



Converting Non-IOS Access Points to IOS

CiscoWorks WLSE and WLSE Express, Release 2.11

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

Text Part Number: OL-6780-01



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

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

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

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

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

Portions of this manual are Copyright 2003 Dell Computer Corporation. All Rights Reserved. Reproduction in any manner whatsoever without the written permission of Dell Computer Corporation is strictly forbidden.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Converting Non-IOS Access Points to IOS

Copyright ©2005, Cisco Systems, Inc. All rights reserved.



Preface v

Audience v

Conventions v

Product Documentation vi

Obtaining Documentation ix

 Cisco.com ix

 Documentation DVD ix

 Ordering Documentation x

Documentation Feedback x

Cisco Product Security Overview x

 Reporting Security Problems in Cisco Products xi

Obtaining Technical Assistance xii

 Cisco Technical Support Website xii

 Submitting a Service Request xiii

 Definitions of Service Request Severity xiii

Obtaining Additional Publications and Information xiv

CHAPTER 1

Converting Access Points to IOS 1-1

Understanding the Conversion Process 1-1

Performing the Conversions 1-2

 Task 1. Satisfy the Prerequisites 1-3

 Prerequisites 1-3

 Adjusting the Timing Parameters 1-6

 Task 2. Configure Access Points To Be Converted 1-7

- Task 3. Configure the WLSE for IOS Conversions 1-9
- Task 4. Create a Conversion Template on the WLSE 1-10
- Task 5. Create and Run the Conversion Job 1-15
 - Creating and Running a Conversion Job 1-15
 - Checking the Progress of a Running Conversion Job 1-18
 - Managing Converted Devices 1-19
- Task 6. Check the Results 1-19

CHAPTER 2

FAQs and Troubleshooting 2-1

Conversion FAQs 2-1

Conversion Troubleshooting 2-4

APPENDIX A

Limitations of the Conversion Process A-1

INDEX



Preface

This guide provides procedures for using the CiscoWorks Wireless LAN Solution Engine to convert access points from non-IOS firmware to IOS firmware. This guide consists of the following:

- [Converting Access Points to IOS](#)
- [FAQs and Troubleshooting](#)
- [Limitations of the Conversion Process](#)

Audience

This document is for system administrators and network administrators who are responsible for managing a wireless network and are familiar with the concepts and terminology of Ethernet and wireless local area networking.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	boldface font
Variables for which you supply values	<i>italic font</i>

Item	Convention
Displayed session and system information	screen font
Information you enter	boldface screen font
Variables you enter	<i>italic screen font</i>
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.

Product Documentation

**Note**

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

[Table 1](#) describes the available product documentation for WLSE 2.11.

Table 1 Product Documentation

Document Title	Available Formats
<i>Release Notes for the CiscoWorks Wireless LAN Solution Engine</i>	On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm
<i>Converting Access Points to IOS</i>	On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm
<i>Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine</i>	On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm
<i>Installation and Configuration Guide for the 1130-19 CiscoWorks Wireless LAN Solution Engine</i>	<ul style="list-style-type: none"> Printed document included with the product. PDF on the WLSE Recovery CD-ROM. On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm
<i>Installation and Configuration Guide for the 1030 CiscoWorks Wireless LAN Solution Engine Express</i>	<ul style="list-style-type: none"> Printed document included with the product. PDF on the WLSE Recovery CD-ROM. On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm
<i>Regulatory Compliance and Safety Information for the 1130-19 CiscoWorks Wireless LAN Solution Engine</i>	<ul style="list-style-type: none"> Printed document included with the product. PDF on the WLSE Recovery CD-ROM. On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm

Table 1 Product Documentation (continued)

Document Title	Available Formats
<i>Regulatory Compliance and Safety Information for the 1030 CiscoWorks Wireless LAN Solution Engine Express</i>	<ul style="list-style-type: none"> Printed document included with the product. PDF on the WLSE Recovery CD-ROM. On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm
<i>User Guide for the CiscoWorks Wireless LAN Solution Engine</i>	<ul style="list-style-type: none"> From the WLSE online help. PDF on the WLSE Recovery CD-ROM. On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm
<i>Upgrading CiscoWorks Wireless LAN Solution Engine Software</i>	<ul style="list-style-type: none"> From the WLSE online help. On Cisco.com: www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm.
<i>Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine</i>	On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm
Context-sensitive online help	Select an option from the WLSE navigation tree, then click Help .
<i>FAQ and Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine</i>	<ul style="list-style-type: none"> From the WLSE online help. On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Documentation DVD

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

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

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

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

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

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

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

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support Website

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

<http://www.cisco.com/techsupport>

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

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



Note

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

Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

<http://www.ciscopress.com>

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

<http://www.cisco.com/packet>

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

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

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

<http://www.cisco.com/ipj>

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

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



Converting Access Points to IOS

You can use the firmware upgrade options provided by WLSE to convert multiple non-IOS access points to IOS at the same time.

This chapter contains the following topics:

- [Understanding the Conversion Process, page 1-1](#)
- [Performing the Conversions, page 1-2](#)

Understanding the Conversion Process

There are two methods for converting non-IOS access points to IOS:

- You can use the WLSE Web interface (the Firmware tab) and create conversion jobs that you can schedule at a desired time. This method is recommended if you have a WLSE. This document describes this method of conversion.
- If you do not have a WLSE, you can download and install the Cisco Aironet Conversion Tool (CAC Tool) from Cisco.com and manually convert access points. For information on this tool, see the CAC documentation on Cisco.com.



Caution

Do not use regular upgrade images. Conversion from non-IOS (VxWorks) to IOS firmware requires a special upgrade image and only certain versions of VxWorks can be converted to IOS. The available upgrade images are listed in [Table 1-1 on page 1-4](#).

