



Cisco Aironet Conversion Tool for Cisco IOS Software, 2.1 Administrator Guide for Windows

July 2004

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-3738-03



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

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

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

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

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

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)



Preface v

Audience	vi
Purpose	vi
Organization	vi
Conventions	vi
Related Publications	vii
Obtaining Documentation	vii
Cisco.com	vii
Documentation CD-ROM	vii
Ordering Documentation	viii
Documentation Feedback	viii
Obtaining Technical Assistance	viii
Cisco TAC Website	viii
Opening a TAC Case	ix
TAC Case Priority Definitions	ix
Obtaining Additional Publications and Information	ix

CHAPTER 1

Overview 1-1

Overview of the Conversion Tool	1-2
Before You Begin	1-3
Obtaining the Conversion Tool Software	1-5
Obtaining the Helper Image	1-5
Installing or Upgrading the Conversion Tool	1-6
Running the Conversion Tool	1-6
Summary of Operations	1-9
Uninstalling the Conversion Tool	1-10
Finding the Configuration Tool Version	1-10
Finding the Access Point Software Version	1-11

CHAPTER 2

Device Configuration 2-1

- Device Configuration Window 2-2
- Device Type Options 2-3
- Source Configuration Parameters 2-3
- Target Configuration Parameters 2-4
- Hot Standby Configuration 2-6
- Interface for Communicating with Target Access Point 2-7
- Next Button 2-7

CHAPTER 3

Security Configuration 3-1

- Security Configuration Window 3-2
- LEAP Configuration for a Repeater 3-4
- User Manager Configuration 3-5
- AAA Server Configuration 3-5
- WEP Key Configuration 3-6

CHAPTER 4

Using the Conversion Tool 4-1

- Adding a Task 4-2
- Starting a Task 4-8
- Viewing the Task Log 4-9
- Log Error Messages 4-11
 - Warning Error Messages 4-15
- Viewing the Cisco IOS Configuration 4-18
- Adding Multiple Tasks 4-19

APPENDIX A

Upgrading an Access Point to Cisco IOS Operation Without the Conversion Tool A-1

- Cisco IOS Upgrade Procedure A-1

APPENDIX B

Requirements and Limitations B-1

- Important Note B-2
- System Requirements B-2
- Conversion Tool Operating Cautions B-3
- Limitations in the Cisco IOS Configuration B-5

INDEX



Preface

This section describes the objectives, audience, organization, and conventions of the *Cisco Aironet Conversion Tool for Cisco IOS Software, 2.1 Administrator Guide for Windows*.

The following topics are covered in this section:

- [Audience, page vi](#)
- [Organization, page vi](#)
- [Conventions, page vi](#)
- [Related Publications, page vii](#)
- [Obtaining Documentation, page vii](#)
- [Obtaining Technical Assistance, page viii](#)

Audience

This publication is for the administrator responsible for upgrading existing VxWorks Cisco Aironet 350 or 1200 series access points to Cisco IOS operation. The administrator should be familiar with Cisco Aironet access points and with network structures, terms, and concepts.

Purpose

This publication describes the Cisco Aironet Conversion Tool for Cisco IOS Software (hereafter called the *conversion tool*) and provides instructions for upgrading VxWorks 350 and 1200 series access points to Cisco IOS operation. This publication also provides instructions for storing a Cisco IOS configuration file on your PC.

Organization

This guide contains the following sections:

[Chapter 1, “Overview,”](#) provides an overview of the conversion tool and how to obtain it.

[Chapter 2, “Device Configuration,”](#) describes the device configuration parameters.

[Chapter 3, “Security Configuration,”](#) describes the security configuration parameters.

[Chapter 4, “Using the Conversion Tool,”](#) describes how to use the tool.

[Appendix A, “Upgrading an Access Point to Cisco IOS Operation Without the Conversion Tool,”](#) describes how to upgrade a VxWorks access point to Cisco IOS operation without converting the configuration data.

[Appendix B, “Requirements and Limitations,”](#) describes the conversion tool’s requirements and limitations.

Conventions

This publication uses the following conventions to convey instructions and information:

- Commands and keywords are in **boldface** type.

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

**Caution**

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

Related Publications

For more information about access points, refer to the following publications:

- *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* provides configuration information.
- *Cisco Aironet 1200 Series Access Point Hardware Installation Guide* provides hardware installation information.
- *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* provides a description of Cisco IOS commands supported by the 1200 and 350 series access points.
- *Cisco Aironet 350 Series Access Point Hardware Installation Guide* provides hardware installation information.

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

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

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

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

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

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

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

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

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco TAC Website

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

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

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

Opening a TAC Case

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

TAC Case Priority Definitions

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

<http://www.ciscopress.com>

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

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

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

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

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

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

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

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



Overview

This chapter provides an overview of the conversion tool used by administrators to upgrade VxWorks Cisco Aironet 350 or 1200 series access points and their configuration to Cisco IOS operation.

The following topics are covered in this chapter:

- [Overview of the Conversion Tool, page 1-2](#)
- [Before You Begin, page 1-3](#)
- [Obtaining the Conversion Tool Software, page 1-5](#)
- [Obtaining the Helper Image, page 1-5](#)
- [Installing or Upgrading the Conversion Tool, page 1-6](#)
- [Running the Conversion Tool, page 1-6](#)
- [Summary of Operations, page 1-9](#)
- [Uninstalling the Conversion Tool, page 1-10](#)
- [Finding the Configuration Tool Version, page 1-10](#)
- [Finding the Access Point Software Version, page 1-11](#)

Overview of the Conversion Tool

The conversion tool is a special utility that is used by administrators to do the following:

- Create a Cisco IOS configuration using the configuration of an existing VxWorks 350 or 1200 series access point. [Table 1](#) identifies the access points, VxWorks versions, and images supported by the conversion tool.



Note The conversion tool does not support VxWorks 350 and 1200 series access points running operating system version 12.04. Access points running operating system version 12.04 must be downgraded to a supported operating system version before using the conversion tool.

Table 1 Supported Access Points, VxWorks Versions, and Images

Access Points	VxWorks Versions	Helper Image Filename	Cisco IOS Version (after conversion)
AP1200 AP1220	12.03T, 12.02T1, 12.01T1, 12.00T, 11.56, or 11.54T	AP1200-Cisco-IOS-Upgrade-Image-v3.img	12.2(11)JA3
AP350	12.03T, 12.02T1, 12.01T1, 12.00T, 11.23T, or 11.21	AP350-Cisco-IOS-Upgrade-Image-v2.img	12.2(13)JA1

- Store a Cisco IOS configuration file on your PC for later use.
- Upgrade VxWorks 1200 series access points to Cisco IOS operation by combining the Cisco IOS configuration file with a 1200 series helper image.
- Upgrade VxWorks 350 series access points to Cisco IOS operation by combining the Cisco IOS configuration file with a 350 series helper image.



Note The conversion tool does not support 802.11g radios. You must ensure that the VxWorks access points do not contain 802.11g radios before using the conversion tool.

To find your access point software version (Cisco IOS or VxWorks) refer to the [“Finding the Access Point Software Version”](#) section on page 1-11.



Caution

The conversion tool cannot reverse the Cisco IOS upgrade process. Be sure you want to upgrade your access point to Cisco IOS operation before using the conversion tool.



Tip

If you want to upgrade a VxWorks 350 or 1200 series access point to Cisco IOS operation without preserving the existing configuration for that access point, refer to Appendix A.

Before You Begin

Before you begin, you must observe the following conversion tool requirements:

- The conversion tool operates only on a PC with the Windows 2000 or XP operating system and is not supported if Terminal Services is installed.
- The conversion tool requires the following minimum PC hardware:
 - Processor: Pentium III or equivalent
 - Speed: 850 MHz
 - RAM: 128 MB
 - Hard disk free space: 250 MB (4 MB for each helper image upgrade task)

When using the minimum PC hardware, the conversion tool supports up to 14 parallel helper image upgrades. You can enter up to 20 tasks, but only 14 of the tasks (maximum) can be helper image upgrades, and the remaining tasks can be used to store the access point's Cisco IOS configurations on your hard disk. Prior to starting multiple helper image upgrade tasks, you should verify that your PC has sufficient disk space.

**Note**

When you upgrade your access points, you can recover disk space on your PC by deleting the Cisco IOS configurations (with helper images) that were saved in the ConversionToolDirectory/images folder.

**Note**

The limit of 14 parallel helper image upgrades depends solely on the ability of the system and the network to handle multiple TFTP jobs. Faster systems, disks, and networks may be able to handle more parallel upgrade tasks, though too many tasks impact the speed of the individual tasks.

- The person installing and running the conversion tool must be logged in and must be the administrator of the PC.
- All access points (source and target) must have a user enabled with full access privileges (Write, SNMP, Ident, Firmware, and Admin)..

**Note**

For additional information on SNMP, refer to the *Cisco IOS Software Configuration Guide for Access Points*.

- SNMP must be enabled on the source and target access points.
- The conversion tool uses SNMP commands to obtain configuration data from the source access point, but some security information cannot be accessed using SNMP. Before you use the conversion tool, you should obtain the following source access point security information:
 - The WEP keys used for the radio interfaces and VLANs
 - The LEAP passwords for repeater access points
 - The passwords used with the User Manager Configuration
 - AAA Server Configuration Secret Keys

- The upgrade process requires the following minimum contiguous free space in your VxWorks access points to be successful:
 - 4.0 MB for 1200 series access points
 - 4.2 MB for 350 series access points



Note You can verify the amount of contiguous free memory in your access point by connecting to your access point using the console port or a Telnet session and entering the command **:vxdiag_memshow**. The amount of contiguous free memory is listed in the *max block* column.

Complete these steps to increase the amount of free memory in your access point:

- If your access point runs an .ini configuration file acquired by choosing the **Download All System Configuration** options from the Web interface, replace the configuration with an .ini file acquired by choosing the **Download Non-Default System Configuration** option.
- On Cisco Aironet 1200 series access points, you can remove the 802.11a radio module to obtain additional free space.

If necessary, you can free additional memory in your access point by performing these steps:

- Access the **Advanced** page (Setup > Associations > Advanced).
 - Disable the **RFC 1493 802.1D Statistics in MIB (dot1dTpFdbTable)** and the **Aironet Extended Statistics in MIB (awcTpFdbTable)** options.
 - Enable the **Map Multicast Entries to Broadcast Entry** option.
- The conversion tool should be used over Ethernet LANs and not over slower networks.



Caution

You must ensure that the same Ethernet and duplex settings are configured on all VxWorks access points and switches prior to beginning the conversion process. Different settings can result in inoperable access points that constantly power off and on.

- The Cisco Aironet 350 access point conversion process can take up to 30 minutes.
- Cisco IOS access points do not allow the radio interface to adopt the Ethernet port identity that allows the radio and Ethernet interfaces to use the same IP and MAC addresses.



Caution

During the Cisco IOS conversion process, the radio interface MAC address for your access points might change from the original setting, resulting in lost repeater associations and failure of the hot standby option. This happens because Cisco IOS software does not support the VxWorks *Adopt Primary Port Identity* option for the radio interfaces. Before you begin the conversion process, Cisco recommends that you change your VxWorks configurations to disable the *Adopt Primary Port Identity* option and to use the actual radio interface MAC address in all repeater and hot standby configuration settings.

- If your VxWorks access points are configured to use BOOTP, you must change their configurations to support DHCP prior to running the conversion tool to avoid a conversion failure. For access point configured for BOOTP, the access point IP address changes during the conversion process, and the conversion tool is unable to complete the access point conversion.

