

Table 7-4 Advanced Client Adapter Status (continued)

Status	Description
Current Signal Strength	The signal strength for all received packets. The higher the value, the stronger the signal. <b>Range:</b> 0 to 100% or 0 to -100 dBm
Current Signal Quality	The signal quality for all received packets. The higher the value, the clearer the signal. <b>Range:</b> 0 to 100% <b>Note</b> This field appears only if you selected signal strength to be displayed as a percentage. See the Signal Strength Display Units parameter in <a href="#">Table 7-2</a> for information.
Current Noise Level	The level of background radio frequency energy in the current radio band. The lower the value, the less background noise present. <b>Range:</b> 0 to -100 dBm <b>Note</b> This field appears only if you selected signal strength to be displayed in dBm. See the Signal Strength Display Units parameter in <a href="#">Table 7-2</a> for information.
Up Time	The amount of time (in hours:minutes:seconds) since the client adapter has been receiving power. If the adapter has been running for more than 24 hours, the time is displayed in days, hours:minutes:seconds.
802.11b Preamble	Indicates whether your client adapter is using only long radio headers or short and long radio headers. <b>Value:</b> Short & Long or Long Only <b>Note</b> This field contains a value only when the client adapter is operated in 2.4-GHz 11-Mbps or 2.4-GHz 54-Mbps mode. <b>Note</b> Refer to the 802.11b Preamble parameter in <a href="#">Table 5-3</a> for information on using radio headers.
Current Receive Rate	The rate at which your client adapter is currently receiving data packets. <b>Value:</b> 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps
Current Transmit Rate	The rate at which your client adapter is currently transmitting data packets. <b>Value:</b> 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps
Channel	The channel that your client adapter is currently using for communications. This field displays <i>Scanning</i> while the client adapter searches for a channel. <b>Value:</b> Dependent on radio band and regulatory domain <b>Note</b> Refer to the Channel parameter in <a href="#">Table 5-3</a> for information on setting the channel for your client adapter. <b>Note</b> Refer to <a href="#">Appendix D</a> for a list of channel identifiers, channel center frequencies, and regulatory domains for each channel.

**Table 7-4** *Advanced Client Adapter Status (continued)*

Status	Description
Frequency	<p>The radio frequency that your client adapter is currently using for communications. This field displays <i>Scanning</i> while the client adapter searches for a frequency.</p> <p><b>Value:</b> Dependent on radio band and regulatory domain</p> <p><b>Note</b> Refer to the Wireless Mode parameter in <a href="#">Table 5-3</a> for information on setting the frequency for your client adapter.</p>
Channel Set	<p>The regulatory domain for which your client adapter is currently configured. This value is not user selectable.</p> <p><b>Value:</b> America, EMEA, Japan, or Rest of World</p> <p><b>Note</b> Refer to <a href="#">Appendix D</a> for a list of channel identifiers, channel center frequencies, and regulatory domains for each channel.</p>

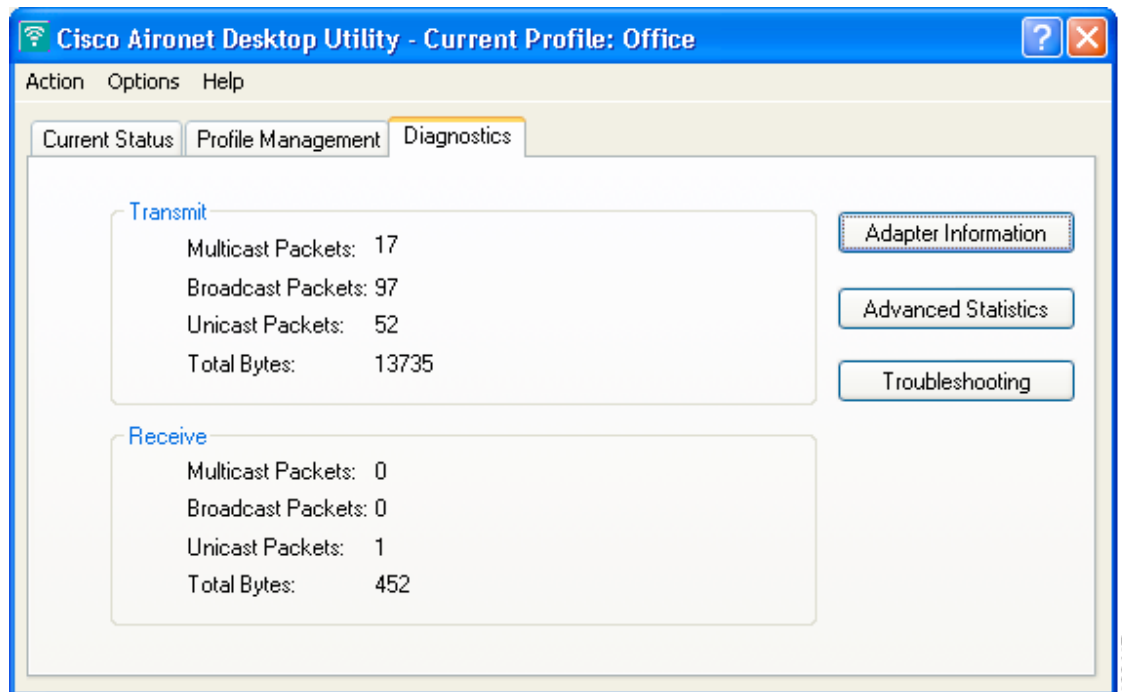
Click **OK** to close the Advanced Status window.

## Viewing Statistics for Your Client Adapter

ADU enables you to view statistics that indicate how data is being received and transmitted by your client adapter.

To view your client adapter's statistics, open ADU and click the **Diagnostics** tab. The Cisco Aironet Desktop Utility (Diagnostics) window appears (see [Figure 7-4](#)).

**Figure 7-4** Cisco Aironet Desktop Utility (Diagnostics) Window



This window displays basic transmit and receive statistics for your client adapter. The statistics are calculated on a relative or cumulative basis as specified by the Data Display parameter and are continually updated at the rate specified by the Refresh Interval parameter. Instructions for changing the Data Display and Refresh Interval settings are provided in [Table 7-2](#).



**Note**

The receive and transmit statistics are host statistics. That is, they show packets and errors received or sent by the Windows device.



**Note**

To run the Cisco Aironet Troubleshooting Utility, click **Troubleshooting**. Refer to [“Using the Cisco Aironet Troubleshooting Utility”](#) on page 10-3 for more information.



**Note**

To view client adapter information, click **Adapter Information**. Refer to [“Viewing Client Adapter Information”](#) on page 9-10 for more information.

Table 7-5 describes each statistic that is displayed for your client adapter.

**Table 7-5 Basic Client Adapter Statistics**

Statistic	Description
<b>Transmit Statistics</b>	
Multicast Packets	The number of multicast packets that were transmitted.
Broadcast Packets	The number of broadcast packets that were transmitted.
Unicast Packets	The number of unicast packets that were transmitted successfully.
Total Bytes	The number of bytes of data that were transmitted successfully.
<b>Receive Statistics</b>	
Multicast Packets	The number of multicast packets that were received.
Broadcast Packets	The number of broadcast packets that were received.
Unicast Packets	The number of unicast packets that were received successfully.
Total Bytes	The number of bytes of data that were received successfully.

Click **Advanced Statistics** if you want to view additional statistics for your client adapter. The Advanced Statistics window appears (see Figure 7-5).

**Figure 7-5 Advanced Statistics Window**

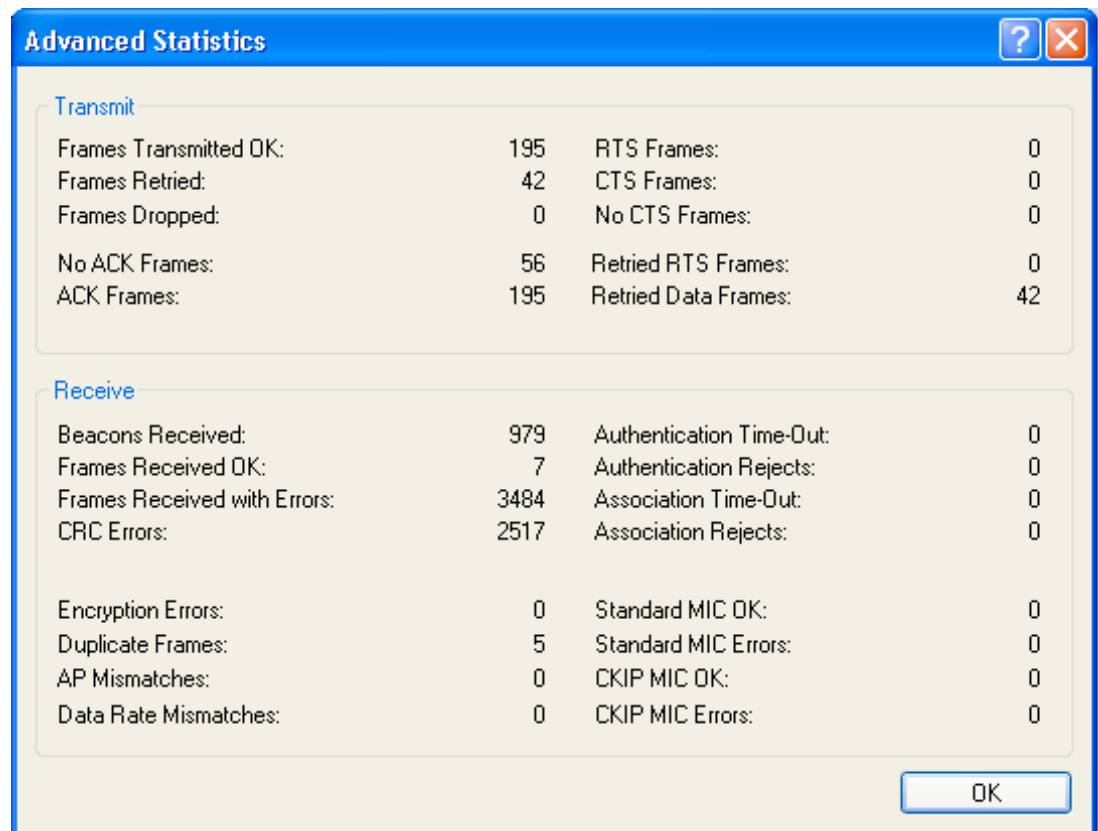


Table 7-6 interprets each element of the Advanced Statistics window.

**Table 7-6 Advanced Client Adapter Statistics**

Status	Description
<b>Transmit Statistics</b>	
Frames Transmitted OK	The number of frames that were transmitted successfully.
Frames Retried	The number of frames that were retried.
Frames Dropped	The number of frames that were dropped because of errors or collisions.
No ACK Frames	The number of transmitted frames that did not have their corresponding Ack frame received successfully.
ACK Frames	The number of transmitted frames that had their corresponding Ack frame received successfully.
RTS Frames	The number of request-to-send (RTS) transmissions that were attempted.
CTS Frames	The number of clear-to-send (CTS) frames that were received in response to a successfully transmitted RTS frame.
No CTS Frames	The number of request-to-send (RTS) transmissions that were unsuccessful. The access point sends CTS frames in response to the client's RTS frames. This field keeps track of each time the client does not receive a CTS back from the access point.
Retried RTS Frames	The number of request-to-send (RTS) frames that were retransmitted.
Retried Data Frames	The number of normal data frames that were retransmitted.
<b>Receive Statistics</b>	
Beacons Received	The number of beacon frames that were received successfully.
Frames Received OK	The number of all frames that were received successfully.
Frames Received with Errors	The number of frames that were received with an invalid checksum.
CRC Errors	The number of cyclic redundancy check (CRC) errors detected in the data portion of the frame.
Encryption Errors	The number of frames that were received with encryption errors.
Duplicate Frames	The number of duplicate frames that were received.
AP Mismatches	The number of times the client adapter tried to associate to an access point but was unable to because the access point was not the adapter's specified access point. <b>Note</b> Refer to the Access Point 1 through Access Point 4 parameters on <a href="#">page 5-13</a> for information on specifying access points.
Data Rate Mismatches	The number of times the client adapter tried to associate to an access point but was unable to because the adapter's data rate was not supported by the access point. <b>Note</b> Refer to the Wireless Mode parameter in <a href="#">Table 5-3</a> for information on supported data rates.

**Table 7-6** *Advanced Client Adapter Statistics (continued)*

<b>Status</b>	<b>Description</b>
Authentication Time-Out	The number of times the client adapter tried to authenticate to an access point but was unable to because the access point did not respond fast enough (timed out).
Authentication Rejects	The number of times the client adapter tried to authenticate to an access point but was rejected.
Association Time-Out	The number of times the client adapter tried to associate to an access point but was unable to because the access point did not respond fast enough (timed out).
Association Rejects	The number of times the client adapter tried to associate to an access point but was rejected.
Standard MIC OK	The number of frames that were received with the correct message integrity check (MIC) value.
Standard MIC Errors	The number of frames that were discarded due to an incorrect message integrity check (MIC) value.
CKIP MIC OK	The number of frames that were received with the correct message integrity check (MIC) value when CKIP was being used.  <b>Note</b> This field is displayed only if MIC is enabled on the access point.
CKIP MIC Errors	The number of frames that were discarded due to an incorrect message integrity check (MIC) value when CKIP was being used.  <b>Note</b> This field is displayed only if MIC is enabled on the access point.

Click **OK** to close the Advanced Statistics window.





## Using the Aironet System Tray Utility (ASTU)

---

This chapter explains how to use the Aironet System Tray Utility (ASTU) to access status information about your client adapter and perform basic tasks.

The following topics are covered in this chapter:

- [Overview of ASTU, page 8-2](#)
- [The ASTU Icon, page 8-2](#)
- [Tool Tip Window, page 8-3](#)
- [Pop-Up Menu, page 8-5](#)



## Overview of ASTU

ASTU is an optional application that provides a small subset of the features available through ADU. Specifically, it enables you to access status information about your client adapter and perform basic tasks. ASTU is accessible from an icon in the Windows system tray, making it easily accessible and convenient to use. The ASTU icon appears only if a client adapter is installed into your computer and you did not disable ASTU during installation.

ASTU provides information and options in the following ways:

- In the appearance of the icon itself
- Through a tool tip window that appears when you hover the cursor over the icon
- Through a pop-up menu that appears when you right-click the icon
- Through a Connection Status window that appears when you double-click the icon

## The ASTU Icon





The appearance of the ASTU icon indicates the connection status of your client adapter. ASTU reads the client adapter status and updates the icon every 1 to 5 seconds, depending on the value entered for the Refresh Interval on the Display Settings window. [Table 8-1](#) interprets the different appearances of the ASTU icon.





### Note

Windows 2000 and XP may display their own wireless network connection status icon in the system tray. Cisco recommends that you turn off the Windows icon and use the ASTU icon to monitor your wireless connection.

**Table 8-1** *Interpreting the ASTU Icon*

Icon	Description
	A white icon indicates that the client adapter's radio is disabled.
	A dark gray icon indicates that the client adapter is not associated to an access point (in infrastructure mode) or another client (in ad hoc mode).
	A light gray icon indicates that the client adapter is associated to an access point (in infrastructure mode) or another client (in ad hoc mode) but the user is not EAP authenticated.
	A green icon indicates that the client adapter is associated to an access point (in infrastructure mode) or another client (in ad hoc mode), the user is authenticated if the client adapter is configured for EAP authentication, and the signal strength is excellent or good.

