Using the Conversion Tool

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

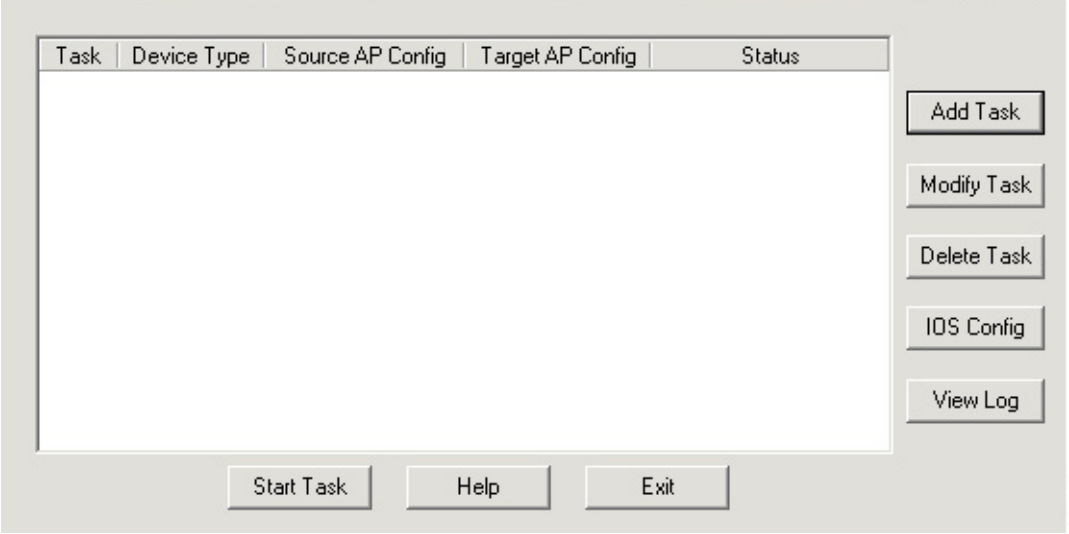
Adding a Task

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:

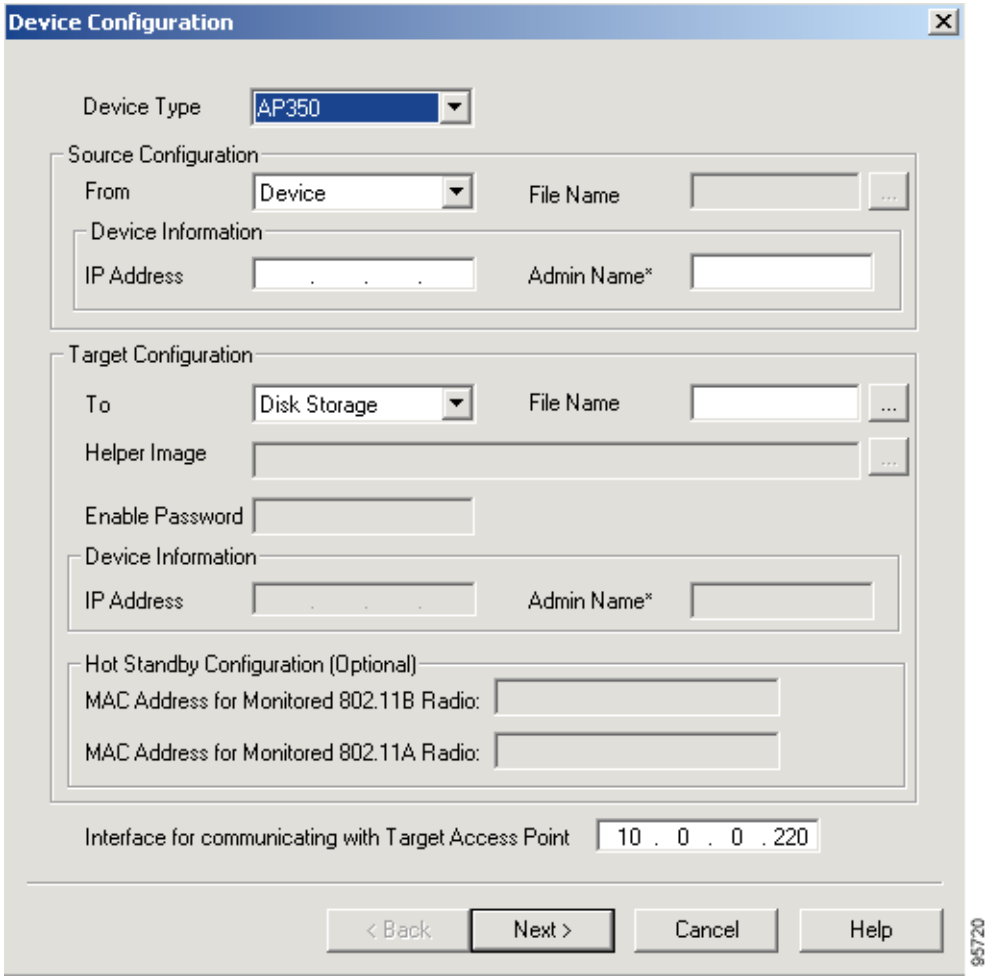
Step 1 Activate the conversion tool by double-clicking the conversion tool icon on your desktop or by selecting **Start > Programs > CAC Tool** (or your installation folder name) **> CAC Tool.** The conversion tool window appears (see Figure 4-1).