The WLSE automatically converts most of the non-IOS configuration data to IOS-style configuration. However, certain key data are not automatically converted and must be specified as part of the upgrade job. Therefore, when you use the WLSE to convert to IOS, you first define a non-IOS configuration template that includes certain parameters. This template is assigned to the devices during the upgrade process.

Performing the Conversions



Caution

After you convert a non-IOS access point to IOS, you *cannot reverse the process*. The access point cannot be converted back to non-IOS firmware.

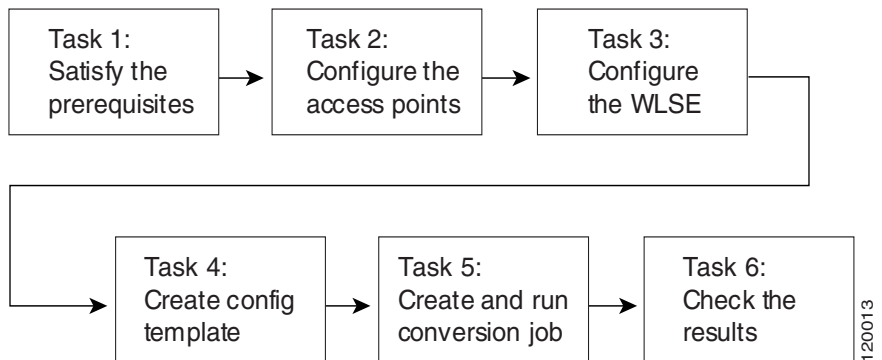


Caution

Run a conversion job with one access point *before* running a job on multiple devices. If you are converting more than one type of access point, run a test job on each type of device. If possible, do not run the tests on your production network.

Figure 1-1 illustrates the major tasks in the conversion process.

Figure 1-1 Conversion Process Overview



The following sections describe these tasks in greater detail:

- [Task 1. Satisfy the Prerequisites, page 1-3](#)
- [Task 2. Configure Access Points To Be Converted, page 1-7](#)
- [Task 3. Configure the WLSE for IOS Conversions, page 1-9](#)
- [Task 4. Create a Conversion Template on the WLSE, page 1-10](#)
- [Task 5. Create and Run the Conversion Job, page 1-15](#)
- [Task 6. Check the Results, page 1-19](#)

Task 1. Satisfy the Prerequisites

This section contains the following information:

- [Prerequisites, page 1-3](#)
- [Adjusting the Timing Parameters, page 1-6](#)

Prerequisites

Before creating a conversion job, you must satisfy the following prerequisites:

- Be sure the access points to be converted are running one of the supported versions of non-IOS (VxWorks firmware)—see [Table 1-1](#). If the access points are not running a supported version, you must upgrade the VxWorks firmware before you can convert them.

For versions earlier than 12.01T1, you must upgrade to a supported version before you can run the conversion.

Table 1-1 Supported Images and Versions

VxWorks ¹ Device	VxWorks Versions ²	Image Name	IOS Version Identifier ³	Version Field Alternate Entry
AP1200 AP1220	12.01T1 12.02T1 12.03T 12.04	AP1200-Cisco-IOS-Upgrade-Image-v3.img	12.2(11)JA3	12.2
AP350	12.01T1 12.02T1 12.03T 12.04	AP350-Cisco-IOS-Upgrade-Image-v2.img	12.2(13)JA1	12.2

1. Repeaters cannot be converted by the WLSE.
2. VxWorks Version 12.05 on AP 1200 and AP 350 is not supported for conversion.
3. This will be the IOS version on the AP after conversion.
 - Repeater conversion is not supported. To convert a repeater, try one of these options:
 - Use the CAC tool (see [Understanding the Conversion Process, page 1-1](#)).
 - Physically move the repeater to a site where Ethernet is available, put it into root mode, convert it, then set it into repeater mode and reinstall it in its original location.
 - You must have access to the WLSE Firmware and Configure tabs and all of their subtabs. Only WLSE users with full permissions can convert access points. These permissions are determined by your user role.
For information about user roles, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.11* or the online help for the **Admin > User Admin** subtab.
 - If you are converting non-IOS APs that are located across slow WAN links from WLSE (for example, WAN link at 128Kbps or 64Kbps), try resetting the timeout and retry parameters to larger values (see [Adjusting the Timing Parameters, page 1-6](#)) before converting these APs. Because the default

settings that are applicable to conversion process are tuned to work well with APs on a LAN network, these settings might need to be modified to work for converting APs located across WAN links.

- If you plan to install new hardware (such as an 11g radio), convert the firmware *before* installing the hardware. *The conversion tool does not support 802.11g radios.*
- If an AP is configured for BOOTP, change it to DHCP before the conversion.
- If you use DHCP to assign IP addresses to access points, set the DHCP lease period or use the DHCP reservation feature as follows:
 - After an image is uploaded to an access point, the access point is rebooted. If you are using DHCP to assign IP addresses to the access points to be converted, make sure that the IP addresses will not expire during the time required to run the firmware job and reboot the access points.
 - You can set the DHCP lease period accordingly or use the DHCP reservation feature. The WLSE firmware module provides IP and MAC addresses for the reservation feature.
- To avoid power cycling, make sure the switch and AP's power and duplex settings are the same.
- Review the limitations of the conversion process (see [Limitations of the Conversion Process, page A-1](#)).

VLAN Conversions

- When a non-IOS AP that is being converted has defined VLANs but the native VLAN is not defined on this AP, the WLSE will not proceed with the conversion process. The conversion job for such AP will fail with the appropriate error message in the run log for that job.
- WLSE will convert all the VLANs defined on a non-IOS AP, but only if they are mapped to an SSID. However, if the VLAN is a *native* VLAN, it is *always* converted.
- Before the conversion, make sure the SSID mapped to the native VLAN is defined as an infrastructure SSID.



Note

If a *non-native* VLAN SSID is defined as the infrastructure SSID, the infrastructure SSID command will not be created.

