Release Notes for Cisco Aironet 802.11a/b/g Client Adapters (CB21AG and PI21AG) Install Wizard 4.4

Contents

This document contains the following sections:

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

Introduction

This document describes system requirements, important notes, new and changed information, installation and upgrade procedures, caveats for CB21AG and PI21AG client adapter Install Wizard release 4.4, and the following software included in the Install Wizard file:

- CB21AG and PI21AG client adapter driver release 4.4
- Aironet Desktop Utility (ADU) release 4.4
- Cisco Aironet Site Survey Utility release 1.5

Note If you use the Cisco Aironet Client Administration Utility (ACAU), use ADU version 4.4 with ACAU version 4.4 to ensure the proper operation of both utilities. The software build number for ACAU version 4.4 is 4.4.0.69, and the software build number for ADU version 4.4 is 4.4.0.69.

System Requirements

You need the following items in order to install Install Wizard 4.4 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, you need 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, you need the following:
  - A hardware token device from OTP vendors or the Secure Computing SofToken program (2.1 or later).
  - Your hardware or software token password.
- If your client adapter is installed on a Windows 2000 device and uses PEAP (EAP-MSCHAPV2) with machine authentication, you need the Microsoft 802.1X supplicant.
- All necessary infrastructure devices (such as access points, servers, gateways, user databases, etc.) 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, you need 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
- If you want to use the Network Managed Test feature in the Diagnostics tab of the ADU, you need to run software release 4.2 (or later) on the Cisco Wireless LAN Controller (controller).
- If you want the client adapter to use Management Frame Protection (MFP), you need to run software release 4.1.181 or later on the controller.

Important Notes

Client MFP Incorrectly Enabled for WPA Sessions

If a client that supports MFP attempts to associate to a WLAN that is configured for both WPA and WPA2, authentication fails if WPA is negotiated for the session. This behavior is a controller issue that is tracked in CSCsm39923.

To address this issue from the client side, two registry entries have been added to software build 4.4.0.69. Both registry entries have settings that can be configured through the network control panel.

The first registry entry is called *ccx5FeatureEnable*. To configure this entry, perform the following steps:

Step 1 Right click **Properties** on the device icon in Network Connection dialog box of the control panel.

Step 2 Click **Configure**, and select the **Advanced** tab.

Step 3 Click **MFP** in the Property column.

Step 4 Choose the policy setting from the drop-down list in the Value column.

- Disable—Management Frame Protection is disabled. With MFP disabled, the client does not advertise MFP support. The client cannot connect to networks that require the use of MFP.
- Enable—Management Frame Protection is enabled. With MFP enabled, the client can connect to networks where use of MFP is disabled, optional, or required. Use the MFP Policy setting

Choose the MFP policy setting that is suitable to your network.

The second registry entry is called ccxMFPPolicy. To configure this entry, perform the following steps:

Step 1 Right click **Properties** on the device icon in Network Connection dialog box of the control panel.

Step 2 Click **Configure**, and select the **Advanced** tab.

Step 3 Click **Management Frame Protection Policy** in the Property column.

Step 4 Choose the policy setting from the drop-down list in the Value column.

- Use MFP Setting of Network—This setting configures the registry entry ccxMFPPolicy to 0. When this setting is chosen, the client follows the MFP policy of the network. The client looks at the MFP bit advertised by the network in the SFA IE of the probe response. If that bit is set, then the client also sets the MFP bit in the SFA IE of the association request, confirms the MFP bit in the SFA IE that is returned in the association response frame, and obeys the rules of MFP.

Note The Use MFP Setting of Network value is the default policy in build 4.4.0.69.

- Always Advertise MFP Support—This setting configures the registry entry ccxMFPPolicy to 1. When this setting is chosen, the client always advertises MFP support while connecting to a CCX version 5-enabled network. The client sets the MFP bit in the SFA IE of association request. It obeys the rules of MFP only if the association response from the access point also has the MFP bit set in the SFA IE.

  This policy is consistent with the CCX version 5 specification for MFP. The policy is required to pass MFP tests for certification.

Note The Always Advertise MFP Support setting is not interoperable with some controller and access point software versions that are currently in the field. Do not use this setting until the infrastructure network is upgraded to the proper version.

EAP-FAST with PEAP-GTC Authentication Fails When Using Auto-provisioning

When a profile is configured with 802.1X EAP-FAST with PEAP-GTC as the authentication method and auto-provisioning enabled, authentication fails. However, if an existing PAC is chosen, the domain username in the PAC is entered, and the correct password is entered in the password window, authentication succeeds. The failure also occurs when EAP-FAST with EAP-TLS is used. This behavior can be the result of validating the client certificate on the RADIUS server. With PEAP-GTC, a client-side certificate does not exist.

Transmit Power of Transmitted Packets Not Intended Power

After a change in channel, the transmit power of transmitted packets might be lower or higher than the intended transmit power.

PMKID Caching Not Working with CB21AG

With a 4400 controller, a wireless LAN is configured with WPA2 and with 802.1X selected as the key management method. A client sends a PMKID in the association request, but the PMKID does not match the controller PMKID cache.

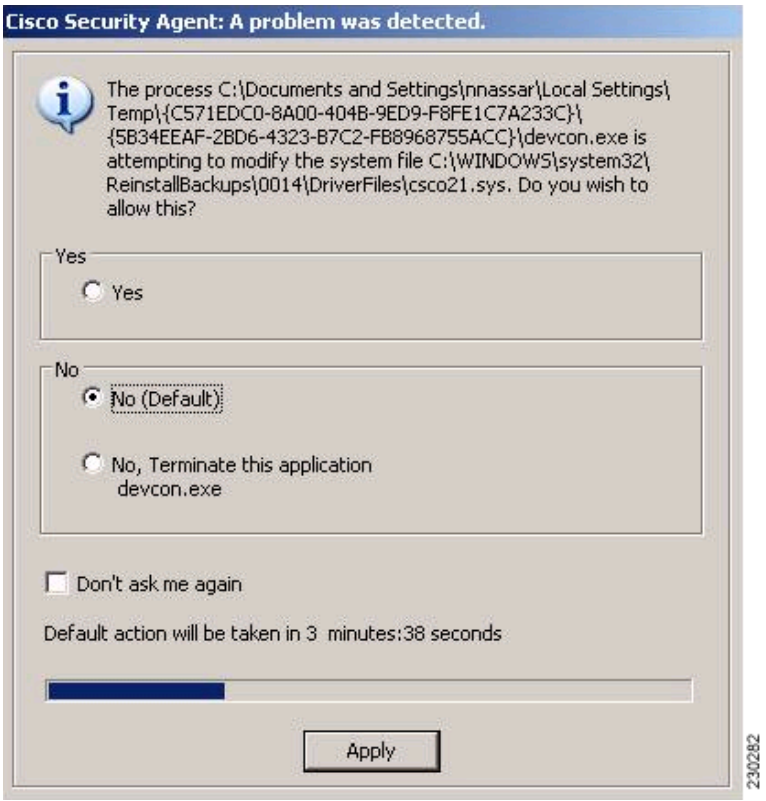
Conflict between Cisco Security Agent 5.0 and the Install Wizard for the CB21AG or PI21AG

If you have Cisco Security Agent (CSA) 5.0 installed on your computer and you attempt to run Install Wizard 4.4 (setup.exe) for the Cisco Aironet CB21AG or PI21AG wireless client, you might encounter one of two conditions that prevents the completion of software installation:

- If you click **No**, you are instructing the CSA to disallow devcon.exe of the client installation software from executing its tasks. The installation then appears to stall. The installation does not complete, and the computer must be rebooted. To avoid this behavior, disable the CSA before installing the wireless client software.
- If you click **Yes**, you are instructing the CSA to allow devcon.exe of the client installation software to execute its tasks. However, the CSA might block cmd.exe from executing. The installation then appears to stall, and the computer must be rebooted.