**Table 8-1** *Interpreting the ASTU Icon (continued)*

Icon	Description
	A yellow icon indicates that the client adapter is associated to an access point (in infrastructure mode) or another client (in ad hoc mode), the user is authenticated if the client adapter is configured for EAP authentication, and the signal strength is fair.
	A red icon indicates that the client adapter is associated to an access point (in infrastructure mode) or another client (in ad hoc mode), the user is authenticated if the client adapter is configured for EAP authentication, and the signal strength is poor.

## Tool Tip Window

When you hover the cursor over the ASTU icon, the Tool Tip window appears (see [Figure 8-1](#)).


**Note**

If the client adapter's radio is disabled, a message appears instead of the Tool Tip window to inform you that the wireless network interface is disabled.

**Figure 8-1** *Tool Tip Window*

Office	136214
Test AP 1	
Associated	
Excellent	
11.0 Mbps, 11b	
Cisco Aironet 802.11a/b/g Wireless Adapter #3 169.254.42.170	

This window provides information on the current status of your client adapter. [Table 8-2](#) lists and describes each element of the Tool Tip window.

**Table 8-2** *Tool Tip Window Elements*

Status Element	Description
Active profile	<p>The network configuration (or profile) that your client adapter is currently using.</p> <p><b>Note</b> If auto profile selection is enabled, the active profile does not appear until the client is associated to an access point.</p>
SSID	<p>The name of the network to which your client adapter is currently associated.</p> <p><b>Note</b> When the client adapter is not associated and auto profile selection is disabled, this field shows the profile's SSID. When the client adapter is not associated and auto profile selection is enabled, this field is left blank.</p> <p><b>Note</b> Refer to the SSID1 parameter in <a href="#">Table 5-2</a> for information on setting the client adapter's SSID.</p>

Table 8-2 Tool Tip Window Elements (continued)

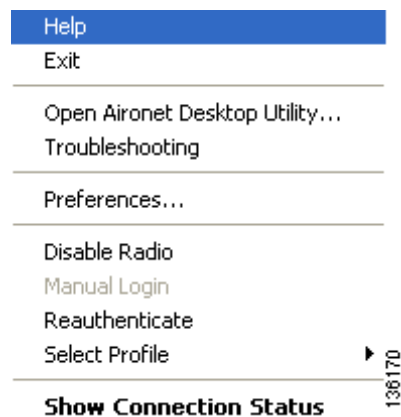
Status Element	Description														
Connection status	<p>The operational mode of your client adapter.</p> <p><b>Value:</b> Not Associated, Associated, Authenticating, Authenticated, Authentication Failed, or Authentication Failed Retrying</p>														
	<table border="1"> <thead> <tr> <th>Connection Status</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Not Associated</td> <td>The client adapter has not established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).</td> </tr> <tr> <td>Associated</td> <td>The client adapter has established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).</td> </tr> <tr> <td>Authenticating</td> <td>The client adapter is associated to an access point, and the EAP authentication process has begun but not yet succeeded.</td> </tr> <tr> <td>Authenticated</td> <td>The client adapter is associated to an access point, and the user is EAP authenticated.</td> </tr> <tr> <td>Authentication Failed</td> <td> <p>The client adapter is associated to an access point, but the user has failed to EAP authenticate.</p> <p><b>Note</b> This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i>.</p> </td> </tr> <tr> <td>Authentication Failed Retrying</td> <td> <p>The client adapter is associated to an access point, the user has failed to EAP authenticate, but another authentication attempt is being made.</p> <p><b>Note</b> This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i>.</p> </td> </tr> </tbody> </table>	Connection Status	Description	Not Associated	The client adapter has not established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).	Associated	The client adapter has established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).	Authenticating	The client adapter is associated to an access point, and the EAP authentication process has begun but not yet succeeded.	Authenticated	The client adapter is associated to an access point, and the user is EAP authenticated.	Authentication Failed	<p>The client adapter is associated to an access point, but the user has failed to EAP authenticate.</p> <p><b>Note</b> This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i>.</p>	Authentication Failed Retrying	<p>The client adapter is associated to an access point, the user has failed to EAP authenticate, but another authentication attempt is being made.</p> <p><b>Note</b> This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i>.</p>
Connection Status	Description														
Not Associated	The client adapter has not established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).														
Associated	The client adapter has established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).														
Authenticating	The client adapter is associated to an access point, and the EAP authentication process has begun but not yet succeeded.														
Authenticated	The client adapter is associated to an access point, and the user is EAP authenticated.														
Authentication Failed	<p>The client adapter is associated to an access point, but the user has failed to EAP authenticate.</p> <p><b>Note</b> This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i>.</p>														
Authentication Failed Retrying	<p>The client adapter is associated to an access point, the user has failed to EAP authenticate, but another authentication attempt is being made.</p> <p><b>Note</b> This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i>.</p>														

**Table 8-2** *Tool Tip Window Elements (continued)*

Status Element	Description
Link quality	The client adapter's signal strength for all received packets. <b>Value:</b> Excellent, Good, Fair, Poor, or No Link
Link speed and 802.11 mode	The rate at which your client adapter is currently transmitting data packets and the 802.11 mode that your client adapter is currently using for communications. <b>Link speed value:</b> 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps <b>802.11 mode value:</b> 11a, 11b, or 11g
Client adapter type	A description of your client adapter.
Client adapter IP address	The IP address of your client adapter.

## Pop-Up Menu

When you right-click the ASTU icon, the ASTU pop-up menu appears (see [Figure 8-2](#)).

**Figure 8-2** *ASTU Pop-Up Menu*

The following sections describe each ASTU pop-up menu option.



### Note

If you used the Aironet System Tray Utility Preferences window or your system administrator used an administrative tool to deactivate certain ASTU menu options, these options do not appear in the menu and therefore cannot be selected.

## Help

This option enables you to access the online help.

## Exit

This option closes ADU and ASTU.



### Note

To reactivate ADU, double-click the **Aironet Desktop Utility** icon on your computer desktop. To reactivate ASTU, choose the **Enable Tray Icon** option from the ADU Action drop-down menu.

## Open Aironet Desktop Utility

This option activates ADU.

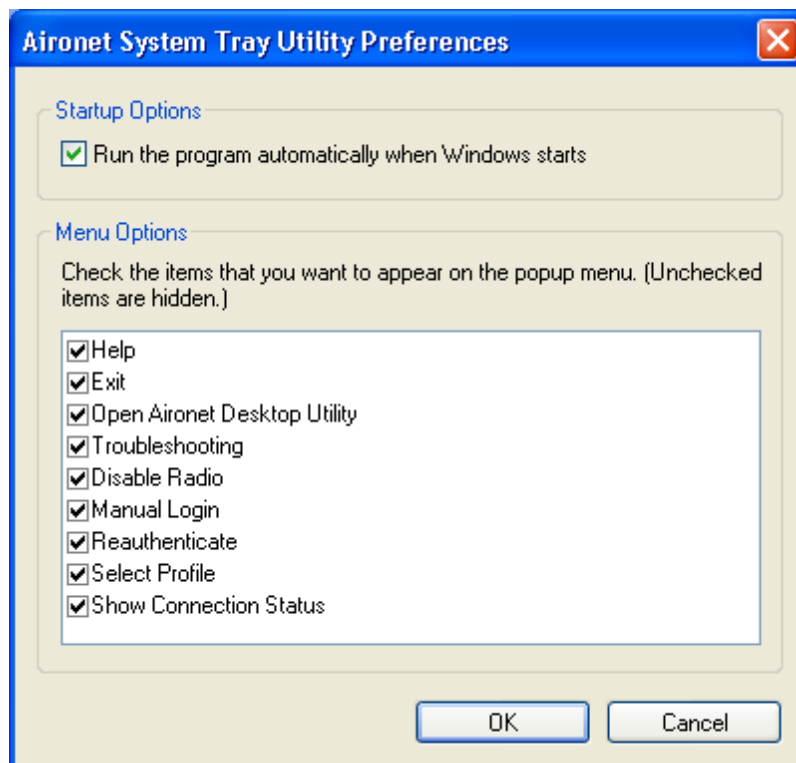
## Troubleshooting

This option activates the troubleshooting utility, which enables you to identify and resolve configuration and association problems with your client adapter. Refer to the [“Using the Cisco Aironet Troubleshooting Utility”](#) section on page 10-3 for detailed instructions on using this utility.

## Preferences

When you choose this option, the Aironet System Tray Utility Preferences window appears (see [Figure 8-3](#)).

**Figure 8-3** Aironet System Tray Utility Preferences Window



This window enables you to determine when ADU and ASTU run and to choose the options that appear on the ASTU pop-up menu. Follow these steps to make your selections.

- Step 1** If you want ASTU to run automatically when Windows starts, make sure the **Run the program automatically when Windows starts** check box is checked. Otherwise, uncheck this check box.



**Note** If you do not choose this option and later want to run ASTU, you must choose the **Enable Tray Icon** option from the Action drop-down menu in ADU.

- Step 2** In the Menu Options portion of the window, make sure the check boxes of all the options that you want to appear in the ASTU pop-up menu are checked. Any options that are not checked will not be included in the menu.



**Note** The Preferences option cannot be deselected. It always appears in the ASTU pop-up menu.

- Step 3** Click **OK** to save your changes.

## Enable/Disable Radio

This option enables you to disable or enable the client adapter's radio. Disabling the radio prevents the adapter from transmitting RF energy. You might want to disable the client adapter's radio in the following situations:

- You are not transmitting data and want to conserve battery power.
- You are using a laptop on an airplane, hospital, or any other location where radio transmission is not allowed and want to prevent the adapter's transmissions from potentially interfering with the operation of certain devices.

When the radio is enabled, it periodically sends out probes even if it is not associated to an access point (in infrastructure mode) or another client (in ad hoc mode), as required by the 802.11 specification. Therefore, it is important to disable it around devices that are susceptible to RF interference.



**Note** If the client adapter's radio is disabled, your client adapter is not associated, and a message appears when you hover the cursor over the ASTU icon to inform you that the wireless network interface is disabled.



**Note** If your client adapter's radio is disabled before your computer enters standby or hibernate mode or before you reboot the computer, the radio remains disabled when the computer resumes. You must enable the radio to resume operation.

If the radio is enabled, choose **Disable Radio** to disable the radio.

If the radio is disabled, choose **Enable Radio** to enable the radio.

## Manual Login

This option enables you to manually invoke the authentication process for a profile that is configured to use a manually prompted LEAP or EAP-FAST username and password. When you choose this option, the Enter Wireless Network Password window appears. Enter your LEAP or EAP-FAST credentials and click **OK**. The LEAP or EAP-FAST Authentication Status window appears, and the authentication process begins.



**Note**

Refer to [Chapter 5](#) for information on setting a manual LEAP or EAP-FAST profile and [Chapter 6](#) for details on the authentication process.

## Reauthenticate

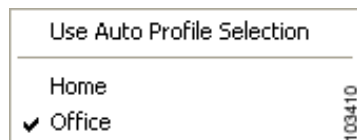
This option forces your client adapter to try to reauthenticate using the username and password of the current profile. It is available for all EAP-enabled profiles. When you choose this option, the authentication process begins.

If your client adapter is unable to authenticate using the specified username and password, you may be prompted to re-enter them. If you click **Cancel**, a message appears indicating that the current profile will be disabled until you choose the Reauthenticate option, reboot your computer, or eject and reinsert the client adapter.

## Select Profile

This option enables you to select the active profile for your client adapter. When you choose this option, a profiles submenu appears (see [Figure 8-4](#)).

**Figure 8-4 Profiles Submenu**



From this menu, you can choose between the following options:

- **Use Auto Profile Selection**—Causes the client adapter's driver to automatically select a profile from the list of profiles that were set up in ADU to be included in auto profile selection.

If the client adapter loses association for more than 10 seconds (or for more than the time specified by the LEAP/EAP-FAST authentication timeout value on the LEAP/EAP-FAST Settings window if LEAP/EAP-FAST is enabled), the driver switches automatically to another profile that is included in auto profile selection. The adapter will not switch profiles as long as it remains associated or reassociates within 10 seconds (or within the time specified by the LEAP/EAP-FAST authentication timeout value). To force the client adapter to associate to a different access point (in infrastructure mode) or another client (in ad hoc mode), you must select a new profile.



**Note**

This option is available only if two or more profiles are included in auto profile selection.

**Note**

Login scripts are not reliable if you use auto profile selection with LEAP or EAP-FAST. If you authenticate and achieve full network connectivity before or at the same time as you log into the computer, the login scripts will run. However, if you authenticate and achieve full network connectivity after you log into the computer, the login scripts will not run.

- **A specific profile**—When you select a profile from the list of available profiles, the client adapter attempts to establish a connection to an access point (in infrastructure mode) or another client (in ad hoc mode) using the parameters that were configured for that profile.

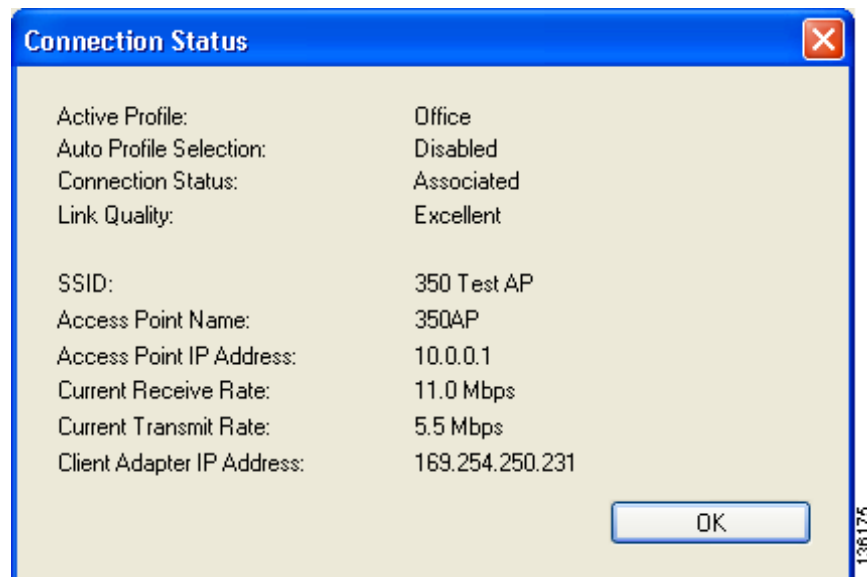
If the client adapter cannot associate to the access point (or other client) or loses association while using the selected profile, the adapter does not attempt to associate using another profile. To get it to associate, you must select a different profile or select Use Auto Profile Selection.

Simply click the desired profile to select it. A check mark appears beside the profile, and the client adapter attempts to establish a connection using the selected profile.

## Show Connection Status

When you choose this option, the Connection Status window appears (see [Figure 8-5](#)).

**Figure 8-5** Connection Status Window



This window provides information on the current status of your client adapter. [Table 8-3](#) interprets each element of the Connection Status window.

**Note**

You can also access the Connection Status window by double-clicking the ASTU icon.



