# Release Notes for Cisco Aironet 802.11a/b/g Client Adapters (CB21AG and PI21AG) Install Wizard 3.0

## Contents

This document contains the following sections:


- Introduction, page 2
- System Requirements, page 2
- Important Notes, page 3
- New and Changed Information, page 6
- Installing or Upgrading Client Adapter Software, page 7
- Installing a Microsoft Hot Fix for Group Policy Delay, page 23
- Finding Version Numbers, page 24
- Caveats, page 25
- Troubleshooting, page 28
- Related Documentation, page 29
- Obtaining Documentation, page 29
- Documentation Feedback, page 30
- Cisco Product Security Overview, page 30
- Obtaining Technical Assistance, page 31
- Obtaining Additional Publications and Information, page 33



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



Copyright © 2006 Cisco Systems, Inc. All rights reserved.

# Introduction

This document describes system requirements, important notes, new and changed information, installation and upgrade procedures, and caveats for CB21AG and PI21AG client adapter Install Wizard release 3.0 and the following software included in the Install Wizard file:

- CB21AG and PI21AG client adapter driver release 3.0
- Aironet Desktop Utility (ADU) release 3.0
- Cisco Aironet Site Survey Utility release 1.3.01

# System Requirements

You need the following items in order to install Install Wizard 3.0 and use its software components:

- One of the following Cisco Aironet client adapters:
  - CB21AG PC-Cardbus card
  - PI21AG PCI card
- A computer running the Windows 2000 or XP operating system

  **Note** Cisco recommends a 300-MHz (or greater) processor.

- Service Pack 2 for Windows XP (Professional, Home); Service Pack 4 for Windows 2000.
- 20 MB of free hard disk space (minimum)
- 128 MB of RAM or greater (recommended)
- If your wireless network uses EAP-TLS or PEAP authentication, Certificate Authority (CA) and user certificates for EAP-TLS authentication or CA certificate for PEAP authentication
- If your wireless network uses PEAP (EAP-GTC) authentication with a One-Time Password (OTP) user database:
  - A hardware token device from OTP vendors or the Secure Computing SofToken program (version 2.1 or later)
  - Your hardware or software token password
- The Microsoft 802.1X supplicant, if your client adapter is installed on a Windows 2000 device and uses PEAP (EAP-MSCHAPV2) with machine authentication
- All necessary infrastructure devices (such as access points, servers, gateways, user databases, etc.) must be properly configured for any authentication type you plan to enable on the client.
- The following information from your system administrator:
  - The logical name for your workstation (also referred to as *client name*)
  - The protocols necessary to bind to the client adapter, such as TCP/IP
  - The case-sensitive service set identifier (SSID) for your RF network
  - If your network setup does not include a DHCP server, the IP address, subnet mask, and default gateway address of your computer

- The wired equivalent privacy (WEP) keys of the access points with which your client adapter will communicate, if your wireless network uses static WEP for security
- The username and password for your network account
- Protected access credentials (PAC) file if your wireless network uses EAP-FAST authentication with manual PAC provisioning

# Important Notes

## Mismatch between HP DC5 100 PCI Bus Controller and PCI Key Cache Register on PI21AG Chip

A mismatch exists between the HP DC5100 PCI bus controller and the PCI key cache register on the chip of the PI21AG. The key cache uses a 48-bit register in which the PI21AG sends out two writes on the PCI bus back to back (DWORD and WORD). The controller on the device cannot handle two consecutive write cycles on the bus, which causes a fatal error on the PCI bus.

You should slow down the write operations to the key cache by performing a register read before and after a register write. To slow down the write operations, install registry key "singleWriteKC=1." The path of the "singleWriteKC=1" registry key is the following:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}

You should not see any system degradation or performance hits, as the key cache is only changed every few minutes. An additional read before the second write cycle only lasts a few micro seconds in the PCI space.

## Installing the CB21AG Intermediate Driver Manually

In some instances, the installation of the CB21AG software might not work as expected because the intermediate driver might not have installed correctly. In this situation, the installer might not detect this condition, and the rest of the software will not function correctly.

The CB21AG intermediate driver must be installed manually. To install the intermediate driver manually, follow these steps:

**Step 1** Insert the client adapter.

**Step 2** Click on "Network Connections" in the Start > Settings menu in Windows XP, or right click on "My Network Places" in Windows 2000. Find the CB21AGg instance.

**Step 3** Right click on the Cisco CB21AG instance, and left click on Properties.

**Step 4** Choose the "Install" option and then add a new service.

**Step 5** Choose the "Have disk" button. Go to \windows\system32 directory and choose wsimd.inf.

**Step 6** Highlight and select "Wireless Intermediate Driver" and click "ok" button. The wireless IMD is bound to the adapter.

**Step 7** Reboot system.

## Incompatibility between PACs Created by ACS Version 3.x.xx and ACS Version 4.0.xx

PACs that are created by ACS version 3.x.xx are not compatible with ACS version 4.0.xx. Client stations must import new PACs. If you select auto-provisioning, new PACs will automatically be generated and used. However, if you select manual provisioning, you must manually export new PACs to the client stations.

If a user wants to authenticate to ACS version 4.0.xx and version 3.x.xx at different times, both PACs must remain on the client station. The ADU is capable of automatically selecting the appropriate PAC.

However, if you experiences authentication failures after upgrading the software, delete all the PACs provisioned from the 3.x.xx server.

## Conflict with Third-Party Supplicants

When using release 3.0, you might encounter a conflict with third-party supplicants (such as the Meetinghouse Aegis or the Juniper Odyssey) that causes the Cisco client adapter to lose connection. If you encounter such a conflict, disable third-party supplicants.

## Customized Installation Images (Notice to IT Professionals)

**Caution** Use caution when bundling the client adapter software into a customized installation image. If the registry settings are modified, the software may not install and uninstall properly.

## Client Adapter Software Compatibility

**Caution** Cisco Aironet CB21AG and PI21AG client adapter software is incompatible with other Cisco Aironet client adapter software. The Aironet Desktop Utility (ADU) must be used with CB21AG and PI21AG cards, and the Aironet Client Utility (ACU) must be used with all other Cisco Aironet client adapters.

## Installing the Novell Client

If you are going to use the Novell Client, be sure to install it on your computer prior to installing the client adapter software.

## Enabling CCKM Fast Secure Roaming

If you want to enable CCKM on the client adapter, you must choose the WPA/WPA2/CCKM security option, regardless of whether you want the adapter to use WPA or WPA2. The configuration of the access point to which your client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.

## Access Point Setting for LEAP or EAP-FAST Authentication

Access points must be set for both Network-EAP and open authentication in order to associate to CB21AG and PI21AG client adapters running LEAP with WPA/WPA2/CCKM or EAP-FAST.

## EAP-FAST Fails When Access Point Configured as Local RADIUS Server

The client adapter fails to authenticate using EAP-FAST when the access point is running Cisco IOS Release 12.3(2)JA2 and is configured as a local RADIUS server. The following message appears: "Unable to EAP-FAST authenticate the wireless user in the specified amount of time. Network infrastructure might be down."

## GINA Error on Bootup

If your computer ever experiences a GINA error on bootup, boot to the safe mode command prompt. Then copy the msgina.dll file in the WinNT\System32 directory (Windows 2000) or Windows\System32 directory (Windows XP) over to a file named cscogina.dll. The **copy** command enables you to copy a source file (msgina.dll) to a destination file (cscogina.dll) within the same directory.

## Reboot Required When Uninstalling ACU and ADU

**Caution** When you uninstall ACU and ADU, be sure to reboot your computer when prompted. Otherwise, the system may be rendered unable to boot, displaying the message "The Logon User Interface DLL cswGina.dll failed to load. Contact your system administrator to replace the DLL or restore the original DLL."

## Uninstalling Software Components

All profiles and stored PAC files are deleted if you use the **Uninstall the previous installation** option on the Previous Installation Detected Install Wizard window to uninstall the client adapter software. Cisco recommends that you use the Profile Manager's export feature to save your profiles before uninstalling the software.

## Profiles for PC-Cardbus Cards

The profiles for PC-Cardbus cards are tied to the slot in which the card is inserted. Therefore, you must always insert your PC-Cardbus card into the same slot, create profiles for both slots, or export the profiles for one slot and import them for the other slot.

## Auto Profile Selection Enables Scan of Wireless Modes in Auto-Selected Profiles

When you enable auto profile selection, the client adapter ignores the selected profile's wireless mode setting and scans the wireless modes specified by all the profiles in the auto profile selection list for an available network. Using this method, the client does not need to disassociate nor change the current profile while looking for networks in other profiles.

## ASTU Exit Option

The Exit option on the Aironet System Tray Utility (ASTU) pop-up menu closes both ASTU and ADU.