When you run setup.exe, the CSA opens the following dialog box (see Figure 1).

Figure 1 Cisco Security Agent Dialog Box



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 write cycles on the PCI bus consecutively (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 cycle before and after a register write cycle. 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 performance degradation because the key cache is only changed every few minutes. An additional read cycle 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 **Network Connections** in the Start > Settings menu in Windows XP, or right-click **My Network Places** in Windows 2000. Find the CB21AG instance.

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

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

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

Step 6 Select **Wireless Intermediate Driver** and click **OK**. The wireless IMD is bound to the adapter.

Step 7 Reboot system.

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

PACs that are created by ACS 3.x.xx are not compatible with ACS 4.0.xx. Client stations must import new PACs. If you select auto-provisioning, new PACs are automatically 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 4.0.xx and 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 experience authentication failures after upgrading the software, delete all the PACs provisioned from the 3.x.xx server.

Conflict with Third-Party Supplicants

When using CB21AG and PI21AG release 4.4, you might encounter a conflict with third-party supplicants (such as 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 is 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) 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 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. With this method, the client does not need to disassociate or to 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 wireless network settings. Simply ignore the Windows icon and use the ASTU icon to verify 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-4211-06) 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

Management Frame Protection

CB21AG and PI21AG release 4.4 supports Management Frame Protection (MFP) when available and enabled on the wireless infrastructure. The CB21AG and PI21AG have MFP automatically enabled.

Installing or Upgrading Client Adapter Software

This section describes how to initially install or upgrade to CB21AG and PI21AG Install Wizard 4.4 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 4.4, follow the instructions in the "Upgrading the Client Adapter Software" section on page 21.

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 the "Routine Procedures" chapter of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* 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 Ensure that the client adapter is inserted into your computer.

Step 2 Ensure 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 latest 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 2) and the Cisco Aironet Installation Program window (see Figure 3).

Figure 2 Preparing Setup Window

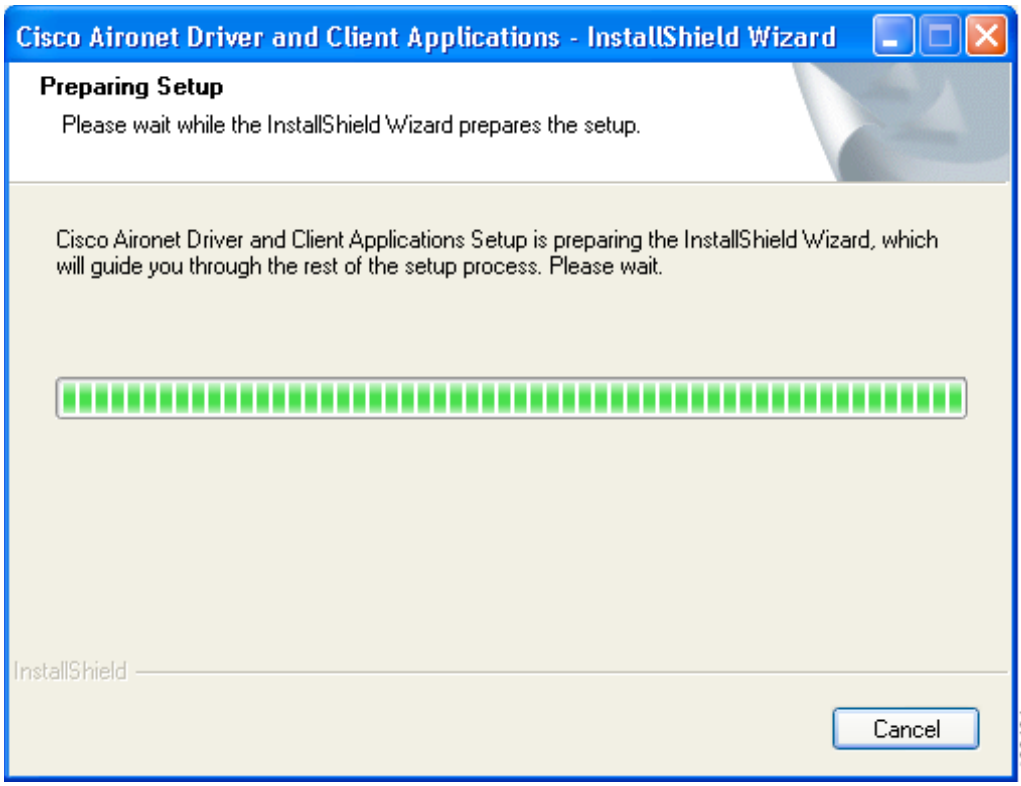
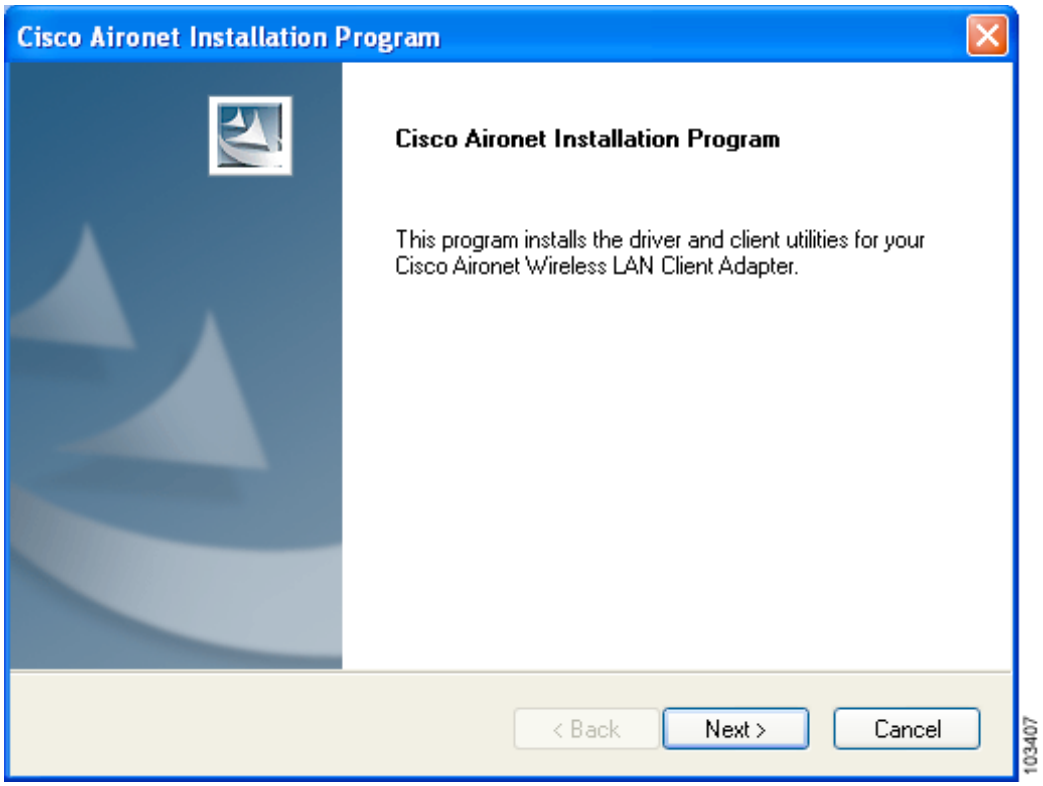
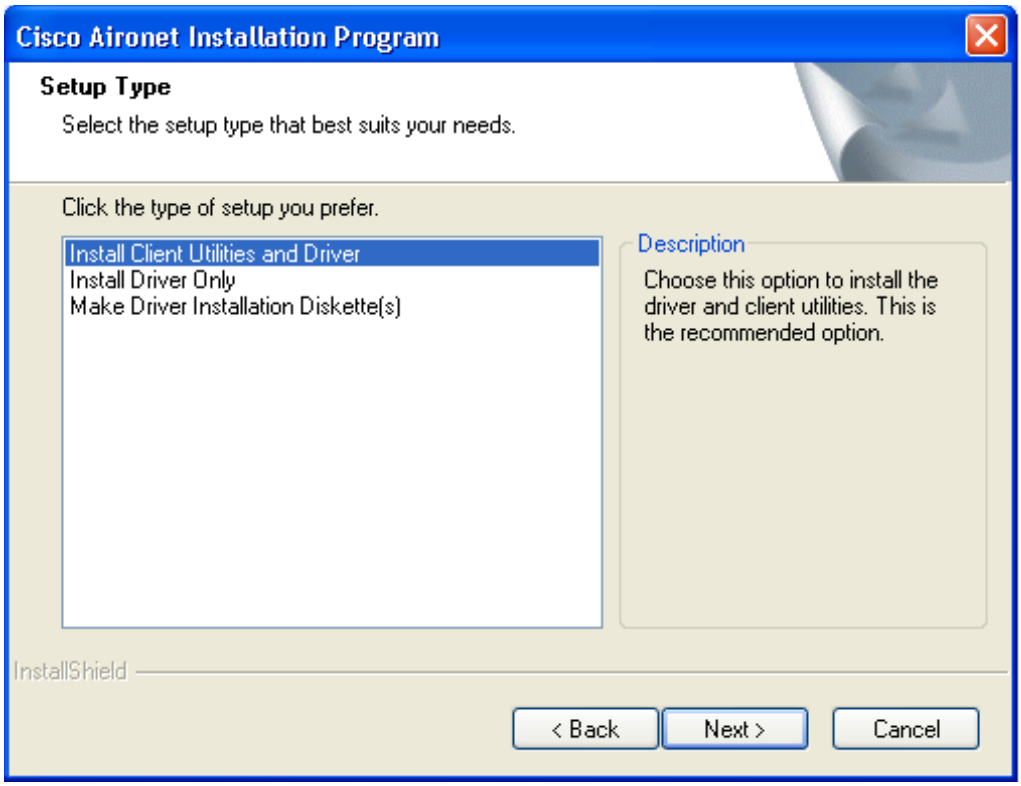