- WLSE always converts VLANs that are mapped to the SSID in a non-IOS AP—regardless of whether the VLANs are enabled or disabled. If the VLANs are disabled, the corresponding VLAN's interface will be closed except for the native VLAN.

**Note**

Be sure that the configuration of the switch port and the AP VLAN configuration—including the native VLAN—match. Proceeding with conversion when the AP and Switch port VLAN configurations do not match may lead to loss of connectivity to the AP after conversion.

**Note**

VLAN tagging is effective only when VLANs created in the non-IOS AP are enabled at the *global* level. WLSE creates VLANs in the IOS after a conversion—even if local VLAN tagging is disabled in the non-IOS AP before the conversion. Even when global VLAN Tagging is disabled, an AP might contain inactive VLANs. Because WLSE creates VLANs for these inactive VLANs in the conversion process, the loss of connectivity can occur.

Adjusting the Timing Parameters

On the WLSE, you can set timing parameters that apply to all firmware jobs or you can set the timing parameters for conversion jobs only. These conversion-only parameters set the following:

- **Per device job operation timeout**—Sets the timeout for uploading a conversion image.
- **Conversion SNMP Retries**—Sets the timeout for installing the conversion image.

Procedure

Step 1 Select **Firmware > Advanced Parameters**.

Step 2 Set the **Per device job operation timeout** parameter as follows:

This value multiplied by 2 is the timeout for *uploading* a conversion image. The default value is 1200 seconds or 20 minutes (600 seconds multiplied by 2).

For example, if the upload of the upgrade image takes 50 minutes, increasing the value to 1500 seconds would set the timeout to 50 minutes (1500 seconds multiplied by 2 = 3000 seconds = 50 minutes).

- Step 3** Set the **Conversion SNMP Retries** parameter. This parameter is used in the conversion tool for the IOS installation timeout. It is *not* the regular SNMP retries parameter.



Note Although installation of the image is not normally affected by a slow link, you can reset the value of this parameter to extend the timeout if the AP is slow in installing the IOS image.

This value multiplied by 2 is the timeout for *installing* the conversion image after it is uploaded. The default value is 50 minutes (25 minutes multiplied by 2).

For example, if the IOS installation takes 60 minutes, increase the timeout value to 30.

Task 2. Configure Access Points To Be Converted

Before You Begin

- Make sure each access point to be converted is running a supported version of non-IOS (VxWorks) firmware (see [Table 1-1 on page 1-4](#)). If the APs are not running a supported version, you will have to upgrade VxWorks before you can use the WLSE to convert them.
- Be sure that the access points to be converted are under WLSE management (have been discovered, inventoried, and managed).

For information about managing devices, see the WLSE online help or the “Managing Devices” chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.11*. You can view this guide on Cisco.com at cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm.

Procedure

- Step 1** Log into each access point. The Summary Status screen appears.
- Step 2** Select **Setup > Security > User Information**. The User Information screen appears.
- Step 3** If the current user does not have all permissions enabled, create a user on the AP with the same name as the community string value and set the permissions for that user:
- Select **Add New User**. The User Management dialog appears.

- Enter the user name and password, then confirm the password.
- Enable these capability settings:
 - Write
 - SNMP
 - Ident
 - Firmware
 - Admin



Note These permissions will be assigned to the access point community strings. The AP community strings are used by the WLSE to manage the APs after conversion.



Note If the SNMP, Ident, and Firmware boxes are checked, the value entered for the user name will be used as the SNMP read/write community string.

d. Click **Apply**.

Step 4 Enable SNMP on the access point:

- a. From the Summary Status screen, select **Setup > SNMP**. The SNMP Setup screen appears.
- b. Select **Enabled**.
- c. Click **Apply**.

Step 5 Go to [Task 3. Configure the WLSE for IOS Conversions](#).

Task 3. Configure the WLSE for IOS Conversions

Configuring the WLSE for performing AP conversion involves importing the upgrade/conversion image and configuring the WLSE device credentials section with the SNMP community strings that were configured on the AP in Task 2.

Procedure

Step 1 Log into the WLSE's web interface.

Step 2 Select **Devices > Discover > Device Credentials > SNMP Communities**.

- Make sure all community strings for all access points to be converted (created in Task 2) are entered into the SNMP Communities table.
- Make sure you specify at least 2 SNMP retries.

Step 3 Locate the special conversion/upgrade image on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/sw-wireless.shtml>

For information about the images to use for conversion, see [Table 1-1 on page 1-4](#).

Step 4 Download the upgrade or conversion image on to the local hard drive of your workstation.

- Step 5** To import the image to the WLSE, select **Firmware > Images > Import > From Desktop**.
- Step 6** If you are importing the upgrade image to convert a 1200 AP, import the image with device type as AP1200. If the upgrade image is for converting AP350 type, import this image with device type as AP350. Do not select AP350-IOS.
- Step 7** Make sure the Version field contains the correct IOS version identifier. See [Table 1-1 on page 1-4](#).

**Caution**

The Version field must be set correctly. If it is not, the image will be incompatible with the access points that you are converting.

- Step 8** Go to [Task 4. Create a Conversion Template on the WLSE](#).

Task 4. Create a Conversion Template on the WLSE

Whenever a conversion job is created, a non-IOS template that includes the security parameters must be provided. This section describes how to create this template and provides details about the required parameters.

**Caution**

Failure to provide a non-IOS template that includes the minimum security parameters will result in loss of access to the AP via console, Telnet, or browser after the conversion. Failure to provide the optional parameters may result in incomplete IOS configurations.

All other parameters on the access points will retain their values after conversion. If you set parameters in the conversion template in addition to those described in the following procedure, the extra parameters will be ignored.