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.**

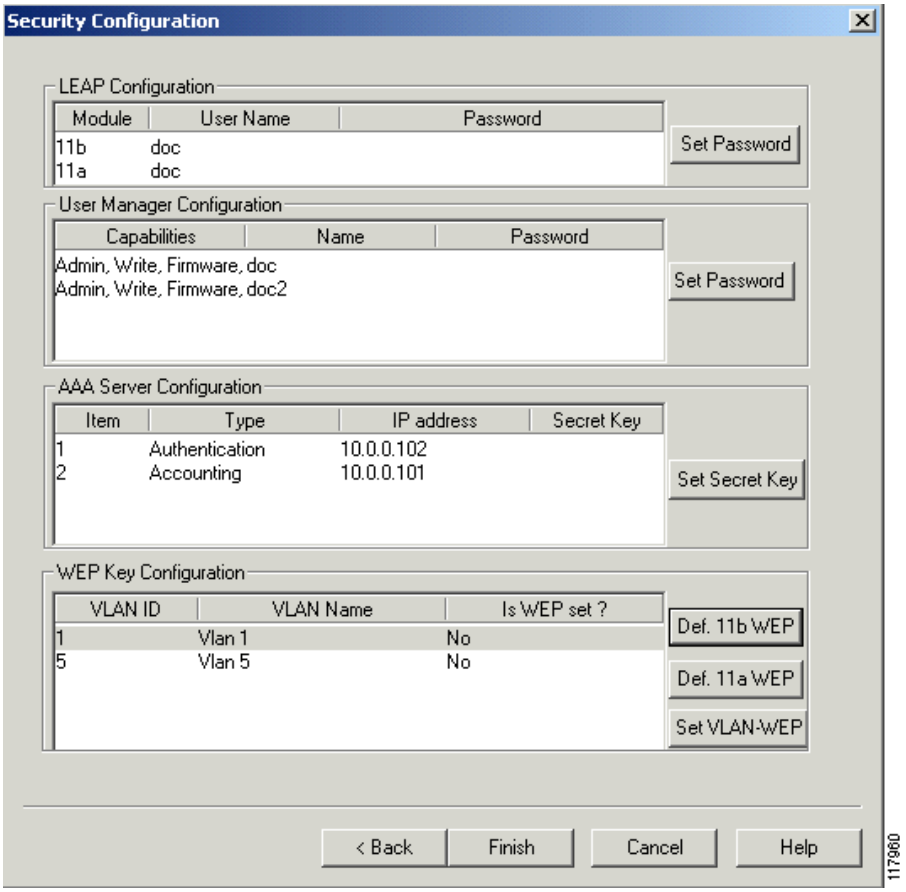
Step 14 Click **Get Security Configuration** on the Security Configuration window. A message appears indicating that the conversion tool is trying to gather security information from the access point. When the security information is available, the Security Configuration window displays the security 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



Step 15 In the LEAP Configuration area, follow these steps for each radio interface listed:

a. Select a radio interface entry.

b. Click **Set Password**.

c. 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:

a. Select a user entry.

b. Click **Set Password**.

c. 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:

a. Select a server entry.

b. Click **Set Secret Key**.

c. 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:

a. Select a VLAN entry and click **Set VLAN WEP**.

b. 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.

c. 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.

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

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

a. Click **Def. 11b WEP**. The WEP Key Configuration window appears.

b. Enter the WEP keys in the Encryption Key fields.

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

d. Set the transmit WEP key by clicking **Transmit with Key** for one WEP key entry.

Note Only one transmit WEP key can be selected.

e. Click **Def. 11a WEP**. The WEP Key Configuration window appears.

f. 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.

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

h. Set the transmit WEP key by clicking **Transmit with Key** for one WEP key entry.