Figure 3 Cisco Aironet Installation Program Window



Step 19 Click **Next**. The Setup Type window appears (see Figure 4).

Figure 4 Setup Type Window



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

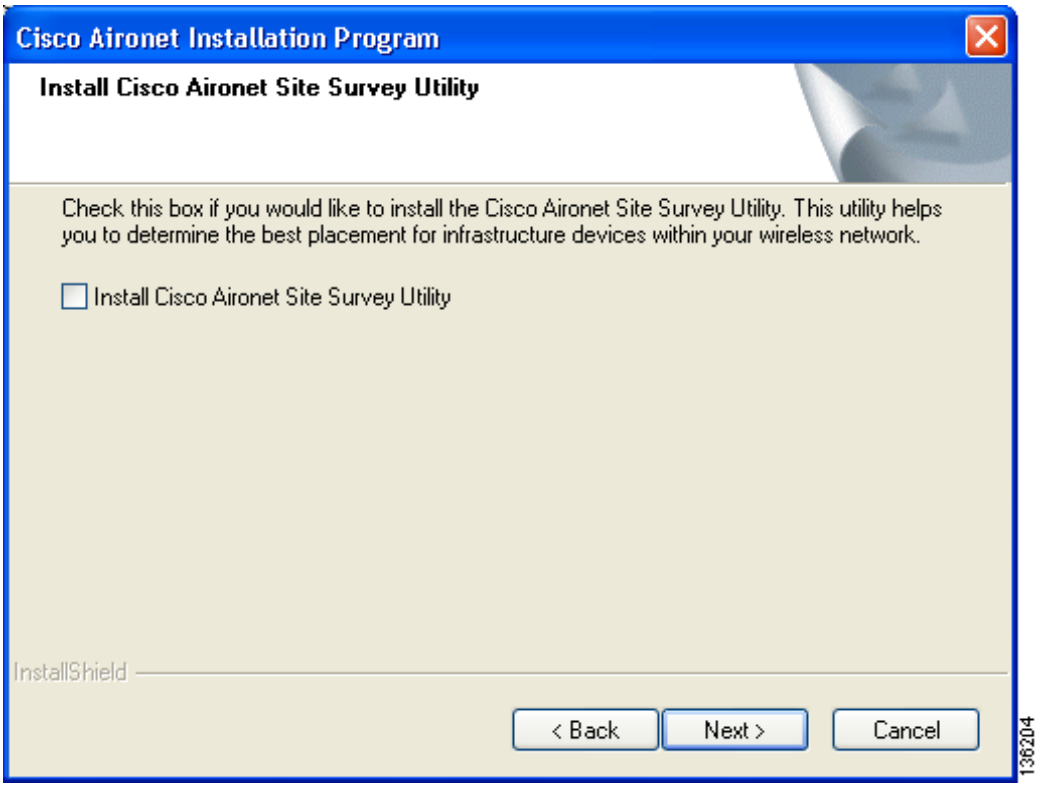
Note To ensure compatibility among software components, Cisco recommends that you install the client utilities and driver.

- **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 5), check the **Install Cisco Aironet Site Survey Utility** check box if you want to install a utility that helps you determine the best placement of infrastructure devices within your wireless network. Click **Next**.

Figure 5 Install Cisco Aironet Site Survey Utility Window



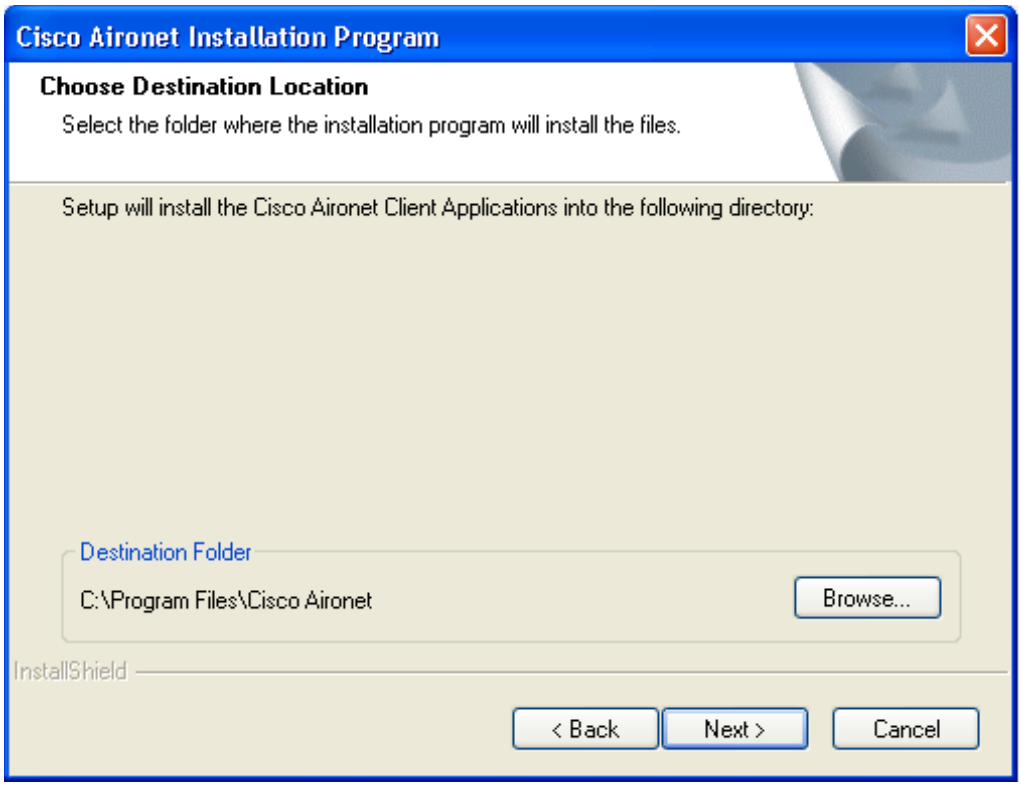
Note See Appendix F of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for instructions on using the utility.