Obtaining the Conversion Tool Software

To obtain the latest conversion tool software from the Cisco Web site, follow these steps:

-
- Step 1** Use your web browser to go to the Cisco Software Center at the following URL:
<http://www.cisco.com/cisco/software/navigator.html>
 - Step 2** Click the link for wireless software.
 - Step 3** Click the link for access points.
 - Step 4** Click the links for your specific access point.
 - Step 5** Click the link for the Aironet VxWorks to Cisco IOS conversion tool and image.
 - Step 6** Click the link for the 2.1 tool.
 - Step 7** Click the **Aironet-AP-Cisco-IOS-Conversion-Tool-v2.1.exe** file (where *v2.1* is the version number).
 - Step 8** Click **Download**.
 - Step 9** Read and accept the terms and conditions of the Software License Agreement.
 - Step 10** Save the file to your computer's hard drive; then exit the web browser.
-

Obtaining the Helper Image

The conversion tool uses a 350 or 1200 series access point helper image file to upgrade your VxWorks access point to Cisco IOS operation. To obtain the most recent 350 or 1200 series access point helper image from the Cisco Web site, follow these steps:

-
- Step 1** Use your web browser to go to the Cisco Software Center at the following URL:
<http://www.cisco.com/cisco/software/navigator.html>
 - Step 2** Click the link for wireless software.
 - Step 3** Click the links for the 350 or 1200 series access point.
 - Step 4** Click the link for the Aironet VxWorks to Cisco IOS conversion tool and image.
 - Step 5** Click the link for the 2.0 or 3.0 image.
 - Step 6** Click the 350 or 1200 series access point helper image file with the highest version number, such as AP350-Cisco-IOS-Upgrade-Image-v2.img or AP1200-Cisco-IOS-Upgrade-Image-v3.img (where *v2* or *v3* is the version number).
 - Step 7** Click **Download**.
 - Step 8** Read and accept the terms and conditions of the Software License Agreement.
 - Step 9** Save the file to your computer's hard drive; then exit the web browser.
-

Installing or Upgrading the Conversion Tool

Follow these steps to install or upgrade the conversion tool on your PC:

-
- Step 1** Close any Windows programs that are running.
 - Step 2** Prior to installing a new version of the conversion tool, you must uninstall any previous versions installed on your PC. (For additional information, refer to the [“Uninstalling the Conversion Tool”](#) section).
 - Step 3** Locate and double-click the downloaded conversion tool software on your hard drive. The conversion tool setup program activates.



Note If you did not uninstall the conversion tool, a message appears indicating that the conversion tool (CAC Tool) is already installed on your PC, click **OK** and uninstall the conversion tool. (For additional information, refer to the [“Uninstalling the Conversion Tool”](#) section).

- Step 4** Click **Next** on the Welcome window.
 - Step 5** If you want to specify a destination folder, click **Browse** to locate a different folder.
 - Step 6** Click **Next** to accept the destination folder. The Select Program Folder window appears.
 - Step 7** Specify a folder. Click **Next** to accept the folder.
 - Step 8** Click **Yes** or **No** to place a conversion tool shortcut on your PC desktop. The Setup Complete window appears.
 - Step 9** On the Setup Complete window, you can select to view a Readme file and launch the conversion tool by clicking the corresponding check boxes. Click **Finish** to complete the installation.
-

Running the Conversion Tool

The conversion tool installs and uses a TFTP server as a service (*CACToolTFTPService*) on your PC. When the tool is active, the TFTP server is active and when you exit the tool, the TFTP server is deactivated.

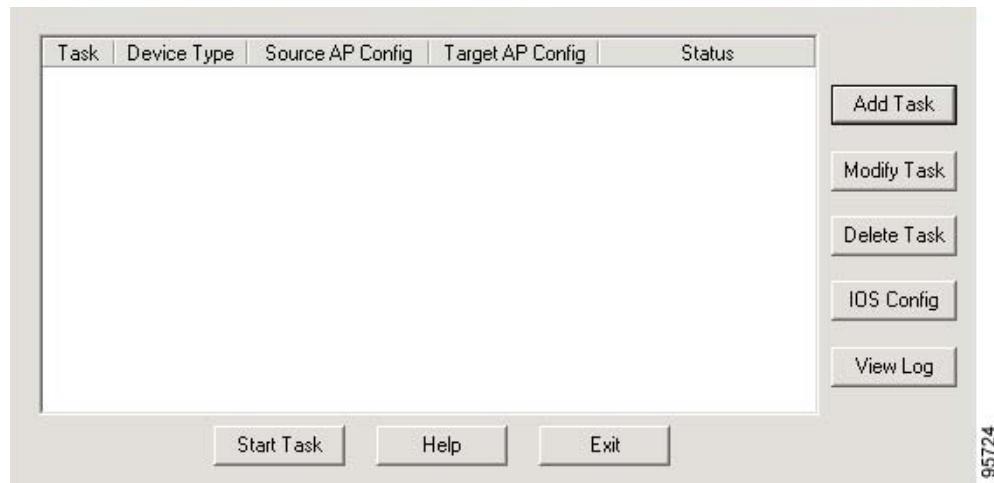


Note Prior to running the tool, you must deactivate any other TFTP servers you have installed on your PC.

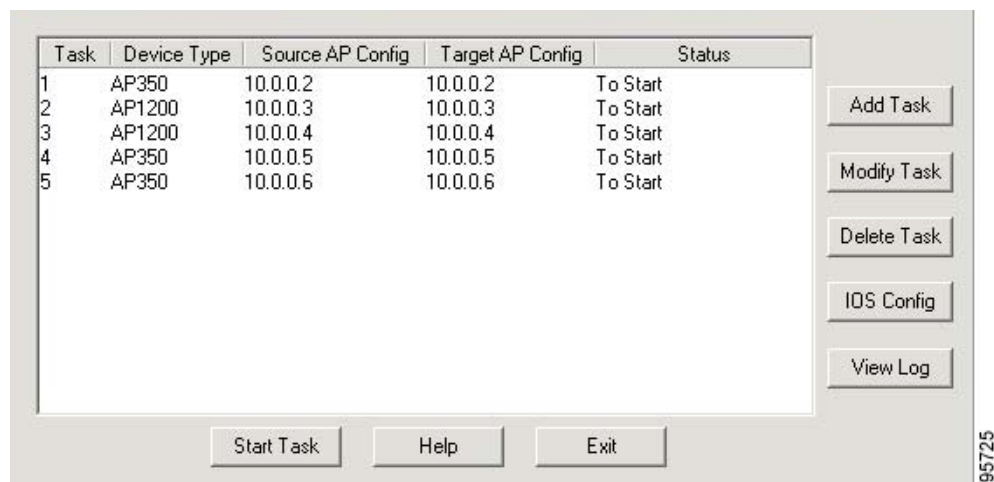
You activate the conversion tool by double clicking the **conversion tool** icon on your PC desktop or by clicking **Start > Programs > CAC Tool (or the name of your installation folder) > CAC Tool** (depending on the installation options selected). When you activate the conversion tool, the main window ([Figure 1-1](#)) appears. This window enables you to add, modify, delete, or start operating tasks that control the activities performed by the conversion tool. The buttons on the main window enable you to view an operating log, view the Cisco IOS configuration file, and exit the tool.



Note To use the conversion tool, you must be an administrator on the PC where the conversion tool is running.

Figure 1-1 Conversion Tool Main Window

The main window lists the operating tasks that have been added using the Add Task button (Figure 1-2).

Figure 1-2 Task Entries on Main Window

Each operating task listed on the main window contains the following fields:

- Task—a number used to identify the task.
- Device Type—indicates the access point type (350 or 1200 series access point)
- Source AP Config—indicates the location for the configuration information. Possible options are:
 - IP address of the VxWorks 1200 or 350 series access point used to obtain the configuration information.
 - Disk Storage—indicates the configuration file is located on your hard disk.
- Target AP Config—indicates the destination for the configuration information. Possible options are the IP address of the destination access point or Disk Storage to indicate that the file will be stored on your hard disk.

- Status—indicates the status of the task. Possible options are:
 - To Start—indicates the task is waiting to start.
 - Progress bar—indicates that the task progress by the length of the bar.
 - Learning Configuration—indicates that the conversion tool is obtaining configuration information from the source access point.
 - Completed—indicates that the task has executed successfully without any detected errors.
 - Error—indicates that an error has occurred during the execution of the task. For additional details on the error, click **View Logs**.
 - Warning—indicates that the conversion tool was not able to read some configuration data from the source access point. For additional information on the warning, click **View Logs**. If you are upgrading an access point, you may need to manually enter the missing configuration parameters into the access point.
 - Uploading Image—indicates that the helper image and configuration parameters are being uploaded into the target access point.
 - Checking Device Status—indicates that the conversion tool is checking the access point status after the image upgrade.

The conversion tool uses special colors in the status bar to provide a quick indication of the status (see [Table 1-2](#)).

Table 1-2 Status Bar Colors

Color	Description
Blue	Indicates that the task is progressing normally. Displayed during Learning Configuration and Uploading Image status indications.
Amber	Indicates that a status warning indication has occurred. Your attention is required to correct the problem in the access point configuration.
Red	Indicates that a status error indication has occurred. Your attention is required to identify the problem.

The buttons on the conversion tool main window are described in [Table 1-3](#).

Table 1-3 Conversion Tool Main Window Buttons

Buttons	Description
Add Task	Enables you to add single or multiple operating tasks to be performed.
Modify Task	Enables you to modify the information contained in a task.
Delete Task	Enables you to delete a task.
IOS Config	Enables you to view the contents of the Cisco IOS configuration file.
View Log	Enables you to view completion or error information on the operations performed.
Start Task	Starts the task operations.
Help	Provides help information on the conversion tool.
Exit	Closes and exits the conversion tool.

Summary of Operations

The conversion tool enables you to upgrade a single access point or multiple access points. The tool enables you to obtain the configuration data from a VxWorks access point and store the converted Cisco IOS configuration on your hard disk or directly apply the Cisco IOS configuration to a single access point. You can use the stored Cisco IOS configuration file on your hard disk to upgrade a single access point or multiple access points.

The following list indicates the basic operations needed to convert the configuration and upgrade a single access point:

1. Obtain the conversion tool software.
2. Obtain the 350 or 1200 series access point helper image file.
3. Click the Device Type down-arrow and select **AP350** or **AP1200**.
4. Add a conversion tool task with the following parameters:
 - a. Source Configuration—Device, IP address, and administrator username (refer to the [“Source Configuration Parameters”](#) section on page 2-3).
 - b. Target Configuration—Device, helper image file, password (if needed), IP address, and administrator username (refer to the [“Target Configuration Parameters”](#) section on page 2-4).
 - c. Hot Standby Configuration—Monitored radio MAC addresses (if needed). For additional information refer to the [“Hot Standby Configuration”](#) section on page 2-6.
 - d. Your PC’s network adapter IP address (refer to the [“Interface for Communicating with Target Access Point”](#) section on page 2-7).
 - e. Security Configuration—Passwords, secret keys, and WEP keys (refer to the [“Security Configuration”](#) section on page 3-1).



Note If you choose not to enter the Security Configuration information, your access point will be configured with default security settings.

5. Start the task and wait for it to complete.

If your task was to upgrade a VxWorks access point into a Cisco IOS access point, you should carefully review the Cisco IOS configuration data (refer to the [“Viewing the Cisco IOS Configuration”](#) section on page 4-18). Because of differences between VxWorks and Cisco IOS configuration parameters, you should also review the [“Limitations in the Cisco IOS Configuration”](#) section on page B-5.

The process for upgrading multiple access points is similar to upgrading a single access point. For additional information refer to the [“Adding Multiple Tasks”](#) section on page 4-19.

Uninstalling the Conversion Tool

Follow these steps to uninstall the conversion tool from your PC:

-
- Step 1** Double-click **My Computer > Control Panel > Add/Remove Programs**.
 - Step 2** Select **Cisco Aironet Conversion Tool for Cisco IOS Software**.
 - Step 3** Click **Add/Remove** or **Change/Remove**. The conversion tool setup program activates and uninstalls the tool and the icon from your PC.
 - Step 4** Close the **Add/Remove** and **Control Panel** windows.
-


Note

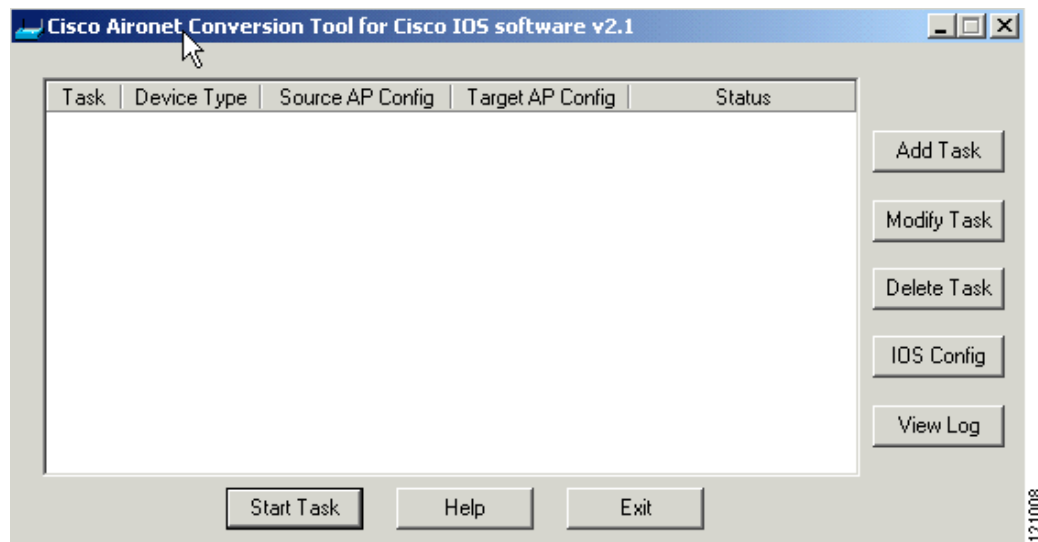
You can also select **Start > Programs > CAC Tool** (or the name of your installation folder) > **UnInstall** to uninstall the conversion tool.