## Windows Wireless Network Connection Icon Shows Unavailable Connection (Windows XP Only)

If your computer is running Windows XP and you configured your client adapter using ADU, the Windows Wireless Network Connection icon in the Windows system tray may be marked with a red *X* and show an unavailable connection even though a wireless connection exists. This condition is caused by a conflict between ADU and Windows XP's wireless network settings. Simply ignore the Windows icon and use the ASTU icon to check the status of your client adapter's wireless connection.

## Supporting Documentation

The *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* (OL-4211-05) pertains specifically to CB21AG and PI21AG client adapters. If you are using a Cisco Aironet 340, 350, or CB20A client adapter, refer to the Installation and Configuration Guide for that client adapter and your computer's operating system.

# New and Changed Information

## EAP-FAST Enhancements

The following is a list of EAP-FAST enhancements, which are accessible through the ADU user interface:

- Support of additional EAP authentication methods

  Version 3.0 of ADU supports three EAP methods in both the PAC auto provisioning phase and the EAP-FAST authentication phase. These methods are:

  - EAP-MSCHAPv2
  - EAP-GTC
  - EAP-TLS
- PAC configuration and management screens

Version 3.0 of ADU has updated PAC configuration screens.

- Minor updates to other screens

For more information about the new updates, refer to chapters 6 and 5 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide*, OL-4211-05.

## PAC Export

In the previous version, when an EAP-FAST profile is exported or imported, the PAC data linked with the profile was getting ignored. To solve this problem, version 3.0 of ADU supports the exporting of PAC data using .PAC files.

# Installing or Upgrading Client Adapter Software

This section describes how to initially install or upgrade to CB21AG and PI21AG Install Wizard 3.0 on a computer running Windows 2000 or XP. If the client adapter software is not installed on your computer, follow the instructions in the "Installing or Upgrading Client Adapter Software" section below. If you are upgrading your client adapter software to release 3.0, follow the instructions in the "Upgrading the Client Adapter Software" section on page 19.

# Installing the Client Adapter Software

This section describes how to install Cisco Aironet CB21AG or PI21AG client adapter driver and utilities from a single executable file named *WinClient-802.11a-b-g-Ins-Wizard-vx.exe*, where *x* represents the release number. Follow these steps to install these client adapter software components on a computer running Windows 2000 or XP.

**Caution** Cisco Aironet CB21AG and PI21AG client adapter software is incompatible with other Cisco Aironet client adapter software. The Aironet Desktop Utility (ADU) must be used with CB21AG and PI21AG cards, and the Aironet Client Utility (ACU) must be used with all other Cisco Aironet client adapters.

**Caution** Do not eject your client adapter at any time during the installation process, including during the reboot.

**Note** This procedure is meant to be used the first time the Cisco Aironet CB21AG or PI21AG client adapter software is installed on your computer. If this software is already installed on your computer, follow the instructions in Chapter 9 to upgrade the client adapter software.

**Note** Only one CB21AG or PI21AG client adapter can be installed and used at a time. The software does not support the use of multiple CB21AG or PI21AG cards.

**Step 1** Make sure the client adapter is inserted into your computer.

**Step 2** Make sure that you have a Cisco Connection Online (CCO) username and password.

**Step 3** If you do not have a CCO username and password, go to Cisco's main page (http://www.cisco.com) and click Register (top). Then, follow the instructions to create a CCO username and password.

**Step 4** Browse to the following location:

http://www.cisco.com/public/sw-center/

**Step 5** Click **Wireless Software**.

**Step 6** Click **Wireless LAN Access**.

**Step 7** Click **Cisco Wireless LAN Client Adapters**.

**Step 8** Click **Cisco Aironet Wireless LAN Client Adapters**.

**Step 9** Perform one of the following steps:

- If you are using a PC-Cardbus card, click **Cisco Aironet 802.11a/b/g CardBus Wireless LAN Client Adapter (CB21AG)**.
- If you are using a PCI card, click **Cisco Aironet 802.11a/b/g PCI Wireless LAN Client Adapter (PI21AG)**.

**Step 10** When prompted, enter your CCO username and password, and click **OK**.

**Step 11** Click **Aironet Client Installation Wizard (Firmware, Driver, Utility)**.

**Step 12** Click **Windows 2000 or Windows XP**.

**Step 13** Click the link with the greatest release number.

**Step 14** Click the Install Wizard file (**WinClient-802.11a-b-g-Ins-Wizard-v*xx*.exe**), where ***xx*** is the version number.

**Step 15** If prompted, enter your CCO username and password, and click **OK**.

**Step 16** Complete the encryption authorization form, read and accept the terms and conditions of the Software License Agreement, select the file again to download it, and save the file on your computer's Desktop.

**Step 17** Use Windows Explorer to find the installer.

**Step 18** Double-click the installer. The "Starting InstallShield Wizard" message appears followed by the Preparing Setup window (see Figure 1) and the Cisco Aironet Installation Program window (see Figure 2).

