log file contains information about files installed during software installation, as well as any errors that occurred. To view install.log and other WLSE system logs, select **Administration > Appliance > Status > View Log File**.

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 the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

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/>

Cisco will continue to support documentation orders using the Ordering tool:

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

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

- Instructions for ordering documentation using the Ordering tool are at this URL:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can 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 non emergencies.

- Non emergencies—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.htm

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>