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 6).

Figure 6 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.

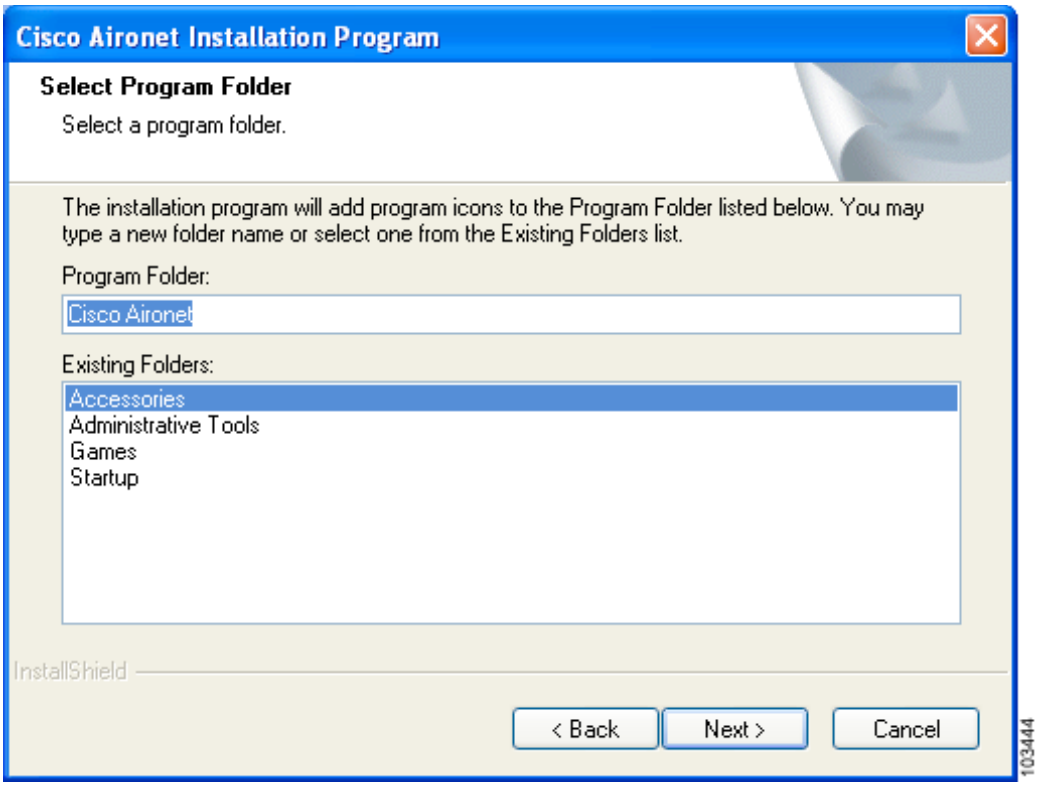
  Note If you want to install the client utilities in a different directory, click **Browse**, choose a different directory, click **OK**, and click **Next**.

- If you chose the Make Driver Installation Diskette(s) option in Step 20, insert a 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 7).

Figure 7 Select Program Folder Window

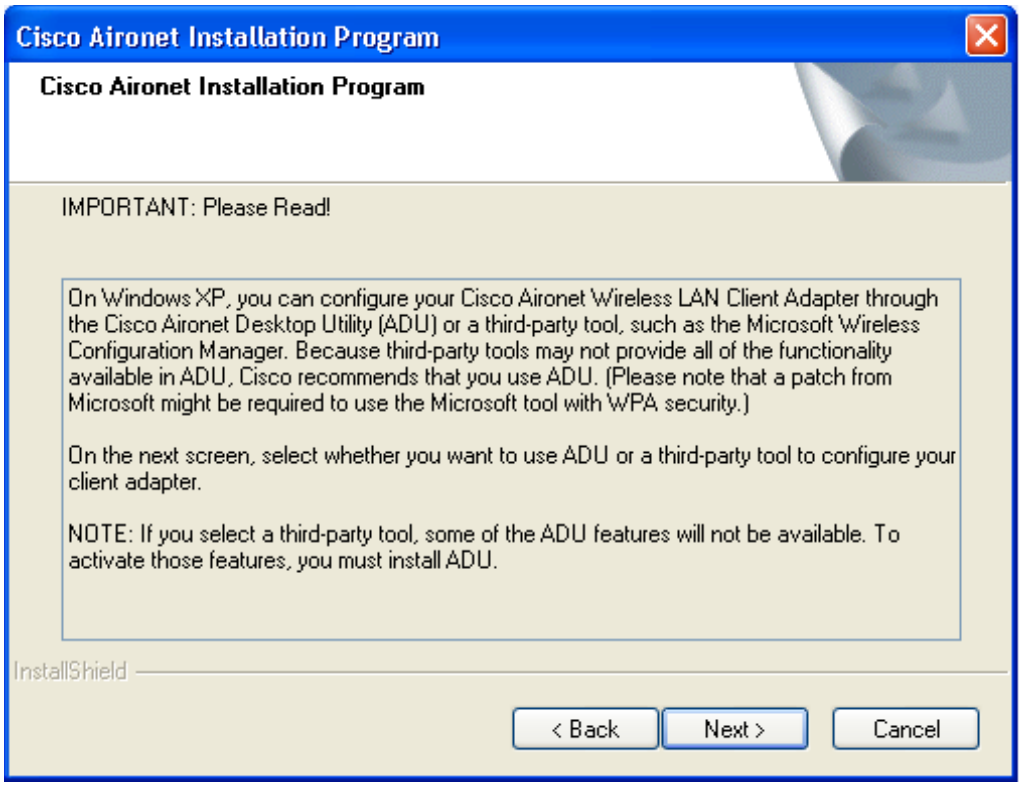


Step 25 Click **Next** to add program icons to the Cisco Aironet program folder.

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**.