*Figure 1 Preparing Setup Window*

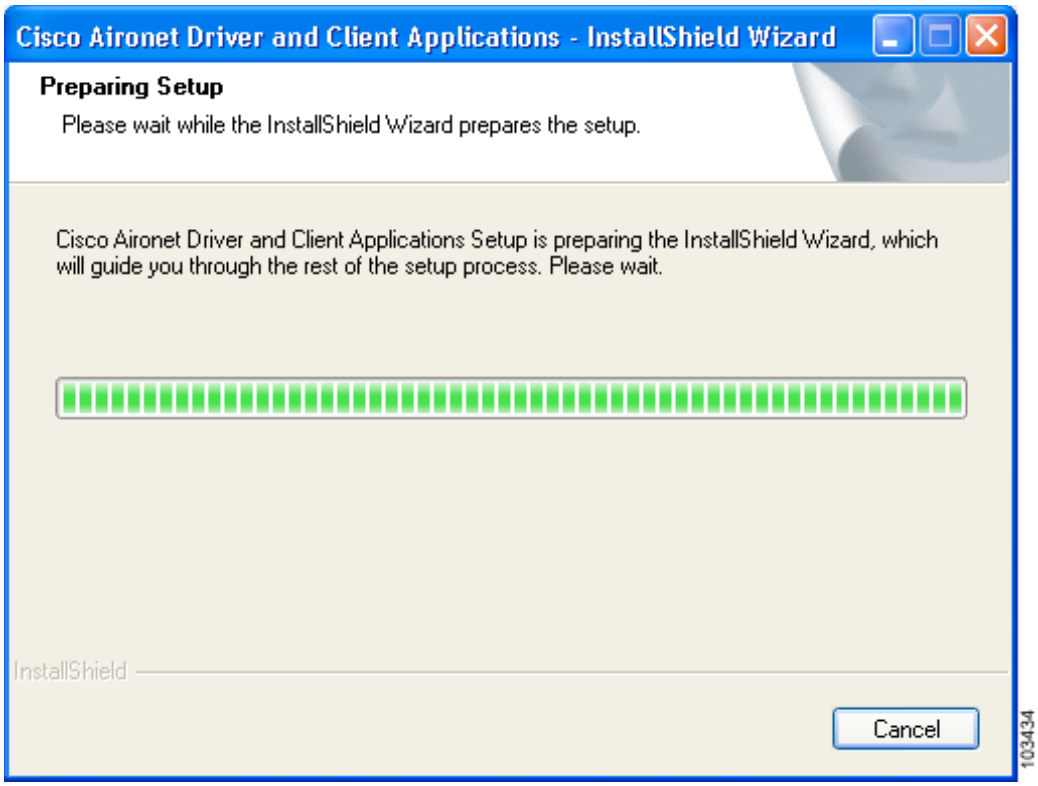
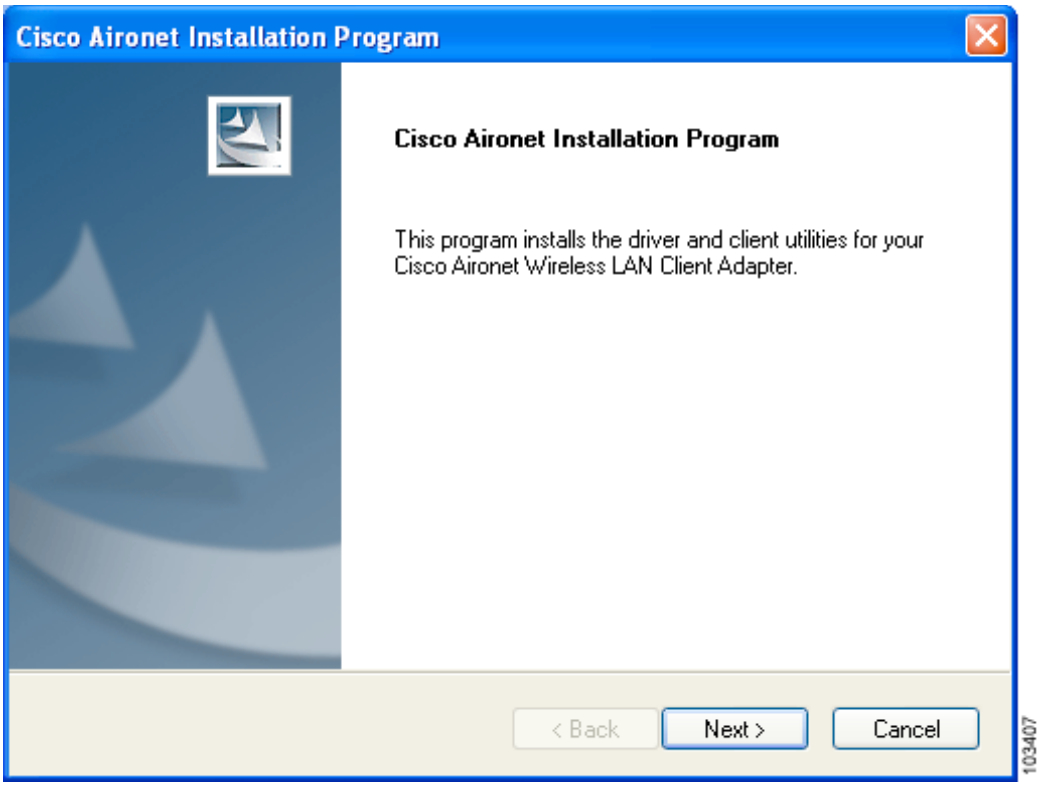
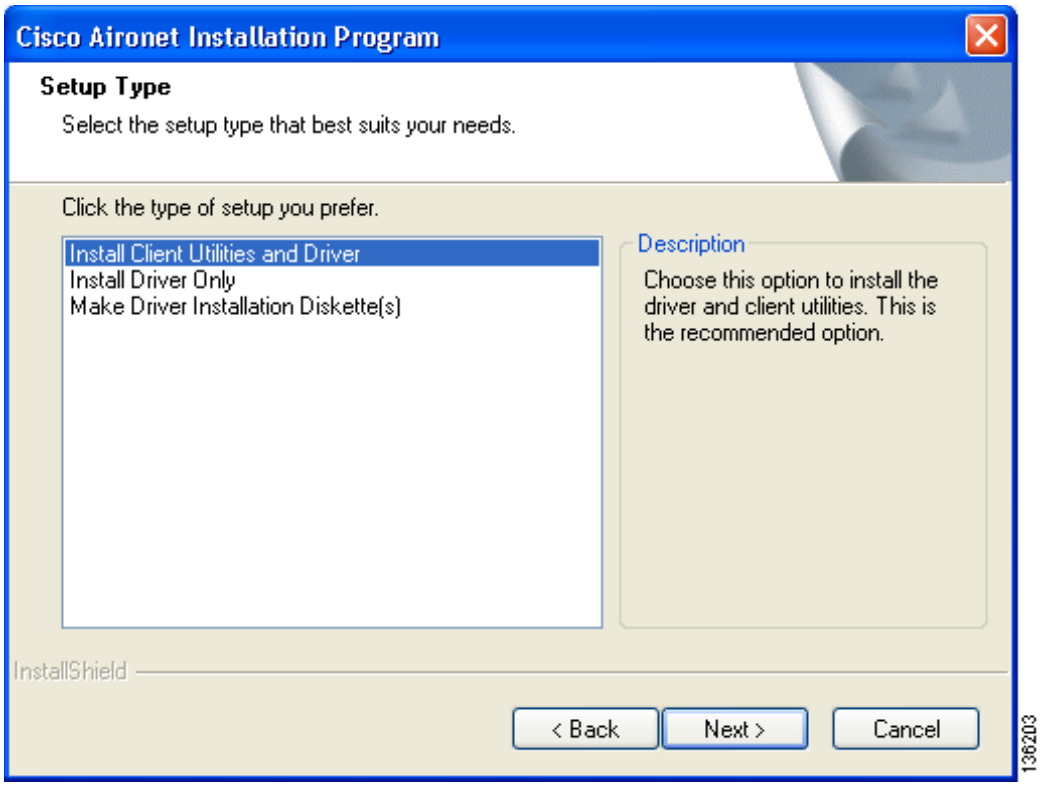


*Figure 2 Cisco Aironet Installation Program Window*




**Step 19** Click **Next**. The Setup Type window appears (see Figure 3).

*Figure 3 Setup Type Window*




**Step 20** Choose one of the following options and click **Next**:

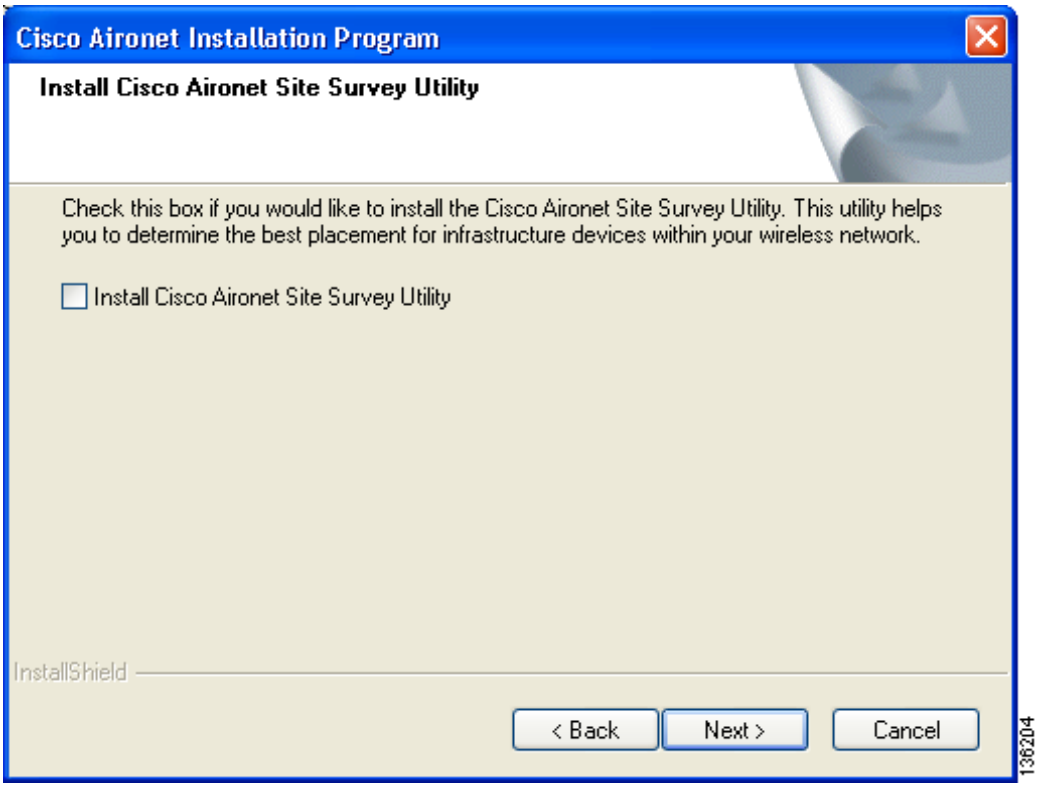
**Note** To ensure compatibility among software components, Cisco recommends that you install the client utilities and driver.

- **Install Client Utilities and Driver**—Installs the client adapter driver and client utilities.
- **Install Driver Only**—Installs only the client adapter driver. If you choose this option, click **Next** and go to Step 32.
- **Make Driver Installation Diskette(s)**—Enables you to create driver installation diskettes that can be used to install drivers using the Windows Device Manager.

**Note** If you choose one of the first two options and a client adapter is not inserted into your computer, the following message appears: "The device may not be present or could have been ejected/unplugged from the system. Insert or reinsert it now." Insert the client adapter and click **OK**. If you proceed without the client adapter inserted, the installation continues, but the driver installation is incomplete. You must manually install the driver later using the Update Device Driver Wizard. See Chapter 9 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for instructions.

**Step 21** When the Install Cisco Aironet Site Survey Utility window appears (see Figure 4), check the **Install Cisco Aironet Site Survey Utility** check box if you want to install a utility that helps you to determine the best placement of infrastructure devices within your wireless network. Click **Next**.