Before You Begin

Follow these guidelines when you create the conversion template:

- You must set the required and optional security parameters in a non-IOS template in case the parameters on the access points are write-only. During the firmware conversion job, write-only parameters cannot be extracted from the access points. Therefore, such parameters must be entered a second time

by applying a template so the access point is configured correctly after the conversion. Failure to set security parameters has other effects (see [Conversion Troubleshooting, page 2-4](#)).

- When you run a conversion job, WLSE retrieves the non-IOS configuration file from the non-IOS AP and converts this file to equivalent IOS commands. However, because of the non-IOS AP behavior, the converted configuration file will not include any security-related parameters. For example, WLSE does not convert the username and password information to the equivalent IOS command. For this IOS command to be generated, you must define these security parameters in a non-IOS template, then use this template in the conversion job. For a complete list of the required security parameters, see [Table 1-2 on page 1-12](#).
- If User Manager is enabled on the AP, be sure to enter the following security information in the conversion template: User Identifier, User Name, User Password, Confirm User Password and Capabilities. If these parameters are not defined, you might not be able to log in to the upgraded AP through Telnet, the console port, or the browser.

Procedure

Step 1 Select **Configure > Templates**.

Step 2 Select **non-IOS**.

Step 3 Enter a unique name.

For details about acceptable job names, see the “Naming Guidelines” topic in the online help or the “Naming Guidelines” appendix in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.11* on Cisco.com at www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11.index.htm.

Step 4 Click **Create New**.

Step 5 From the left pane, select **Security > Local Admin Access > Add User**.

Step 6 Set the security parameters listed in [Table 1-2](#):



Note *You must set these parameters in the template. Otherwise, the conversion will fail and you will have to log in to each access point and configure it manually.*

Table 1-2 Required Security Parameters

Parameter	Description
User Identifier	Enter any integer except 0.
User Name	This username will become the Telnet user name and the read/write SNMP community string on the converted access points. These credentials are necessary for the WLSE to communicate with access points. Note This user name and password <i>must match</i> the user name and password that was entered when you created the new user on the access point (see Task 2. Configure Access Points To Be Converted , page 1-7).
User Password	This password will be the Telnet user password on the converted access points
Confirm User Password	Enter the password a second time.
Capabilities	All capabilities should be selected. Note You must add at least one username and password combination with Admin+Firmware+SNMP+Identity+Write capabilities.

- Step 7** Click the double-arrow button (>>) to add each user to the **Users to Add** list.
- Step 8** From the left pane, select **Template Categories**.
- Step 9** Set the optional security parameters from the list in [Table 1-3 on page 1-13](#). The parameters you set depend on the level of security that you require on your access points.



Note Any parameters in [Table 1-3](#) that are not set in the template will produce informational messages during [Task 4. Create a Conversion Template on the WLSE](#). These messages will not prevent the firmware job from running successfully.

Table 1-3 Optional Security Parameters

Template Category and Subcategory	Setting
Choose one:	
Association > VLANs	<p>Select this option when VLANs already exist on the APs and you want to preserve the encryption key values.</p> <ul style="list-style-type: none"> • Enter a value for VLAN ID. • Enter values for WEP Key 1 through WEP Key 4. • Select the size of each WEP key.
11a Radio > Data Encryption	<p>Select this option when the access point is using 11a radios and has no predefined VLANs.</p> <ul style="list-style-type: none"> • Enter values for Encryption Key 1 through Encryption Key 4. • For each key, select Transmit Key. • Select the Key Size for each encryption key.
Security > Local AP/Client Security	<p>Select this option when the access point is using 11b radios and has no predefined VLANs.</p> <ul style="list-style-type: none"> • Enter values for Encryption Key 1 through Encryption Key 4. • For each key, select Transmit Key. • Select a Key Size for each encryption key.
Security > Authentication Server	<ul style="list-style-type: none"> • Enter the IP address (do not enter the server name). • Select the Server Type. • Enter values for Port, Shared Secret, Retran Int (sec), Max Retran. • Specify EAP Auth, MAC Auth, User Auth, and MIP Auth. <p>Note You must enter <i>all</i> of these parameters in the template for each server you want to retain after the conversion. Failure to provide the complete set will result in missing AAA-related commands in the IOS configuration.</p>

Table 1-3 Optional Security Parameters (continued)

Template Category and Subcategory	Setting
Services > Accounting	<ul style="list-style-type: none"> • Select enable from the Enable Accounting dropdown list. • Enter the IP address (do not enter the server name). • Select Server Type. • Enter values for Port, Shared Secret, Retran (sec), Max Retran, Enable Update. • Select EAP Authentication, Non-EAP Authentication, or both. <p>Note You must enter <i>all</i> of these parameters in the template for each server you want to retain after the conversion. Failure to provide the complete set will result in missing AAA-related commands in the IOS configuration.</p>

Step 10 From the left pane, select **Preview** to see your changes before you apply them.

Step 11 From the left pane, select **Save** to save the template.

A confirmation dialog appears asking if you want to apply this configuration template to one or more devices. *Do not apply the template now*. This template will be used in the next step.

Step 12 Select **No** to save the template *without* proceeding to the job definition screen.

Step 13 Go to [Task 5. Create and Run the Conversion Job](#).

Task 5. Create and Run the Conversion Job

This section explains how to:

- Create, save, and run a conversion job—See [Creating and Running a Conversion Job, page 1-15](#)
- Monitor a running conversion job—See [Checking the Progress of a Running Conversion Job, page 1-18](#)
- Manage the converted devices—See [Managing Converted Devices, page 1-19](#)

Creating and Running a Conversion Job

Before You Begin

**Caution**

Run a conversion job with one access point *before* running a job on multiple devices. If you are converting more than one type of access point, run a test job on each type of device. If possible, do not run the tests on your production network.

**Caution**

Limit each job to 10 access points, and run only one job at a time. Problems encountered while converting large numbers of access points can cause disruptions in the network.