**Table 8-3** Connection Status Window Elements

Status Element	Description	
Active Profile	The network configuration (or profile) that your client adapter is currently using.	
Auto Profile Selection	Indicates whether your client adapter is using auto profile selection. <b>Value:</b> Enabled or Disabled	
Connection Status	The operational mode of your client adapter. <b>Value:</b> Not Associated, Associated, Authenticating, Authenticated, Authentication Failed, or Authentication Failed Retrying	
	<b>Connection Status</b>	<b>Description</b>
	Not Associated	The client adapter has not established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).
	Associated	The client adapter has established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).
	Authenticating	The client adapter is associated to an access point, and the EAP authentication process has begun but not yet succeeded.
	Authenticated	The client adapter is associated to an access point, and the user is EAP authenticated.
	Authentication Failed	The client adapter is associated to an access point, but the user has failed to EAP authenticate. <b>Note</b> This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i> .
	Authentication Failed Retrying	The client adapter is associated to an access point, the user has failed to EAP authenticate, but another authentication attempt is being made. <b>Note</b> This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i> .

**Table 8-3** Connection Status Window Elements (continued)

Status Element	Description
Link Quality	The client adapter's signal strength for all received packets. <b>Value:</b> Excellent, Good, Fair, Poor, or No Link
SSID	The name of the network to which your client adapter is currently associated. <b>Note</b> Refer to the SSID1 parameter in <a href="#">Table 5-2</a> for information on setting the client adapter's SSID.
Access Point Name	The name of the access point to which your client adapter is associated. It is shown only if the client adapter is in infrastructure mode, the access point was configured with a name, and Aironet Extensions are enabled (on access points running Cisco IOS Release 12.2(4)JA or later). <b>Note</b> This field shows up to 15 characters although the name of the access point may be longer.
Access Point IP Address	The IP address of the access point to which your client adapter is associated. It is shown only if the client adapter is in infrastructure mode, the access point was configured with an IP address, and Aironet Extensions are enabled (on access points running Cisco IOS Release 12.2(4)JA or later). <b>Note</b> If Aironet Extensions are disabled, the IP address of the associated access point is shown as 0.0.0.0.
Current Receive Rate	The rate at which your client adapter is currently receiving data packets. <b>Value:</b> 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps
Current Transmit Rate	The rate at which your client adapter is currently transmitting data packets. <b>Value:</b> 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps
Client Adapter IP Address	The IP address of your client adapter.





## Routine Procedures

---

This chapter provides procedures for common tasks related to the client adapter.

The following topics are covered in this chapter:

- [Removing a Client Adapter, page 9-2](#)
- [Client Adapter Software Procedures, page 9-3](#)
- [Enabling or Disabling Your Client Adapter's Radio, page 9-11](#)

## Removing a Client Adapter

Follow the instructions in this section to remove a PC-Cardbus card or PCI card from a computing device, when necessary.

**Caution**

---

These procedures and the physical connections they describe apply generally to conventional Cardbus slots and PCI expansion slots. In cases of custom or nonconventional equipment, be alert to possible differences in Cardbus slot and PCI expansion slot configurations.

---

## Removing a PC-Cardbus Card

To remove a PC-Cardbus card after it is successfully installed and configured (such as when your laptop is to be transported), completely shut down your computer and pull the card directly out of the Cardbus slot. When the card is reinserted and the computer is rebooted, your connection to the network should be re-established.

**Note**

---

If you need to remove your PC-Cardbus card but do not want to shut down your computer, double-click the **Safely Remove Hardware** icon in the Windows system tray, choose the Cisco Aironet client adapter you want to remove under Hardware devices, click **Stop**, and click **OK** to close each open window. Then pull the card directly out of the card slot.

---

## Removing a PCI Card

Because PCI client adapters are installed inside desktop computers, which are not designed for portable use, you should have little reason to remove the adapter. However, instructions are provided below in case you need to remove your PCI card.

- 
- Step 1** Completely shut down your computer.
  - Step 2** Remove the computer cover.
  - Step 3** Remove the screw from the top of the CPU back panel above the PCI expansion slot that holds your client adapter.
  - Step 4** Disassemble the antenna from the base.
  - Step 5** Pull up firmly on the client adapter to release it from the slot and carefully tilt the adapter to slip its antenna through the opening near the slot.
  - Step 6** Reinstall the screw on the CPU back panel and replace the computer cover.
-

# Client Adapter Software Procedures

This section provides instructions for the following procedures:

- Upgrading the client adapter software, [page 9-3](#)
- Manually installing or upgrading the client adapter driver, [page 9-6](#)
- Uninstalling the client adapter software, [page 9-6](#)
- ADU procedures, [page 9-7](#)
- ASTU procedures, [page 9-11](#)

## Upgrading the Client Adapter Software

Follow these steps to upgrade your Cisco Aironet CB21AG or PI21AG client adapter software to a more recent release using the settings that were selected during the last installation.

**Note**

If you want to upgrade your client adapter software using new installation settings, uninstall the previous installation (see the instructions on [page 9-6](#)); then install the new software (see the instructions on [page 3-9](#)).

**Step 1**

Make sure the client adapter is inserted into your computer.

**Note**

If your client adapter is not inserted, the installation continues, but the driver installation is incomplete. You must manually upgrade the driver later using the Update Device Driver Wizard. See the “[Manually Installing or Upgrading the Client Adapter Driver](#)” section on [page 9-6](#) for instructions.

**Step 2**

Use Windows Explorer to find the Install Wizard file.

**Step 3**

Double-click the file. The “Starting InstallShield Wizard” message appears followed by the Preparing Setup window (see [Figure 9-1](#)) and the Previous Installation Detected window (see [Figure 9-2](#)).

Figure 9-1 Preparing Setup Window

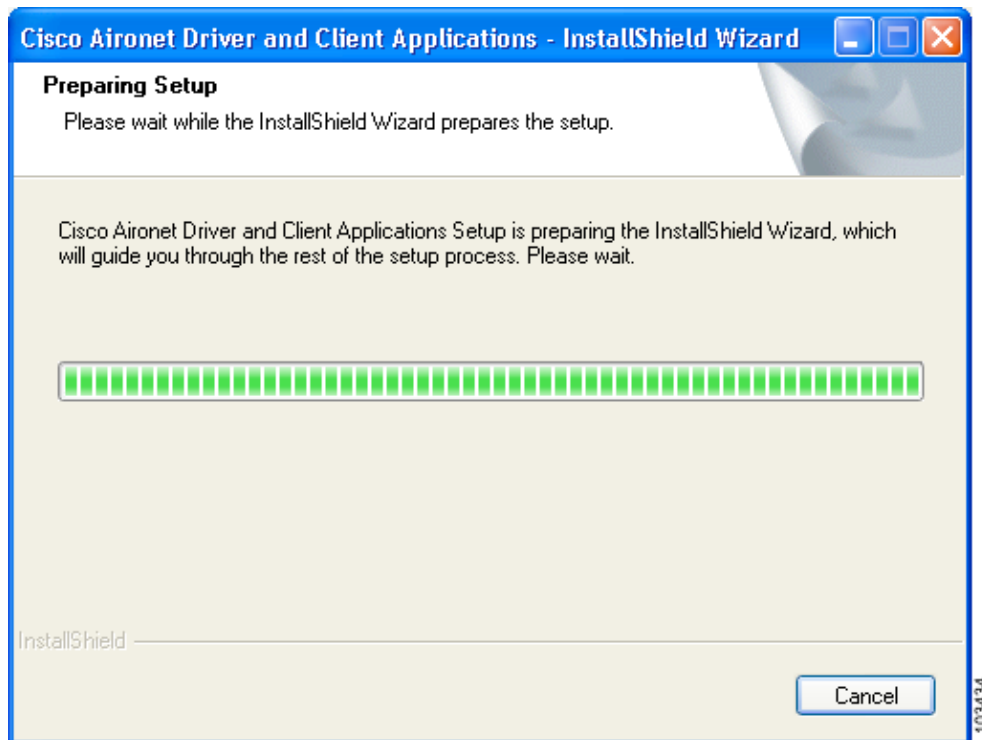
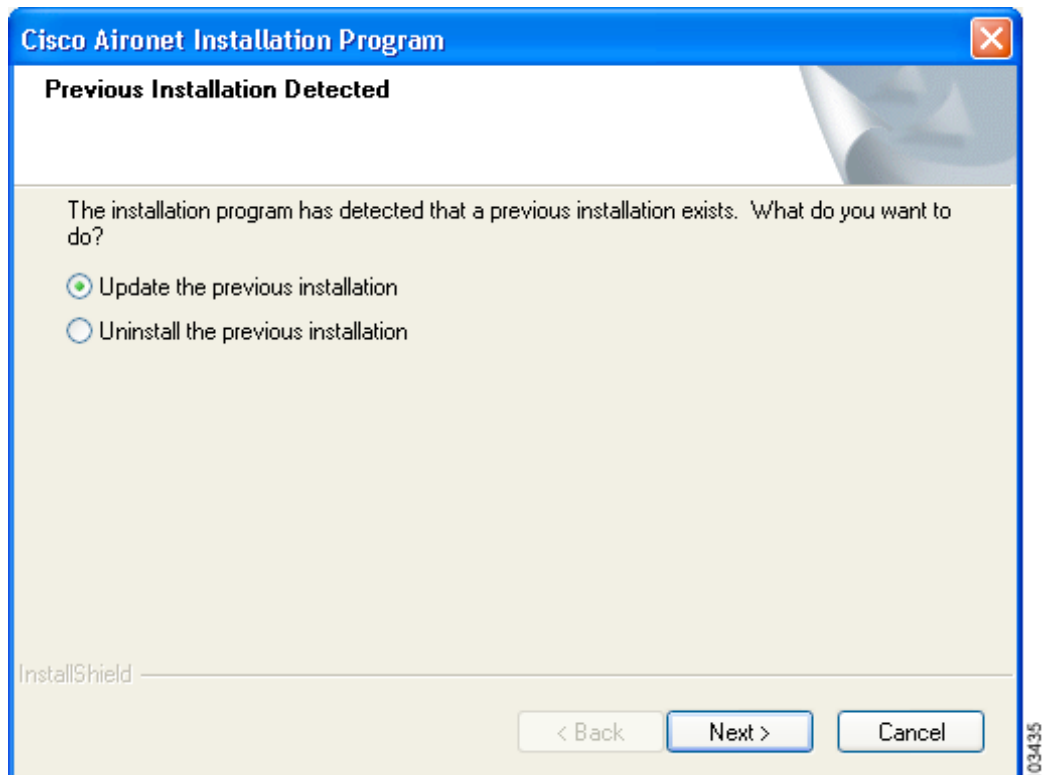


Figure 9-2 Previous Installation Detected Window



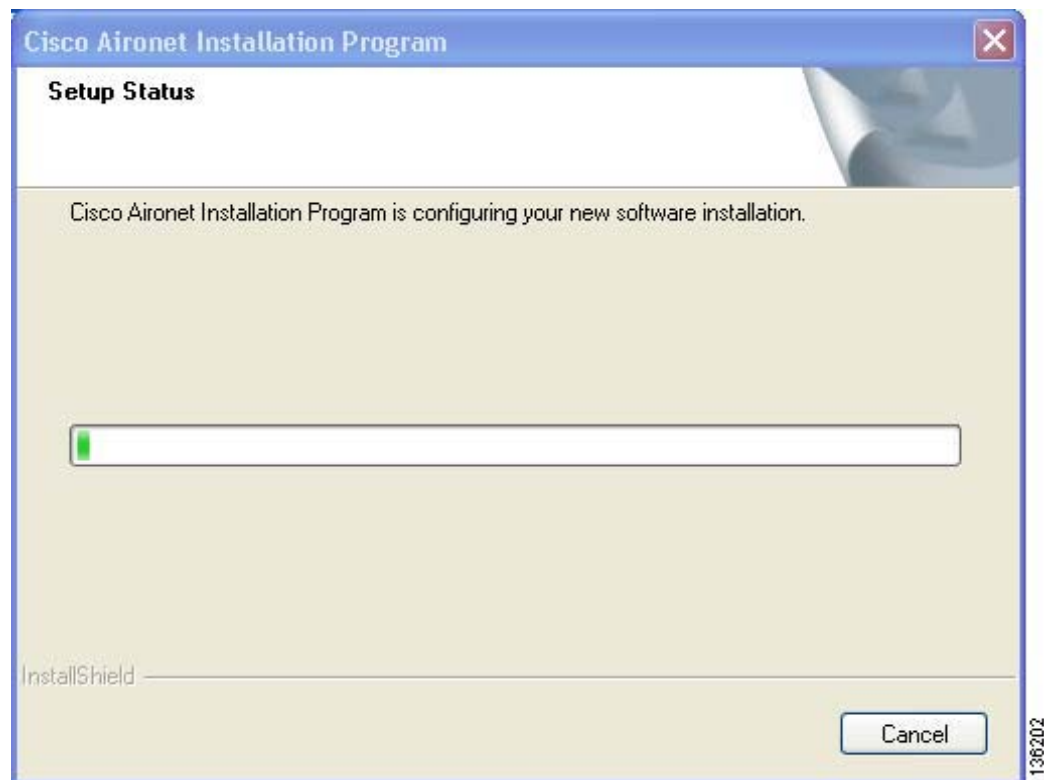
- Step 4** Choose **Update the previous installation** and click **Next**.
- Step 5** When a message appears indicating that you are required to restart your computer at the end of the installation process, click **Yes**.



**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 9-3](#)).

**Figure 9-3** Setup Status Window



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

- Step 6** 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.



## Manually Installing or Upgrading the Client Adapter Driver

If you installed or upgraded the client adapter software without the client adapter inserted into your computer, the driver installation is incomplete. Follow these steps to manually install or upgrade the client adapter driver.

- 
- Step 1** Insert the client adapter into your computer.
- Step 2** Click **Start > Settings > Control Panel > Administrative Tools > Computer Management > Device Manager > Network Adapters**.
- Step 3** Right-click **Cisco Aironet 802.11a/b/g Wireless Adapter**.
- Step 4** Click **Properties**.
- Step 5** Choose the **Driver** tab and click **Update Driver**.
- Step 6** Use the update wizard to select the driver from the *root\windows\system32* directory (such as *C:\Windows\system32*) and finish the update procedure.
- Step 7** Follow these steps to activate the newly updated driver:
- Click **Start > Settings > Control Panel > Network Connections** or **Network and Dial-up Connections**.
  - Right-click the wireless connection.
  - Choose **Disable**.
  - Repeat Steps a and b.
  - Choose **Enable**.
- 

## Uninstalling the Client Adapter Software

This section provides instructions for uninstalling the software for your Cisco Aironet CB21AG or PI21AG client adapter. This procedure is necessary if you want to remove installed client adapter software from your computer or downgrade to a previous release.

**Note**

If you want to downgrade to an earlier release of client adapter software, use this procedure to uninstall the current software. Then install the older software.

**Note**

When you uninstall the client adapter software, any existing profiles and stored PAC files are removed. If you want to save your profiles for later use, follow the instructions in [Chapter 4](#) to export your profiles before uninstalling the software.

---

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



**Note** If your client adapter is not inserted, the driver cannot be uninstalled.

---

**Step 2** Use Windows Explorer to find the Install Wizard file.



**Note** If you do not have the Install Wizard's setup.exe file, you can access the client adapter software by clicking **Control Panel > Add/Remove Programs > Cisco Aironet Installation Program > Remove**. Then follow the steps below beginning with the Preparing Setup window in [Step 3](#).

---

**Step 3** Double-click the file. The "Starting InstallShield Wizard" message appears followed by the Preparing Setup window (see [Figure 9-1](#)) and the Previous Installation Detected window (see [Figure 9-2](#)).

**Step 4** Choose **Uninstall the previous installation** and click **Next**.

**Step 5** When a message appears indicating that you are required to restart your computer at the end of the operation, click **Yes**. (If you click **No**, you are asked to confirm your decision. If you proceed, the installation process terminates.)