***Figure 4 Install Cisco Aironet Site Survey Utility Window***



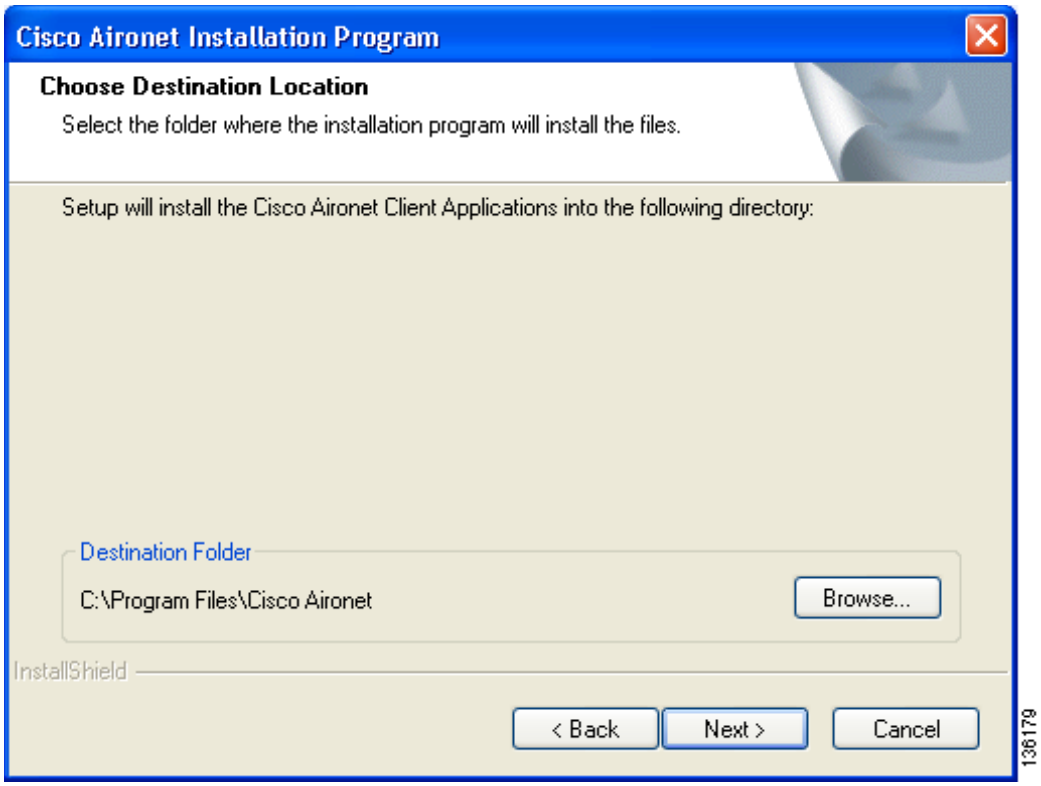

**Note** See Appendix F of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for instructions on using the utility.

**Step 22** If a message appears indicating that you are required to restart your computer at the end of the installation process, click **Yes**.

**Note** If you click **No**, you are asked to confirm your decision. If you proceed, the installation process terminates.

The Choose Destination Location window appears (see Figure 5).

*Figure 5 Choose Destination Location Window*




**Step 23** Perform one of the following:

- If you chose the first option in Step 20, click **Next** to install the client utility files in the C:\Program Files\Cisco Aironet directory.

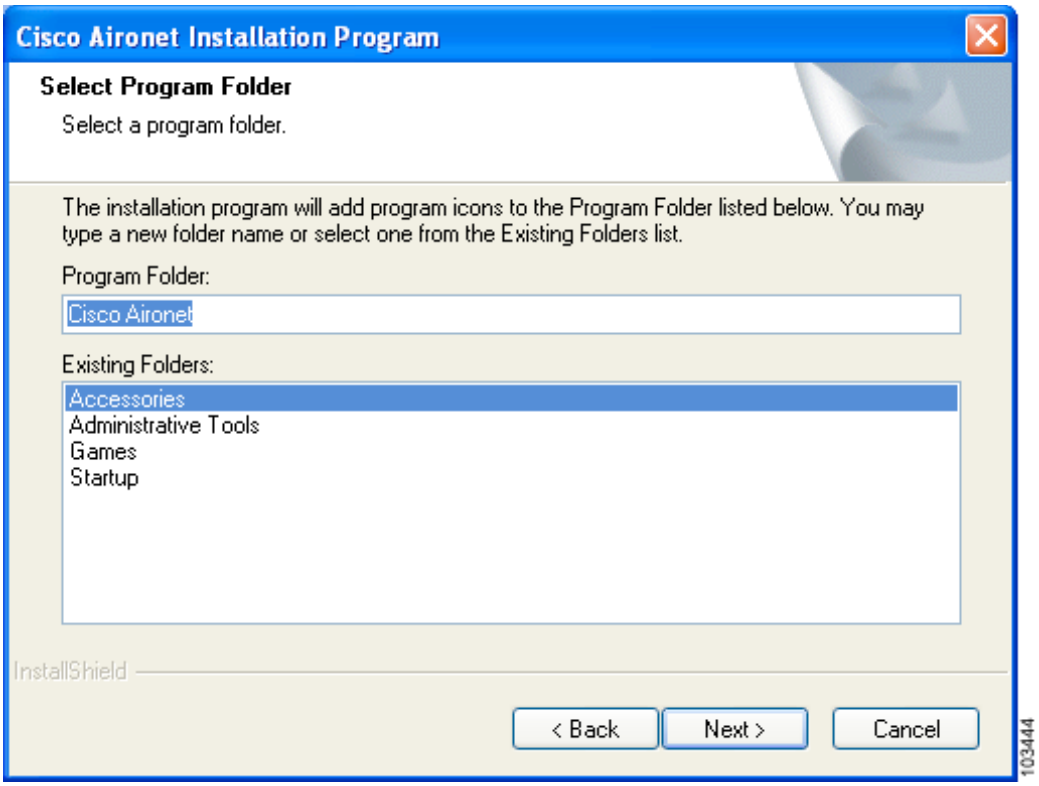
  **Note** If you want to install the client utilities in a different directory, click **Browse**, choose a different directory, click **OK**, and click **Next**.

- If you chose the Make Driver Installation Diskette(s) option in Step 20, insert a floppy disk into your computer and click **Next** to copy the driver to the diskette. Go to Step 32.

  **Note** If you want to copy the driver to a different drive or directory, click **Browse**, choose a new location, click **OK**, and click **Next**.

**Step 24** The Select Program Folder window appears (see Figure 6).

*Figure 6 Select Program Folder Window*

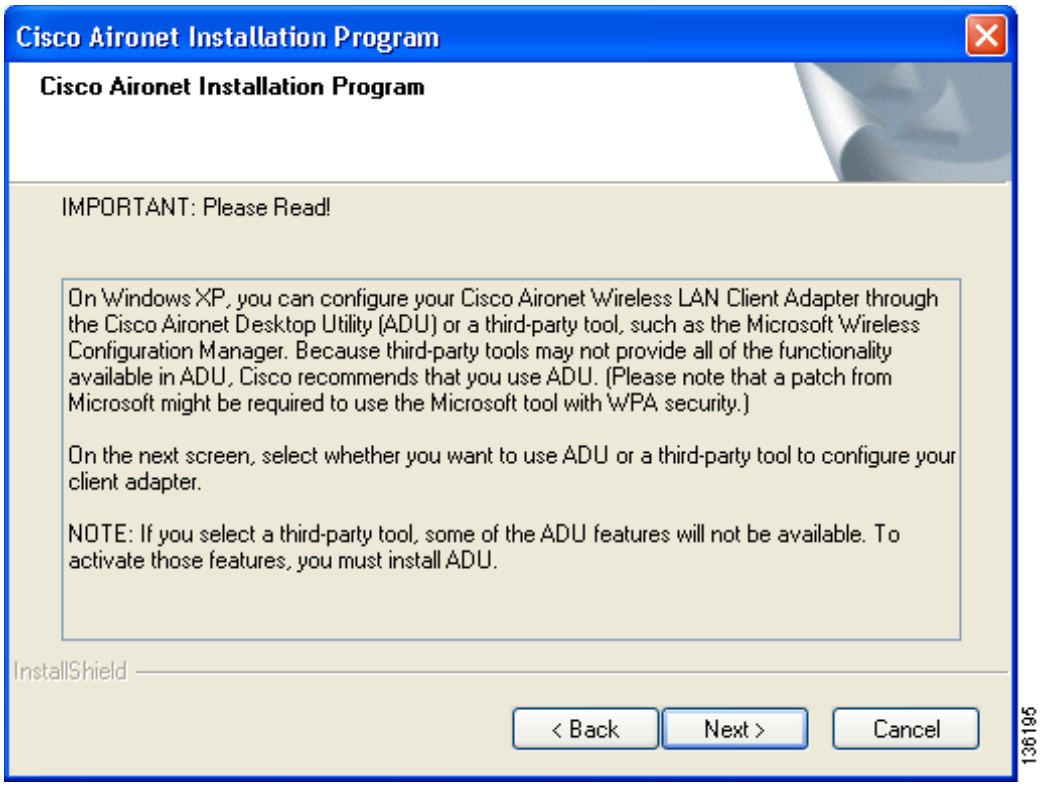



**Step 25** Click **Next** to add program icons to the Cisco Aironet program folder.

**Note** If you want to specify a different program folder, choose a folder from the Existing Folders list or type a new folder name in the Program Folder field and click **Next**.