Procedure

Step 1 Log on to the WLSE and select **Firmware > Jobs**.

For information about using the firmware upgrade options, see the WLSE online help or the “Upgrading Firmware” chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.11*. You can view this guide on Cisco.com at cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm.

Step 2 Click **Create Job**.

Step 3 Enter the following:

- A name for the job and an optional description.
Job names must be unique. Do not use the same job name for firmware jobs and other jobs (such as configuration and radio management jobs).
- Select **SNMP**.



Note

Although the job conversion screens in the WLSE Firmware tab list both SNMP and HTTP as protocols to use for conversion, only SNMP is allowed for conversions. *The job will fail if you select HTTP.*

Step 4 From the left pane, click **Select Image**. Expand the device folder and select the special conversion image.

Step 5 From the left pane, click **Select Devices**.

- a. Expand the folder that contains the access points to be converted.
- b. From the Available Devices list, select a group or individual devices and click **Add**.



Note

Normally, you should include no more than 10 access points in a job.

Step 6 From the left pane, click **Schedule Job**.

- To run the job immediately after you finish creating the job, select **Run Now**.
- To schedule the job for later, select the date and time.

Step 7 From the left pane, click **Options**. To specify job options:

- a. (Optional) In the Email settings section, you can specify email notification upon completion of the job.



Note

Do not use the Remote Server option. It is not applicable for non-IOS to IOS conversions.

- b. The IOS Security Parameters section appears only if you selected a valid conversion image in Step 3. If it does not appear, return to **Select Image** and select the correct image.

- c. In the IOS Security Parameters section:
- Enter the enable password. This password will become the AP enable password after the APs are converted to IOS. *All converted access points will have the same enable password.*



Note Please remember this password. If this password is forgotten, there is no way to recover it after the conversion job has completed and it has been assigned to the AP. To recover this password, you must use the password recovery procedure on the IOS AP.

- Select the non-IOS conversion template from the Select Config Template list. This is the same template that was created in [Task 4. Create a Conversion Template on the WLSE](#).

Step 8 From the left pane, click **Save** to validate the job settings, view a job summary, and run the job immediately or add it to the list of scheduled jobs.

The Save window shows information about the job. For details about the messages in this window, see the Firmware online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.11*.



Note If there are warning or error messages in the Save window, the job will either fail or it will only succeed on the devices that have no warnings or errors. You can edit your job choices to eliminate the problems, then click **Save** in the left pane.

Step 9 When the job is ready to run, click **Save** in the Save window. The Job Summary page displays basic information about the job, and the job will run immediately or will be added to the job list if it is scheduled for a later time.

Step 10 Monitor the progress of the job (see [Checking the Progress of a Running Conversion Job, page 1-18](#)).

Checking the Progress of a Running Conversion Job

Procedure

- Step 1** Use the device console to monitor the progress of the job.
- Step 2** When the job is done, select **Firmware > Jobs**.
- Step 3** Select the job name and click **Job Run Detail**.
- If the job status is “not verified:”
 - First, *check the access points* to find out if they have been converted. For detailed information about the conversion status of each device, click **Job Run Log**.
 - If they have *not* been converted, rerun the job.
 - If they have been converted, *do not run the job again* on the converted access points.



Note

A job status of “not verified” does not always mean the job failed. The WLSE has internal timeout parameters for firmware upgrades. If the WLSE is unable to communicate successfully with the access point within the period specified by the timeout, it will declare the upgrade job unverified. The WLSE may have timed out before confirming that the job succeeded. To change the timing parameters, see [Adjusting the Timing Parameters, page 1-6](#).

- If the job status is “failed,” you can increase the value of the Conversion SNMP retries timeout parameter and rerun the job. To change this parameter, see [Adjusting the Timing Parameters, page 1-6](#).

For additional troubleshooting help, see [FAQs and Troubleshooting, page 2-1](#).

- Step 4** After the conversion job has completed successfully, you must set the devices in the managed state (see [Managing Converted Devices, page 1-19](#)).
-

Managing Converted Devices

The converted access points must be in the managed state (that is, discovered, inventoried, and managed) before you can use the WLSE to monitor or configure them or use any of the other WLSE network management or radio management features.

Procedure

-
- Step 1** After the conversion job has completed successfully, all access points in the job will come up as IOS. WLSE automatically detects these converted APs as IOS AP types and moves them into the appropriate System groups.
- Step 2** Select **Devices > Discover > Inventory > Run Inventory**.
- Step 3** Select the newly converted devices and click **Run Inventory**.
- After the inventory process completes, the access points will be in the managed state on the WLSE. All supported WLSE IOS AP functionality can be used against these APs.
- Step 4** Go to [Task 6. Check the Results](#).
-

Task 6. Check the Results

After the conversion:

- You must run an inventory before you can use any of the WLSE IOS AP features.
- The access points will be running a version of IOS. The available upgrade images and the IOS versions after conversion are listed in [Table 1-1 on page 1-4](#).
- The sysOID changes.
- The device type and group membership changes. [Table 1-4](#) summarizes the group membership and device type changes:

Table 1-4 *Device Type and Group Membership Change Summary*

Before Conversion		After Conversion	
Device Type	Group	Device Type ¹	Group
Cisco Aironet AP350	AP350	Cisco Aironet AP350	AP350-IOS
Cisco Aironet AP1200	AP1200	Cisco Aironet AP1210	AP1210 ²
Cisco Aironet AP1220	AP1200	Cisco Aironet AP1230	AP1210

1. The software images listed in the WLSE Supported Device Table now apply to the converted access points.
2. The WLSE does not differentiate between the AP1200 and the AP1220 and both are placed in the same group (1210) after the conversion



FAQs and Troubleshooting

This chapter consists of the following sections:

- [Conversion FAQs, page 2-1](#)
- [Conversion Troubleshooting, page 2-4](#)

For additional FAQ and troubleshooting information on firmware jobs, see the Firmware chapter in the *FAQ and Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*. You can access this guide by clicking **Troubleshooting** in the WLSE online help or on Cisco.com at http://cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11.