**Step 6** When prompted to confirm your decision, click **OK**. The process to uninstall the files begins.

**Step 7** When prompted to uninstall the device driver, click **Yes**.

**Step 8** When a message appears indicating that your computer needs to be rebooted, click **OK** and allow your computer to restart. The client adapter software and its program folder have been uninstalled.



**Note** This procedure does not remove the Install Wizard file. If you want to remove it from your computer, find the file using Windows Explorer and delete it.

---

## ADU Procedures

This section provides instructions for the following procedures:

- Opening ADU, [page 9-8](#)
- Exiting ADU, [page 9-8](#)
- Finding the version of ADU and other software components, [page 9-9](#)
- Viewing client adapter information, [page 9-10](#)
- Accessing online help, [page 9-10](#)

## Opening ADU

To open ADU, perform one of the following:

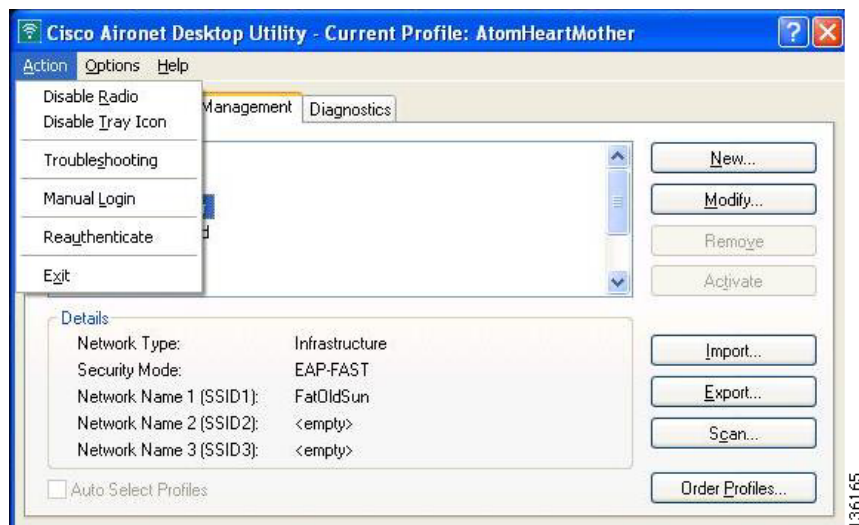
- Double-click the **Aironet Desktop Utility** icon on your desktop.
- Choose **Aironet Desktop Utility** from the folder in the Windows Start Menu that you chose during installation (the default location is **Start > Programs > Cisco Aironet > Aironet Desktop Utility**).
- Right-click the ASTU icon in the Windows system tray and choose **Open Aironet Desktop Utility**.

## Exiting ADU

To exit ADU, perform one of the following:

- Choose **Exit** from the Action drop-down menu (see [Figure 9-4](#)).
- Right-click the ASTU icon in the Windows system tray and choose **Exit**.

**Figure 9-4** Action Drop-Down Menu

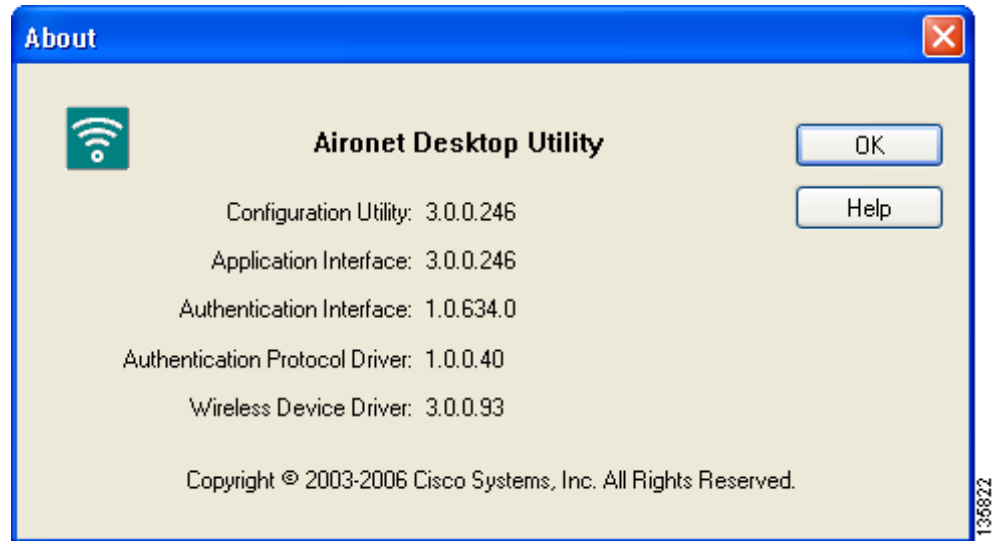


## Finding the Version of ADU and Other Software Components

Follow these steps to find the current version of ADU and other software components.

- Step 1** Open ADU.
- Step 2** Choose the **About Aironet Desktop Utility** option from the Help drop-down menu. The About window appears (see [Figure 9-5](#)).

**Figure 9-5** About Window



[Table 9-1](#) lists and describes the software components shown in the About window.

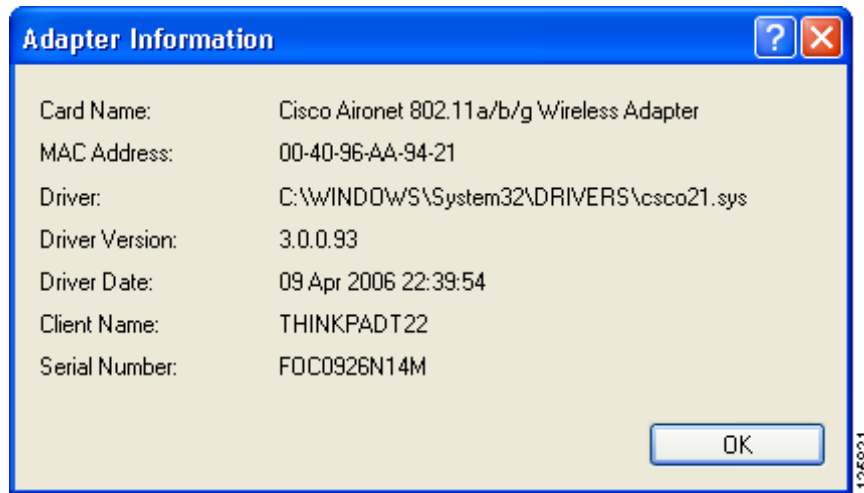
**Table 9-1** Software Components Shown in About Window

Software Component	Description
Configuration Utility	Aironet Client Administration Utility (ACAU) version
Application Interface	Aironet Desktop Utility (ADU) version
Authentication Interface	Supplicant version
Authentication Protocol Driver	Protocol driver version
Wireless Device Driver	Windows NDIS miniport driver version

## Viewing Client Adapter Information

To view information about your client adapter, open ADU. Click the **Diagnostics** tab and **Adapter Information**. The Adapter Information window appears (see [Figure 9-6](#)).

**Figure 9-6** Adapter Information Window



[Table 9-2](#) interprets each element of the Adapter Information window.

**Table 9-2** Adapter Information

Status	Description
Card Name	A description of your client adapter.
MAC Address	The MAC address assigned to your client adapter at the factory.
Driver	The filename and location of your client adapter's driver.
Driver Version	The version of the NDIS device driver that is currently installed on your computer.
Driver Date	The date that your client adapter's driver was created.
Client Name	The name your client adapter uses when it associates to an access point. <b>Note</b> Refer to the Client Name parameter in <a href="#">Table 5-2</a> for information on setting the client name.
Serial Number	The serial number of your client adapter.

Click **OK** to close the Adapter Information window.

## Accessing Online Help

To access the ADU online help, open ADU. Then choose the **Aironet Desktop Utility Help** option from the Help drop-down menu.

## ASTU Procedures

Refer to [Chapter 8](#) for instructions on using ASTU.

## Enabling or Disabling Your Client Adapter's Radio

Your client adapter's radio can be enabled or disabled. Disabling the radio prevents the adapter from transmitting RF energy. You might want to disable the client adapter's radio in the following situations:

- You are not transmitting data and want to conserve battery power.
- You are using a laptop on an airplane and want to prevent the adapter's transmissions from potentially interfering with the operation of certain devices.

When the radio is enabled, it periodically sends out probes even if it is not associated to an access point (in infrastructure mode) or another client (in ad hoc mode), as required by the 802.11 specification. Therefore, it is important to disable it around devices that are susceptible to RF interference.

**Note**

---

Your client adapter is not associated while its radio is disabled.

---

**Note**

---

If your client adapter's radio is disabled before your computer enters standby or hibernate mode or before you reboot the computer, the radio remains disabled when the computer resumes. You must enable the radio to resume operation.

---

You can use ADU or ASTU to enable or disable the client adapter's radio. Follow the instructions below to use ADU or refer to the [“Enable/Disable Radio” section on page 8-7](#) to use ASTU.

If your client adapter's radio is enabled, open ADU and choose **Disable Radio** from the Action drop-down menu (see [Figure 9-4](#)) to disable the radio.

If your client adapter's radio is disabled, open ADU and choose **Enable Radio** from the Action drop-down menu (see [Figure 9-4](#)) to enable the radio.





## Troubleshooting

---

This chapter provides information for diagnosing and correcting common problems that may occur when you install and operate the client adapter.

The following topics are covered in this chapter:

- [Accessing the Latest Troubleshooting Information, page 10-2](#)
- [Interpreting the Indicator LEDs, page 10-2](#)
- [Troubleshooting the Client Adapter, page 10-3](#)
- [Error Messages, page 10-12](#)



## Accessing the Latest Troubleshooting Information

This chapter provides basic troubleshooting tips for your client adapter. For more up-to-date and detailed troubleshooting information, refer to the TAC web site. To access this site, go to Cisco.com, click **Technical Support > Product Support > Wireless**. Then choose your product and click **Troubleshooting** to find information on the problem you are experiencing.

## Interpreting the Indicator LEDs

The client adapter shows messages through its two LEDs. [Table 10-1](#) interprets the LED operating messages.

**Table 10-1** LED Operating Messages

Status LED (green)	Activity LED (amber)	Condition
Off	Off	Client adapter is not receiving power.
Blinking slowly	Off	Client adapter is in power save mode.
On	Off	Client adapter has awakened from power save mode.
Alternating blink:		Client adapter is scanning for the wireless network for which it is configured.
On	Off	
Off	On	
Blinking slowly	Blinking slowly	Client adapter is associated to an access point (in infrastructure mode) or another client (in ad hoc mode).
Blinking quickly	Blinking quickly	Client adapter is transmitting or receiving data while associated to an access point (in infrastructure mode) or another client (in ad hoc mode).

# Troubleshooting the Client Adapter

This section provides troubleshooting tips should you encounter problems with your client adapter. Use [Table 10-2](#) to quickly find specific troubleshooting information.

**Table 10-2**      *Troubleshooting Information*

<b>Troubleshooting Information</b>	<b>Page Number</b>
Using the troubleshooting utility	<a href="#">10-3</a>
Disabling the Microsoft Wireless Configuration Manager	<a href="#">10-8</a>
Disabling the Microsoft 802.1X supplicant	<a href="#">10-8</a>
Client adapter recognition problems	<a href="#">10-8</a>
Resolving resource conflicts	<a href="#">10-9</a>
Problems associating to an access point	<a href="#">10-10</a>
Problems connecting to the network	<a href="#">10-11</a>
Prioritizing network connections	<a href="#">10-11</a>
Parameters missing from Profile Management windows	<a href="#">10-11</a>
Windows Wireless Network Connection icon shows unavailable connection (Windows XP only)	<a href="#">10-11</a>

## Using the Cisco Aironet Troubleshooting Utility

The Cisco Aironet Troubleshooting Utility enables you to identify and resolve configuration and association problems with your client adapter. It is meant to be used only when the client adapter is in infrastructure mode because it assesses the connection between the adapter and an access point.

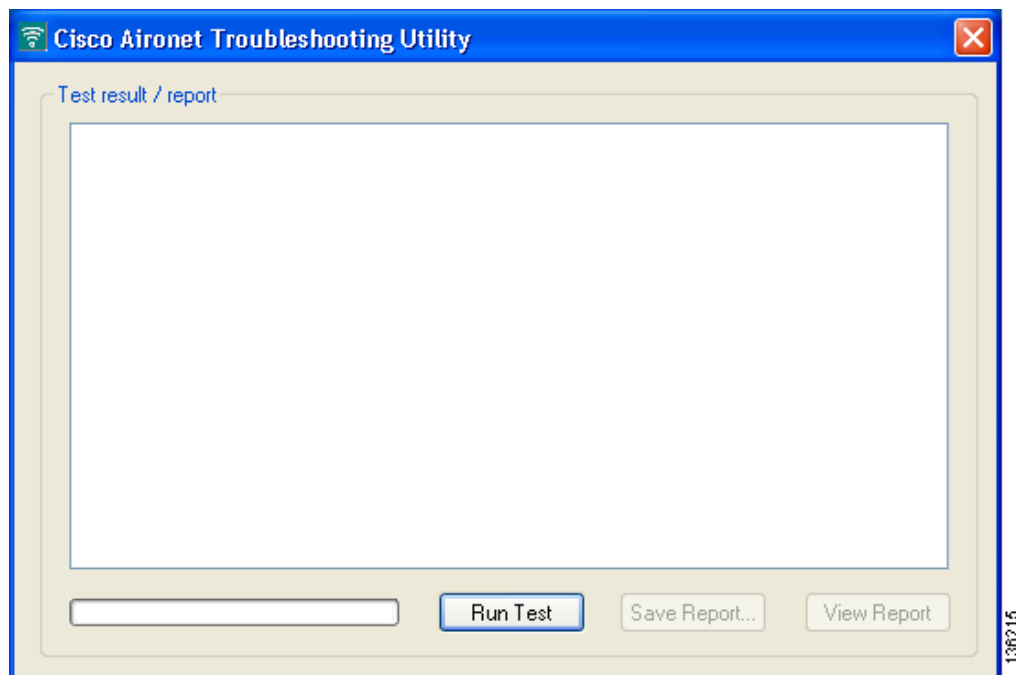
Follow the instructions in one of the subsections below to use the utility to diagnosis your client adapter's operation, save a detailed report to a text file, or access online help.

## Diagnosing Your Client Adapter's Operation

- Step 1** Perform one of the following to activate the troubleshooting utility:
- Open ADU; choose **Troubleshooting** from the Action drop-down menu.
  - Open ADU; click the **Diagnostics** tab and **Troubleshooting**.
  - Right-click the ASTU icon; choose **Troubleshooting** from the pop-up menu.

The Cisco Aironet Troubleshooting Utility window appears (see [Figure 10-1](#)).