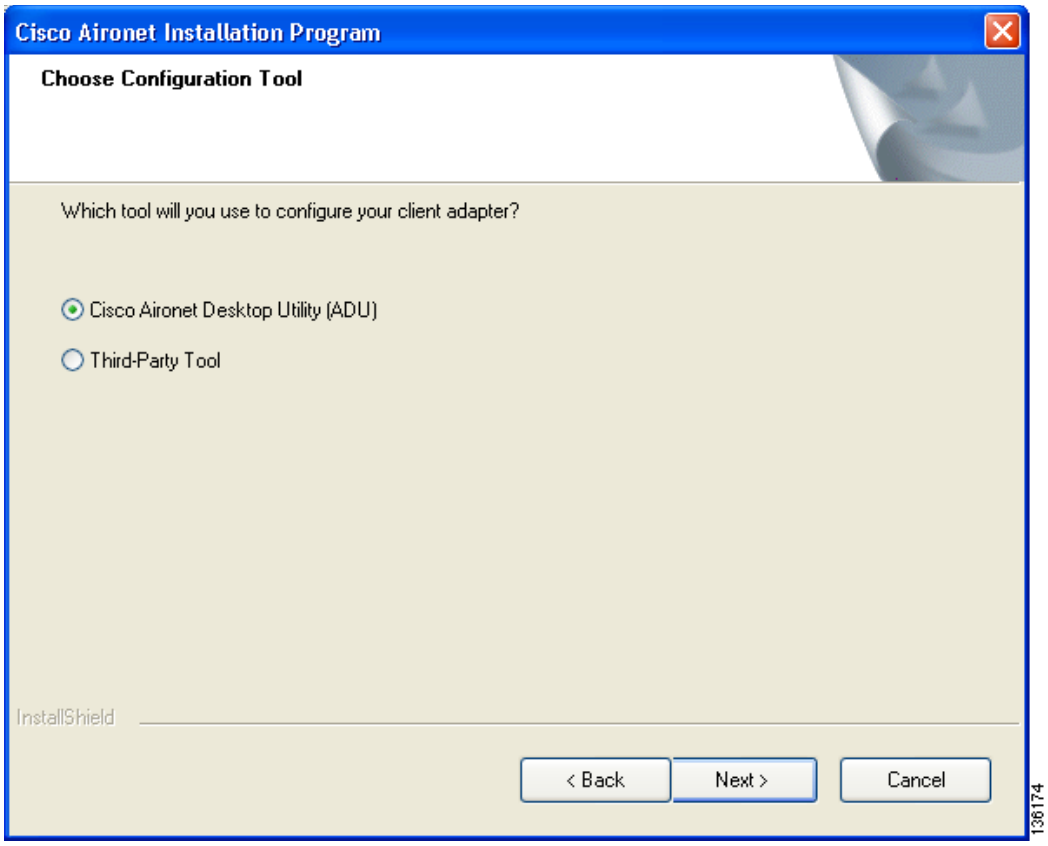
**Step 26** If your computer is running Windows 2000, go to Step 32. If your computer is running Windows XP, the window titled IMPORTANT: Please Read! appears (see Figure 7).

*Figure 7 IMPORTANT: Please Read! Window*




**Step 27** Read the information displayed and click **Next**. The Choose Configuration Tool window appears (see Figure 8).

*Figure 8 Choose Configuration Tool Window*




**Step 28** Choose one of the following options:

- **Cisco Aironet Desktop Utility (ADU)**—Enables you to configure your client adapter using ADU.
- **Third-Party Tool**—Enables you to configure your client adapter using a third-party tool such as the Microsoft Wireless Configuration Manager in Windows XP.

Table 1 compares Windows XP and ADU client adapter features.

*Table 1 Comparison of Windows XP and ADU Client Adapter Features*

| Feature | Windows XP | ADU |
|---|---|---|
| Configuration parameters | Limited | Extensive |
| Capabilities | | |
| Create profiles | Yes | Yes |
| Enable/disable radio | No | Yes |

*Table 1 Comparison of Windows XP and ADU Client Adapter Features*

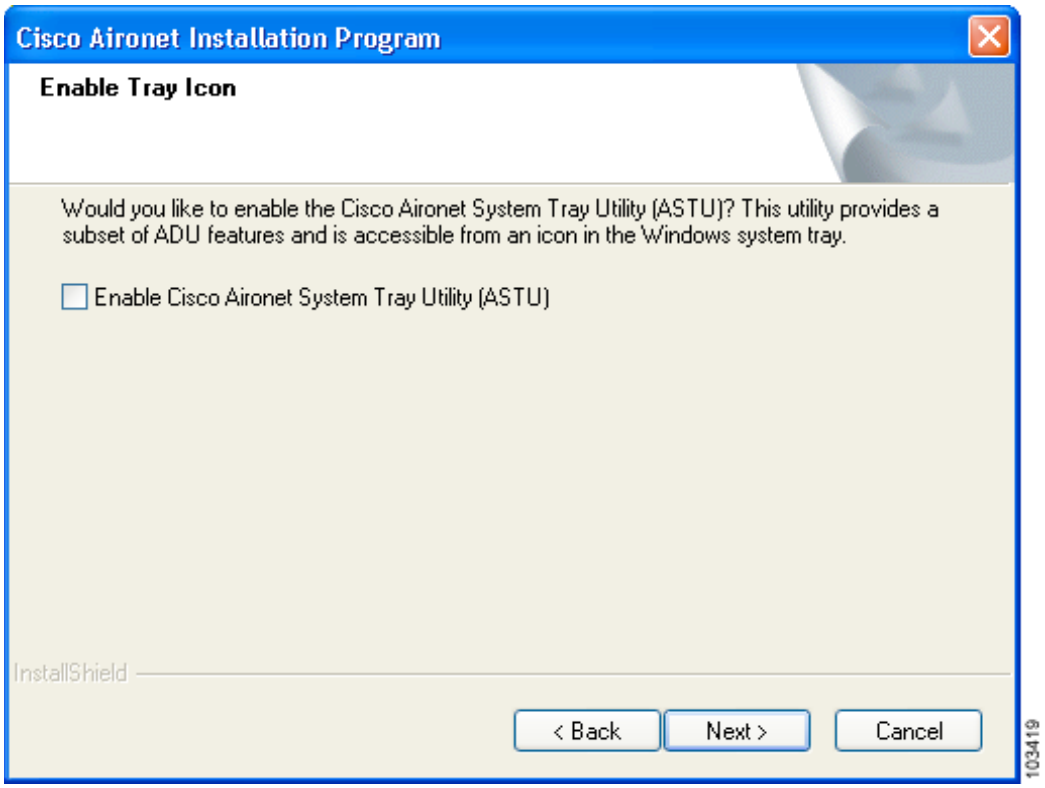
| Feature | Windows XP | ADU |
|---|---|---|
| Security | | |
| Static WEP | Yes | Yes |
| LEAP or EAP-FAST authentication with dynamic WEP | No | Yes |
| EAP-TLS or PEAP authentication | Yes | Yes |
| Status and statistics | | |
| Status window | Limited | Extensive |
| Statistics window (transmit & receive) | No | Yes |

**Note** If you choose Cisco Aironet Desktop Utility (ADU) above, the Microsoft Wireless Configuration Manager is disabled. If you ever manually enable it, you are prompted to disable it whenever ADU is activated.

**Step 29** Click **Next**.

**Step 30** If you chose Cisco Aironet Desktop Utility (ADU) in Step 28, go to Step 32. If you chose Third-Party Tool, the Enable Tray Icon window appears (see Figure 9).