Finding the Configuration Tool Version

To find the conversion tool version number follow these steps:

-
- Step 1** On the main window of the conversion tool, right-click the conversion tool name in the title line as shown by the cursor in [Figure 1-3](#).

Figure 1-3 Conversion Tool Title Line



Step 2 When the right-click window appears, click **About CAC Tool**.

The conversion tool About window (Figure 1-4) appears and contains the conversion tool version number. Version 2.1 is shown in the figure.

Figure 1-4 Conversion Tool About Window



Finding the Access Point Software Version

To find the version of Cisco IOS running on your access point, use a Telnet session to log into the access point and enter the **show version EXEC** command. This example shows command output from an access point running Cisco IOS Release 12.2(8)JA:

```
ap1200>show version
Cisco Internetwork Operating System Software
IOS (tm) C1200 Software (C1200-K9W7-M), Version 12.2(8)JA
Copyright (c) 1986-2003 by Cisco Systems, Inc.
```

On access points running Cisco IOS software, you can also find the software version on the System Software Version page in the access point's browser interface.

If your access point does not run Cisco IOS software, the software version appears at the top left of most pages in the browser interface. The home page on access points not running Cisco IOS software looks like Figure 1-5.

Figure 1-5 Home Page on VxWorks Access Points

Nwc-Lab5b-Bucki2 **Summary Status**

Cisco 1200 Series AP 12.00T

CISCO SYSTEMS

Uptime: 11 days, 20:21:48

Home Map Network Associations Setup Logs Help

Current Associations			
Clients: 0 of 3	Repeaters: 0 of 0	Bridges: 0 of 0	APs: 4

Recent Events		
Time	Severity	Description
7 days, 00:18:17	Info	Deauthenticating 00070eb96eb6, reason "Inactivity"
6 days, 23:51:37	Info	Station 00070eb96eb6 Associated
6 days, 23:51:37	Info	Station 00070eb96eb6 Authenticated
6 days, 23:50:32	Info	Deauthenticating 0040963398c9, reason "Inactivity"
6 days, 23:41:07	Info	Station 0040963398c9 Associated

Network Ports				<i>Diagnostics</i>
Device	Status	Mb/s	IP Addr.	MAC Addr.
Ethernet	Up	100.0	192.168.138.15	00059a3842c5
AP Radio: Internal	Up	11.0	192.168.138.15	00059a3842c5
AP Radio: Module	Up	54.0	192.168.138.15	00059a3842c5

90023



Device Configuration

This section describes the device configuration settings. The following topics are covered in this section:

- [Device Configuration Window, page 2-2](#)
- [Source Configuration Parameters, page 2-3](#)
- [Target Configuration Parameters, page 2-4](#)
- [Interface for Communicating with Target Access Point, page 2-7](#)
- [Next Button, page 2-7](#)

Device Configuration Window

The Device Configuration window (Figure 2-1) appears when you click the Add Task or Modify Task button on the main window. In this window you enter source (origin) and target (destination) access point configuration parameters. The source or target can be specified as a device or a disk storage location for a Cisco IOS configuration file created by the conversion tool. The device selection indicates that the source or destination is a VxWorks access point that is identified using the IP address field. When you have completed the Device Configuration window settings, click **Next**.


Note

The administrator username (Admin Name) must have admin, SNMP, firmware, and write capabilities on the access point. For additional information on SNMP, refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

The disk storage selection specifies that the source or destination is a Cisco IOS configuration file on your hard disk drive.

Figure 2-1 Device Configuration Window


Note

Your PC running the conversion tool must have an appropriate IP address and be able to ping the source or target access points. You can use either an Ethernet or a radio interface.

When you upgrade a target access point to Cisco IOS operation, the conversion tool uses an access point helper image file with a Cisco IOS configuration to create the Cisco IOS image for the target access point. The Cisco IOS configuration is created by the conversion tool using information obtained from a source VxWorks 350 or 1200 series access point. The helper image file is obtained from the Cisco Web site (refer to the “[Obtaining the Conversion Tool Software](#)” section on page 1-5).

Device Type Options

The Device Type section of the Device Configuration window enables you to specify the type of VxWorks access point that is being upgraded to Cisco IOS software. [Table 2-1](#) describes the available Device Type options.

Table 2-1 Device Type Options

Parameter	Description
Device Type	Specifies the device type used in the upgrade process. AP350 specifies the VxWorks 350 series access point and AP1200 specifies the VxWorks 1200 series access point. Range: AP350 or AP1200 Default: AP350

Source Configuration Parameters

The Source Configuration section of the Device Configuration window contains parameters that pertain to the source of the configuration information, which can be a device (access point) or disk storage (file location). When disk storage is specified, you must enter the path and filename of the Cisco IOS configuration file. When an access point is specified, you must enter the access point IP address and the username of an administrator that possesses admin, SNMP, firmware, and write capabilities on the access point.



Caution

You must ensure that the same Ethernet and duplex settings are configured on all VxWorks access points and switches prior to beginning the conversion process. Different settings can result in inoperable access points that constantly power off and on.

Table 2-2 describes the source configuration parameters.

Table 2-2 Source Configuration Parameters

Parameter	Description
From	Specifies the location of the source configuration. Click the drop-down menu to select the location. When the source location is an access point, select the Device option. When the source location is a configuration file, select the Disk Storage option. Options: Device or Disk Storage Default: Device
IP Address	Specifies the IP address of the source access point where the conversion tool obtains configuration information. Range: x.x.x.x, where x is a value from 0 to 255. Default: none
File Name	Specifies the path and filename for the Cisco IOS configuration file located on your PC. You can use the browse (...) button to browse to the location of the file. Path: drive:\directory\filename Default: C:\Program Files\Cisco Systems\CAC Tool\
Admin Name	Specifies an administrator username that has admin, SNMP, firmware, and write capabilities on the access point. Range: alphanumeric characters (case sensitive) Default: none Note Be careful entering the name because the entry is case sensitive and is not visible.

Target Configuration Parameters

The Target Configuration section of the Device Configuration window contains parameters that pertain to the target or destination of the configuration information, which can be a device (access point) or disk storage (file location). When disk storage is specified, you must enter the path and filename of the Cisco IOS configuration file. When an access point is specified, it is upgraded to Cisco IOS operation. Enter the access point's IP address, a username of an administrator that possesses admin, SNMP, firmware, and write capabilities on the access point, and the path and filename of the helper image file.



Caution

The conversion tool cannot reverse the Cisco IOS upgrade process. Be sure you want to upgrade your access point to Cisco IOS operation before selecting the Device option.



Note

The conversion tool maintains the host name and IP address configuration settings of the target access point. These target access point settings are not changed even when the source configuration parameters specify the use of a stored Cisco IOS configuration file.

Table 2-3 describes the target configuration parameters.

Table 2-3 Target Configuration Parameters


Parameters	Description
To	<p>Specifies the target location. Click the drop-down menu to select the location. When the target location is an access point, select the Device option. When the target location is a configuration file on your hard disk, select the Disk Storage option.</p> <p>Option: Device or Disk Storage</p> <p>Default: Disk Storage</p>
File Name	<p>Specifies the path and filename for the Cisco IOS configuration file to be stored on your PC. You can use the browse (...) button to browse to the location in which to save the file.</p> <p>Path: drive:\directory\filename</p> <p>Default: C:\Program Files\Cisco Systems\CAC Tool\</p>
Helper Image	<p>Specifies the path and filename of the helper image file on your PC.</p> <p>Path: drive:\directory\filename</p> <p>Default: none</p>
Enable Password	<p>Specifies the password used to login to the access point and used to prevent unauthorized users from reconfiguring your access point.</p> <p>Range: A string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. It can contain the question mark (?) character if you precede the question mark with the key combination (Ctrl-V) when you create the password; for example, to create the password abc?123, do this:</p> <ol style="list-style-type: none"> 1. Enter abc 2. Enter Ctrl-V 3. Enter ?123 <p>Note After the conversion, when your access point prompts you to enter the password, you need not precede the question mark with the Ctrl-V; you can simply enter abc?123 at the password prompt.</p> <p>Default: none</p> <p> Caution When using Ctrl-V, avoid accidentally inserting text from your Windows clipboard. Always check your password field to ensure that the correct number of characters is shown. Ctrl-V should not insert extra characters. If extra characters are detected, you can clear the Windows clipboard using the Windows clipboard viewer. Reenter your password.</p>

Table 2-3 Target Configuration Parameters (continued)

Parameters	Description
IP Address	Specifies the IP address of the target access point to be upgraded to Cisco IOS operation. Range: x.x.x.x, where x is a value from 0 to 255. Default: none
Admin Name	Specifies a username that has admin, SNMP, firmware, and write capabilities on the access point. Range: alphanumeric characters Default: none

Hot Standby Configuration

When the target location is an access point, you can specify the radio interface MAC addresses for the access point that the standby unit monitors. Hot Standby mode designates an access point as a backup for another access point. Typically, the standby access point is placed near the access point it monitors and is configured exactly the same. The standby access point associates with the monitored access point as a client and queries the monitored access point regularly through both the Ethernet and the radio ports. If the monitored access point fails to respond, the standby access point takes the monitored access point's place in the network. [Table 2-4](#) describes the Hot Standby configuration parameters.



Note

Access points using Cisco IOS software can be configured to support Hot Standby mode using the 2.4-GHz and 5-GHz radio interfaces.



Note

If your access point supports only one radio interface, provide the MAC address for that interface only.



Caution

During the Cisco IOS conversion process, the radio interface MAC address for your access points might change from the original setting, resulting in lost repeater associations and failure of the hot standby option. This happens because Cisco IOS software does not support the VxWorks *Adopt Primary Port Identity* option for the radio interfaces. Before you begin the conversion process, Cisco recommends that you change your VxWorks configurations to disable the *Adopt Primary Port Identity* option and to use the actual radio interface MAC address in all repeater and hot standby configuration settings.

Table 2-4 Hot Standby Configuration Parameters

Parameter	Description
MAC Address for Monitored 802.11B Radio	<p>Specifies the MAC address of the 802.11b (2.4-GHz) radio interface in the monitored access point. The MAC address is a unique 12-digit hexadecimal number used in radio data packets to identify your access point radio.</p> <p>Range: xxxx.xxxx.xxxx or xx:xx:xx:xx:xx:xx (where x is a value from 0 to 9 and a to f)</p> <p>Default: none</p>
MAC Address for Monitored 802.11A Radio	<p>Specifies the MAC address of the 802.11a (5-GHz) radio interface in the monitored access point. The MAC address is a unique 12-digit hexadecimal number used in radio data packets to identify your access point radio.</p> <p>Note When the AP350 device type is selected, this MAC address field is unavailable because an IEEE 802.11A radio is not supported on a 350 series access point.</p> <p>Range: xxxx.xxxx.xxxx or xx:xx:xx:xx:xx:xx (where x is a value from 0 to 9 and a to f)</p> <p>Default: none</p>

Interface for Communicating with Target Access Point

This field of the Device Configuration window specifies the IP address of your Ethernet adapter or your wireless client adapter that the conversion tool must use to communicate with the source and target access points. The conversion tool initially specifies the IP address of your primary network adapter. If the displayed address is not for the correct adapter, change the IP address to specify the correct adapter.



Note

When your PC contains multiple network adapters (Ethernet and wireless client), the conversion tool only verifies that the source access point is reachable from any of the network adapters. You must ensure that the specified adapter has an appropriate IP address to enable you to ping the source and target access points.

Next Button

When you complete the parameter entries on the Device Configuration window, click **Next**.

If you specified a target access point, a message appears indicating that the conversion tool cannot reverse the Cisco IOS upgrade process. Click **Yes**.