**Figure 10-1** Troubleshooting Utility Window

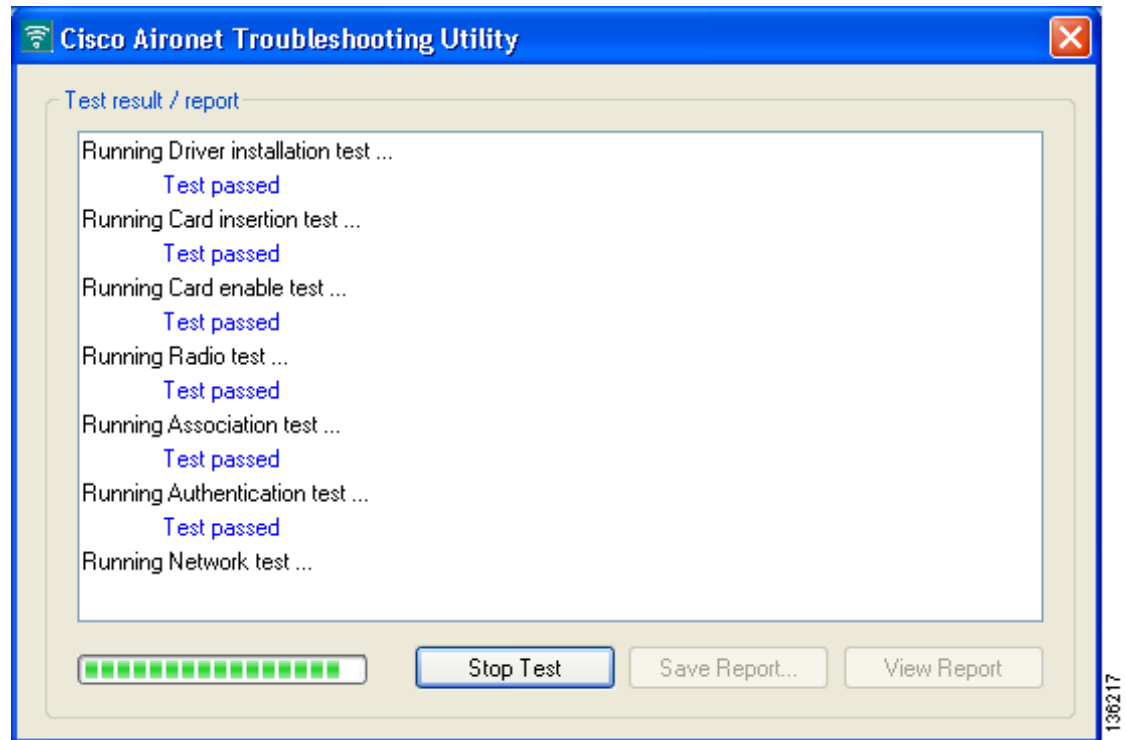


**Step 2** Click **Run Test**. The utility performs the following series of seven tests to check the operation of your client adapter and to identify specific problems if they exist:

1. Driver installation test
2. Card insertion test
3. Card enable test
4. Radio test
5. Association test
6. Authentication test
7. Network test

The utility runs and then displays the results for each test (see [Figure 10-2](#)).

**Figure 10-2** Troubleshooting Utility Window (with Test Results)



One of the following status messages appears for each test:

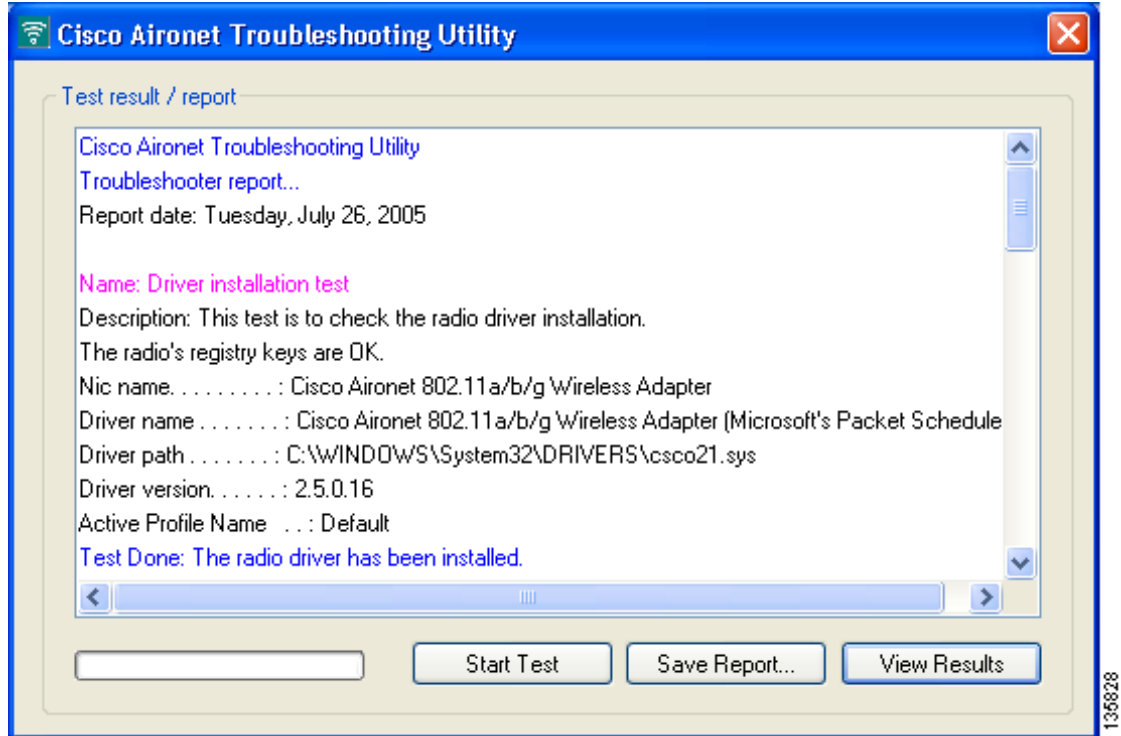
- **Test passed**—The test completed successfully.
- **Test bypassed**—The test was skipped because it was not required for the active profile.
- **Test failed**—The test failed. Follow the instructions in [Step 3](#) to obtain more details.



**Note** You can click **Stop Test** at any time to stop the testing process, or you can click **Start Test** after the testing process has stopped to run the test again.

- Step 3** To view more detailed information, click **View Report**. A report appears that provides more detailed results for your client adapter (see [Figure 10-3](#)).

**Figure 10-3** Troubleshooting Utility Window (Detailed Report)



**Note** The report contains valuable information that, if necessary, could be used by your system administrator or TAC to analyze any problems. Follow the instructions in the next section if you want to save the report to a text file.

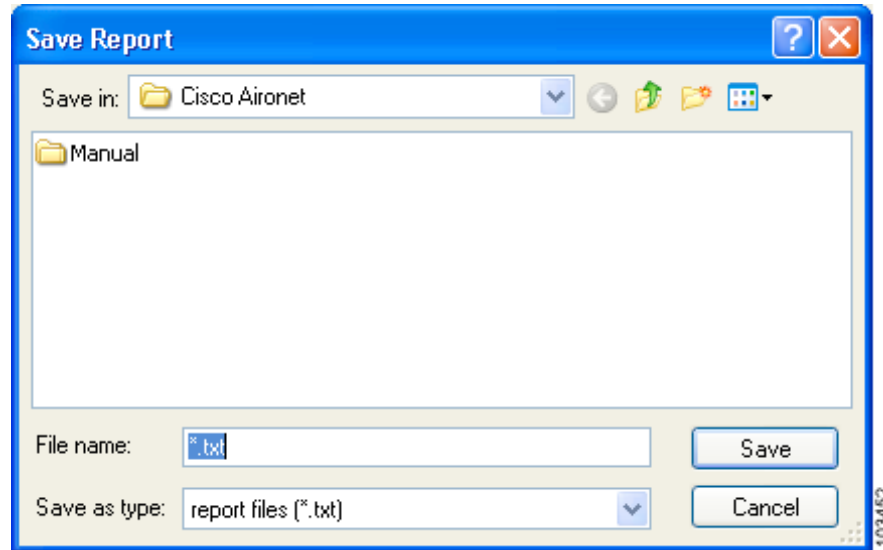
- Step 4** If a problem is discovered, the report provides some possible repair suggestions. Follow the repair instructions carefully and run the troubleshooting utility again.

## Saving the Detailed Report to a Text File

Follow the steps below to save the detailed troubleshooting report to your computer's hard drive.

- Step 1** Click **Save Report**. The Save Report window appears (see [Figure 10-4](#)).

**Figure 10-4** Save Report Window



- Step 2** Enter a name for the detailed report in the File name field. The report is saved as a \*.txt file.
- Step 3** Use the Save in box at the top of the window to specify the location on your computer's hard drive where the file will be saved.



**Note** The default location is the directory where ADU is installed (such as C:\Program Files\Cisco Aironet).

- Step 4** Click **Save**. The file is saved as a text file in the location specified.

## Disabling the Microsoft Wireless Configuration Manager (Windows XP Only)

If any conflicts arise between ADU and the Microsoft Wireless Configuration Manager on a computer running Windows XP, follow these steps to disable the Microsoft configuration manager.



**Note** Disabling the Microsoft Wireless Configuration Manager on Windows XP also disables the Microsoft 802.1X supplicant. If you chose to configure your client adapter using ADU during installation, the Microsoft 802.1X supplicant should already be disabled.

- 
- Step 1** Double-click **My Computer**, **Control Panel**, and **Network Connections**.
  - Step 2** Right-click **Wireless Network Connection** and click **Properties**.
  - Step 3** Click the **Wireless Networks** tab and uncheck the **Use Windows to configure my wireless network settings** check box.
  - Step 4** Click **OK** to save your settings.
- 

## Disabling the Microsoft 802.1X Supplicant (Windows 2000 Only)

The Microsoft 802.1X supplicant can be installed on a computer running Windows 2000 through either a Microsoft hot fix or Windows 2000 Service Pack 4. If any conflicts arise between ADU and the Microsoft 802.1X supplicant, follow these steps to disable the Microsoft supplicant on a Windows 2000 computer.



**Note** The Microsoft 802.1X supplicant, if installed, should have been disabled during installation.

- 
- Step 1** Double-click **My Computer**, **Control Panel**, and **Network and Dial-up Connections**. Right-click **Local Area Connection**. Click **Properties**. The Local Area Connection Properties window appears.
  - Step 2** Click the **Authentication** tab.
  - Step 3** Uncheck the **Enable network access control using IEEE 802.1X** or **Enable IEEE 802.1x authentication for this network** check box.
  - Step 4** Click **OK** to save your settings.
- 

## Client Adapter Recognition Problems

If your computer's PCMCIA adapter does not recognize your client adapter, check your computer's BIOS and make sure that the PC card controller mode is set to PCIC compatible.



**Note** A computer's BIOS varies depending on the manufacturer. For support on BIOS-related issues, consult your computer's manufacturer.

## Resolving Resource Conflicts

If you encounter problems while installing your client adapter on a computer running a Windows operating system, you may need to specify a different interrupt request (IRQ) or I/O range for the adapter.

The default IRQ for the client adapter is IRQ 10, which may not work for all systems. Follow the steps for your specific operating system to obtain an available IRQ.

During installation the adapter's driver installation script scans for an unused I/O range. The installation can fail if the I/O range found by the driver installation script is occupied by another device but not reported by Windows. An I/O range might not be reported if a device is physically present in the system but not enabled under Windows. Follow the steps for your specific operating system to obtain an available I/O range.

### Resolving Resource Conflicts in Windows 2000

- 
- Step 1** Double-click **My Computer**, **Control Panel**, and **System**.
  - Step 2** Click the **Hardware** tab and **Device Manager**.
  - Step 3** Double-click **Network Adapters** and the Cisco Systems Wireless LAN Adapter.
  - Step 4** In the General window, the Device Status field indicates if a resource problem exists. If a problem is indicated, click the **Resources** tab.
  - Step 5** Uncheck the **Use automatic settings** check box.
  - Step 6** Under Resource Settings or Resource Type, click **Input/Output Range**.
  - Step 7** Look in the Conflicting Device list at the bottom of the window. If it indicates that the range is being used by another device, click the **Change Setting** button.
  - Step 8** Scroll through the ranges in the Value dialog box and choose one that does not conflict with another device. The Conflict Information window at the bottom of the window indicates if the range is already being used.
  - Step 9** Click **OK**.
  - Step 10** Under Resource Settings or Resource Type, click **Interrupt Request**.
  - Step 11** Look in the Conflicting Device list at the bottom of the window. If it indicates that the IRQ is being used by another device, click the **Change Setting** button.
  - Step 12** Scroll through the IRQs in the Value dialog box and choose one that does not conflict with another device. The Conflict Information window at the bottom of the window indicates if the IRQ is already being used.
  - Step 13** Click **OK**.
  - Step 14** Reboot your computer.
-



## Resolving Resource Conflicts in Windows XP


**Note**

These instructions assume you are using the Windows XP classic view, not the category view.

- 
- Step 1** Double-click **My Computer**, **Control Panel**, and **System**.
- Step 2** Click the **Hardware** tab and **Device Manager**.
- Step 3** Under Network Adapters, double-click the Cisco Systems Wireless LAN Adapter.
- Step 4** In the General window, the Device Status field indicates if a resource problem exists. If a problem is indicated, click the **Resources** tab.
- Step 5** Uncheck the **Use automatic settings** check box.
- Step 6** Under Resource Settings, click **I/O Range**.
- Step 7** Look in the Conflicting Device list at the bottom of the window. If it indicates that the range is being used by another device, click the **Change Setting** button.
- Step 8** Scroll through the ranges in the Value dialog box and choose one that does not conflict with another device. The Conflict Information window at the bottom of the window indicates if the range is already being used.
- Step 9** Click **OK**.
- Step 10** Under Resource Settings, click **IRQ**.
- Step 11** Look in the Conflicting Device list at the bottom of the window. If it indicates that the IRQ is being used by another device, click the **Change Setting** button.
- Step 12** Scroll through the IRQs in the Value dialog box and choose one that does not conflict with another device. The Conflict Information window at the bottom of the window indicates if the IRQ is already being used.
- Step 13** Click **OK**.
- Step 14** Reboot your computer.
- 

## Problems Associating to an Access Point

Follow the instructions below if your client adapter fails to associate to an access point.

- If possible, move your workstation a few feet closer to an access point and try again.
- Make sure that the client adapter is securely inserted into your computer's client adapter slot.
- If you are using a PCI card, make sure that the antenna is securely attached.
- Make sure that the access point is turned on and operating.
- Check that all parameters are set properly for both the client adapter and the access point. These include the SSID, EAP authentication, WEP activation, network type, channel, etc.
- Follow the instructions in the previous section to resolve any resource conflicts.
- If the client adapter still fails to establish contact, refer to the [“Obtaining Technical Assistance”](#) section in the Preface for technical support information.

## Problems Connecting to the Network

After you have installed the appropriate driver and client utilities, contact your IS department if you have a problem connecting to the network. Proxy server, network protocols, and further authentication information might be needed to connect to the network.

**Note**

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.

## Prioritizing Network Connections

If your computer has more than one network adapter enabled (such as a Cisco Aironet client adapter and an Ethernet card), you can choose which one to use by assigning a priority to your network connections. Follow the steps below to prioritize your network connections.

- 
- Step 1** Right-click the **My Network Places** icon on your desktop.
  - Step 2** Click **Properties**.
  - Step 3** Choose the **Advanced** menu option at the top of the window.
  - Step 4** Click **Advanced Settings**. Your network connections are listed in the Connections box on the Adapters and Bindings tab.
  - Step 5** Use the arrows beside the Connections box to move the network connection that you want to use to the top.
  - Step 6** Click **OK**.
- 

## Parameters Missing from Profile Management Windows

If some parameters are unavailable on the Profile Management windows, your system administrator may have used an administrative tool to deactivate these parameters. In this case, these parameters cannot be selected.

## 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 is caused by a conflict between the wireless network settings of ADU and Windows XP. Simply ignore the Windows icon and use the ASTU icon to check the status of your client adapter's wireless connection.