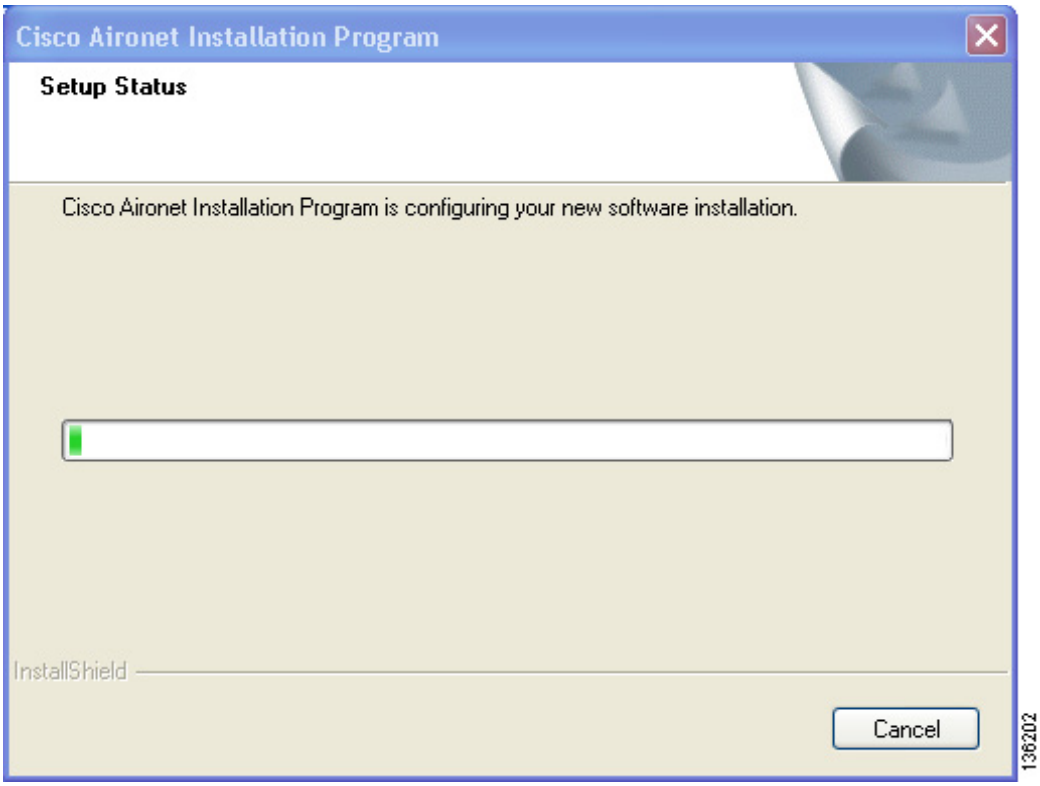
*Figure 9 Enable Tray Icon Window*



**Step 31** Check the **Enable Cisco Aironet System Tray Utility (ASTU)** check box if you want to be able to use ASTU even though you have chosen to configure your client adapter through a third-party tool instead of ADU and click **Next**.

**Step 32** When prompted to insert your client adapter, click **OK**. The Setup Status window appears (see Figure 10).

***Figure 10 Setup Status Window***




The installation process begins, and you are notified as each software component is installed.

**Step 33** When a message appears indicating that your computer needs to be rebooted, click **OK** and allow your computer to restart.

**Step 34** If the Windows Found New Hardware Wizard appears after your computer reboots, click **Next**, allow the wizard to install the software for the client adapter, and click **Finish**.

**Step 35** If your network setup does not include a DHCP server and you plan to use TCP/IP, follow these steps for your operating system.

- **Windows 2000**
  - **a.** Double-click **My Computer**, **Control Panel**, and **Network and Dial-up Connections**.
  - **b.** Right-click **Local Area Connection *x*** (where *x* represents the number of the connection).
  - **c.** Click **Properties**.
  - **d.** In the Components Checked Are Used by This Connection field, click **Internet Protocol (TCP/IP)** and **Properties**.

e. Choose **Use the following IP address** and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator).

f. Click **OK** to close each open window.

- **Windows XP**

a. Double-click **My Computer**, **Control Panel**, and **Network Connections**.

b. Right-click **Wireless Network Connection *x*** (where *x* represents the number of the connection).

c. Click **Properties**.

d. In the This Connection Uses the Following Items field, click **Internet Protocol (TCP/IP)** and **Properties**.

e. Choose **Use the following IP address** and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator).

f. Click **OK** to close each open window.

**Step 36** If you are prompted to restart your computer, click **Yes**.

**Step 37** Now that your client adapter is properly installed, it is ready to be configured.

- If you are planning to configure your client adapter through ADU, go to Chapter 4 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for more information.
- If you are planning to configure your client adapter through the Windows XP Wireless Configuration Manager, go to Appendix E of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for more information.
- If you are planning to configure your client adapter through another third-party tool, refer to the documentation for that application.

**Note** If you want to be able to use ADU's Group Policy Delay parameter, follow the instructions below to download and install a necessary hot fix before configuring your client adapter.

**Note** If you experienced problems during or after installation, refer to Chapter 10 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for more information for troubleshooting information.

# Upgrading the Client Adapter Software

Follow these steps to upgrade your CB21AG or PI21AG client adapter software to release 3.0 using the settings that were selected during the last installation.

**Note** If you want to upgrade your client adapter software using new installation settings, you must uninstall the previous installation [see the instructions in Chapter 9 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide*] and then follow the instructions in the "Installing the Client Adapter Software" section on page 7 to install the new software.

**Step 1** Make sure the client adapter is inserted into your computer.

**Step 2** Make sure that you have a Cisco Connection Online (CCO) username and password.

**Step 3** If you do not have a CCO username and password, go to Cisco's main page (http://www.cisco.com) and click Register (top). Then, follow the instructions to create a CCO username and password.

**Step 4** Browse to the following location:

http://www.cisco.com/public/sw-center/

**Step 5** Click **Wireless Software**.

**Step 6** Click **Wireless LAN Access**.

**Step 7** Click **Cisco Wireless LAN Client Adapters**.

**Step 8** Click **Cisco Aironet Wireless LAN Client Adapters**.

**Step 9** Perform one of the following steps:

- If you are using a PC-Cardbus card, click **Cisco Aironet 802.11a/b/g CardBus Wireless LAN Client Adapter (CB21AG)**.
- If you are using a PCI card, click **Cisco Aironet 802.11a/b/g PCI Wireless LAN Client Adapter (PI21AG)**.

**Step 10** When prompted, enter your CCO username and password, and click **OK**.

**Step 11** Click **Aironet Client Installation Wizard (Firmware, Driver, Utility)**.

**Step 12** Click **Windows 2000 or Windows XP**.

**Step 13** Click the link with the greatest release number.

**Step 14** Click the Install Wizard file (**WinClient-802.11a-b-g-Ins-Wizard-v*xx*.exe**), where ***xx*** is the version number.

**Step 15** If prompted, enter your CCO username and password, and click **OK**.

**Step 16** Complete the encryption authorization form, read and accept the terms and conditions of the Software License Agreement, select the file again to download it, and save the file on your computer's Desktop.

**Step 17** Use Windows Explorer to find the installer.

**Step 18** Double-click the installer. The "Starting InstallShield Wizard" message appears followed by the Preparing Setup window (see Figure 11) and the Cisco Aironet Installation Program window (see Figure 12).