The Security Configuration window displays to enable you to enter security parameters. For additional information refer to [Chapter 3, “Security Configuration.”](#)



Security Configuration

This section describes the security configuration settings. The following topics are covered in this section:

- [Security Configuration Window, page 3-2](#)
- [LEAP Configuration for a Repeater, page 3-4](#)
- [User Manager Configuration, page 3-5](#)
- [AAA Server Configuration, page 3-5](#)
- [WEP Key Configuration, page 3-6](#)

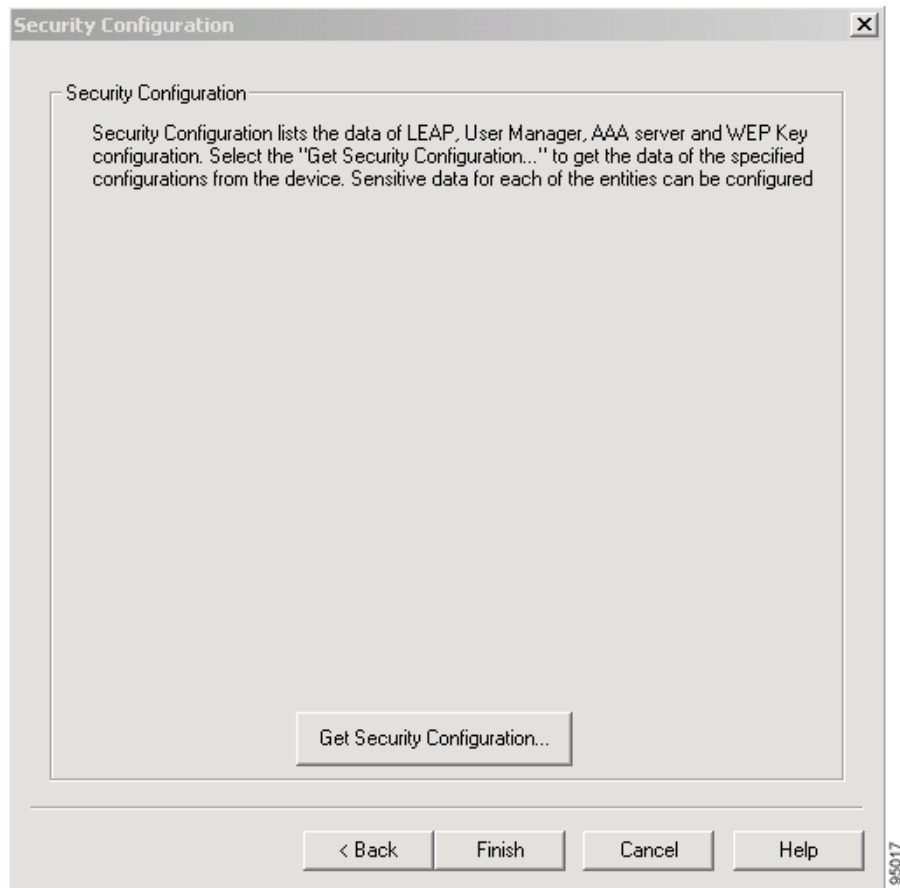
Security Configuration Window

The conversion tool cannot access the security passwords, secret keys, and WEP keys from an access point. The access point administrator must enter these parameters to allow the conversion tool to create a complete Cisco IOS configuration. Figure 3-1 shows the Security Configuration window with the Get Security Configuration button.


Note

If the source configuration is set for Disk Storage, the Security Configuration Window is not displayed.

Figure 3-1 Security Configuration Window



Cisco does not recommend that you bypass the entering of security information by clicking **Finish** on the Security Configuration window and clicking **No** on the message asking if you would like to configure the Security Configuration, for the following reasons:

- If you bypass the entry of security information and User Manager is disabled in your source access point, **the upgraded access point will only allow you to login using the console port.**
- If you bypass the entry of security information and if User Manager is enabled in your source access point, **the upgraded access point might not allow you to login.** All access to the access point may be blocked (Telnet, browser, and the console port). If this occurs, you must reset the access point to defaults using the mode button (refer to the Troubleshooting section of the *Cisco Aironet 1200 Series Access Point Hardware Installation Guide* or the *Cisco Aironet 350 Series Access Point Hardware Installation Guide*).

Clicking the Get Security Configuration button enables the conversion tool to obtain security information from your access point. When your VxWorks access point is powered up, click **Get Security Configuration** and a message appears indicating that the conversion tool is trying to gather security information from your access point.

When the conversion tool obtains the security information, the next Security Configuration window appears (Figure 3-2) and enables you to enter the passwords, secret keys, and WEP keys for your access point. When you have entered all security parameters, click **Finish** and the conversion tool's main window appears displaying your new task (see Figure 1-2 on page 1-7).

**Note**

The conversion tool encrypts the entered passwords, secret keys, and WEP keys for extra security.

Figure 3-2 Security Configuration Window

LEAP Configuration

Module	User Name	Password
11b	doc	
11a	doc	

Set Password

User Manager Configuration

Capabilities	Name	Password
Admin, Write, Firmware, doc		
Admin, Write, Firmware, doc2		

Set Password

AAA Server Configuration

Item	Type	IP address	Secret Key
1	Authentication	10.0.0.102	
2	Accounting	10.0.0.101	

Set Secret Key

WEP Key Configuration

VLAN ID	VLAN Name	Is WEP set ?
1	Vlan 1	No
5	Vlan 5	No

Def. 11b WEP
Def. 11a WEP
Set VLAN-WEP

< Back Finish Cancel Help

117960

The Security Configuration window buttons are described in [Table 3-1](#).

Table 3-1 Security Configuration Window Buttons

Buttons	Configuration Area	Description
Set Password	LEAP	Enables you to enter the password for each LEAP configuration entry.
Set Password	User Manager	Enables you to enter the password for each user manager entry.
Set Secret Key	AAA Server	Enables you to enter the Secret key for each AAA server entry.
Def. 11b WEP	WEP Key	Enables you to enter the WEP key for the 802.11b (2.4-GHz) radio interface. Used for non-VLAN setup.
Def. 11a WEP		Enables you to enter the WEP key for the 802.11a (5-GHz) radio interface. Used for non-VLAN setup. This button is not available on 350 series access points.
Set VLAN WEP		Enables you to set the WEP key for each VLAN configuration entry.
Back	–	Ignores any entered parameters and returns to the Device Configuration window.
Finish	–	Accepts the security configuration parameters and closes the window.
Cancel	–	Closes the window and ignores any entered configuration parameters.
Help	–	Provides online help for the window.

LEAP Configuration for a Repeater

The LEAP configuration parameters are used when the access point is configured as a repeater and is required to authenticate to a LEAP server as a client before network access is allowed. LEAP authentication requires a valid username and password. For each entry listed, you must enter the LEAP password using the Set Password button. The following fields are displayed:

- Module—identifies the radio interface.
 - 11b—indicates the 802.11b (2.4-GHz) radio interface.
 - 11a—indicates the 802.11a (5-GHz) radio interface.
- User Name—indicates the LEAP username that is used for authentication.
- Password—indicates the LEAP password that is used for authentication. You must enter this parameter using the Set Password button.

User Manager Configuration

The User Manager Configuration area of the Security Configuration window identifies the users with special access privileges to the access point. For each entry, you must enter the user's password using the Set Password button.

The following fields are displayed:

- Capabilities—indicates the user's access privileges on the access point.
 - Administrator—The user can view most system windows. To view all system windows and make changes to the system, the user must have Write capability.
 - Write—The user can change system settings. A user with Write capability also automatically has Admin capability.
 - Firmware—The user can update the access point's firmware. A user with Firmware capability also automatically has Write and Admin capabilities.
 - Identity—The user can change the access point's identity settings (IP address and SSID). A user with Ident capability also automatically has Write and Admin capabilities.
 - SNMP—Designates the username as an SNMP community name. SNMP management stations can use this SNMP community name to perform SNMP operations. The SNMP check box does not grant SNMP write capability to the user; it only designates the username as an SNMP community name.
- Name—indicates the username.
- Password—indicates the user's password. You must enter this parameter using the **Set Password** button.

AAA Server Configuration

The AAA Server Configuration area of the Security Configuration window lists the authentication, authorization, and accounting servers used by the access point. For each entry, you must enter the secret key clicking the **Set Secret Key** button.

**Note**

If host names are used for RADIUS, accounting, and NTP servers, the converted Cisco IOS 350 series access points are unable to use DNS to obtain the corresponding IP addresses. Cisco recommends that you change your VxWorks configurations to use IP addresses rather than host names for RADIUS, accounting, and NTP servers, or to configure the servers after the converted access points boot up.

WEP Key Configuration

The WEP Key Configuration area of the Security Configuration window lists the VLANs defined in the access point. For each VLAN entry, you must enter the WEP keys using the **Set VLAN WEP** button.

When VLANs are not defined and WEP security is used on the access point, you must enter the WEP keys for the radio interfaces supported by the access point. To enter the WEP keys, click **Def. 11b WEP** for the 802.11b (2.4-GHz) radio and click **Def. 11a WEP** for the 802.11a (5-GHz) radio.

When you click the Set VLAN WEP, Def. 11b WEP, or Def. 11a WEP buttons, a WEP Key window (Figure 3-3) appears. You can enter up to four WEP keys and select either a 40-bit or a 128-bit key size.


Note

For 40-bit encryption, you must enter 10 hexadecimal digits; for 128-bit encryption, you must enter 26 hexadecimal digits. Hexadecimal digits include the numbers 0 through 9 and the letters A through F. The letters are not case sensitive.

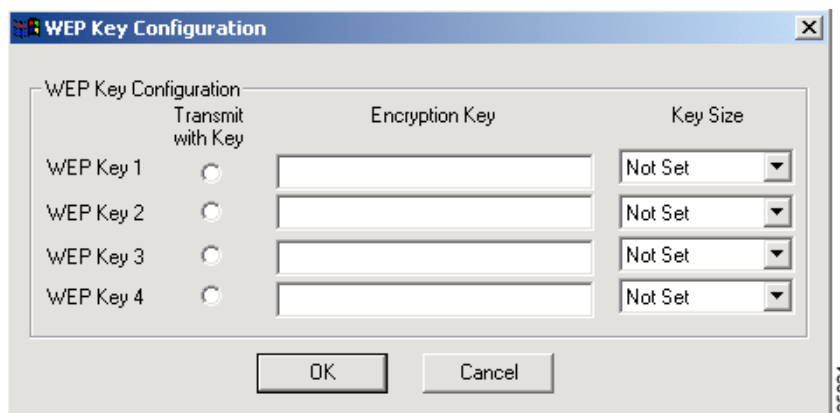
The Key Size drop-down menu enables you to select 40-bit or 128-bit encryption for each WEP key. The *not set* option clears the WEP key. You must set one of the WEP keys as the transmit key by clicking the **Transmit with Key** selection box.


Note

If your access point is configured for Network-EAP as the authentication type, you must select key 1 as the transmit key.

Figure 3-3 shows the WEP Key Configuration window.

Figure 3-3 WEP Key Configuration Window


Note

The Transmit with Key selection boxes are unavailable on the VLAN WEP key window.



Using the Conversion Tool

This section provides instructions on the typical use of the conversion tool. The following topics are covered in this section:

- [Adding a Task, page 4-2](#)
- [Starting a Task, page 4-8](#)
- [Viewing the Task Log, page 4-9](#)
- [Log Error Messages, page 4-11](#)
- [Viewing the Cisco IOS Configuration, page 4-18](#)
- [Adding Multiple Tasks, page 4-19](#)

Adding a Task

When you begin using the conversion tool, you must first define tasks that identify the operations to be performed and provide additional information.

Follow the steps below to add a single or multiple tasks:

- Step 1** Activate the conversion tool by double-clicking the conversion tool icon on your desktop or by selecting **Start > Programs > CAC Tool** (or your installation folder name) > **CAC Tool**. The conversion tool window appears (see [Figure 4-1](#)).

Figure 4-1 Conversion Tool Main Window



Step 2 Click **Add Task**. The Device Configuration window appears.

Figure 4-2 Device Configuration Window

Step 3 Click the Device Type drop-down arrow to specify the VxWorks access point type. Select one of the following:

- AP350—indicates that the device is a 350 series access point.
- AP1200—indicates that the device is a 1200 series access point.