Conversion FAQs

FAQ Summary

- [What are the supported non-IOS \(VxWorks\) versions for converting APs to IOS APs?](#)
- [Are there other requirements for the non-IOS access points to be converted?](#)
- [What tasks will the conversion job perform?](#)
- [Why does the conversion take so much time?](#)
- [Why is the remote server option not supported for non-IOS to IOS conversion?](#)
- [Why is it recommended to upgrade only up to 10 devices at a time?](#)

- [Why do I need to provide a separate non-IOS template in the Options page?](#)
 - [How do I increase the SNMP timeout?](#)
 - [In the Options screen, why am I not seeing the “Provide IOS Parameters” link?](#)
 - [When should I increase the advanced firmware parameters \(Firmware > Advanced Parameters\)?](#)
-

- Q.** What are the supported non-IOS (VxWorks) versions for converting APs to IOS APs?
- A.** See [Table 1-1 on page 1-4](#).
- Q.** Are there other requirements for the non-IOS access points to be converted?
- A.** See [Task 1. Satisfy the Prerequisites, page 1-3](#).
- Q.** What tasks will the conversion job perform?
- a. Download the .ini file from the non-IOS device.
 - b. Combine the security template with the downloaded .ini file.
 - c. Convert the non-IOS configuration to IOS configuration.
 - d. Encapsulate the IOS configuration with the upgrade image.
 - e. Disable the radios, set the event log message count to zero, and reboot.
 - f. After the device comes up, upload the special image.
 - g. After the image is uploaded, the device will reboot itself.
 - h. While rebooting, IOS will be installed.
 - i. Save the running configuration file to the startup configuration file.
- Q.** Why does the conversion take so much time?
- A.** Conversion is different from a normal firmware upgrade because the conversion image is larger. It takes time to create the image with the converted configuration, upload the image, install IOS, and reboot the AP twice. A 350 AP takes up to 25 minutes to convert, and a 1200 or 1220 AP takes up to 20 minutes to convert.

- Q.** Why is the remote server option not supported for non-IOS to IOS conversion?
- A.** The remote server option works well when the same image is applied to multiple APs. For conversion, the upgrade image is unique for each device because the image includes the device configuration file. Therefore, pushing the same image to each device cannot be done during conversions.
- Q.** Why is it recommended to upgrade only up to 10 devices at a time?
- A.** On slow band lengths, the conversion process is time consuming. The limit allows easier for monitoring and successful completion of the job.
- Q.** Why do I need to provide a separate non-IOS template in the Options page?
- A.** The configured security parameters in the AP cannot be retrieved because they have write-only permissions. Therefore, such parameters must be re-entered by applying a template to make sure the access point is configured correctly after the conversion.
- Q.** How do I increase the SNMP timeout?
- A.** See [Adjusting the Timing Parameters, page 1-6](#).
- Q.** In the Options screen, why am I not seeing the “Provide IOS Parameters” link?
- A.** This link will be shown only if you chose a special non-IOS to IOS upgrade image. The upgrade image names for 350 or 1200 series access points are listed in [Table 1-1 on page 1-4](#).
- Q.** When should I increase the advanced firmware parameters (**Firmware > Advanced Parameters**)?
- A.** See [Adjusting the Timing Parameters, page 1-6](#).

Conversion Troubleshooting

Symptom Summary

- Some of the configuration parameters in the non-IOS AP are not being converted.
 - The conversion job is failing with an SNMP timeout error.
 - My AP is unreachable after conversion, even though I had no problems during conversion.
 - The message ERROR: Ethernet port is not configured as primary port is in the conversion job log.
 - After conversion from VxWorks to IOS when hot standby features are being used, the standby AP does not properly associate with the active unit. The standby unit incorrectly tries to take on an active role, even though the active unit is fully functional.
 - I cannot log in to a converted access point.
 - IOS commands are failing.
 - The message Policy_policy_fallback_policy was created using CLI. It must be deleted via CLI to ensure proper operation of the web interface is produced by IOS software in the migrated configuration. This message is displayed under the Policy tab.
-

Symptom Some of the configuration parameters in the non-IOS AP are not being converted.

Possible Cause There are certain limitations to the conversion process.

Recommended Action Please check [Limitations of the Conversion Process, page A-1](#).

Symptom The conversion job is failing with an SNMP timeout error.

Possible Cause Lack of memory or timeout values are too small.

Recommended Action Check the firmware job log.

- If the conversion gets as far as “Waiting for IOS Install” in the job log and then fails, it could be because there is not enough memory. After the time out for the IOS install elapses, the job fails with an SNMP timeout error.

To check the available free memory on the AP, issue the CLI command `:vxdiag_memshow` on the non-IOS AP.

- Otherwise, try increasing the SNMP timeout.

To increase the SNMP timeout, see [Adjusting the Timing Parameters, page 1-6](#). Then rerun the job.

Symptom My AP is unreachable after conversion, even though I had no problems during conversion.

Possible Cause There are many possible causes.

Recommended Action Try the standard troubleshooting steps, such as:

- Purging the device
- Doing an SNMP ping from the WLSE
- Examining the console output
- Rebooting the device
- Checking the power connections and cabling

If these steps do not solve the problem please contact the TAC with the following information:

- Non-IOS configuration of the access point before conversion
- IOS configuration of the access point after conversion
- Non-IOS conversion template
- Job run log—Display the job run detail for the firmware job, then click **Job Run Log** to display the output

Symptom The message `ERROR: Ethernet port is not configured as primary port` is in the conversion job log.

Possible Cause The AP was configured to have one of the radio interfaces as the primary port.