*Figure 11 Preparing Setup Window*

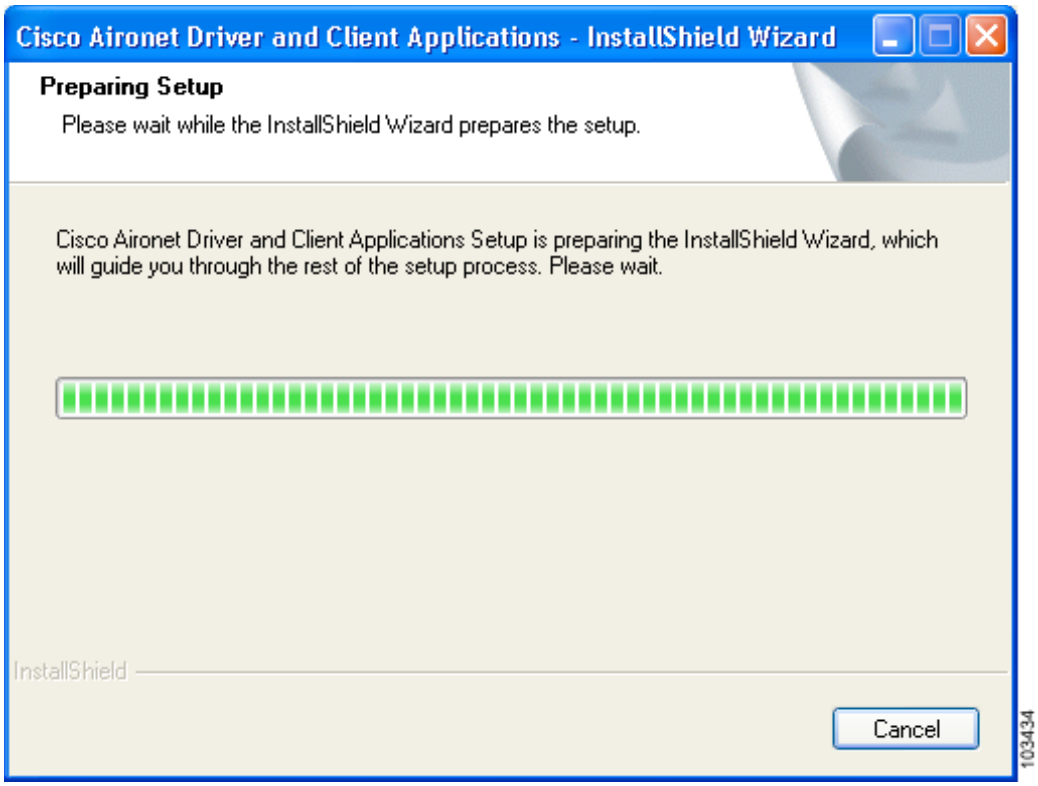
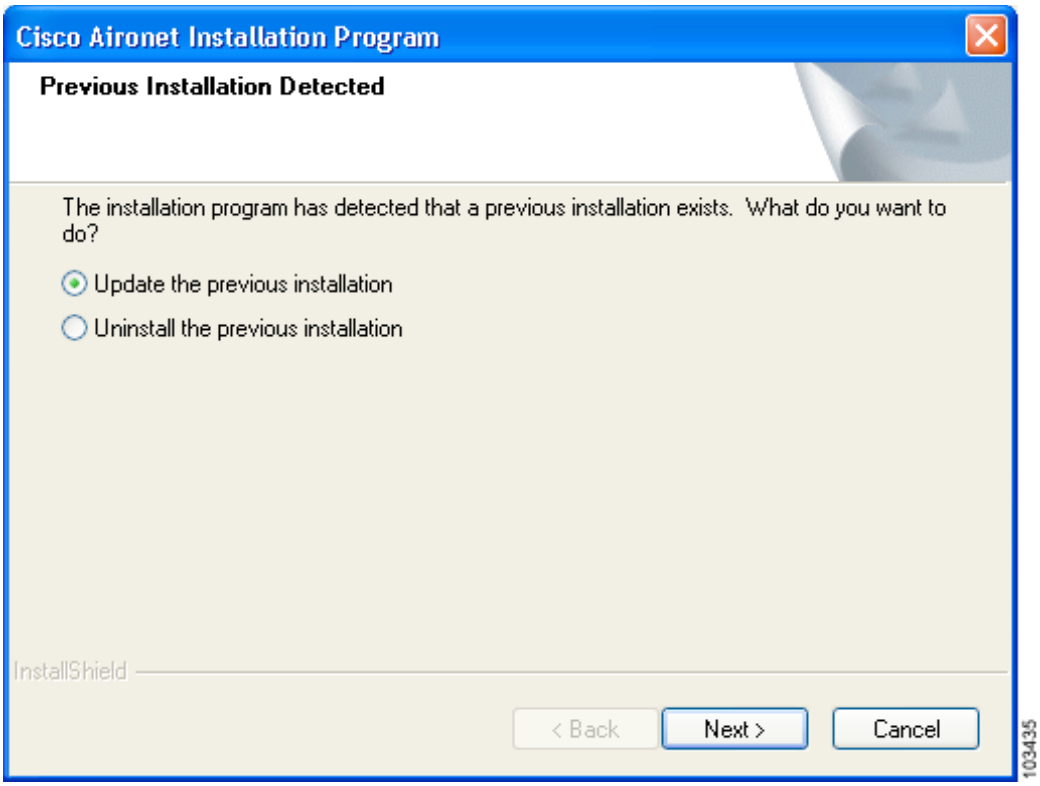


*Figure 12 Previous Installation Detected Window*



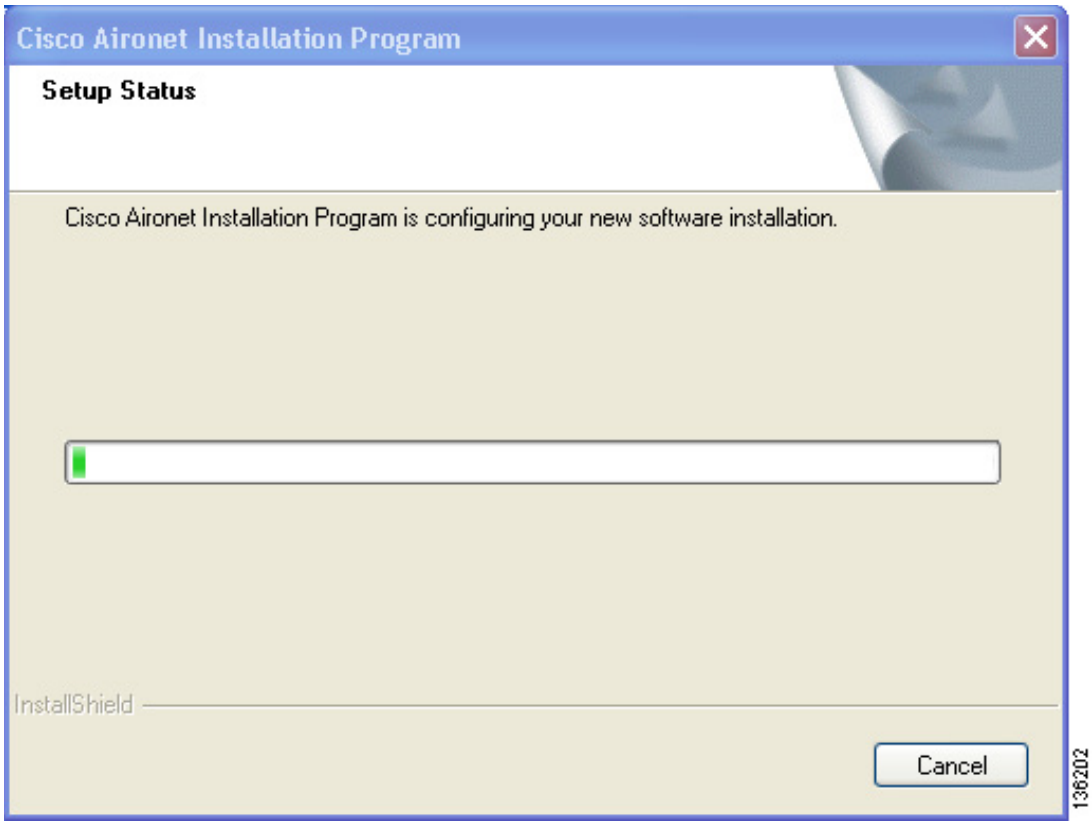

**Step 19** Choose **Update the previous installation** and click **Next**.

**Step 20** When a message appears indicating that you are required to restart your computer at the end of the installation process, click **Yes**.

**Note** If you click **No**, you are asked to confirm your decision. If you proceed, the installation process terminates.

The Setup Status window appears (see Figure 13).

*Figure 13 Setup Status Window*




The upgrade process begins, and you are notified as each software component is installed.

**Step 21** When a message appears indicating that your computer needs to be rebooted, click **OK** and allow your computer to restart. The client adapter's software has been upgraded.

# Installing a Microsoft Hot Fix for Group Policy Delay

If you want to use the Group Policy Delay parameter on the Profile Management (Security) window in ADU, you must install a Microsoft hot fix on computers running Windows 2000. The hot fix is incorporated into Windows XP Service Pack 2 and later.

The Group Policy Delay parameter enables you to specify how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. Follow the steps below to obtain and install the hot fix.

**Note** You must be a registered Cisco customer and log into Cisco.com in order to download the hot fix. If you are unable to access the hot fix from Cisco.com, contact Microsoft Support to obtain it. The Windows 2000 support page provides the contact information:
http://support.microsoft.com/default.aspx?scid=fh;EN-US;win2000

**Step 1** Use your computer's web browser to access the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/aironet_hotfix

**Step 2** If prompted, enter your Cisco Connection Online (CCO) username and password, and click **OK**.

**Note** To create a CCO username and password, visit http://www.cisco.com.

**Step 3** Click the hot fix file (userenv.zip).

**Step 4** Complete the encryption authorization form and click **Submit**.

**Step 5** Click the file again to download it.

**Step 6** Save the file to your computer's hard drive.

**Step 7** Find the file using Windows Explorer, double-click it, and extract its files to a folder.

**Step 8** Reboot your computer and press **F8** while your computer is booting.

**Step 9** When the boot menu appears, select **Safe Mode with Command Prompt**.

**Note** You must complete this procedure in safe mode; otherwise, system file protection (SFP) will silently restore the original version of the file you are replacing.

**Step 10** Copy the hot fix file (userenv.dll) to %systemroot%\System32 and overwrite the existing version of this file.

**Step 11** Delete the copy of userenv.dll in %systemroot%\System32\DllCache.

**Step 12** Restart your computer.

# Finding Version Numbers

Follow the instructions in this section to find the version numbers of your client adapter's software components.

## Finding the Driver Version

To find the driver version that is currently installed for your client adapter, open ADU, click the **Diagnostics** tab, and click **Adapter Information**. The Driver Version field on the Adapter Information window shows the current driver version.

## Finding the Version of ADU and Other Software Components

To find the version of ADU and other software components installed for your client adapter, open ADU and choose the **About Aironet Desktop Utility** option from the Help drop-down menu. The About window shows the current version of the following software components: ADU, ACAU, the authentication supplicant, the protocol driver, and the Windows NDIS miniport driver.

# Caveats

This section describes the open, resolved, and closed caveats for the software components in this release.