Step 4 In the Source Configuration area, click the From drop-down arrow to specify the source location for configuration information. Select one of the following:

- Device—indicates that a VxWorks access point is used to create a Cisco IOS configuration file.
- Disk Storage—indicates that a Cisco IOS configuration file is stored on your hard disk drive.

Step 5 When Device is selected for the source, follow these steps:

- a. Enter the IP address of the source access point in the IP Address field.
- b. Enter the access point administrator's username in the Admin Name field.

Step 6 When you select Disk Storage for the source, enter the directory path and filename for the Cisco IOS configuration file in the File Name field or browse to the file location using the browse (...) button.



Note The Cisco IOS configuration file must be the one created by the conversion tool and have a .cfg extension.

Step 7 In the Target Configuration area, click the drop-down arrow to specify the target location. Select one of the following:

- Device—indicates that a VxWorks access point is the target device.
- Disk Storage—indicates that the Cisco IOS configuration file will be stored on your hard disk drive.

Step 8 When you select Device for the Target Configuration, follow these steps:

- a. Enter the IP address of the target access point in the IP Address field.
- b. Enter the access point administrator's username in the Admin Name field.
- c. Enter the path and filename for the Cisco IOS helper image file in the helper image field or browse to the file location using the browse (...) button.



Note A Cisco IOS helper image file is used with an Cisco IOS configuration to upgrade a VxWorks 350 or 1200 series access point to Cisco IOS operation.

- d. Enter the password for the target access point in the Enable Password field. The password is activated when the target access point is upgraded to Cisco IOS operation (for additional information refer to the “[Target Configuration Parameters](#)” section on page 2-4).

Step 9 If you select Disk Storage for the Target Configuration, enter the directory path and filename for the Cisco IOS configuration file in the File Name field or browse to the file location using the browse (...) button. Go to [Step 22](#).

Step 10 If your access point is configured for hot standby, follow these steps:

- a. Enter the MAC address for the monitored access point's 802.11b (2.4-GHz) radio interface.
- b. If the 5-GHz radio interface is supported on your access point, enter the MAC address for the monitored access point's 802.11a (5-GHz) radio interface.



Note If your access point supports only one radio interface, provide the MAC address for that interface only.



Caution

During the Cisco IOS conversion process, the radio interface MAC address for your access points might change from the original setting, resulting in lost repeater associations and failure of the hot standby option. This happens because Cisco IOS software does not support the VxWorks *Adopt Primary Port Identity* option for the radio interfaces. Before you begin the conversion process, Cisco recommends that you change your VxWorks configurations to disable the *Adopt Primary Port Identity* option and to use the actual radio interface MAC address in all repeater and hot standby configuration settings.

Step 11 Verify the IP address shown in the Interface for communicating with Target Access Point field. If necessary, enter a new IP address for the network adapter (Ethernet or radio) that the conversion tool should use to communicate with the access point.

Step 12 When you have completed all entries on the Device Configuration window, click **Next**.

- Step 13** If the target location is an access point, click **Yes** to the message indicating that the **Cisco IOS upgrade is a one-way process**.
- Step 14** Click **Get Security Configuration** on the Security Configuration window. A message appears indicating that the conversion tool is trying to gather security information from the access point. When the security information is available, the Security Configuration window displays the security data collected (see [Figure 4-3](#)).

**Caution**

If User Manager is disabled in your VxWorks access point and if you bypass the conversion tool's Security Configuration window, **you can only log in on the upgraded access point using the console port**.

**Caution**

If User Manager is enabled in your VxWorks access point and if you bypass the conversion tool's Security Configuration window, **you may not be able to log in on the upgraded access point**. All access to the access point may be blocked (Telnet, browser, and the console port). If this occurs, you must reset the access point to defaults using the mode button (refer to the "Troubleshooting" section of the *Cisco Aironet 1200 Series Access Point Hardware Installation Guide* or the *Cisco Aironet 350 Series Access Point Hardware Installation Guide*).

**Note**

If the Source Configuration is from disk storage, the Security Configuration Window is not displayed.

Figure 4-3 Typical Security Configuration Window

The screenshot shows a 'Security Configuration' window with four main sections:

- LEAP Configuration:** A table with columns 'Module', 'User Name', and 'Password'. It lists two entries: '11b doc' and '11a doc'. A 'Set Password' button is to the right.
- User Manager Configuration:** A table with columns 'Capabilities', 'Name', and 'Password'. It lists two entries: 'Admin, Write, Firmware, doc' and 'Admin, Write, Firmware, doc2'. A 'Set Password' button is to the right.
- AAA Server Configuration:** A table with columns 'Item', 'Type', 'IP address', and 'Secret Key'. It lists two entries: '1 Authentication 10.0.0.102' and '2 Accounting 10.0.0.101'. A 'Set Secret Key' button is to the right.
- WEP Key Configuration:** A table with columns 'VLAN ID', 'VLAN Name', and 'Is WEP set?'. It lists two entries: '1 Vlan 1 No' and '5 Vlan 5 No'. To the right are three buttons: 'Def. 11b WEP', 'Def. 11a WEP', and 'Set VLAN WEP'.

At the bottom of the window are four buttons: '< Back', 'Finish', 'Cancel', and 'Help'. A small number '117960' is visible in the bottom right corner of the window frame.

- Step 15** In the LEAP Configuration area, follow these steps for each radio interface listed:
- Select a radio interface entry.
 - Click **Set Password**.
 - Enter the LEAP password on the Password Configuration window and click **OK**.
- Step 16** In the User Manager Configuration area, follow these steps for each user listed:
- Select a user entry.
 - Click **Set Password**.
 - Enter the user password on the Password Configuration window and click **OK**.
- Step 17** In the AAA Server Configuration area, follow these steps for each server entry listed:
- Select a server entry.
 - Click **Set Secret Key**.
 - Enter the server's secret key on the AAA Server Configuration window and click **OK**.

- Step 18** In the WEP Key Configuration area, follow these steps for each VLAN entry listed:
- Select a VLAN entry and click **Set VLAN WEP**.
 - Enter the VLAN's WEP keys in the Encryption Key fields on the WEP Key Configuration window.



Note Each VLAN can support up to four WEP keys. For 40-bit encryption, you must enter 10 hexadecimal digits; for 128-bit encryption, you must enter 26 hexadecimal digits. Hexadecimal digits include the numbers 0 through 9 and the letters A through F. The letters are not case sensitive.

- For each WEP key entered, select either **40** or **128** bits using the Key Size drop-down arrow.



Note The Transmit with Key selections are unavailable for VLANs.

- Click **OK** on the WEP Key Configuration window.

- Step 19** In the WEP Key Configuration area, follow these steps:

- Click **Def. 11b WEP**. The WEP Key Configuration window appears.
- Enter the WEP keys in the Encryption Key fields.
- For each WEP key entered, select either **40** or **128** bits using the Key Size drop-down arrow.
- Set the transmit WEP key by clicking **Transmit with Key** for one WEP key entry.



Note Only one transmit WEP key can be selected.

- Click **Def. 11a WEP**. The WEP Key Configuration window appears.
- Enter the WEP keys in the Encryption Key fields.



Note For 40-bit encryption, you must enter 10 hexadecimal digits; for 128-bit encryption, you must enter 26 hexadecimal digits. Hexadecimal digits include the numbers 0 through 9 and the letters A through F. The letters are not case sensitive.

- For each WEP key entered, select either **40** or **128** bits using the Key Size drop-down arrow.
- Set the transmit WEP key by clicking **Transmit with Key** for one WEP key entry.



Note Only one transmit WEP key can be selected.

- Click **OK** on the WEP Key Configuration window.

- Step 20** Verify that all listed entries on the Security Configuration window contain the correct password, secret key, or WEP settings. Click **OK** on the Security Configuration window.

- Step 21** If you receive an error message indicating a password or secret key is missing, enter the missing value.

- Step 22** The main conversion tool window should indicate that the added task is ready to start.

To add multiple tasks repeat Steps 1 to 21.

Starting a Task

You must first add a task before the task can be started. When a task is added, it is visible on the main window of the conversion tool. Follow the steps below to start a single task or multiple tasks.


Note

The conversion tool starts all tasks at the same time.

Step 1 Click **Start Task**.

When you start the operating task, the conversion tool indicates its status in the status field on the main window. Typical status indications are:

- To Start—indicates that the task is waiting to start.
- Progress bar—indicates the task progress by the length of the bar.
- Learning Configuration—indicates that the conversion tool is obtaining configuration information from the source access point.
- Completed—indicates that the task has executed successfully without any detected errors.
- Error—indicates that an error has occurred during the execution of the task. For additional details on the error, click **View Log**.

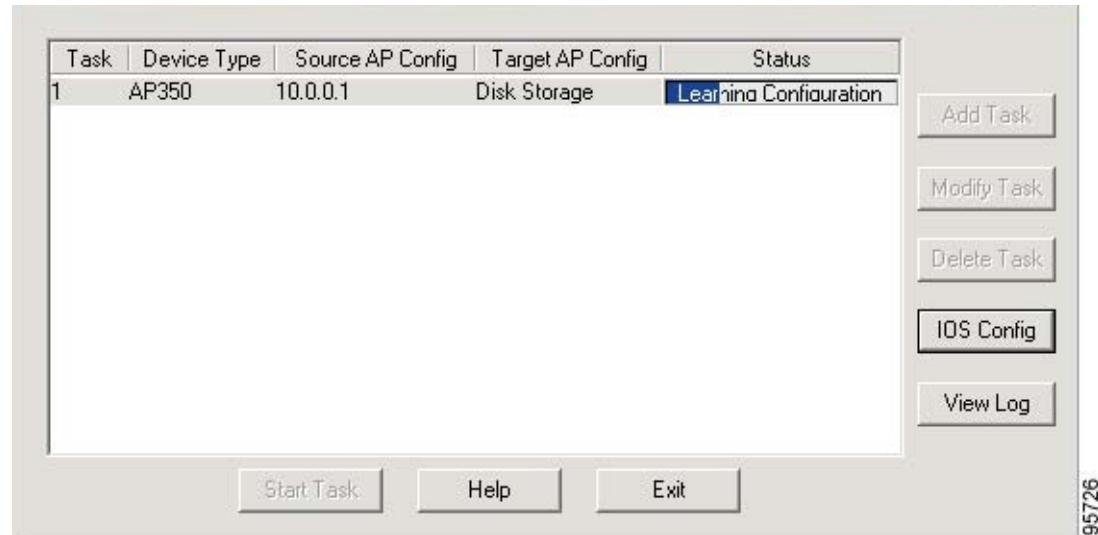

Note

The View Log button displays the conversion tool log file only when a task process has ended.

- Warning—indicates that the conversion tool was not able to read some configuration data from the source access point. For additional information on the warning, click **View Log**. If you are upgrading an access point, you may need to manually enter the missing configuration parameters into the access point.
- Uploading Image—indicates that the helper image and configuration parameters are being uploaded into the target access point.
- Checking Device Status—indicates that the conversion tool is checking the access point status after the image upgrade.

Figure 4-4 shows the conversion tool window with the Learning Config and progress bar status indicators.

Figure 4-4 Learning Config Status Indication



- Step 2** If your task status indicates Error, click **View Log** to view the task log information to try to determine the cause of the error (refer to the “[Viewing the Task Log](#)” section on page 4-9).



Note The View Log button displays the conversion tool log file only when a task process has ended.

- Step 3** If your task status indicates Completed, the task has successfully completed the specified operations. If your task was to convert a VxWorks configuration into a Cisco IOS configuration, you should carefully review the Cisco IOS configuration data (refer to the “[Viewing the Cisco IOS Configuration](#)” section on page 4-18). Because of differences between VxWorks and Cisco IOS configuration parameters, you should also review the “[Limitations in the Cisco IOS Configuration](#)” section on page B-5.