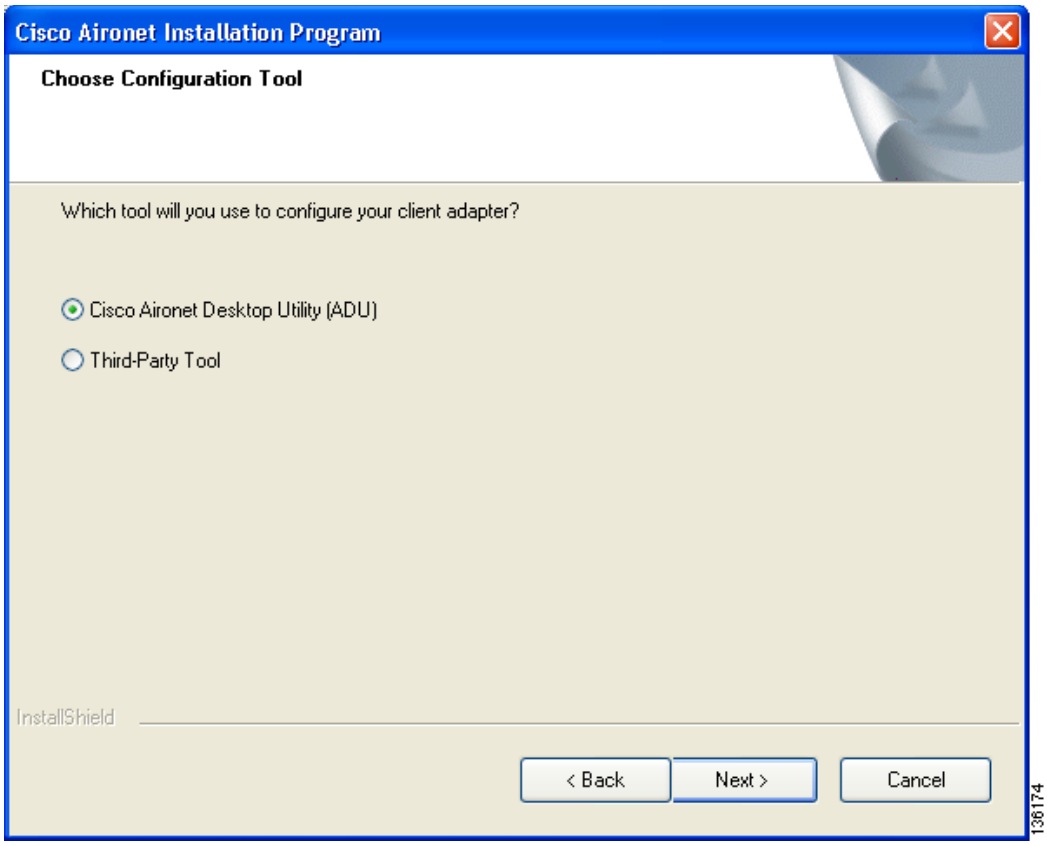
Step 26 If your computer is running Windows 2000, go to Step 32. If your computer is running Windows XP, the window titled IMPORTANT: Please Read! appears (see Figure 8).

Figure 8 IMPORTANT: Please Read! Window



Step 27 Read the information displayed and click **Next**. The Choose Configuration Tool window appears (see Figure 9).

Figure 9 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 (continued)

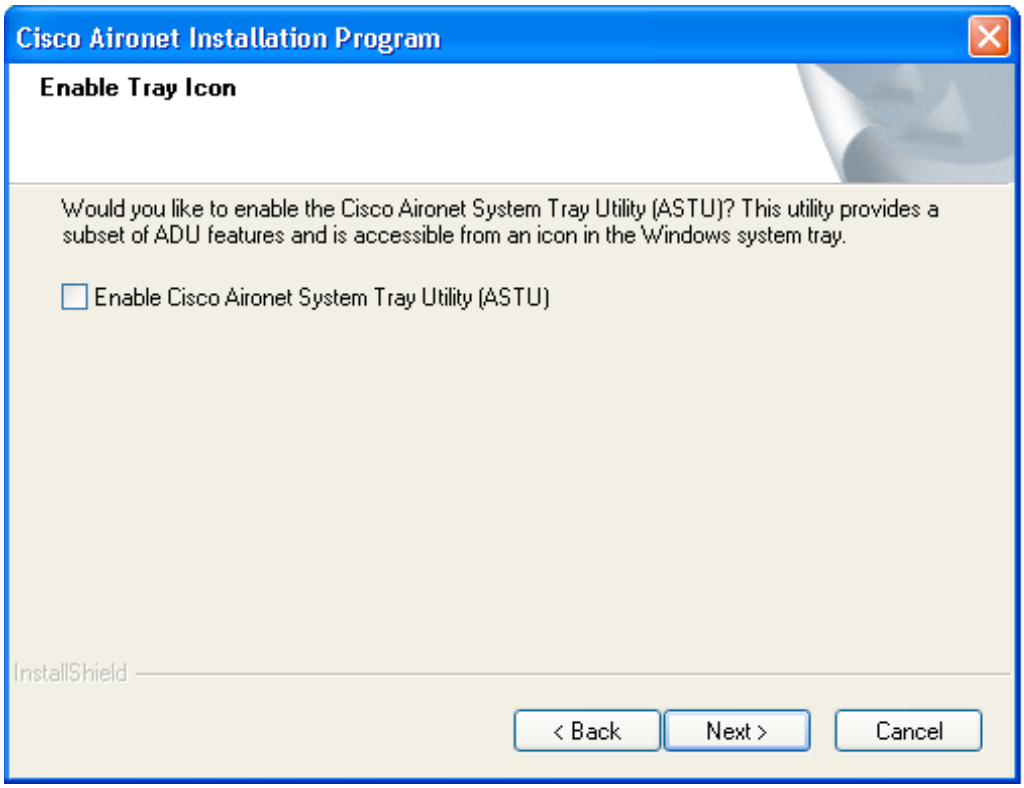
Feature	Windows XP	ADU
Security		
Static WEP	Yes	Yes
LEAP or EAP-FAST authentication with dynamic WEP	No	Yes
EAP-TLS or PEAP authentication	Yes	Yes
Status and statistics		
Status window	Limited	Extensive
Statistics window (transmit & receive)	No	Yes

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 10).

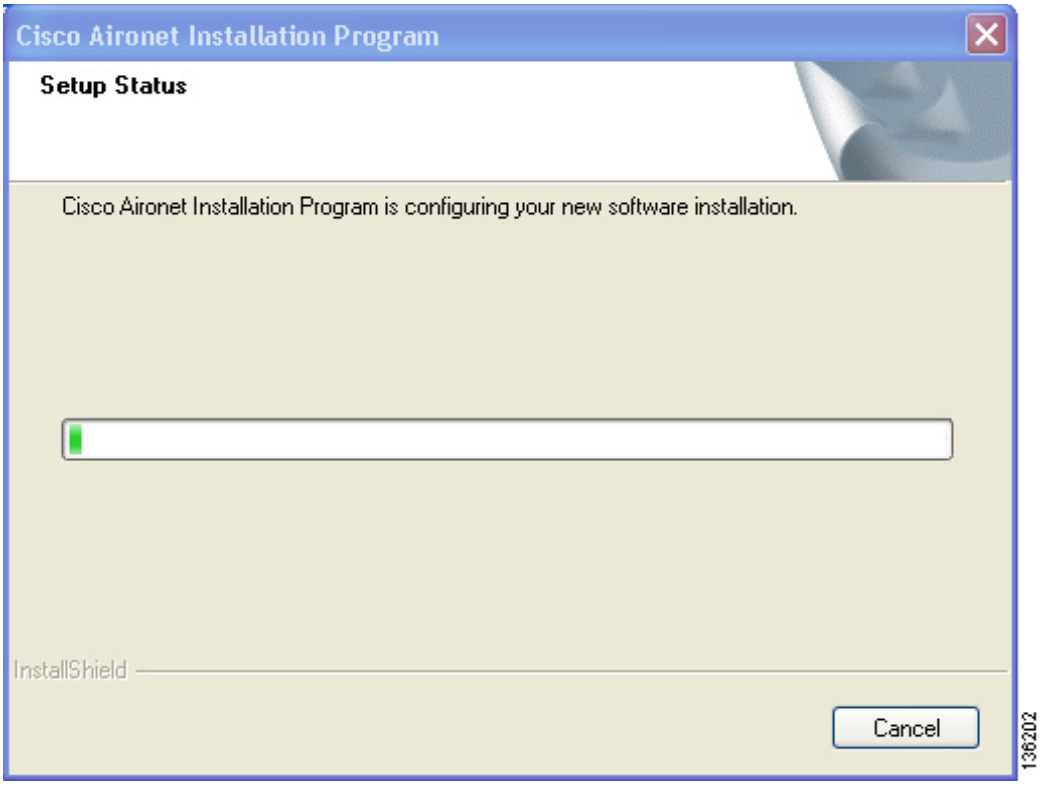
Figure 10 Enable Tray Icon Window



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. Click **Next**.