# Error Messages

This section provides a list of error messages that may appear during the installation, configuration, or use of your client adapter. The messages are listed in alphabetical order within each section, and an explanation as well as a recommended user action are provided for each message.

**Error Message** ADU can hold only 16 profiles. To add another profile, either delete an existing profile or modify an existing profile.

**Explanation** You attempted to create a new profile, import a profile, or activate a profile from the scan list on the Available Infrastructure and Ad Hoc Networks window after the maximum number of profiles had already been reached.

**Recommended Action** Modify an existing profile or delete a profile and then create a new one.

**Error Message** An error occurred opening C:\directory\filename

**Explanation** You selected the wrong file type while attempting to open the AP scan list file in the site survey utility.

**Recommended Action** Locate the AP scan list file (SST\_APScanList.apsl) and open it.

**Error Message** Are you sure you want to delete this PAC from your local system? If deleted, you may disrupt authentication with the EAP-FAST profiles that use this PAC.

**Explanation** You are about to delete a PAC from either the Global or Private PAC store.

**Recommended Action** If you want to delete the PAC, click **Yes**. Otherwise, click **No**.

**Error Message** At least one wireless checkbox must be selected.

**Explanation** You clicked **OK** or selected another Profile Management tab before selecting any Wireless Mode options on the Profile Management (Advanced) window.

**Recommended Action** Choose at least one of the Wireless Mode options.

**Error Message** Authentication failed.

**Explanation** The domain logon failed for an unknown reason.

**Recommended Action** Try again to authenticate. If this message reappears, verify that all of the proper certificates have been loaded onto your computer and that your client adapter's current profile has been configured properly. If the domain logon continues to fail, contact your system administrator.

**Error Message** Authentication failed because server rejected username or password.

**Explanation** The domain logon failed because your username or password is invalid.

**Recommended Action** Re-enter your username and password on the Define PEAP (EAP-GTC) Configuration window or the Define PEAP (EAP-MSCHAP V2) Configuration window and save your settings. Then try again to authenticate.

**Error Message** Authentication failed due to invalid client attributes (e.g., Login Name).

**Explanation** The domain logon failed because of an invalid client configuration setting, such as a mistyped login name.

**Recommended Action** Return to the PEAP configuration windows, verify your settings, and make any necessary modifications.

**Error Message** Authentication failed due to invalid client certificate.

**Explanation** The domain logon failed because of an invalid client certificate.

**Recommended Action** Contact your system administrator to obtain a valid certificate.

**Error Message** Authentication failed due to invalid server certificate.

**Explanation** The domain logon failed because of an invalid server certificate.

**Recommended Action** Contact your system administrator.

**Error Message** Authentication failed due to invalid server/domain name.

**Explanation** The domain logon failed because of an invalid server/domain name.

**Recommended Action** Make sure the Specific Server or Domain field is blank on the Advanced Configuration window for PEAP (EAP-GTC) or PEAP (EAP-MSCHAP V2). Then follow the instructions in the [“Enabling PEAP \(EAP-GTC\)”](#) section on page 5-48 or the [“Enabling PEAP \(EAP-MSCHAP V2\) Machine Authentication with Machine Credentials”](#) section on page 5-55 to correctly enter your username in the Login Name field.

**Error Message** Authentication timed out. Do you want to retry?

**Explanation** LEAP or EAP-FAST authentication failed because the authentication server is down.

**Recommended Action** Click **Retry** to try to authenticate again using the same credentials or click **Cancel** to cancel the operation.

**Error Message** Cannot load oemres.dll.

**Explanation** The oemres.dll file cannot be installed.

**Recommended Action** Uninstall the current client adapter software; then install the latest release.

**Error Message** Cisco Aironet 802.11a/b/g wireless adapter software update can't proceed. Please insert the adapter in the system and try again.

**Explanation** You attempted to upgrade your client adapter's software when the adapter was not inserted into your computer.

**Recommended Action** Click **OK**, insert your client adapter, and start the upgrade process again.

**Error Message** DHCP failure.

**Explanation** The domain logon failed because of a DHCP failure.

**Recommended Action** Try again to authenticate. If this message reappears, contact your system administrator.

**Error Message** During installation, you chose not to use Microsoft Wireless Configuration Manager to control your Cisco Aironet Wireless LAN Client Adapter. However, it is currently enabled for this device. Do you want to disable it?

**Explanation** The Microsoft Wireless Configuration Manager is enabled and can be used to control your client adapter.

**Recommended Action** If you want to switch control from the Microsoft Wireless Configuration Manager to ADU, click **Yes**. Otherwise, click **No**.

**Error Message** Entry must be xx characters long. Please enter xx more characters.

**Explanation** The static WEP key that you entered on the Define Pre-Shared Keys window does not contain the correct number of characters.

**Recommended Action** Re-enter the static WEP key following the guidelines in the [“Enabling Static WEP” section on page 5-26](#).

**Error Message** Error importing the EAP-FAST PAC file.

**Explanation** An error occurred while a PAC file was being imported. The operation was not completed.

**Recommended Action** Try again to import the PAC file. If the same message appears, obtain a new PAC file from your system administrator and import it.

**Error Message** Failed to initialize supplicant. This error may be due to the absence of a valid machine certificate or the incomplete configuration of profiles.

**Explanation** The domain logon failed because the EAP supplicant could not be initialized.

**Recommended Action** Verify that a valid machine certificate has been loaded onto your computer and that your client adapter's current profile has been configured properly.

**Error Message** Failed to open PAC stores.

**Explanation** An error occurred when you attempted to access the global or private PAC store.

**Recommended Action** Try again. If the second attempt fails, contact your system administrator.

**Error Message** In order to select an Ad Hoc network, you must have a Network Name. Do you want to enter a Network Name?

**Explanation** You chose Ad Hoc for Network Type on the Profile Management (Advanced) window, but a network name was not entered on the Profile Management (General) window.

**Recommended Action** If you want to set up an ad hoc network, click **Yes** and enter a network name in the SSID1 field on the Profile Management (General) window. Otherwise, click **No**.

**Error Message** Invalid profile data. Please enter valid profile data.

**Explanation** You improperly configured a profile (for example, you set up the profile to use EAP-TLS authentication, but no certificates are installed on your computer).

**Recommended Action** Modify the profile's configuration settings.

**Error Message** Make sure the same new password is entered twice.

**Explanation** You did not enter the same EAP-FAST password in both the New Password and Verify New Password fields on the Please Change Password window.

**Recommended Action** Carefully re-enter your new EAP-FAST password in both the New Password and Verify New Password fields on the Please Change Password window.

**Error Message** No user certificates were found on your computer. Machine certificates will be used for Domain Logon if "Use Machine Information For Domain Logon" check box is checked.

**Explanation** You chose the EAP-TLS option on the Profile Management (Security) window, but no user certificates were found on your computer.

**Recommended Action** Perform one of the following:

- If you want the client to attempt to log into a domain using machine authentication with a machine certificate and machine credentials, check the **Use Machine Information For Domain Logon** check box when the Define Certificate window appears.
- If you want the client to authenticate using user credentials, install the appropriate user certificate on your computer.

**Error Message** Please enter a Passphrase.

**Explanation** You clicked **OK** on the Define WPA/WPA2 Pre-Shared Key window before entering a passphrase.

**Recommended Action** Enter a WPA/WPA2 passphrase on the Define WPA/WPA2 Pre-Shared Key window and then click **OK**.

**Error Message** Please enter a profile name.

**Explanation** While creating a new profile, you clicked **OK** or chose another Profile Management tab before entering a profile name on the Profile Management (General) window.

**Recommended Action** Enter a profile name.

**Error Message** Please enter at least one Pre-Shared Key.

**Explanation** You clicked **OK** on the Define Pre-Shared Keys window before entering a static WEP key.

**Recommended Action** Enter at least one static WEP key on the Define Pre-Shared Keys window.

**Error Message** Please enter exactly 12 characters, or leave the entry field empty.

**Explanation** You entered fewer than 12 characters in one of the fields on the Preferred Access Points window.

**Recommended Action** Leave the fields on the Preferred Access Points window empty or re-enter the MAC address for the specified access point, which must be exactly 12 characters.

**Error Message** The configuration name you entered is already being used. Enter a unique name.

**Explanation** While creating a new profile, you entered a profile name on the Profile Management (General) window that already exists.

**Recommended Action** Enter a new profile name.

**Error Message** 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?

**Explanation** The client adapter's authentication attempt failed because a valid PAC was not found. ADU matches the username and server name that it is trying to use with those in the PAC. If they do not match or the configured PAC does not exist, ADU searches the private and global stores. If a matching PAC is found, the user is prompted with this message before the PAC is used.

**Recommended Action** Click **Yes** to attempt to authenticate using another PAC on your system without having to reconfigure your profile.

**Error Message** The device may not be present or could have been ejected/unplugged from the system. Insert or reinsert it now.

**Explanation** You attempted to install the client adapter software without the adapter being inserted into your computer.

**Recommended Action** 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 the [“Manually Installing or Upgrading the Client Adapter Driver”](#) section on page 9-6 for instructions.

**Error Message** The driver files you wish to remove will not be removed as the corresponding card is not inserted.

**Explanation** You attempted to uninstall the client adapter software without the adapter being inserted into your computer.

**Recommended Action** Insert the client adapter and click **OK**.

**Error Message** The EAP-FAST auto provisioning or PAC updating failed. The current profile is disabled until you correct the PAC configuration in the profile and reauthenticate.

**Explanation** PAC provisioning has failed. No PAC has been provisioned, and the profile is disabled.

**Recommended Action** Try again to authenticate using the existing profile. If automatic PAC provisioning is enabled, make sure to allow a PAC to be provisioned if prompted. If the authentication attempt fails again, modify the profile's PAC configuration settings.



**Error Message** The entered password was incorrect. Please try again.

**Explanation** You incorrectly entered the PAC file password.

**Recommended Action** Carefully re-enter the PAC file password.

**Error Message** The imported PAC already exists on your local machine. Do you want to update it anyway?

**Explanation** You tried to import a PAC file with the same PAC ID as a previously imported PAC file.

**Recommended Action** Click **Yes** to replace the existing PAC with the new one from the imported file or click **No** to cancel the operation.

**Error Message** The new password must be different from the old password.

**Explanation** You entered your old EAP-FAST password in the New Password and/or Verify New Password fields on the Please Change Password window.

**Recommended Action** Enter your new EAP-FAST password in the New Password and/or Verify New Password fields on the Please Change Password window.

**Error Message** The Passphrase must be between 8 and 64 characters.

**Explanation** The WPA/WPA2 passphrase that you entered on the Define WPA/WPA2 Pre-Shared Key window did not contain the correct number of characters.

**Recommended Action** Enter a WPA/WPA2 passphrase with 8 to 63 ASCII text characters or 64 hexadecimal characters.

**Error Message** The password is empty. Please enter a password.

**Explanation** You chose the Use Saved User Name and Password option on the LEAP or EAP-FAST Settings window but did not enter a password, or you did not enter a password on the Enter Wireless Network Password window.

**Recommended Action** Enter your LEAP or EAP-FAST password in the Password field.

**Error Message** The passwords you entered do not match. Please enter them again.

**Explanation** The passwords that you entered in the Password and Confirm Password fields on the LEAP or EAP-FAST Settings window do not match.

**Recommended Action** Re-enter your LEAP or EAP-FAST password in both fields.

**Error Message** The profile will be disabled until you select the Reauthentication option, Windows restarts, or the card is ejected and reinserted. Are you sure?

**Explanation** The username and password for your current profile have expired or are no longer valid. When the Enter Network Password window appeared, prompting you to enter your new username and password, you chose Cancel. The profile was disabled to prevent accidental authentication attempts in the future.

**Recommended Action** Click **No**, enter your username and password when the Enter Wireless Network Password window reappears, and click **OK**. The client adapter should authenticate using your new credentials. If the profile uses saved credentials, edit the profile in ADU by changing the username and password on the LEAP or EAP-FAST Settings window and save your changes. (If you click **Yes**, the profile is disabled until you choose Reauthenticate from ASTU or the Action drop-down menu in ADU, reboot your system, or eject and reinsert the card.)

**Error Message** The specified path does not exist. Please enter another path.

**Explanation** You chose the **Make Driver Installation Diskette(s)** option during installation, but a diskette was not inserted in the computer's A: drive.

**Recommended Action** Insert a floppy diskette into your computer's floppy disk drive, and choose the **Make Driver Installation Diskette(s)** option again.

**Error Message** The user name is empty. Please enter a user name.

**Explanation** You chose the Use Saved User Name and Password option on the LEAP or EAP-FAST Settings window but did not enter a username, or you did not enter a username on the Enter Wireless Network Password window.

**Recommended Action** Enter your LEAP or EAP-FAST username in the User Name field.

**Error Message** This Device is controlled by the Windows XP Automatic Wireless Network Configuration. It may override Network Name, Security and other settings from this profile.

**Explanation** You attempted to activate ADU while the Microsoft Wireless Configuration Manager in Windows XP was enabled. When a message appeared asking if you wanted to disable the Microsoft configuration manager, you chose No.

**Recommended Action** If you want to use ADU to configure your client adapter, disable the Microsoft Wireless Configuration Manager.

**Error Message** This Product does not support this version of Windows. Please check the product documentation for the system requirements.

**Explanation** You tried to install the CB21AG and PI21AG client adapter software on an unsupported Windows operating system.

**Recommended Action** Install the CB21AG and PI21AG client adapter software on a computer running Windows 2000 or XP.

**Error Message** Unable to authenticate wireless user. Please make sure you have entered the right user name and password and try again. If you are using an old PAC with this profile and have not logged on to the network for a long period of time, you may also want to make sure the PAC you are using is not expired by either import a new PAC manually or delete the old PAC if auto provisioning is enabled.

**Explanation** The client adapter's authentication attempt failed either because the wrong user credentials were entered or the profile is using an old PAC.

**Recommended Action** Try to authenticate again using the existing profile. Make sure to enter your username and password correctly. If the authentication attempt fails again, import a new PAC or delete the old PAC if automatic PAC provisioning is enabled.

**Error Message** Unable to copy PAC data. Make sure you have access rights.

**Explanation** Your attempt to copy a PAC from the private store to the global store failed. You may not have the necessary permissions.

**Recommended Action** Try again. If your second attempt fails, contact your system administrator.

**Error Message** Unable to delete the PAC from the local system.

**Explanation** Your attempt to delete a PAC failed.

**Recommended Action** Try again. If your second attempt fails, contact your system administrator.

**Error Message** Unable to EAP-FAST authenticate the wireless user in the specified amount of time. Network infrastructure might be down. You may also want to increase the timeout value for this profile.

**Explanation** The client adapter was unable to EAP-FAST authenticate within the amount of time specified by the EAP-FAST authentication timeout value.

**Recommended Action** Try again to authenticate using the existing profile. If automatic PAC provisioning is enabled, make sure to allow a PAC to be provisioned if prompted. If the authentication attempt fails again, increase the authentication timeout value on the EAP-FAST Settings window and try again.

**Error Message** Unable to save imported PAC data. Access denied.

**Explanation** Your attempt to save an imported PAC file has failed. You may not have the necessary permissions.

**Recommended Action** Try again. If your second attempt fails, contact your system administrator.

**Error Message** WEP Key x must be y characters long. Please enter z more characters.

**Explanation** You entered an incomplete static WEP key on the Define Pre-Shared Keys window and clicked **OK**.

**Recommended Action** Re-enter the static WEP key, making sure to enter the correct number of characters and click **OK**.