Viewing the Task Log

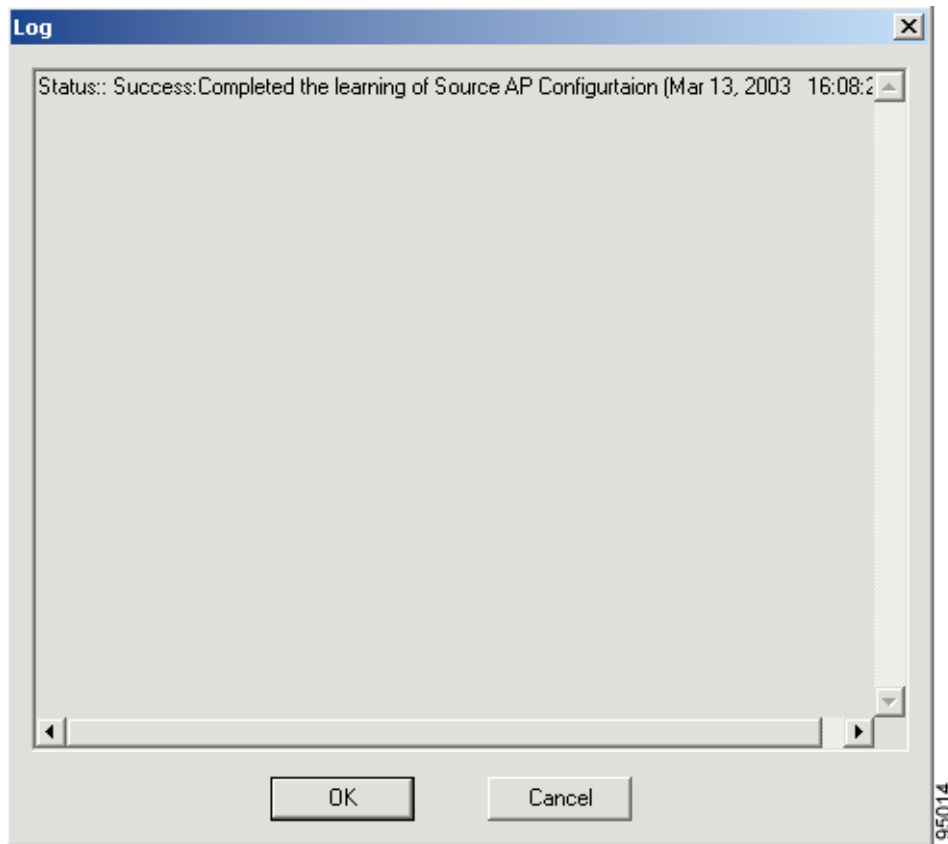
The conversion tool task log provides valuable information about the operations that are processed and indicates whether the task is successfully completed or generated an error. To view the Log information, click **View Log** on the conversion tool main window (see [Figure 4-1](#)).



Note The View Log button displays the conversion tool log file only when a task process has ended.

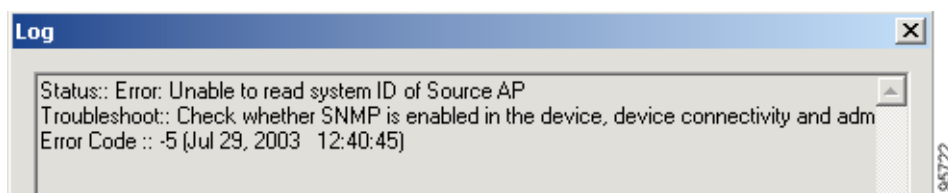
Figure 4-5 shows a typical log file.

Figure 4-5 Successful Task Log



If an error occurred during the execution of the task, the log briefly describes the error and suggests possible troubleshooting suggestions. Figure 4-6 shows an error indication in a task log.

Figure 4-6 Conversion Tool Error Log



The error shown in Figure 4-6 indicates that the conversion tool is *Error: Unable to read System ID of Source AP*. This error can be caused by several incorrectly configured parameters (for additional information refer to the “[Log Error Messages](#)” section on page 4-11).

Log Error Messages

When the conversion tool main window indicates Error in the status field, the log file indicates the specific error condition that caused the problem. The following list contains the error messages displayed in the log file and lists possible corrective actions for the specified error condition:

Error Message Error: Unable to Read Template File.

Explanation The conversion tool is unable to locate the template files that are installed during the installation process.

Recommended Action Ensure that the template files (MIB_Template_11x.ini and MIB_Template_12X.ini) are available in the conversion tool's root directory and start the task again.

Error Message Error: Unable to create IOS CLI File.

Recommended Action Ensure that the hard disk drive specified has sufficient free space for the Cisco IOS configuration file and that the drive does not have restrictive access rights that prevents reading or writing. Start the task again.

Error Message Error: Unable to build Helper Image File.

Recommended Action Ensure that the correct path and helper image file name are specified in the Device Configuration window. Start the task again. If the error occurs again, download a new copy of the Helper Image file and start the task again.

Error Message Error: Unable to set the necessary parameters for uploading the Helper Image.

Recommended Action Ensure that the administrator specified on the Device Configuration window has the correct privileges (SNMP, Firmware, Write, and Admin) on the target access point. Start the task again.

Error Message Error: Unable to identify TFTP server address.

Recommended Action Ensure that the IP address specified in the Interface for Communicating with the Target Access Point field on the Device Configuration window is correct. Start the task again.

Error Message Error: Unable to read Source AP Interface Related information.

Recommended Action Ensure that the source access point is accessible from your PC by pinging the access point. Start the task again.

Error Message Error: Unable to read system ID of Source AP.

Recommended Action Perform the following:

- Ensure that SNMP is enabled in the source access point.
- Verify that you can ping the source access point.
- Ensure that the administrator specified on the Device Configuration window has the correct privileges (SNMP, Firmware, Write, and Admin) on the source access point.

Error Message Error: Unable to read Source AP's version information.

Recommended Action Verify that you can ping the source access point and restart the task.

Error Message Error: Learning of configuration aborted.

Recommended Action Verify that you can ping the source access point and restart the task.

Error Message Error Unable to read the system ID of Target AP.

Recommended Action Perform the following:

- Ensure that SNMP is enabled in the target access point.
- Verify that you can ping the target access point.
- Ensure that the administrator specified on the Device Configuration window has the correct privileges (SNMP, Firmware, Write, and Admin) on the target access point.

Error Message Error: Unable to read the target access point version information.

Recommended Action Verify that you can ping the target access point and restart the task.

Error Message Error: Unable to read the configuration file for the target access point.

Recommended Action Perform the following:

- Ensure that the path and file name for the source configuration file on the Device Configuration window are correct.
- Verify that you can ping the source access point.
- Restart the task.

Error Message Error: Unable to reload the target AP.

Recommended Action Verify that you can ping the target access point and restart the task.

Error Message Error: Unable to upgrade the Target AP.

Recommended Action Perform the following:

- Verify that the CACToolTFTPService is running on your PC.
- Verify that you can ping the target access point.
- Restart the task.



Note Upgrade tasks should not be performed on both root and repeater access points at the same time because this causes the repeater upgrade task to fail.

Error Message Error: Unable to check the device status.

Recommended Action Verify that the target access point is not already running Cisco IOS software and restart the task.

Error Message Error: Unable to load Helper Image.

Recommended Action Perform the following:

- Verify that the file name and path for the Helper Image entered on the Device Configuration window are correct.
- Verify that you can ping the target access point.
- Verify that the administrator specified for the target access point on the Device Configuration window has the correct privileges (SNMP, Firmware, Write, and Admin) on the target access point.
- Restart the task.

Error Message Error: The conversion tool can be used with VxWorks -based AP350 or AP1200 devices only

Recommended Action Verify that your access point is not already running Cisco IOS software and that you are using 350 or 1200 series access points.

Error Message Error: The conversion tool works only with 12.03T, 12.02T1, 12.01T1, 12.00T, 11.56, and 11.54T images of VxWorks based 1200 APs or 12.03T, 12.02T1, 12.01T, 12.00T, 11.23T and 11.21 images of VxWorks based 350 APs.

Explanation Your access point might contain a non-supported version of the operating system.

Recommended Action Upgrade or down-grade your access point to one of supported operating system versions and try the task again.

Error Message Error: Configuration from Source device was not completed successfully.

Explanation The conversion tool was not able to obtain configuration information from the source access point because of error conditions indicated in other error messages.

Recommended Action Examine the other error messages and perform the recommended actions.

Error Message Process aborted: Unable to complete the upgrade process

Explanation This message is displayed when the Exit button is pressed while tasks are running.

Recommended Action Restart the tasks.

Error Message Error: Unable to communicate with target access point.

Recommended Action Perform the following:

- Verify the IP address of the target access point.
- Verify that you can ping the target access point.
- Restart the conversion process.

Error Message Error: Unable to upgrade target access point due to possible free memory shortage.

Recommended Action You need to increase the amount of contiguous free memory in the target access point and restart the task again.

Error Message Error: Setup has detected that unInstallShield is in use. Please close unInstallShield and restart setup. Error 432.

Explanation This error occurs when InstallShield tries to delete UNINST.EXE from the WINNT directory (so that it can install the latest version of the file) and you don't have administrative privileges on the PC or the file has already been deleted.

Recommended Action Perform the following:

- Ensure that you have administrative privileges on the PC before installing the conversion tool.
- Ensure that only one instance of the InstallShield is running by only double-clicking the installation file **Aironet-AP-Cisco-IOS-Conversion-Tool-v2.1.exe**.

Error Message Error: Uninstaller setup failed to initialize. You may not be able to uninstall this product.

Explanation This error occurs when you do not have administrative privileges on the PC and the installation software attempts to save uninstall information in your Windows directory.

Recommended Action Ensure that you have administrative privileges on the PC before installing the conversion tool.

Warning Error Messages

When the conversion tool main window displays *Warning* in the status field, the log file indicates specific configuration parameters that could not be read. You must manually configure the target access point to include the missing configuration parameters. The following list contains the possible warning error messages contained in the log file:

Error Message Error: Unable to read Source AP Fast Ethernet speed, HTTP port, and World mode related information.

Error Message Error: Unable to read Source AP Infrastructure SSID related information.

Error Message Error: Unable to read Source AP Auxiliary SSID related information.

Error Message Error: Unable to read Source AP Interface filter related information.

Error Message Error: Unable to read Source AP VLAN encryption related information—the conversion tool could not obtain the following configuration information: "Single VLAN ID which allows unencrypted packets" and "Optionally allow encrypted packets on the unencrypted VLAN".

Error Message Error: Unable to read Source AP MAC filter related information.

Error Message Error: Native VLAN is not configured in the AP.

Error Message Error: Unable to read Source AP VLAN related information.

Error Message Error: Unable to read Source AP Native VLAN information.

Error Message Error: Unable to read Source AP DSCP-to-COS Conversion related information.

Error Message Error: Unable to read Source AP's Input QoS of the Interface related information.

Error Message Error: Unable to read Source AP's Output QoS of the Interface related information.

Error Message Error: Unable to read Source AP's type of WEP Encryption, i.e., Optional or Mandatory related information.

Error Message Error: Unable to read Source AP 11a module's Preferred Access Point related information.

Error Message Error: Unable to read Source AP 11b module's Preferred Access Point related information.

Error Message Error: Unable to read Source AP's SSID Authentication related information.

Error Message Error: Unable to read Source AP's MAC Authentication related information.

Error Message Error: Unable to read the Source AP's EAP Authentication related information.

Error Message Error: Unable to read Source AP 11b module's Internal Quality of Service related information.

Error Message Error: Unable to read Source AP 11a module's Internal Quality of Service related information.

Error Message Error: Unable to read Source AP 11b module's Country Code related information.

Error Message Error: Unable to read Source AP 11a module's Country Code related information.

Error Message Error: Unable to read Source AP 11b module's Channel Auto Enable related information.

Error Message Error: Unable to read Source AP 11a module's Channel Auto Enable related information.

Error Message Error: Unable to read Source AP 11b module's Least Congested Channel related information.

Error Message Error: Unable to read Source AP 11a module's Least Congested Channel related information.

Error Message Error: Unable to read source AP's Dot11 Hardware related information.

Error Message Error: Unable to read Source AP's Dot11 Station related information.

Error Message Error: Unable to read Source AP's Broadcast Key Rotation Interval related information.

Error Message Error: Unable to read Source AP's Name Server related information.

Error Message Error: Unable to read Source AP's Proxy Mobile IP related information.

Error Message Error: Unable to read Source AP's Local SA Bindings related information.

Error Message Error: Unable to read Source AP's Event Log related information.

Error Message Error: Unable to read Source AP's System Name, Contact, Location, and CDP related information.

Error Message Error: Unable to read Source AP's HTTP, SNMP, and HTTP server related information.

Error Message Error: Unable to read Source AP's Event Notification related information.

Error Message Error: Unable to read Source AP's Hot Standby Frequency and Duration related information.

Error Message Error: Unable to read Source AP's Individual Ethertype Filter related information.

Error Message Error: Unable to read Source AP's IP Protocol Filters related information.

Error Message Error: Unable to read Source AP's IP Port Filters related information.

Error Message Error: Unable to read Source AP's Policy Groups related information.