Note Only one transmit WEP key can be selected.

i. 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:

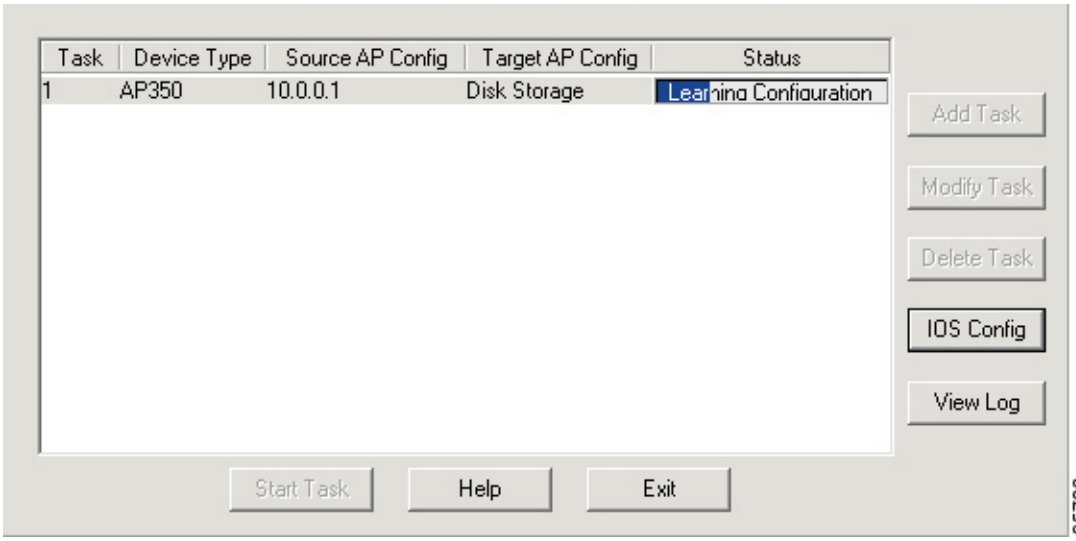
- To Start—indicates that the task is waiting to start.
- Progress bar—indicates the task progress by the length of the bar.
- Learning Configuration—indicates that the conversion tool is obtaining configuration information from the source access point.
- Completed—indicates that the task has executed 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.

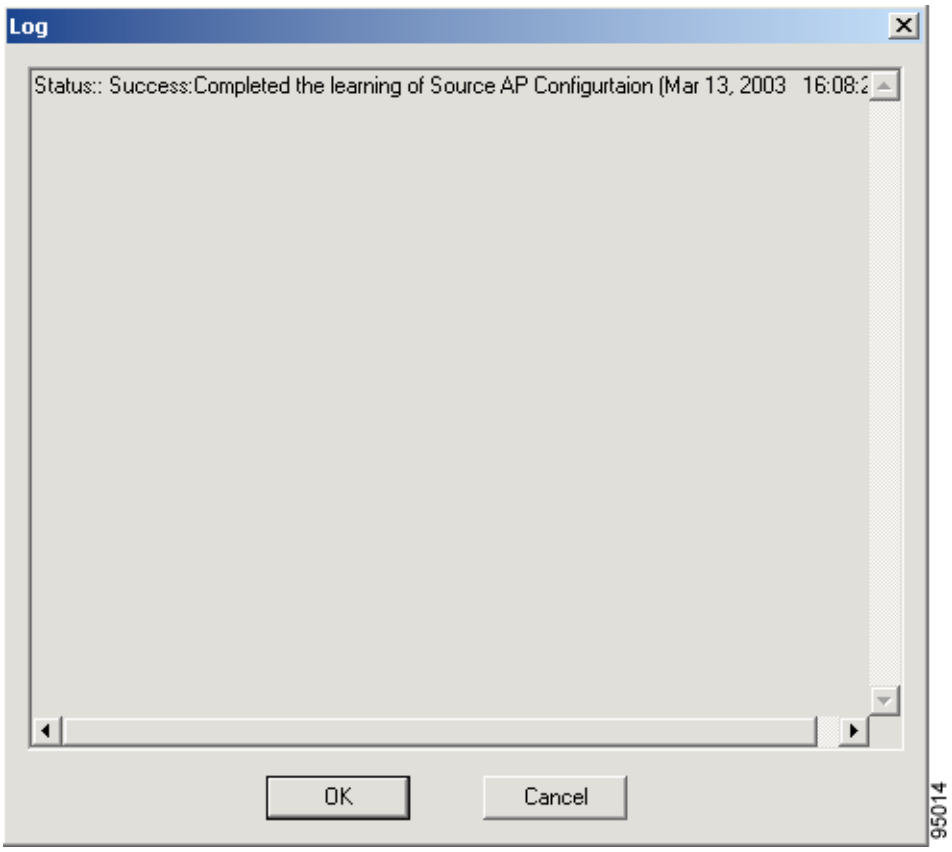
Viewing the Task Log

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.