Step 32 When prompted to insert your client adapter, click **OK**. The Setup Status window appears (see Figure 11).

Figure 11 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 in the next section 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 4.4 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 9 to install the new software.

Step 1 Ensure that the client adapter is inserted into your computer.

Step 2 Ensure 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 12) and the Cisco Aironet Installation Program window (see Figure 13).

Figure 12 Preparing Setup Window

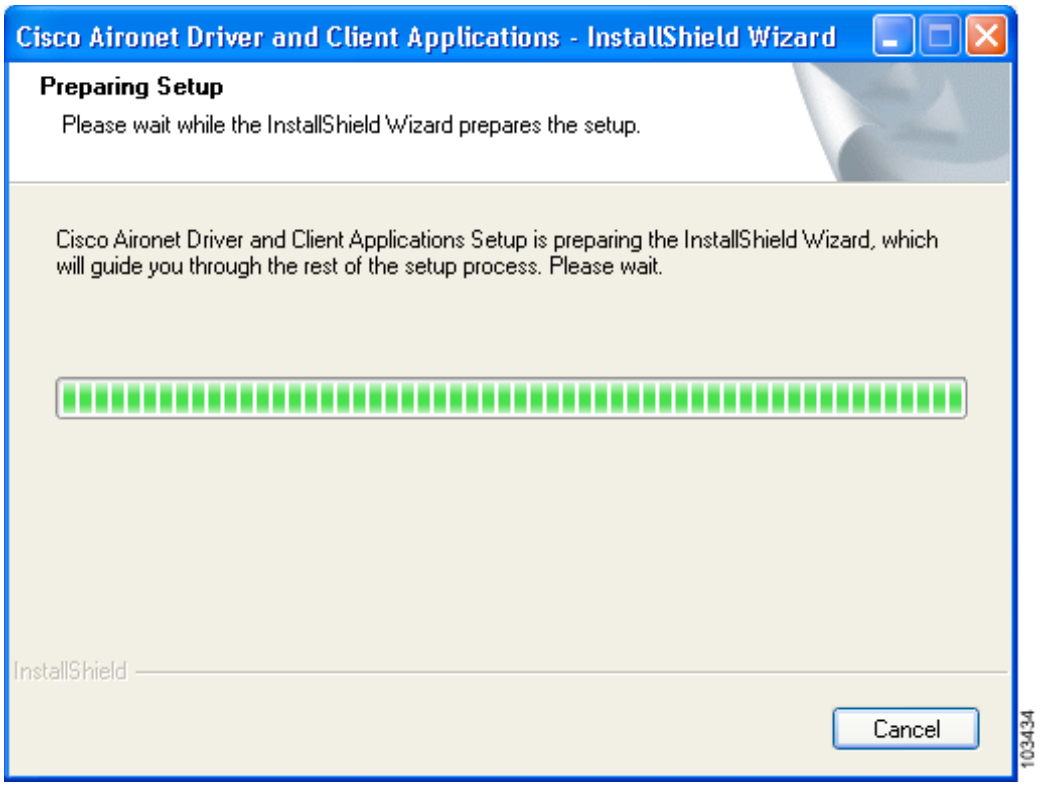
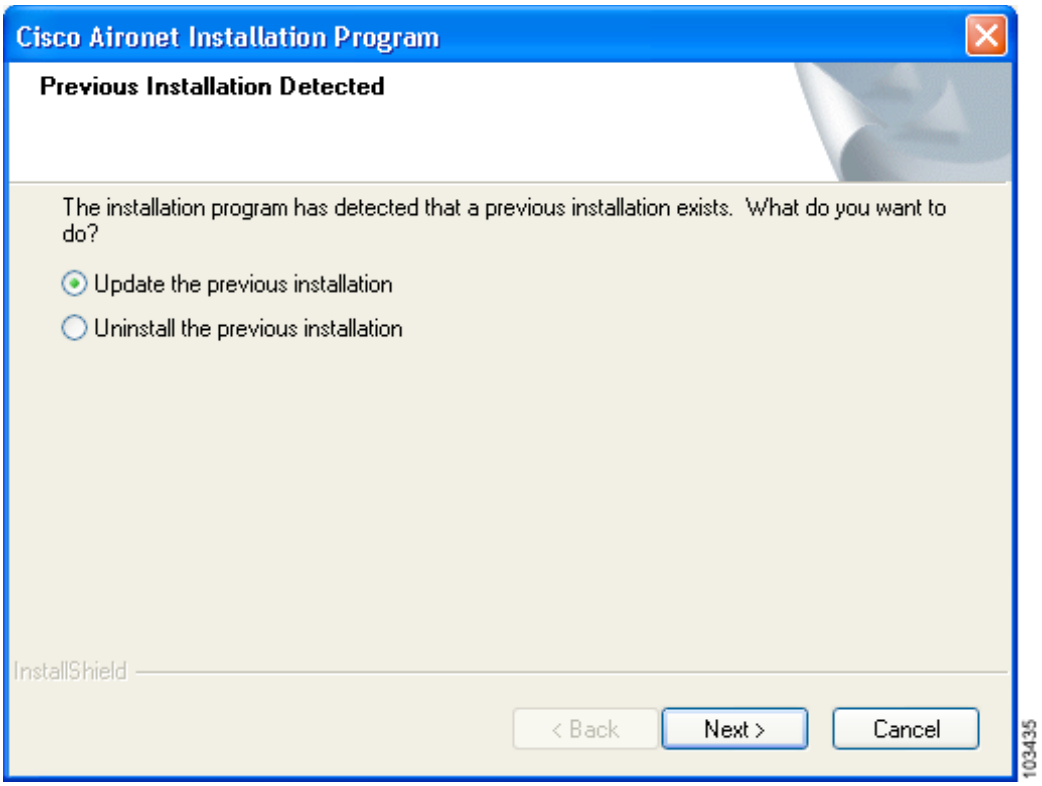