Error Message Error: Unable to read Source AP's Ethertype Filters related information.

Error Message Warning: Reached the maximum number of Ethertype Filters (200-299) that can be configured in IOS—You cannot create any additional new Ethertype filters in the new Cisco IOS configuration.

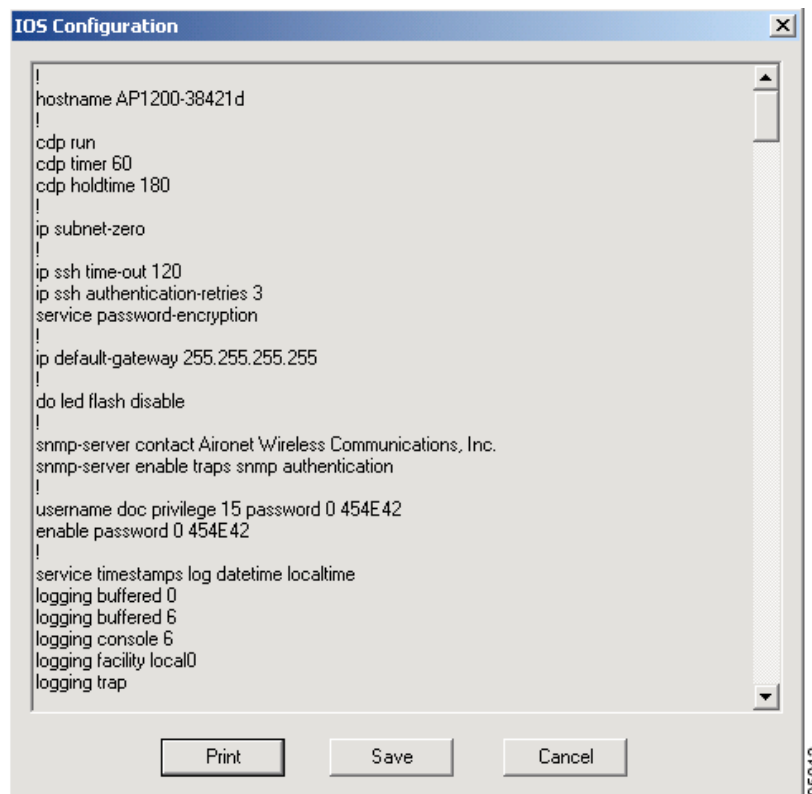
Error Message Error: Unable to save the running config to the startup config.

Recommended Action Please manually save the access point *running config* to the *startup config*.

Viewing the Cisco IOS Configuration

The IOS Config button on the conversion tool window enables you to view the Cisco IOS configuration data obtained from a VxWorks access point by the conversion tool (see [Figure 4-7](#)). The configuration data is visible only after the Cisco IOS configuration is successfully created by the conversion tool.

Figure 4-7 Typical IOS Configuration File



Adding Multiple Tasks

The conversion tool can be used to activate multiple tasks (see [Figure 4-8](#)).

When your PC has the minimum PC hardware (refer to the “[Before You Begin](#)” section on page 1-3), the conversion tool supports up to 14 parallel helper image upgrades. You can enter up to 20 tasks, but only 14 of the tasks (maximum) can be helper image upgrades and the remaining tasks can be used to store access point Cisco IOS configurations on your hard disk. Prior to starting multiple helper image upgrade tasks, you should verify that your PC has sufficient disk space.



Caution

You must ensure that the same Ethernet and duplex settings are configured on all VxWorks access points and switches prior to beginning the conversion process. Different settings can result in inoperable access points that constantly power off and on.



Note

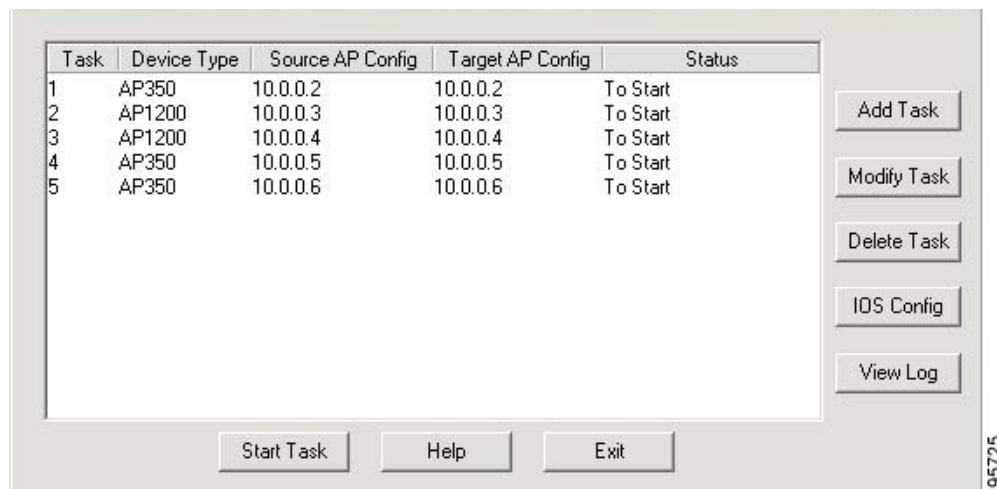
When you have upgraded your access points, you can recover disk space on your PC by deleting the Cisco IOS configurations (with helper images) that were saved in the ConversionToolDirectory/images folder on your PC.



Note

The limit of 14 parallel helper image upgrades depends solely on the ability of the system and the network to handle multiple TFTP jobs. Faster systems, disks, and networks may be able to handle more parallel upgrade tasks, though too many tasks impact the speed of the individual tasks.

Figure 4-8 Typical Conversion Tool Window with Multiple Tasks



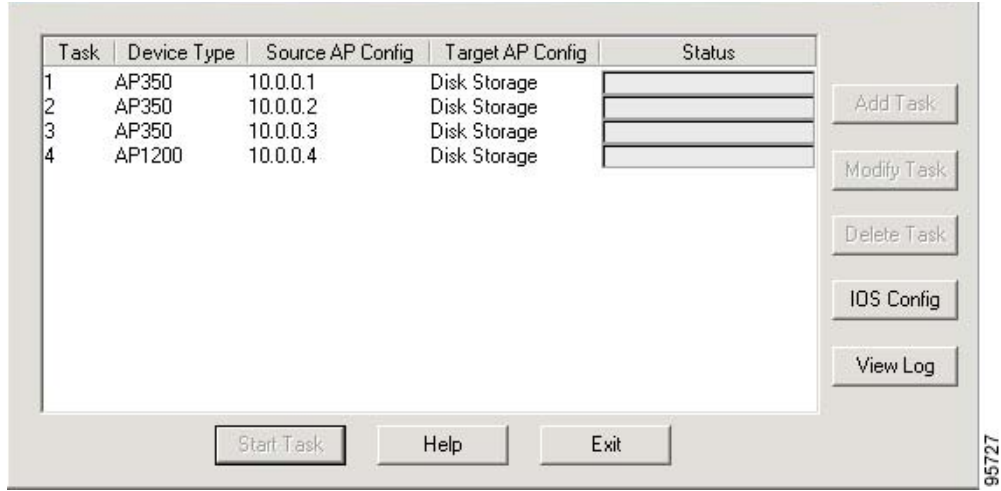
Use the Add Task button to create multiple tasks (refer to the “[Adding a Task](#)” section on page 4-2). [Figure 4-8](#) shows the conversion tool window with a list of four tasks that upgrade VxWorks 350 or 1200 series access points to Cisco IOS operation using a stored Cisco IOS configuration file.



Note

When you click the Start Task button with multiple tasks listed on the conversion tool window, all tasks are activated at the same time (see [Figure 4-9](#)).

Figure 4-9 Typical Conversion Tool Window with Multiple Tasks Starting





Upgrading an Access Point to Cisco IOS Operation Without the Conversion Tool

This appendix provides instructions for upgrading a VxWorks 350 or 1200 series access point to Cisco IOS operation without preserving the existing configuration. The access point configuration is set to default values.

Cisco IOS Upgrade Procedure

If you want to only upgrade a VxWorks 350 or 1200 series access point to Cisco IOS operation and not preserve the existing configuration, you can use the 350 or 1200 series helper image file to upgrade the access point. The procedure described in this section uses your browser interface and the access point's GUI interface.



Note

Cisco recommends that you use the access point's console port to monitor messages during the upgrade process. This allows you to determine when the upgrade process is complete and the access point is rebooting. If you are unable to use the console port, Cisco recommends that you use the conversion tool for the Cisco IOS software upgrade. The conversion tool indicates when the upgrade process is complete.



Note

The upgrade image does not support VxWorks version 12.04. Access points running version 12.04 must be downgraded to a supported operating system version before you can use this upgrade image.



Note

The browser image upgrade process uses popup messages. You must disable any browser popup blockers before beginning the upgrade process.

To upgrade the access point, follow these steps:

- Step 1** Obtain the 350 or 1200 series access point helper image file (refer to [“Obtaining the Helper Image” section on page 1-5](#)).
- Step 2** Use your browser to connect to the VxWorks 350 or 1200 series access point.
- Step 3** Click **Setup** on the Summary Setup window.
- Step 4** Under Services, click **Cisco Services**.

Step 5 Under Fully Update Firmware, click **Through Browser**.

Step 6 Browse to the helper image file using the **Browse** button.

Step 7 Click **Browser Update Now**. The upgrade process begins.

When the upgrade completes, a message appears indicating that you should wait 30 seconds for the access point to reboot.

**Caution**

The total Cisco IOS software upgrade process can take from 5 to 30 minutes and the access point's Status LED turns red during the firmware upgrade. **Do not remove power to terminate the upgrade process because your access point will become inoperable.**

**Caution**

If you are using the console port, the "Cisco IOS automatic field upgrade image, ESC to terminate" message appears. **Do Not press the Esc key because your access point will become inoperable.**

**Note**

Your Cisco IOS 350 or 1200 series access point is now configured with default parameters.

To access your Cisco IOS access point, you can browse to your access point's IP address and use *Cisco* as the username and password.



Requirements and Limitations

This appendix describes the requirements, cautions, and limitations of the conversion tool.

- [Important Note, page B-2](#)
- [System Requirements, page B-2](#)
- [Conversion Tool Operating Cautions, page B-3](#)
- [Limitations in the Cisco IOS Configuration, page B-5](#)

Important Note

The conversion tool uses a software program (*SNMP.DLL*) provided by Hewlett-Packard. The following Hewlett-Packard copyright statement pertains to the *SNMP.DLL* software:

Copyright (C) 1999
Hewlett-Packard Company

ATTENTION: USE OF THIS SOFTWARE IS SUBJECT TO THE FOLLOWING TERMS.

Permission to use, copy, modify, distribute and/or sell this software and/or its documentation is hereby granted without fee. User agrees to display the above copyright notice and this license notice in all copies of the software and any documentation of the software; Hewlett-Packard makes no representations about the suitability of this software for any purpose. It is provided "AS-IS" without warrant of any kind, either express or implied. User hereby grants a royalty-free license to any and all derivatives based upon this software code base.

System Requirements

The conversion tool has the following system requirements:

- [Table 1](#) identifies the supported access points, VxWorks versions, and images:



Note The conversion tool does not support VxWorks 350 and 1200 series access points running operating system version 12.04. Access points running operating system version 12.04 must be downgraded to a supported operating system version before using the conversion tool.

Table 1 Supported Access Points, VxWorks Versions, and Images

Access Points	VxWorks Versions	Helper Image Filename	Cisco IOS Version (after conversion)
AP1200 AP1220	12.03T, 12.02T1, 12.01T1, 12.00T, 11.56, or 11.54T	AP1200-Cisco-IOS-Upgrade-Image-v3.img	12.2(11)JA3
AP350	12.03T, 12.02T1, 12.01T1, 12.00T, 11.23T, or 11.21	AP350-Cisco-IOS-Upgrade-Image-v2.img	12.2(13)JA1

- The conversion tool operates only on a PC with the Windows 2000 or XP operating system and is not supported if Terminal Services is installed.
- The conversion tool requires the following minimum PC hardware:
 - Processor: Pentium III or equivalent
 - Speed: 850 MHz
 - RAM: 128 MB
 - Hard disk free space: 250 MB (4 MB for each helper image upgrade task)

When using the minimum PC hardware, the conversion tool supports up to 14 parallel helper image upgrades. You can enter up to 20 tasks, but only 14 of the tasks (maximum) can be helper image upgrades and the remaining tasks can be used to store access point Cisco IOS configurations on your hard disk. Prior to starting multiple helper image upgrade tasks, you should verify that your PC has sufficient open disk space.