Recommended Action Set Ethernet as the primary port. Otherwise the AP might have a different MAC address after conversion. If DHCP is enabled, the AP might have a different IP address, and the WLSE will not be able to contact the device.

Symptom After conversion from VxWorks to IOS when hot standby features are being used, the standby AP does not properly associate with the active unit. The standby unit incorrectly tries to take on an active role, even though the active unit is fully functional.

Possible Cause This condition occurs when the active unit is configured before conversion so that the Ethernet and radio interfaces are both using the same MAC and IP addresses.

Recommended Action To ensure that hot standby functionality works correctly after conversion, do one of the following:

- Before converting (recommended), ensure that the active unit running VxWorks is configured so that the radio and Ethernet interfaces each have their own unique IP and MAC addresses. Under **Setup > AP Radio > Identification**, the primary should be set so the radio interface does *not* adopt primary port identity. Be sure that the standby unit is monitoring the MAC address of the radio interface of the primary.

This option is recommended because it ensures continuous availability of a backup access point during the conversion process. The conversion job should be sequenced so that the standby AP is fully converted and operational before conversion is started on the active unit. Then, when the active unit resets during conversion, the standby can take over its functions.

- After converting, configure the standby unit so it is monitoring the MAC address of the radio interface on the active unit.

Note that in the case when an active unit that has failed is restored to service, the AP that was taking its place should be reset to force it back into a standby role, and any clients that it was serving should be forced to reassociate with the newly restored active AP.

Symptom I cannot log in to a converted access point.

Possible Cause The proper security information was not entered in the conversion template.

Recommended Action

- If User Manager is *enabled* on the AP and you do not enter the following security information in the conversion template (under **Configure > Template > NonIOS Template> SECURITY > Local Admin Access**): User Identifier, User Name, User Password, Confirm User Password and Capabilities, you might not be able to log in to the converted AP through Telnet, the console port, or the browser. If this occurs, you must reset the AP to its defaults. For more information about resetting the AP to its default configuration, see the access point documentation.
- If User Manager is *disabled*, authentication is not required but you can use only the console port to log in to the upgraded access point.

Symptom The message `Policy_policy_fallback_policy` was created using CLI. It must be deleted via CLI to ensure proper operation of the web interface is produced by IOS software in the migrated configuration. This message is displayed under the Policy tab.

Possible Cause The configured setting for DSCP is not a specific value (0, 1, 2, 3, 4, 5, 6, 7, 11, 12, 21, 22, 23, 31, 32, 33, 41, 42, or 43).

Recommended Action Even though this error message is displayed, the migrated configuration and its associated functionality are correct.

Symptom IOS commands are failing.

Possible Cause For some VxWorks parameter settings, if the values are set outside the ranges listed in the following table, the IOS command will fail.

Command	IOS Range
Maximum RTS Retries and Maximum Date Retries	1 to 128
Data Beacon Rate	1 to 100
Beacon Period	20 to 4000
WEP Key Rotation Interval	1 to 10
BTIM	1 to 100

Recommended Action If the IOS command fails, you must manually enter the command or apply a configuration template after the conversion.



Limitations of the Conversion Process

Because of differences between the configuration settings in non-IOS APs and IOS configuration settings, the conversion process has the following limitations.

Settings	Limitations	Implications and Workarounds
AAA	Retransmission settings range from 1 to 100.	If the configured setting is greater than 100, the migrated setting is 100. If the configured setting is less than 1, the migrated setting is 1.
	Separate EAP and non-EAP server settings do not migrate.	Once a server is enabled, all users are configured to use that server.
	LEAP usernames do not migrate.	
	Following AAA server parameters do not migrate: <ul style="list-style-type: none"> • Port configuration settings for TACACS server • 802.1X protocol version for EAP authentication • Update delay per server 	

Settings	Limitations	Implications and Workarounds
Boot server and DHCP	BOOTP is not supported by IOS.	You should convert from BOOTP to DHCP before proceeding with the AP conversion.
	Following Boot Server parameters do not migrate: <ul style="list-style-type: none"> • DHCP Multiple-Offer Timeout • DHCP Requested Lease Duration • DHCP Minimum Lease Duration • DHCP Client Identifier Value 	
	Only DHCP configuration settings with a Client Identifier type of Ethernet migrate; all other Client Identifier types are discarded.	
	If DHCP is configured, the fall-back IP address will not be configured.	
CDP	CDP information on a per-interface basis does not migrate.	
Ethernet	Following parameters do not migrate: <ul style="list-style-type: none"> • Optimize Network for maximum multicast packets per second • Loss of backbone connectivity timeout • Maximum multicast packets per second 	

Settings	Limitations	Implications and Workarounds
Filters	Default multicast address filtering for an interface does not migrate.	
	Separate filters are created for Ethertype filters, IP port filters, and IP protocol filters that have been set to non-default priority.	Conversion may create multiple filters with the same numeric identifier, but the conversion inserts a numeric index to differentiate the filters.
	If both port and protocol filters are applied on an interface, this setting does not migrate.	
	IP port filters—Will be created in the format IP access list extended Port_ <i>PortId</i> .	
	Ethertype filters—A maximum of 100 Ethertype filters can be created. Ethertype filters will not have associated names; instead, they will have associated numbers ranging from 200 to 299.	
	Protocol filters—Will be created in the format IP access list extended PF_ <i>ProtocolId</i> .	
	Ether filters —Will be created in one of the following formats: <ul style="list-style-type: none"> access-list <i>Numeric_Value</i> permit deny <i>Protocol-Type</i> 	
	MAC-based filters—Only MAC-based filter settings with the following will migrate: <ul style="list-style-type: none"> SSIDs associated to a VLAN MAC authentication enabled 	
FTP and TFTP	Configuration parameters do not migrate.	
HTTP	Only the HTTP port and the Enable or Disable settings will migrate.	
Policy Groups	Policy groups are created in the format policy-map_policy <i>Name Policy_ID</i> .	
	Policy groups without an associated VLAN do not migrate.	