Figure 13 Previous Installation Detected Window



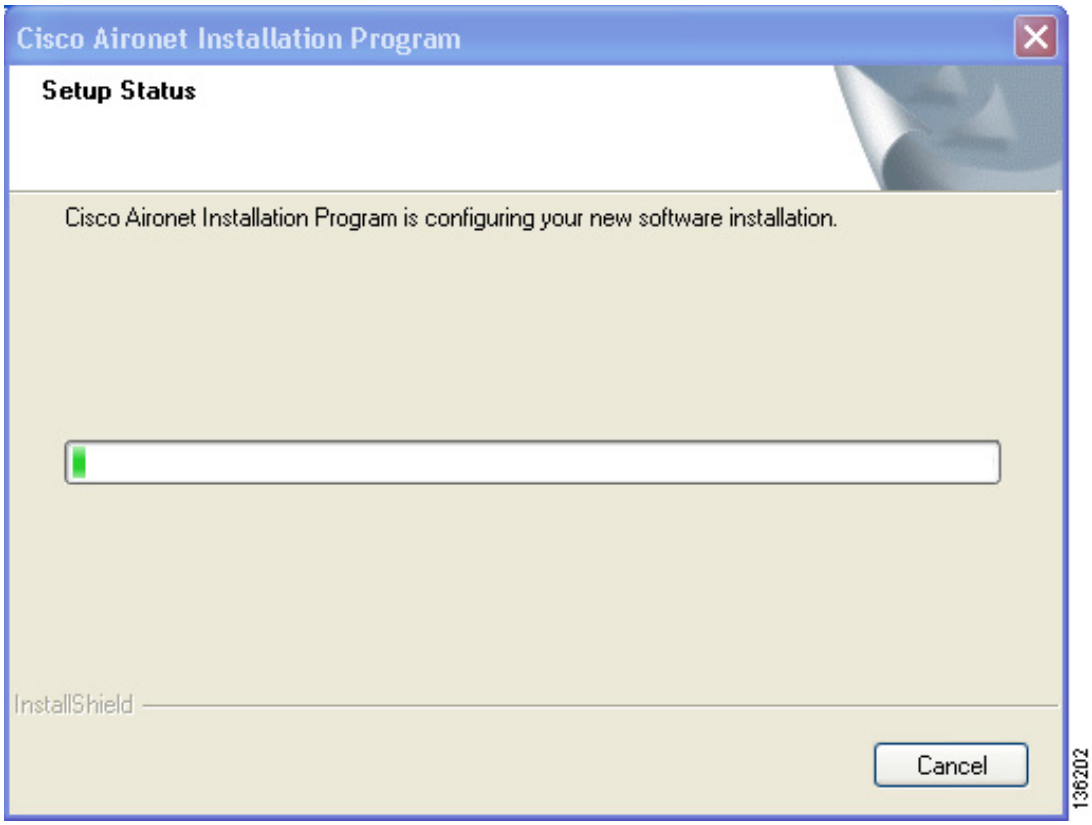
Step 19 Choose **Update the previous installation** and click **Next**.

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 14).

Figure 14 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) silently restores 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 ADU Version 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 and resolved caveats for the software components in this release.

Open Caveats

The following caveats are open in release 4.4:

- CSCsk60117—Clients experiencing disconnects when roaming

  Clients experience roaming delays of between 1 and 7 seconds with various configurations.

  Workaround: None.

- CSCsm22095—802.1X profile changed after being converted by profile migration tool

  A profile that uses 802.1X LEAP is configured with the Automatically Prompt for User Name and Password option enabled. The profile is created with the 350 ACU. The ADU is installed, and the profile migration tool (PMT) is run. When the same profile is verified in the ADU, the profile uses 802.1X LEAP with the Use Windows User Name and Password option.

  Workaround: None.

- CSCsm53534—Driver install fails if installed using install disk in Windows 2000 environment. This happens intermittently.

  The driver is installed by downloading and running a setup.exe file. The user verifies that a driver is not installed already. The driver is then installed through the Windows Device Manager. After running the setup.exe file, Windows displays a message that indicates that the installation is complete. The user clicks the Finish button in the user interface. The Windows Device Manager now shows that the driver is installed. When the user opens the Windows Network and Dial-up Connections window, the user selects the icon for the NIC and attempts to open the Properties window. The user then sees the "An unexpected error has occurred" message. The user restarts the machine. The Windows Device Manager shows the incomplete installation of the driver software for the NIC. Also, there is no entry for the NIC in the Windows Network and Dial-up Connections window.

  Workaround: None.

- CSCsu39899—EAP-FAST authentication fails when you select *Use Windows User Name and Password* and *Use Machine Information for Domain Logon* for client authentication.

  Workaround: Ensure that the user and machine PACs are loaded on the client station and that the user PAC is copied to the user public store.

- CSCsu45289—When configured with an EAP-FAST profile, client reassociation might fail after log in.

  Workaround: Install a public PAC or use auto PAC provisioning to store the PAC in the public store.

- CSCsu95035—EAP-FAST profile might disappear after login when you use the .dat file to install ADU. This occurs when one user (*user A*) changes one or more profiles or adds profiles, and a second user logs (*user B*) onto that same station. This only occurs if the .dat file that is created by ACAU is configured with the *overwrite* option.

  Workaround: User that is configuring the profiles (*user A*) should not use the *overwrite* option. Another workaround is to export the profiles before another user (*user B*) logs on to the same station and then reimport the profiles after *user B* logs on. This process must be followed for all subsequent users that log onto that same station.

- CSCsv34451—In periods of heavy traffic, BSOD might occur when you insert or remove the adapter.

  Workaround: To prevent this condition, use either the Windows safe-eject feature or disable the device from the Windows Network Control Panel or Windows Device Manager.

- CSCsv52176—Client authentication allowed with an expired certificate. When an expired certificate is used, the user is prompted with a dialog box with following text: *The server validation settings on your wireless profile do not match this server....* rather than indicating that the certificate has expired.

  Workaround: Click the OK button to accept the certificate, or Cancel to reject the certificate.

Resolved Caveats

The following caveats are resolved in release 4.4:

- CSCsi11424—CASSU signal strength percentage value is inconsistent with the percentage value in ADU.

  When not displayed as a percentage, the Current Signal Strength value in the ADU is consistent with the value in the CASSU. However, when displayed as a percentage, the value is not the same in the ADU and in the CASSU.

- CSCsi48025—ADU dims when you disable QoS in the interface

  An ADU associated to an access point is configured with open WEP 128-bit encryption. The CB21AG is selected as the local area connection. In the local area connection Properties window, QoS Packet Scheduler is disabled. In the Windows Task Manager, the ADU is dimmed.

- CSCsi63193—Installation of ADU with PI21AG stalls on Acer desktop

  The installation of the ADU with PI21AG stalls on the Acer 6900 Veriton desktop with Windows XP SP2.

- CSCsj10654—Client MFP failed with 802.11h frame spoofing

  After the controller is configured to use a RADAR-detecting channel, a client is associated with WPA version 2 AES-CCMP with 802.1X. On an 802.11h access point, a RADAR-detection event is triggered. A valid 802.11h channel change frame is captured with a sniffer. The access point has client MFP enabled from the controller.

  When the channel change frame is replayed to the client, the ADU disconnects the client adapter. The client adapter then reassociates with the controller access point.

- CSCsj23076—Signal quality in CASSU is not consistent with current signal quality in the ADU

  The signal strength quality percentage in the CASSU interface is not the same in the ADU interface. When the device is taken out of access point range, the current signal quality is still 100% in the ADU, but signal quality is 0% in the CASSU.

- CSCsj64455—Supported Features Advertisement information element bit 0 is 0 not 1 on the client

  When client MFP is disabled on the controller for a particular WLAN, beacons and probe responses that originate from access points in this WLAN have the SFA IE bit 0 set to 0. When a client associates with WPA version 2(MFP) EAP, the SFA IE bit 0 is 0, not 1. When a client associates with WPA version 2 (MFP) EAP with CCKM, the SFA IE bit 0 is 0, not 1.

- CSCsj84780—ADU dimmed after installation

  The ADU interface is dimmed even though the CB21AG client adapter is not configured to use Windows Wireless Zero Configuration (WZC).

- CSCsk01565—After LEAP domain logon, ADU usually asks for the authentication again

  The client uses LEAP security with the automatic prompt option and WPA data encryption. When the device is booted up, the user logs onto the domain. LEAP shows the progress of the authentication and gets an IP address to log in. After login, LEAP asks for authentication data again.

- CSCsk04387—PAC expires itself with local RADIUS server even if no expiration date is set

  A network has two access points with local RADIUS servers for EAP-FAST authentication. Even if the PAC has no expiration date, the PAC expires a few days after the initial authentication.