**Error Message** 'x' is not a hexadecimal character.

**Explanation** The character you entered on the Define Pre-Shared Keys window is not a hexadecimal character.

**Recommended Action** Re-enter the static WEP key following the guidelines in the [“Enabling Static WEP” section on page 5-26](#).

**Error Message** You are not registered with the authentication server. A security credential is required to register this device. Do you want to obtain a security credential?

**Explanation** Automatic PAC provisioning is enabled for this profile. However, a valid PAC matching the server to which the client adapter is connecting could not be found.

**Recommended Action** Click **Yes** to provision a new PAC for this server using your existing credentials or click **No** to cancel the operation. If you click **No**, the client adapter is unable to authenticate using the existing profile.

**Error Message** You can have only one SSID in an Ad Hoc Network. The SSID selections on the General Page will be adjusted.

**Explanation** You chose the Ad Hoc option on the Profile Editor (Advanced) window when multiple SSIDs were specified on the Profile Editor (General) window.

**Recommended Action** Click **OK**. Only SSID1 now appears on the Profile Editor (General) window. If you want to specify multiple SSIDs, choose **Infrastructure** for the Network Type parameter on the Profile Editor (Advanced) window.

**Error Message** You can have only one SSID in a WPA Passphrase network. The other SSIDs on the General tab will be disabled. Do you want to continue?

**Explanation** You chose the WPA/WPA2 Passphrase security option on the Profile Management (Security) window when multiple SSIDs were specified on the Profile Management (General) window.

**Recommended Action** Click **Yes** to allow SSID2 and SSID3 to be disabled for this profile or click **No** to cancel the operation.

**Error Message** You chose not to copy your private PAC. If you experience wireless connection problems during Windows domain logon or logged off stage, you must reconfigure the profile to use a global PAC.

**Explanation** When you were prompted to copy your PAC to the global store so that it will be available when you are not logged on, you clicked No.

**Recommended Action** The profile will use the private PAC for authentication. However, if you experience any wireless connection problems, you may need to reconfigure your profile to use a global PAC.

**Error Message** You do not have a valid Protected Access Credentials (PAC), the PAC you provided does not match the authentication server, or the PAC is expired. You may proceed with authenticating if the server supports auto provisioning. Do you want to proceed and accept auto provisioning?

**Explanation** You activated an EAP-FAST profile that is configured for automatic PAC provisioning and does not specify a PAC authority for which you have a current valid PAC.

**Recommended Action** If you want to attempt to auto-provision a PAC from the server, click **Yes**. Otherwise, click **No**. If you choose No, a message appears indicating that the client adapter was unable to EAP-FAST authenticate.

**Error Message** You failed to change your EAP-FAST domain/network password. Make sure you enter a new password that complies with the password policy and try again. Do you want to retry now?

**Explanation** An error occurred when you attempted to change your EAP-FAST password.

**Recommended Action** Click **Yes** to try again. When the Enter Wireless Network Password window appears, enter your new password. Otherwise, click **No** to cancel the operation.

**Error Message** You have just changed your network password. You must change your saved password settings in the EAP-FAST profiles before connecting again.

**Explanation** Your network password has changed.

**Recommended Action** Update your EAP-FAST password on the EAP-FAST Settings window for any EAP-FAST profiles that are configured with a saved username and password.

**Error Message** You must configure the PEAP-GTC settings properly. User information, password, or machine information is incomplete.

**Explanation** You improperly configured a PEAP (EAP-GTC) profile.

**Recommended Action** Modify the profile's configuration settings, making sure to enter all necessary information.

**Error Message** You must define a certificate to use EAP-TLS. Click Configure to select a certificate.

**Explanation** You chose the EAP-TLS option on the Profile Management (Security) window and clicked **OK** without selecting a certificate.

**Recommended Action** Click **Configure** and select a certificate on the Define Certificate window.

**Error Message** You must enter a valid login name to use EAP-TLS. Click Configure to enter a login name.

**Explanation** You chose the EAP-TLS option on the Profile Management (Security) window and clicked **OK** without entering your EAP-TLS login name.

**Recommended Action** Click **Configure** and enter your EAP-TLS login name on the Define Certificate window.

**Error Message** You must enter the correct old password in order to change the new password.

**Explanation** You incorrectly entered your old EAP-FAST password on the Please Change Password window.

**Recommended Action** Carefully re-enter your old EAP-FAST password on the Please Change Password window.

**Error Message** You must select a PAC or enable Allow Automatic PAC Provisioning.

**Explanation** While configuring a profile for EAP-FAST, you did not enable automatic PAC provisioning or select a PAC authority from the drop-down list on the EAP-FAST Settings window.

**Recommended Action** Choose a PAC authority from the drop-down list on the EAP-FAST Settings window. If the list is empty, import a PAC file.

**Error Message** You must select a Passphrase to use WPA/WPA2.

**Explanation** You chose the WPA/WPA2 Passphrase option on the Profile Management (Security) window and clicked **OK** without entering a passphrase.

**Recommended Action** Enter a WPA/WPA2 passphrase on the Define WPA/WPA2 Pre-Shared Key window.

**Error Message** You must set at least one Pre-Shared Key.

**Explanation** You chose the Pre-Shared Key (Static WEP) option on the Profile Management (Security) window and clicked **OK** without entering a static WEP key.

**Recommended Action** Enter a static WEP key on the Define Pre-Shared Keys window and then click **OK**.

**Error Message** Your security setting is invalid for an Ad Hoc network. If you want, security will be disabled for you. You can also configure security to Pre-shared keys. Do you want to disable security?

**Explanation** Pre-Shared Key (Static WEP) is the only valid security option for an ad hoc network. You chose Ad Hoc for Network Type on the Profile Management (Advanced) window when a security option other than static WEP was already selected.

**Recommended Action** If you want to configure this profile for use in an ad hoc network, click **Yes** to disable security. Otherwise, click **No**.

**Error Message** You selected a private PAC for EAP-FAST authentication. It may not be accessible when the user is logged off or during the domain logon process. Confirm if you want to copy the selected PAC into the global PAC store.

**Explanation** You selected a private PAC and the No Network Connection Unless User Is Logged In check box is unchecked. Therefore, the PAC may not be accessible during domain logon or when you are logged off.

**Recommended Action** If you want a copy of the PAC to be added to the global store so that it will be available when you are not logged on, click **Yes**. If you do not want a copy of the PAC to be added to the global store, click **No**.



## Technical Specifications

---

This appendix provides technical specifications for the Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters.

The following topics are covered in this appendix:

- Physical Specifications, [page A-26](#)
- Radio Specifications, [page A-27](#)
- Power Specifications, [page A-30](#)
- Safety and Regulatory Compliance Specifications, [page A-30](#)



Table A-1 lists the technical specifications for the Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters.

**Table A-1 Technical Specifications for CB21AG and PI21AG Client Adapters**

<b>Physical Specifications</b>	
Size	
PC-Cardbus card	4.5 in. L x 2.1 in. W x 0.2 in. H (11.3 cm L x 5.4 cm W x 0.5 cm H)
PCI card	
Standard PCI card	4.7 in. L x 0.7 in. W x 4.8 in. H (12 cm L x 1.8 cm W x 12.1 cm H)
Low-profile PCI card	4.7 in. L x 0.7 in. W x 3.1 in. H (12 cm L x 1.8 cm W x 7.9 cm H)
Weight	
PC-Cardbus card	1.55 oz (44 g)
PCI card	
Standard PCI card with antenna	3.6 oz (103 g)
Standard PCI card without antenna	1.9 oz (55 g)
Low-profile PCI card with antenna	3.5 oz (98 g)
Low-profile PCI card without antenna	1.7 oz (49 g)
Enclosure	
PC-Cardbus card	Type II Cardbus
PCI card	Standard or low-profile Type II PCI
Connector	
PC-Cardbus card	68-pin Cardbus
PCI card	62-pin PCI
Status indicators	Green and amber LEDs; see <a href="#">Chapter 10</a>
Operating temperature	32°F to 158°F (0°C to 70°C)
Storage temperature	32°F to 185°F (0°C to 85°C)
Humidity (non-operational)	90% relative humidity
ESD	15 kV (human body model)

Table A-1 Technical Specifications for CB21AG and PI21AG Client Adapters (continued)

Radio Specifications	
Type	
802.11a	Orthogonal frequency division multiplexing (OFDM)
802.11b/g	Direct-sequence spread spectrum (DSSS) and orthogonal frequency division multiplexing (OFDM)
Power output	
<b>Note</b> Refer to <a href="#">Appendix D</a> for limitations on radiated power (EIRP) levels in the European community and other countries.	
802.11a	40 mW (16 dBm) @ 6, 9, 12, 18, 24 Mbps 25 mW (14 dBm) @ 6, 9, 12, 18, 24, 36 Mbps 20 mW (13 dBm) @ 6, 9, 12, 18, 24, 36, 48, 54 Mbps 13 mW (11 dBm) @ 6, 9, 12, 18, 24, 36, 48, 54 Mbps 10 mW (10 dBm) @ 6, 9, 12, 18, 24, 36, 48, 54 Mbps <b>Note</b> The maximum power setting varies according to individual country regulations.
802.11b/g	100 mW (20 dBm) @ 1, 2, 5.5, 11 Mbps 63 mW (18 dBm) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24 Mbps 50 mW (17 dBm) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36 Mbps 30 mW (15 dBm) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 Mbps 20 mW (13 dBm) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps 10 mW (10 dBm) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps <b>Note</b> The maximum power setting varies according to individual country regulations.
Operating frequency	
802.11a	5.15 to 5.25 GHz in the UNII 1 band* 5.25 to 5.35 GHz in the UNII 2 band* 5.470 to 5.725 GHz in the European band 5.725 to 5.825 GHz in the UNII 3 band* *Depending on the regulatory domain in which the client adapter is used
802.11b/g	2.400 to 2.497 GHz (depending on the regulatory domain in which the client adapter is used)
Usable channels	
802.11a	5170 to 5320 MHz, 5500 to 5700 MHz, and 5745 to 5805 MHz
802.11b/g	2412 to 2484 MHz in 5-MHz increments
Data rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps
Modulation	Differential binary phase shift keying (DBPSK) - 1 Mbps Differential quaternary phase shift keying (DQPSK) - 2 Mbps Complementary code keying (CCK) - 5.5 and 11 Mbps Binary phase shift keying (BPSK) - 6 and 9 Mbps Quaternary phase shift keying (QPSK) - 12 and 18 Mbps 16-quadrature amplitude modulation (16-QAM) - 24 and 36 Mbps 64-quadrature amplitude modulation (64-QAM) - 48 and 54 Mbps

**Table A-1** Technical Specifications for CB21AG and PI21AG Client Adapters (continued)

Receiver sensitivity	
802.11a	<p><b><u>5150 to 5250 MHz</u></b>            –87 dBm @ 6, 9, 12, and 18 Mbps            –82 dBm @ 24 Mbps            –79 dBm @ 36 Mbps            –74 dBm @ 48 Mbps            –72 dBm @ 54 Mbps</p> <p><b><u>5250 to 5350 MHz</u></b>            –89 dBm @ 6, 9, and 12 Mbps            –85 dBm @ 18 Mbps            –82 dBm @ 24 Mbps            –79 dBm @ 36 Mbps            –74 dBm @ 48 Mbps            –72 dBm @ 54 Mbps</p> <p><b><u>5470 to 5725 MHz</u></b>            –87 dBm @ 6, 9, 12, and 18 Mbps            –82 dBm @ 24 Mbps            –79 dBm @ 36 Mbps            –74 dBm @ 48 Mbps            –72 dBm @ 54 Mbps</p> <p><b><u>5725 to 5805 MHz</u></b>            –84 dBm @ 6, 9, and 12 Mbps            –83 dBm @ 18 Mbps            –82 dBm @ 24 Mbps            –79 dBm @ 36 Mbps            –72 dBm @ 48 Mbps            –65 dBm @ 54 Mbps</p>
802.11b/g	–94 dBm @ 1 Mbps –93 dBm @ 2 Mbps –92 dBm @ 5.5 Mbps –90 dBm @ 11 Mbps –86 dBm @ 6, 9, 12, and 18 Mbps –84 dBm @ 24 Mbps –80 dBm @ 36 Mbps –75 dBm @ 48 Mbps –71 dBm @ 54 Mbps

**Table A-1** Technical Specifications for CB21AG and PI21AG Client Adapters (continued)

Receiver delay spread (multipath)		
802.11a/g	400 ns @ 6 Mbps 250 ns @ 9 and 12 Mbps 220 ns @ 18 Mbps 160 ns @ 24 Mbps 100 ns @ 36 Mbps 90 ns @ 48 Mbps 70 ns @ 54 Mbps	
802.11b	350 ns @ 1 Mbps 300 ns @ 2 Mbps 200 ns @ 5.5 Mbps 130 ns @ 11 Mbps	
Range		
802.11a	<b>Indoor (typical)</b> 500 ft (152 m) @ 6 Mbps 400 ft (122 m) @ 18 Mbps 90 ft (27 m) @ 54 Mbps	<b>Outdoor (typical)</b> 950 ft (290 m) @ 6 Mbps 800 ft (244 m) @ 18 Mbps 170 ft (52 m) @ 54 Mbps
	<b>Note</b> The above range numbers assume that the client adapter is being used at maximum transmit power with a Cisco Aironet 1232AG Access Point with a 3.5-dBi dipole antenna. Different range characteristics are likely when using the client adapter with a different access point or a Cisco Aironet 1200 Series Access Point with a different antenna.	
802.11b/g	<b>Indoor (typical)</b> 410 ft (125 m) @ 1 Mbps 300 ft (91 m) @ 6 Mbps 220 ft (67 m) @ 11 Mbps 180 ft (55 m) @ 18 Mbps 90 ft (27 m) @ 54 Mbps	<b>Outdoor (typical)</b> 700 ft (213 m) @ 1 Mbps 650 ft (198 m) @ 6 Mbps 490 ft (149 m) @ 11 Mbps 400 ft (122 m) @ 18 Mbps 110 ft (34 m) @ 54 Mbps
	<b>Note</b> The above range numbers assume that the client adapter is being used at maximum transmit power with a Cisco Aironet 1232AG Access Point with a 2.2-dBi dipole antenna. Different range characteristics are likely when using the client adapter with a different access point or a Cisco Aironet 1200 Series Access Point with a different antenna.	
Antennas		
PC-Cardbus card	Integrated 0-dBi dual-band 2.4/5-GHz diversity antenna	
PCI card	1-dBi dual-band 2.4/5-GHz antenna, permanently attached by 6.6-ft (2-m) cable	

**Table A-1** Technical Specifications for CB21AG and PI21AG Client Adapters (continued)

<b>Power Specifications</b>	
Operational voltage	3.3 V ( $\pm 0.3$ V)
Receive current steady state	
802.11a	318 mA maximum
802.11b	327 mA maximum
802.11g	282 mA maximum
Transmit current steady state	
802.11a	554 mA maximum
802.11b	539 mA maximum
802.11g	530 mA maximum
Sleep mode steady state	203 mA average
<b>Safety and Regulatory Compliance Specifications</b>	
Safety	Designed to meet: <ul style="list-style-type: none"> <li>• UL 60950</li> <li>• CSA 22.2 No. 60950</li> <li>• IEC 60950 Second Ed., including Amendments 1-4 with all national deviations</li> <li>• EN 60950 Second Ed., including Amendments 1-4</li> </ul>
EMI and susceptibility	FCC Part 15.107 & 15.109 Class B ICES-003 Class B (Canada) VCCI (Japan) EN 301.489-1 and EN-301.489-17 (Europe)
Radio approvals	FCC Part 15.247 FCC Part 15.401-15.407 Canada RSS-210 Europe EN-300.328, EN-301.893 ARIB STD-33, ARIB STD-66, ARIB STD-T71 (Japan) AS 4268.2 (Australia) AS/NZS 3548 (Australia and New Zealand)
RF exposure	FCC Bulletin OET-65C Industry Canada RSS-102



## Translated Safety Warnings

---

This appendix provides translations of the safety warnings that appear in this publication. The second warning pertains to the PI21AG client adapter, and the third warning pertains to the CB21AG client adapter.

