



## 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.