## Open Caveats

The following caveats are not resolved in CB21AG and PI21AG client adapter software release 3.0:

- CSCsd31365—When the client connects to an access point that does not broadcast its SSID, the Cisco Aironet Site Survey Utility AP Scan List may not the access point's SSID for a short time.
- CSCsd80390—The "No machine certificates were found on your computer" message is misleading

  When using the Cisco AIR-CB21AG-A-K9 802.11/a/b/g client adapters and running ADU 2.6.0.1, if you try to select **ADU clients using EAP-TLS authentication**, you see a message stating that no machine certificates were found on your computer, even though the application automatically finds the machine certificates. Also, if you select **Use machine Information for Domain Logon** under EAP-TLS configuration, you get the same error message. This message will not cause any problem and should only be seen once.
- CSCsd86612—If a user enters an incorrect password, the ADU will prompt the user to re-enter the password, but the ACS server will not record an invalid login attempt in its logs.

  This behavior is by design. The ACS server does not log an EAP failure because it gives the user a chance to reauthenticate.
- CSCse05471—The CB21 client adapter cannot pass the authentication phase with a Traditional Chinese username

  This only occurs on a machine with the Traditional Chinese language pack and a 2-byte username. When configuring the EAP-FAST authentication with Machine PAC, the STAUT failed to roam between access points.
- CSCse25438—The Advanced Status window of the ADU application shows the wrong SSID information

  In the ADU application, if you click **Current Status** and **Advanced**, you will notice that the Network Name (SSID) field displays only the first two characters of the SSID in the Advanced Status window. This happens when the SSID is a long string of characters with white spaces in between. The window wraps the string around into multiple lines and shows only one line.
- CSCse37717—EAP-FAST roaming fails with machine PAC

  Workaround: Uncheck the **session resume** check box in the ACS 4.0 RADIUS server.

- CSCse44432—PI21AG card in HP DC5100 might result in NMI parity error

  With a PI21AG card, long software installations over the network might fail. If error reporting is enabled in the BIOS, this failure might appear as a BIOS-level blue screen error. If error reporting is not enabled, this failure appears as a loss of network connectivity even though the card appears to be associated.

  This condition occurs when the PI21AG card is used in a HP DC5100 and is associtated to an AP1200 with an 802.11b radio. This condition does not occur with an AP with an 802.11g radio.

- CSCse49324—CB21AG retransmission mechanism has problems with RRM in LWAPP network

  A CB21AG client that is operating in an LWAPP infrastructure loses connection for small periods of time. When the AP is performing radio resource management (RRM), the AP goes off channel. During these periods, the AP cannot hear and answer ACK and RTS frames from the client. The client card initiates a scan for another AP, and network traffic for the client is affected.

  Workaround: Increase the HwTxRetries value from 4 to 14 (registry entry) so that the client card continues to retry for the 20 to 30 milliseconds that the AP is off channel.

# Resolved Caveats

The following caveat has been resolved in release 3.0:

- CSCeh59294—Failure to find domain controller during LEAP authentication

  The client adapter may be unable to find a domain controller when attempting to LEAP authenticate. This state can be a normal condition due to network unavailability.

- CSCeh59374—Switching between profiles is slow

  The client adapter may take up to 40 seconds to switch from one profile to another.

- CSCei30892—Multi-byte username cannot pass EAP-FAST authentication

  The CB21AG and PI21AG client adapters are unable to successfully EAP-FAST authenticate with an ACS server when the username contains multi-byte characters.

- CSCei40773—Incorrect messages on LEAP and EAP-FAST Authentication Status windows

  The LEAP and EAP-FAST Authentication Status windows show a successful status even if an IPX frame type is not detected or a domain controller is not found on the network.

- CSCsb46833—IOS access point with EAP-secured SSID toggles between "Open" and "Secure"

  When an IOS access point is configured with an SSID mapped to a VLAN and the SSID is secured with EAP and WPA-TKIP, then in the site survey utility's AP scan list, the access point may toggle between "Open" and "Secure." In this mode, the access point sends out the network configuration information in the beacon and probe responses. Certain fields may differ between beacons and probe responses when VLANs are enabled. The client adapter driver may report the fields from the beacon frame or probe response frame, whichever is received last.

- CSCsb53874—Timing error prevents MAC address authentication

  When using MAC address authentication, the client adapter fails to authenticate due to a timing error. To work around this problem, do not use MAC address authentication.

- CSCsb80735—LEAP-authenticated CB21AG loses connectivity

  A LEAP-authenticated CB21AG using WEP mandatory encryption might lose connectivity after some time and be unable to find an AP. This condition has been observed for an IBM T42 laptop running Windows XP, service pack 1 or 2.

- CSCsc25020—PEAP-GTC/AES authentication passes with any certificate chosen

  PEAP-GTC/AES authentications passes when “any” is chosen under the trusted root certificate authorities. PEAP-GTC/AES authentications also passes with any vendor certificate chosen under the trusted root certificate authorities.

- CSCsc46853—ADU has to be installed twice

  After the first installation and reboot, all areas are grayed out after clicking on the ADU icon in Profile Management. The user cannot create or modify the profile. After reinstallation and reboot, the user can configure the SSID and associate to an access point.

- CSCsc51460—CB21AG does not associate with an CCKM+AES AP

  A CB21AG client configured for WPA, WPA2, CCKM, or EAP is unable to associate on an SSID that is configured for AES+CCKM.

- CSCsc62060—ADU bundled with Site Survey Utility does not reflect changes to RF correctly

  The Site Survey Utility bundled with the CB21AG card is slow to recognize changes to the RF environment.

- CSCsc78069—Link status showing that the user is authenticating even though the user is already authenticated

  The link status on the ADU is showing "authenticating...." even though the client is already authenticated and is able to pass traffic.

- CSCsc84990—ADU versions 2.1 and 2.5 fail while importing PAC files

  While importing PAC files, the error message “Unable to save imported PAC data. Access denied.” may appear. This problem affects versions 2.1 and 2.5 of ADU.

- CSCsd08479—CB21AG/PI21AG client sometimes does MediaDisconnect if it roams

  A CB21AG/PI21AG client, when roaming twice in rapid succession, might undergo a link-layer media disconnect event, which will cause upper layer applications to lose connectivity for 30-40 seconds.

- CSCsd18192—Client does not display password window on ACS redundancy

  The ADU client does display the password window under these circumstances:

  - upon entering an invalid user name or password.
  - upon changing the user profile from a valid one to an invalid one.

- CSCsd39987—No valid PAC with local RADIUS after few days with EAP-FAST

  CB21AG clients authenticate using EAP-FAST and receive a PAC through auto-provisioning from a local RADIUS server (access point), but between one hour and a few days later, clients do not have a valid PAC when booted. 350 Clients do not see this issue.

- CSCsd44604—Unable to import the EAP-FAST PAC file of ACS 4.0

  The EAP-FAST PAC file that is exported by the CSUtil utility on ACS 4.0 cannot be imported to ADU manually.

# Getting Bug Information on Cisco.com

If you are a Cisco registered user, you can use the Cisco TAC Software Bug Toolkit, which consists of three tools (Bug Navigator, Bug Watcher, and Search by Bug ID Number) that help you to identify existing bugs (or caveats) in Cisco software products.

Access the TAC Software Bug Toolkit at the following URL:

http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl

# Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at

http://www.cisco.com/en/US/support/index.html

Click **Product Support > Wireless**. Then choose your product and **Troubleshooting** to find information on the problem you are experiencing.

# Related Documentation

For more information about ACAU and the Cisco Aironet CB21AG and PI21AG client adapters, refer to the following documents:

- *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Administration Utility Administrator Guide* (OL-7086-03)—Provides instructions for installing ACAU 3.0 and using it to set software installation options and create configuration profiles for CB21AG and PI21AG client adapters.

  http://www.cisco.com/en/US/products/hw/wireless/ps4555/prod_maintenance_guides_list.html

- *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* (OL-4211-05)—Provides instructions for installing, configuring, and troubleshooting CB21AG and PI21AG client adapters on computers running the Microsoft Windows 2000 or XP operating system.

  http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_installation_and_configuration_guides_list.html

- *Release Notes for Cisco Aironet 802.11a/b/g Client Adapters (CB21AG and PI21AG) Install Wizard 3.0* (OL-8338-01)—Describes new features and open and resolved caveats in Install Wizard 3.0.

  http://www.cisco.com/en/US/products/hw/wireless/ps4555/prod_release_notes_list.html

# Obtaining Documentation

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

## Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

## Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

## Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

# Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

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

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

We appreciate your comments.

# Cisco Product Security Overview

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

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

From this site, you will find information about how to:

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

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

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

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

## Reporting Security Problems in Cisco Products

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

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

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

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

**Tip** We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

# Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

# Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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

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

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

# Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

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

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

## Definitions of Service Request Severity

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

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

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

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

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

# Obtaining Additional Publications and Information

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

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

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

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

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

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

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

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

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, 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, 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, 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. (0601R)

Copyright © 2006 Cisco Systems, Inc.
All rights reserved.