Note When you have upgraded your access points, you can recover disk space on your PC by deleting the Cisco IOS configurations (with helper images) that were saved in the ConversionToolDirectory/images folder.



Note The limit of 14 parallel helper image upgrades depends solely on the ability of the system and the network to handle multiple TFTP jobs. Faster systems, disks, and networks may be able to handle more parallel upgrade tasks though too many tasks impact the speed of the individual tasks.

- The person installing and running the conversion tool must be logged in and must be an administrator of the PC.
- All access points (source and target) must have a user enabled with full access privileges (Write, SNMP, Ident, Firmware, and Admin).
- SNMP must be enabled on the source and target access points.



Note For additional information on SNMP, refer to the *Cisco IOS Software Configuration Guide for Access Points*.

- The conversion tool does not support 802.11g radios. You must ensure that the VxWorks access points do not contain 802.11g radios before you use the conversion tool.

Conversion Tool Operating Cautions

You should carefully review the following list of cautions to avoid potential problems when using the conversion tool:

- The conversion tool automatically installs a TFTP server during the installation process and may not detect the presence of an existing TFTP server installed on your PC.



Note You must deactivate existing TFTP servers prior to using the conversion tool.

The conversion tool's TFTP server is activated only when the conversion tool is activated. When you deactivate the conversion tool, the TFTP server is also deactivated.



Note You cannot use the conversion tool's TFTP server for other file transfer purposes.

- The Admin Name setting is not visible in the conversion tool and is displayed as a set of asterisks.

- If you bypass the entry of security information and if User Manager is enabled in your source access point, **you might not be able to log in on the upgraded access point**. All access to the access point might be blocked (Telnet, browser, and the console port). If this occurs, you must reset the access point to defaults using the mode button (refer to the “Troubleshooting” section of the *Cisco Aironet 1200 Series Access Point Hardware Installation Guide* or the *Cisco Aironet 350 Series Access Point Hardware Installation Guide*).
- If you bypass the entry of security information and if User Manager is disabled in your VxWorks access point, **you can only log in on the upgraded access point using the console port**.
- Upgrade tasks should not be performed on both root and repeater access points at the same time because this causes the repeater upgrade task to fail.
- The conversion tool uses SNMP commands to obtain configuration data from the source access point, but some security information cannot be obtained using SNMP. Before you use the conversion tool, obtain the following source access point security information:
 - The WEP keys used for the radio interfaces and VLANs
 - The LEAP passwords for repeater access points
 - The passwords used with the User Manager Configuration
 - AAA Server Configuration Secret Keys
- The upgrade process may not be successful if the configuration of your VxWorks access points was acquired by choosing the Download All System Configuration option on the access point’s System Configuration window. You should use the configuration (.ini) file acquired by choosing the Download Non-Default System Configuration option.
- The upgrade process requires the following minimum contiguous free space in your VxWorks access points to be successful:
 - 4.0 MB for 1200 series access points
 - 4.2 MB for 350 series access points

**Note**

You can verify the amount of contiguous free memory in your access point by connecting to your access point using the console port or a Telnet session and entering the command **:vxdiag_memshow**. The amount of contiguous free memory is listed in the *max block* column.

**Note**

For ways to increase free space, refer to the [“Before You Begin” section on page 1-3](#).

- The conversion tool should be used over Ethernet LANs and not over slower networks.

**Caution**

You must ensure that the same Ethernet and duplex settings are configured on all VxWorks access points and switches prior to beginning the conversion process. Different settings can result in inoperable access points that constantly power off and on.

- The Cisco Aironet 350 access point conversion process can take up to 30 minutes.

- Cisco IOS access points do not allow the radio interface to adopt the Ethernet port identity that allows the radio and Ethernet interfaces to use the same IP and MAC addresses.

**Caution**

During the Cisco IOS conversion process, the radio interface MAC address for your access points might change from the original setting, resulting in lost repeater associations and failure of the hot standby option. This happens because Cisco IOS software does not support the VxWorks *Adopt Primary Port Identity* option for the radio interfaces. Before you begin the conversion process, Cisco recommends that you change your VxWorks configurations to disable the *Adopt Primary Port Identity* option and to use the actual radio interface MAC address in all repeater and hot standby configuration settings.

- If your VxWorks access points are configured to use BOOTP, you must change their configurations to support DHCP prior to running the conversion tool to avoid a conversion failure. For access point configured for BOOTP, the access point IP address changes during the conversion process, and the conversion tool is unable to complete the access point conversion.

Limitations in the Cisco IOS Configuration

Because of differences between the configuration settings in your VxWorks access point and the Cisco IOS configuration settings, the conversion tool has the following limitations:

- The configuration of a Policy Group on an SSID without a VLAN are not migrated.
- 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.
- Separate filters are created for the Ethertype, IP port, and IP protocol filters that have been set to non-default priority. This may create multiple filters with the same numeric identifier, but the conversion tool inserts a numeric index to differentiate the filters.

Port filters, Protocol filters, Ethertype filters, and Policy Groups are created in the following format:

- Port filter—IP access list extended <Port_Filter_Name> _<Numeric_Value>
- Protocol filter—IP access list extended <Protocol_Filter_Name> _<Numeric_Value>
- Ether filter—access-list <Numeric_Value> <permit or deny> <Protocol-Type>
- Policy-Groups—policy-map_policy_ <Name>_<Policy_ID>

- For BOOTP settings, DHCP settings are configured. To avoid incomplete access point conversions, you must change your VxWorks configurations to use DHCP before you begin the Cisco IOS conversion process.
- Only DHCP configuration settings with a Client Identifier type of Ethernet are migrated. All other Client Identifier types are discarded.
- If DHCP is configured, the fall-back IP addresses are not configured.
- Port assignments are not migrated.
- The Hot Standby configuration settings are migrated only when the radio MAC addresses are entered on the conversion tool's Device Configuration window.
- If the station role is configured as Client/NonRoot, the station role is migrated as Root.
- For the Console/Telnet settings, only the Enable and Disable settings are migrated.

- For the HTTP configuration settings, only the HTTP port and the Enable or Disable settings are migrated.
- VLANs (except the Native VLAN) are migrated only when they are associated with an SSID.
- Only MAC based filter settings with SSIDs associated to a VLAN and with MAC authentication enabled are migrated. The log file contains a list of the MAC filters that are not migrated.
- The Alert settings in filters are not migrated.
- AAA server timeout settings range from 1 to 1000. If the configured setting is greater than 1000, the migrated setting is 1000. If the configured setting is less than 1, the migrated setting is 1.
- AAA server 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 accounting server settings are not migrated. After an accounting server is enabled, all the users are configured to use that server.
- System names containing a space are migrated with an underscore (_) replacing the space. For example; a name of *AP 1200* is migrated as *AP_1200*.
- LEAP usernames with a space are not migrated.
- The following Ethernet parameters are not migrated:
 - Optimize Network for maximum multicast packets per second, loss of backbone connectivity timeout value, and maximum multicast packets per second.
- The following Boot Server configuration parameters are not migrated:
 - DHCP Multiple-Offer Timeout
 - DHCP Requested Lease Duration
 - DHCP Minimum Lease Duration
 - DHCP Client Identifier Value
- The FTP and TFTP configuration parameters are not migrated.
- The following AAA Server configuration parameters are not migrated:
 - Port configuration settings for TACACS server
 - 802.1X Protocol Version (for EAP authentication)
 - Update Delay per Server for the Accounting Server
- The following configuration settings are not migrated:
 - Rogue AP Alert Timeout
 - Unknown Class Timeout
 - Multicast Addresses Timeout
 - Infrastructure Hosts, Client Stations, and Repeater Timeout
 - When both port and protocol filters are applied on an interface
 - Default multicast address filtering for an interface
- Maximum RTS Retries settings range from 1 to 128. If the configured setting is greater than 128, the migrated setting is 128.
- Maximum Data Retries settings range from 1 to 128. If the configured setting is greater than 128, the migrated setting is 128.

- Data Beacon Rate (DTIM) settings range from 1 to 100. If the configured setting is greater than 100, the migrated setting is 100.
- Beacon Period settings range from 20 to 4000. If the configured setting is greater than 4000, the migrated setting is 4000 and if the configured setting is less than 20, the migrated setting is 20.
- WEP Key Rotation Interval settings range from 1 to 10. If the configured setting is greater than 10, the migrated setting is 10.
- If the configured settings for the LEAP or EAP transmit key is not set to Key 1, the following error is produced by Cisco IOS software in the migrated configuration:
 - Error: LEAP/EAP authentication does not support the key index#.
- If the configured setting for DSCP is not a specific value (0, 1, 2, 3, 4, 5, 6, 7, 11, 12, 12, 21, 22, 23, 31, 32, 33, 41, 42, or 43), the following error is produced by Cisco IOS software in the migrated configuration when viewing the settings using the HTTP interface:
 - *Policy_policy_fallback_policy* was created using CLI. It must be deleted via CLI to ensure proper operation of the web interface.



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

- If host names are used for RADIUS, accounting, and NTP servers, the converted Cisco IOS access points are unable to use DNS to obtain the corresponding IP addresses. Cisco recommends that you change your VxWorks configurations to use IP addresses rather than host names for RADIUS, accounting, and NTP servers, or to configure the servers after the converted access points boot up.
- If a Native VLAN is not configured, an error warning message is displayed.



A

- AAA server configuration [3-5, 4-6](#)
- Add/Remove Programs [1-10](#)
- Add Task button [1-8, 4-3](#)
- administrator
 - defined [3-5](#)
 - requirements [2-6](#)
 - user [vi](#)
- admin name [2-6](#)
- audience [vi](#)

B

- buttons
 - on Conversion Tool Main Window [1-8](#)
 - on Security Configuration Window [3-4](#)

C

- Cancel button [3-4](#)
- Caution [1-2, 2-4](#)
- Caution, defined [vi](#)
- Cisco Web site [1-5](#)
- completed status [1-8, 4-8](#)
- control panel [1-10](#)
- conventions [vi](#)
- conversion tool
 - installing [1-6](#)
 - main window [1-7](#)
 - obtaining software [1-5](#)
 - running [1-6](#)
 - starting tasks [4-8](#)

- status [1-8](#)

D

- Def.11a WEP button [4-7](#)
- Def. 11b WEP button [3-4](#)
- Delete Task button [1-8](#)
- device [4-3](#)
- Device Configuration tab [2-2](#)
- device type [1-7](#)
- disk storage [1-7](#)
- document organization [vi](#)

E

- error status [1-8, 4-8](#)
- Exit button [1-8](#)

F

- file name parameter [2-5](#)
- Finish button [3-4](#)

G

- Get Security Configuration button [3-2, 4-5](#)

H

- Help button [1-8, 3-4](#)
- helper image file [2-3, 2-5, 4-4](#)

I

icon [4-2](#)
 installing the conversion tool [1-6](#)
 IOS Config button [1-8, 4-18](#)
 IOS configuration file, typical [4-18](#)

L

LEAP configuration [3-4, 4-6](#)

M

Modify Task button [1-8](#)
 multiple tasks [4-19](#)

N

Note, defined [vi](#)

O

obtaining software
 conversion tool [1-5](#)
 helper image file [1-5](#)

P

parameters
 AAA Server Configuration [3-5](#)
 LEAP Configuration [3-4](#)
 Source AP Configuration [2-3](#)
 Target AP Configuration [2-5](#)
 User Manager Configuration [3-5](#)
 WEP Key Configuration [3-6](#)
 password [3-2, 3-4](#)
 progress bar [1-8, 4-8](#)
 purpose [vi](#)

S

secret keys [3-2](#)
 Security Configuration window [3-2](#)
 Set Password button [3-4, 4-6](#)
 Set Secret Key button [3-4, 3-5, 4-6](#)
 Set VLAN WEP button [3-4, 3-6](#)
 source AP config field [1-7](#)
 starting [4-8](#)
 Start Task button [1-8, 4-20](#)
 status [1-8](#)

T

Target AP Config [1-7](#)
 Target Configuration [2-4, 4-4](#)
 task [1-7](#)
 task log [4-9](#)

U

uninstalling, conversion tool [1-10](#)
 user manager configuration [3-5](#)

V

View Log button [1-8](#)
 VLAN [3-6, 4-7](#)

W

WEP key [3-2, 3-6, 4-7](#)