Settings	Limitations	Implications and Workarounds
Port Assignments	<p>Port assignment settings are supported only in the non-IOS environment; therefore, these settings do not migrate.</p> <p>The purpose of the port assignments feature is to ensure that a root AP that has repeaters connected to it will always show the repeaters as neighbors using the same interface for CDP. Thus, an application that is drawing topology maps will always show the same topology.</p>	<p>If you have not made any changes to the default settings in the port assignments page, you can ignore this setting.</p> <p>If repeater APs are reset (possibly due to a power outage), they may appear to be on different interfaces when they come back. Some network management applications might detect this as a change in network topology. You should ignore any messages indicating topology changes from such applications because no actual change in topology has occurred.</p>
Timeouts	<p>The following settings do not migrate:</p> <ul style="list-style-type: none"> • Rogue AP Alert Timeout • Unknown Class Timeout • Multicast Addresses Timeout • Infrastructure Hosts, Client Stations, and Repeater Timeout 	
VLANs	<p>VLANs migrate only when they are associated with an SSID, except for the native VLAN. The native VLAN will migrate even if it is not associated with an SSID.</p>	



Numerics

- 802.11g radios, not supported by conversion [1-5](#)
- 802.1X protocol version for EAP authentication, migration of [A-1](#)

A

- AAA settings, changed or not migrated [A-1](#)
- AP 1200 [1-4, 1-19](#)
- AP 1210 [1-19](#)
- AP 1220 [1-4, 1-19](#)
- AP 1230 [1-19](#)
- AP 350 [1-4, 1-19](#)
- audience for this document [v](#)

B

- BOOTP settings not migrated [A-2](#)
- boot server parameters, migration of [A-2](#)

C

- CAC Tool [1-1](#)

cautions

- conversion template requirements [1-10](#)
- limitation on number of APs in a job and number of jobs [1-15](#)
- run a test job [1-15](#)
- significance of [vi](#)
- upgrade images [1-1](#)
- CDP, per-interface information not migrated [A-2](#)
- Cisco Aironet Conversion Tool [1-1](#)
- conversion jobs
 - checking status [1-18](#)
 - limit on number of APs [1-15, 2-3](#)
 - running [1-15](#)
 - SNMP timeout [2-3](#)
 - time required [2-2](#)
 - timing parameters for [2-3](#)
 - what they do [2-2](#)
- conversion log
 - messages in [1-18, 2-6, 2-7](#)
- convertible APs [1-4](#)
- convertible VxWorks versions [1-4](#)

D

- device types, after conversion [1-19](#)

DHCP

- affects on conversion process [1-5](#)
- settings not migrated [A-2](#)

documentation

- audience for this [v](#)
- locating on Cisco.com [vi](#)
- typographical conventions in [v](#)

E

EAP settings, migration of [A-1](#)

Ether filters, migration of [A-3](#)

Ethernet

- Ethernet port is not configured as primary port message in job log [2-6](#)
- settings not migrated [A-2](#)

Ethernet port is not configured as primary port is in the conversion job log [2-6](#)

Ethertype filters, migration of [A-3](#)

F

FAQs [2-1](#)

filter settings, migration problems [A-3](#)

FTP settings not migrated [A-3](#)

H

hot standby, problem after conversion [2-6](#)

HTTP

not supported for conversion jobs [1-16](#)

settings not migrated [A-3](#)

I

images for conversion, names of [1-10](#)

IOS commands, failure of after conversion [2-8](#)

IP port filters, migration of [A-3](#)

L

LEAP usernames, migration of [A-1](#)

login to AP after conversion [2-7](#)

M

MAC-based filters, migration of [A-3](#)

migration problems

AAA settings [A-1](#)

BOOTP [A-2](#)

CDP [A-2](#)

DHCP [A-2](#)

Ethernet parameters [A-2](#)

filter settings [A-3](#)

FTP configuration [A-1](#)

HTTP settings [A-3](#)

policy groups [A-3](#)

port assignments [A-4](#)

requirements for VLANs [A-4](#)

TFTP configuration [A-1](#)

timeouts [A-4](#)

Multicast Addresses Timeout, not migrated [A-4](#)

P

permissions, for conversion [1-4](#)

Policy_policy_fallback_policy error message [2-7](#)

policy groups, migration problems [A-3](#)

port assignments, not migrated [A-4](#)

protocol filters, migration of [A-3](#)

R

remote TFTP server, not supported for conversion [2-3](#)

repeaters

conversion not supported [1-4](#)

migration [A-4](#)

Repeater Timeout, not migrated [A-4](#)

reversing conversions [1-2](#)

Rogue AP Alert Timeout, not migrated [A-4](#)

S

SNMP timeout, increasing [2-3](#)

sysOID, after conversion [1-19](#)

system groups (WLSE), after conversion [1-19](#)

T

TACACS server settings, migration of port configuration [A-1](#)

template for conversion

optional parameters [1-13](#)

parameters ignored [1-10](#)

required parameters [1-12](#)

why required [2-3](#)

TFTP

remote server conversion method not supported [2-3](#)

settings not migrated [A-3](#)

timeout settings, not migrated [A-4](#)

timing parameters

adjusting on WLSE [1-6](#)

when to increase [2-3](#)

troubleshooting

AP not reachable after conversion [2-5](#)

IOS commands fail [2-8](#)

login fails [2-7](#)

parameters not converted [2-4](#)

SNMP timeout error in conversion log [2-5](#)

standby AP tries to become active [2-6](#)

typographical conventions in this document [v](#)

U

Unknown Class Timeout, not migrated [A-4](#)

V

VLANs

conversion of [1-5](#)

migration requirements for [A-4](#)

VxWorks versions that can be converted [1-4](#)

W

WAN links, affects on conversion [1-4](#)