- CSCsk08004—PC-MY18A computer (NEC MateNX) freezes when the ADU is installed

  PC-MY18A computer (NEC MateNX) with PI21AG stalls with ADU installation and must be rebooted. PCs from other vendors, such as Dell and Fujitsu, exhibit the same behavior.

- CSCsk08053—Destination MAC address invalid with DNS ping test

  After you connect CCXv5 client to the infrastructure device, start the DNS ping test from the Diagnostics tab and wait for the test results. The MAC address is invalid.

- CSCsk52544—After Windows in hibernate mode, ADU switches to WZC

  The ADU is opened, and the CB21AG is associated to an access point. The device is then set to hibernate mode. When the device comes out of hibernate mode, the ADU switches to WZC approximately 10 percent of the time. This behavior is most often seen when the hibernate period is long (overnight).

- CSCsk71038—WLC shows incorrect Power Save Mode in client reporting

  An access point sends an operating parameters request frame to a client. A wireless sniffer verifies that the access point sends the packet and that the client sends a response frame. The WLC Power Save Mode is in Normal Power Save Mode even if the wireless adapter Power Save Mode is set to Maximum Power Save Mode or Constantly Awake Mode.

- CSCsk83295—EAP-FAST auto PAC provisioning still displays dialog box

  When the user logs in, the following message appears:

  ```
  Card Name: Cisco Aironet 802.11a/b/g Wireless Adapter

  The current EAP-FAST profile does not have a PAC or the configured PAC does not match
  the authentication server. Do you want to use another PAC found on your local system
  that matches the authentication server without reconfiguring the current EAP-FAST
  profile?

  YES or NO
  ```

- CSCsk90617—ADU shows incorrect signal quality while increasing attenuation

  Even when the client adapter signal becomes increasingly attenuated, the ADU and the CASSU display the signal quality at 100% (the link speed is down to 2 Mb/s). When the ADU is completely disconnected from the access point, the ADU and the CASSU show the current signal strength at 0%, but the ADU shows the signal quality at 100%.

- CSCsk96247—When Windows logon fails, the computer stalls

  When Windows logon fails after EAP-FAST was successful, the computer stalls.

- CSCsl02673—CB21AG is slow to log in when PC is not a member of a domain

  The login for a PC that is part of a workgroup but not a member of a domain is slow. The supplicant is trying to find a domain controller, which causes the slow login.

- CSCsl90324—EAP-FAST authentication fails when Validate Server Identity is enabled

  A profile is configured with 802.1X EAP-FAST authentication. The Validate Server Identity option and auto-provisioning are enabled. The Trusted Root Certification Authorities is set to Any. Authentication fails. If the Trusted Root Certification Authorities is valid, the authentication still fails. If an existing PAC is selected, the authentication succeeds.

- CSCsm37569—RSNA log request incorrect

  A client adapter that uses EAP-FAST with AES encryption and CCKM receives an RSNA log with incorrect information after the adapter roams from one access point to another after the first access point is shut down. The RSNA log does not include CCKM information.

- CSCsm89230—WPA/WPA2 authentication fails

  Clients experience WPA/WPA2 authentication failures when trying to associate to access points that are running the following Cisco IOS software releases with the following encryption methods:

  - Cisco IOS release 12.4(3g)JA1 with WPA2/AES or WPA2-PSK/AES
  - Cisco IOS release 12.4(10b)JA with WPA/TKIP or WPA-PSK/TKIP

  This condition does not occur with a Cisco IOS software release 12.3(8)JEB or 12.3(8)JEA3.

Closed Caveats

The following caveats were closed in 4.4:

- CSCsi11431—Auto-selected profiles convert correctly but do not function

  Profiles are created for the PCM350 client adapter. These profiles are added to the list of auto-selected profiles. The PCM350 is then unplugged. The CB21AG client adapter is inserted, and the ADU is installed. After rebooting the system, the Profile Migration Tool (PMT) is executed. All profiles are converted successfully, but the auto-selected profiles do not function correctly. The active profile in the ADU is still the default profile.

  Workaround: None.

- CSCsi14938—PEAP (EAP-GTC, EAP MSCHAPv2) Single Sign-On fails

  PEAP machine authentication is enabled on the ACS server, and the client gets a machine certificate via a Group Policy Object. The client uses a profile that is configured to use PEAP (EAP-GTC) or PEAP (MSCHAPv2) with Single Sign-On. The Use Machine Information for Domain Logon option is checked, and Use Windows User name and Password is checked for the profile. The Cached Logons value is set from 10 to 0 in the client registry editor.

  After the system is rebooted, the ADU cannot log onto the Windows domain. The failed machine information logon record cannot be found in the ACS server log.

  Workaround: None.

- CSCsl03991—Authentication failure when changing profiles

  Even if a username and a password are correct, authentication fails when changing profiles.

  Workaround: None.

- CSCsl12054—Two-minute delay during login after reboot

  When the user logs in after reboot, there is a two-minute delay (sometimes longer) after the user enters a valid username and password into the Window GINA If the user logs off and then back in, there is no delay.

  This issue occurs intermittently on various Hewlett-Packard laptops. The issue occurs whether or not machine authentication has been enabled.

  Workaround: None.

- CSCsl74307—ADU driver causes one- or two-minute Windows login delays on some of laptops

  Delays occur when trying to log in via the LAN NIC to a domain if the laptop has the CB21AG driver. After the driver is deleted, the laptop only takes three seconds to log in to the domain.

  Workaround: None.

- CSCsm02824—Case-sensitive username passes EAP-FAST authentication but generates different PACs

  Different PACs are created for the same profile when the user enters a username but changes the case of the username characters. Regardless of how the username is entered, the user enters the same password and can authenticate. However, a PAC for each variation of the same username is created.

  Workaround: None.

- CSCsm02911—Token account can be used in the user fields for PEAP-GTC authentication

  In the ADU, a profile is configured with 802.1X PEAP-GTC. The static password option is enabled. An account is generated from software token or hardware token. This account is entered in the static username and password fields. The client adapter successfully associates to the access point.

  Workaround: None.

- CSCsm02917—Domain user account can be used in the token configuration

  In the ADU, a profile is configured with PEAP-GTC, and the token option is enabled. The domain user account name is entered as the token account name. The profile is activated, and token one-time password dialog box appears. The domain user account password is entered. The adapter authenticates successfully.

  Workaround: None.

- CSCsm37565—DNS resolution test failure

  The DNS resolution portion of diagnostic channel testing is initiated, and a resolvable host name is provided. However, the controller shows that the DNS query was dropped.

  Workaround: None.

- CSCsm37575—Client event log does not contain failed authentication

  EAP-FAST authentication fails because the user enters an invalid password. After the access point sends an event log request frame to the client, the client does not send an event log that includes information about the failed authentication.

  Workaround: None.

- CSCsm42303—ADU does not prompt to re-enter user credentials

  After EAP-FAST re-authentication after a session timeout, EAP-FAST authentication should fail, and an error message window should be displayed. The ADU should also prompt the user to re-enter user credentials. However, the prompt dialog box does not appear, and the connection continues.

  Workaround: Log on to the Windows workstation with the new password.

- CSCsu75684—CB21ag clients might fail reauthentication on an intermittent basis. (Problem found not to be client related)

  Workaround: None.

- CSCsw85317—EAP-FAST authentication fails on a client running on Windows 2000 because an API parameter that supports authentication is not supported on Windows 2000 (Windows XP only).

  Workaround: Install Windows XP.

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-7086-04)—Provides instructions for installing the ACAU 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-4211-06)—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 (CB21AG and PI21AG) Client Administration Utility (ACAU) 4.4* (OL-19065-01)—Describes new features and open and resolved caveats in ACAU 4.4.

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html