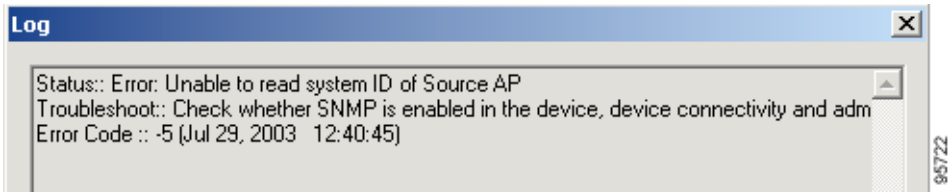
Figure 4-5 shows a typical log file.

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 administative 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, SNTP, 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.`

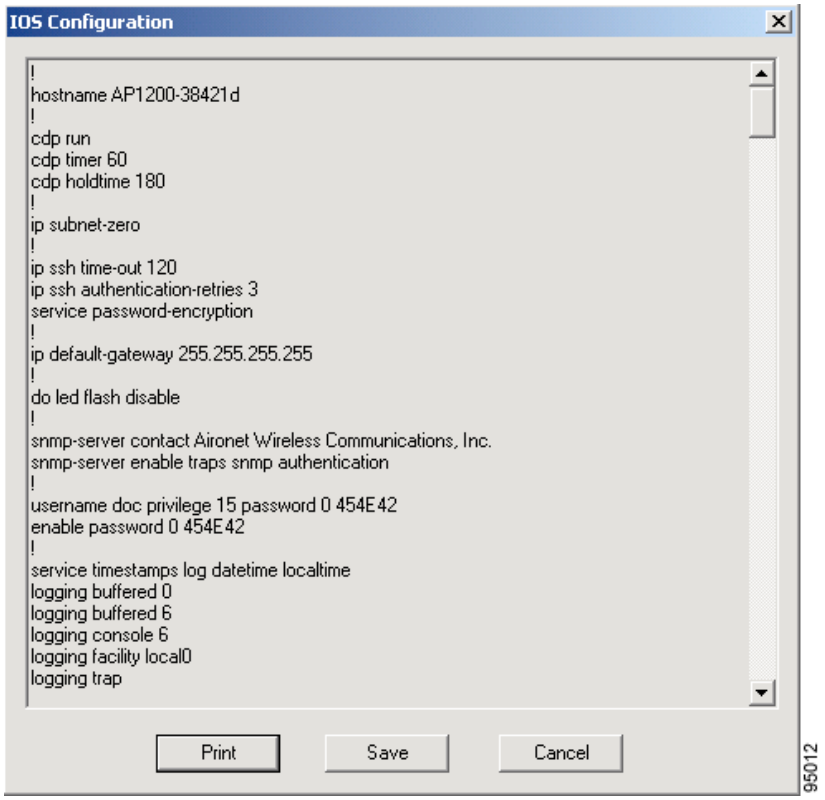
Error Message `Error: Unable to save the running config to the startup config.`

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).

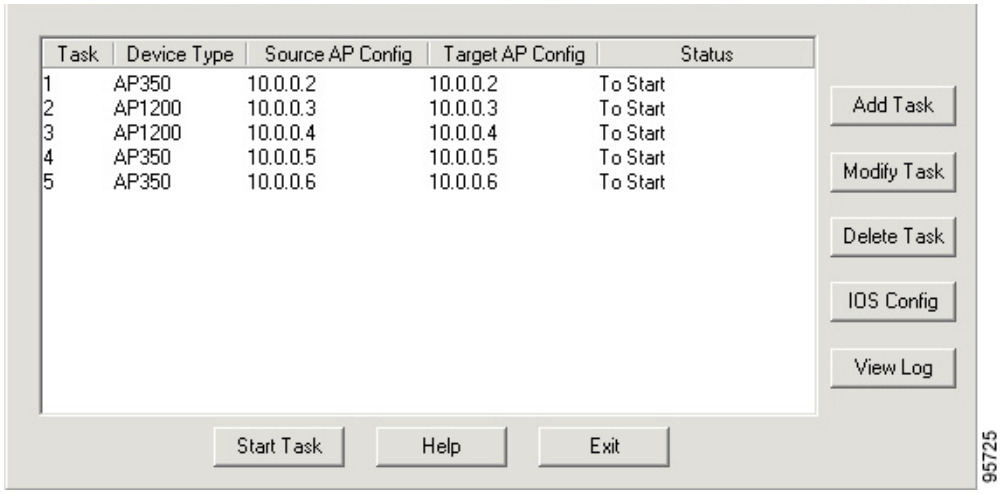
When your PC has the minimum PC hardware (refer to the "Before You Begin" section on page 1-3), the conversion tool supports up to 14 parallel helper image upgrades. You can enter up to 20 tasks, but only 14 of the tasks (maximum) can be helper image upgrades and the remaining tasks can be used to store 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