The following topics are covered in this appendix:

- [Explosive Device Proximity Warning, page B-32](#)
- [Antenna Installation Warning, page B-33](#)
- [Warning for Laptop Users, page B-34](#)

# Explosive Device Proximity Warning



**Warning**

Do not operate your wireless network device near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.

**Waarschuwing**

Gebruik dit draadloos netwerkapparaat alleen in de buurt van onbeschermde ontstekers of in een omgeving met explosieven indien het apparaat speciaal is aangepast om aan de eisen voor een dergelijk gebruik te voldoen.

**Varoitus**

Älä käytä johdotonta verkkolaitetta suojaamattomien räjäytysnallien läheisyydessä tai räjäytysalueella, jos laitetta ei ole erityisesti muunnettu sopivaksi sellaiseen käyttöön.

**Attention**

Ne jamais utiliser un équipement de réseau sans fil à proximité d'un détonateur non blindé ou dans un lieu présentant des risques d'explosion, sauf si l'équipement a été modifié à cet effet.

**Warnung**

Benutzen Sie Ihr drahtloses Netzwerkgerät nicht in der Nähe ungeschützter Sprengkapseln oder anderer explosiver Stoffe, es sei denn, Ihr Gerät wurde eigens für diesen Gebrauch modifiziert und bestimmt.

**Avvertenza**

Non utilizzare la periferica di rete senza fili in prossimità di un detonatore non protetto o di esplosivi a meno che la periferica non sia stata modificata a tale proposito.

**Advarsel**

Ikke bruk den trådløse nettverksenheten nært inntil uisolerte fenghetter eller i et eksplosivt miljø med mindre enheten er modifisert slik at den tåler slik bruk.

**Aviso**

Não opere o dispositivo de rede sem fios perto de cápsulas explosivas não protegidas ou num ambiente explosivo, a não ser que o dispositivo tenha sido modificado para se qualificar especialmente para essa utilização.

**¡Advertencia!**

No utilizar un aparato de la red sin cable cerca de un detonador que no esté protegido ni tampoco en un entorno explosivo a menos que el aparato haya sido modificado con ese fin.

**Varning!**

Använd inte den trådlösa nätverksenheten i närheten av oskyddade tändhattar eller i en explosiv miljö om inte enheten modifierats för att kunna användas i sådana sammanhang.

# Antenna Installation Warning


**Warning**

In order to comply with FCC radio frequency (RF) exposure limits, antennas should be located at a minimum of 7.9 inches (20 cm) or more from the body of all persons.

**Waarschuwing**

Om te voldoen aan de FCC radiofrequentie (RF) blootstellingslimieten dienen antennes zich minstens 20 cm of meer van de lichamen van alle personen bevinden.

**Varoitus**

FCC:n antamien radiotaajuuksille altistumista koskevien rajoitusten mukaan antennien on sijaittava vähintään 20 cm:n päässä kaikista henkilöistä.

**Attention**

Pour se conformer aux limites d'exposition à la fréquence radio préconisées par la FCC (Federal Communications Commission), les antennes doivent se situer à un minimum de 20 cm de toute personne.

**Warnung**

Um die in den FCC-Richtlinien festgelegten Expositionshöchstgrenzen für Radiofrequenzen (RF) nicht zu überschreiten, sollten antennen mindestens 20 cm (7,9 Zoll) vom Körper aller Person entfernt aufgestellt werden.

**Avvertenza**

Per conformarsi ai limiti FCC di esposizione a radiofrequenza (RF), le antenne a devono stare ad una distanza minima di 20 cm dal corpo di ogni persona.

**Advarsel**

I henhold til eksponeringsgrensene for radiofrekvenser (RF), skal antenner befinne seg på en avstand av minst 20 cm eller mer fra mennesker.

**Aviso**

Para estar de acordo com as normas FCC de limites de exposição para frequência de rádio (RF), as antenas devem estar distantes no mínimo 20 cm (7,9 pol) do corpo de qualquer pessoa.

**¡Advertencia!**

Para cumplir con los límites de exposición de radio frecuencia (RF) de la Comisión Federal de Comunicaciones (FCC) es preciso ubicar las antenas a un mínimo de 20 cm (7,9 pulgadas) o más del cuerpo de las personas.

**Varning!**

För att följa FCC-exponeringsgränserna för radiofrekvens (RF), bör antenner placeras på minst 20 cm avstånd från alla människor.



# Warning for Laptop Users



## Warning

This device has been tested and complies with FCC RF Exposure (SAR) limits in typical laptop computer configurations and this device can be used in desktop or laptop computers with side mounted PC Card slots that can provide at least 0.394 in (1 cm) separation distance from the antenna to the body of the user or a nearby person. Thin laptop computers may need special attention to maintain antenna spacing while operating. This device cannot be used with handheld PDAs (personal digital assistants). Use in other configurations may not ensure compliance with FCC RF exposure guidelines. This device and its antenna must not be co-located or operated in conjunction with any other antenna or transmitter.

## Waarschuwing

Dit apparaat is getest en voldoet aan de FCC-beperkingen voor radiofrequentieblootstelling (SAR) bij standaardconfiguraties met een laptopcomputer. Dit apparaat kan worden gebruikt in desktop- of laptopcomputers met PC-kaartsleuven aan de zijkant, waarbij minimaal 1 cm afstand bestaat tussen de antenne en het lichaam van de gebruiker of een persoon in de buurt. Bij smalle laptopcomputers is mogelijk extra aandacht vereist om tijdens gebruik voldoende afstand tot de antenne te houden. Dit apparaat kan niet worden gebruikt in combinatie met mobiele PDA's (personal digital assistants; persoonlijke digitale assistenten). Als u dit apparaat gebruikt in andere configuraties, voldoet het wellicht niet meer aan de FCC-regelgeving met betrekking tot radiofrequentieblootstelling. Dit apparaat en de bijbehorende antenne mogen niet in combinatie met andere antennes of zenders worden gebruikt en ook niet in de buurt van andere antennes of zenders worden geplaatst.

## Varoitus

Tämä laite on testattu ja se noudattaa FCC:n määrittämiä radiotaajuussäteilylle altistumisen (SAR) raja-arvoja tyypillisissä kannettavien tietokoneiden kokoonpanoissa. Tätä laitetta voidaan käyttää pöytä- tai kannettavissa tietokoneissa, joiden sivussa on PC-korttipaikka. Korttipaikassa olevan laitteen antennin etäisyyden käyttäjästä tai lähellä olevasta henkilöstä on oltava vähintään yksi senttimetri. Ohuita kannettavia tietokoneita on ehkä tarkkailtava erityisesti, jotta käyttäjän etäisyys antenniin olisi riittävä käytön aikana. Tätä laitetta ei voi käyttää yhdessä kämmentietokoneiden (PDA) kanssa. Jos laitetta käytetään muunlaisissa kokoonpanoissa, se ei ehkä vastaa FCC:n määrittämiä radiotaajuussäteilylle altistumisen ohjearvoja. Tätä laitetta ja sen antennia ei saa käyttää samassa pisteessä toisen antennin tai lähettimen kanssa tai liitettynä toiseen antenniin tai lähettimeen.

## Attention

Cet appareil a été testé et respecte les limites (TAS - Taux d'absorption spécifique) d'exposition aux RF de la FCC relatives aux configurations standard des ordinateurs portables. Il peut être utilisé dans des ordinateurs de bureau ou portables dotés d'un emplacement pour carte PC latérales et peut fournir une distance de séparation d'au moins 1 cm entre l'antenne et le corps de l'utilisateur ou d'une personne avoisinante. Nous vous recommandons de porter une attention particulière lors de l'utilisation d'ordinateurs portatifs minces afin d'assurer le maintien de l'espacement de l'antenne. Cet appareil ne peut pas être utilisé avec des assistants numériques personnels de poche. L'utilisation dans d'autres configurations risque de ne pas être conforme aux lignes directrices de la FCC sur l'exposition aux RF. Cet appareil et son antenne ne doivent pas se trouver dans le même emplacement ou fonctionner conjointement avec une autre antenne ou un autre émetteur.

- Warnung** Dieses Gerät wurde getestet und entspricht den durch die FCC-Richtlinien festgelegten Grenzwerten für Hochfrequenzstrahlung (SAR) für reguläre Laptop-Computerkonfigurationen. Es kann für Desktop- oder Laptop-Computer mit seitlichem PC-Kartensteckplatz genutzt werden, wobei der Abstand der Antenne vom Benutzer oder anderen in der Nähe befindlichen Personen mindestens 1 cm betragen muss. Insbesondere bei schmalen Laptop-Computern sollte darauf geachtet werden, dass der Abstand während des Betriebs genau eingehalten wird. Dieses Gerät kann nicht für tragbare Handheld-Geräte/PDAs verwendet werden. Bei Verwendung in anderen Konfigurationen ist u.U. die Einhaltung der durch die FCC-Richtlinien festgelegten Grenzwerte für Hochfrequenzstrahlung nicht gewährleistet. Dieses Gerät und die Antenne dürfen nicht zusammen mit anderen Antennen oder Übertragungsgeräten installiert oder verwendet werden.
- Avvertenza** Questo dispositivo è stato testato ed è conforme alle norme sulle emissioni radio (SAR) nelle configurazione tipica di computer portatile. Questo dispositivo può essere utilizzato in desktop o computer portatili con slot per scheda PC laterale che garantisca un minimo spazio di 1 cm (0,394 pollici) tra l'antenna e l'utente o qualsiasi persona nelle vicinanze. I computer portatili sottili richiedono particolare attenzione al mantenimento dello spazio minimo quando in funzione. Questo dispositivo non può essere utilizzato con computer palmari (PDA). L'utilizzo in configurazione differenti non assicura la conformità alle norme sulle emissioni radio. Questo dispositivo e la propria antenna non devono operare congiuntamente ad altre antenne o trasmettitori.
- Advarsel** Denne enheten er testet og overholder grensene for FCC RF-eksponering (SAR) i vanlige konfigurasjoner for bærbare datamaskiner. Den kan brukes i stasjonære eller bærbare datamaskiner som har kortplass på siden, og der det er minst 1 cm avstand mellom antennen og brukeren eller andre personer. Ved bruk av flate bærbare PCer må du være ekstra påpasselig med antenneavstanden. Denne enheten kan ikke brukes sammen med håndholdte PDAer (personal digital assistant). Det er ikke sikkert at bruk i andre konfigurasjoner vil være i samsvar med retningslinjene for FCC RF-eksponering. Denne enheten og antennen må ikke plasseres på samme sted som eller brukes sammen med andre antenner eller sendere.
- Aviso** Este dispositivo foi testado e está em conformidade com os limites SAR de exposição a radiofrequência (RF) da Comissão Federal de Comunicações (FCC), em configurações típicas de portátil, e pode ser utilizado em computadores de secretária ou portáteis com ranhuras de placa PC laterais que permitem um distanciamento mínimo de 1cm. entre a antena e o corpo do utilizador ou de alguém que esteja por perto. Os portáteis finos necessitam de uma atenção especial para manter a distância da antena durante o funcionamento. Este dispositivo não pode ser utilizado com PDAs (personal digital assistants) de mão. A utilização noutras configurações pode não assegurar a conformidade com as directrizes de exposição a radiofrequência (RF) da Comissão Federal de Comunicações (FCC). Este dispositivo e a respectiva antena não devem ser colocados nem postos a funcionar com outras antenas ou transmissores.
- ¡Advertencia!** El dispositivo ha sido probado y cumple los límites de la FCC sobre exposición a radiofrecuencia (SAR o tasa de absorción específica) en cualquier configuración tradicional de equipos portátiles. Además, puede utilizarse en equipos de escritorio o portátiles que cuenten con ranuras de tarjeta PC laterales a una distancia de, al menos, 1 cm (0,394 pulgadas) de la antena al usuario o persona más cercana. Puede que los equipos portátiles de menor grosor requieran atención especial a la hora de mantener la distancia de la antena al utilizarlos. No puede utilizarse este dispositivo con equipos digitales personales portátiles (PDA). Su utilización en otras configuraciones no garantiza el cumplimiento de las directivas de la FCC sobre exposición a radiofrecuencia. Este dispositivo y la antena no deben situarse o accionarse junto con otra antena o transmisor.

**Varning!** Den här enheten har testats och följer FCC-gränserna för radiofrekvensexponering (SAR) i vanliga konfigurationer för bärbara datorer. Den kan användas i stationära eller bärbara datorer med sidmonterade PC-kortöppningar som kan tillhandahålla minst 1 cm med separationsavstånd mellan antennen och användarens kropp eller annan person i närheten. Tunna, bärbara datorer kan behöva speciell uppmärksamhet för att upprätthålla antenntavståndet under användning. Den här enheten kan inte användas med handdator/PDA. Vid användning i andra konfigurationer går det inte att garantera att FCC:s riktlinjer för radiofrekvens följs. Den här enheten och dess antenn får inte placeras tillsammans med eller användas i samband med någon annan antenn eller sändare/mottagare.

**Figyelem** Az eszköz tesztelésen esett át, melynek eredményeként megfelel az FCC RF-sugárzási (SAR) korlátozásainak tipikus laptop-konfigurációk esetén. Az eszköz beszerelhető asztali és laptop számítógépekben lévő, oldalra szerelt PC-kártya csatlakozókba, amennyiben legalább 1 cm távolság van az antenna és a felhasználó vagy egy közeli személy teste között. Vékony laptop számítógépek esetén különösen ügyelni kell használat közben az antennától való távolság betartására. Az eszköz nem használható kézi PDA-kkal (személyi digitális asszisztensekkel). Más konfigurációk esetén előfordulhat, hogy az eszköz nem felel meg az FCC RF-sugárzási előírásainak. Az eszközt és annak antennáját nem szabad más antennával vagy adó-vevővel egy helyen elhelyezni vagy üzemeltetni.

**Предупреждение** Это устройство протестировано и признано соответствующим ограничениям FCC, касающимся высокочастотного излучения (SAR), для обычных конфигураций портативных компьютеров. Оно может использоваться на переносных или портативных компьютерах с боковыми гнездами для плат PC, которые обеспечивают зазор не менее 0,394 дюйма (1 см) между антенной и телом пользователя или другого лица, находящегося в непосредственной близости. Возможно, потребуется соблюдать особую осторожность при обеспечении зазора антенны в тонких портативных компьютерах. Это устройство нельзя использовать для карманных компьютеров. Использование в других конфигурациях не может гарантировать соответствие директивам FCC, касающимся высокочастотного излучения. Это устройство и его антенну нельзя располагать рядом или использовать совместно с другой антенной или передатчиком.

**警告** 将本设备用于典型膝上型计算机配置已经过测试并且符合 FCC RF 辐射暴露 (SAR) 限制; 本设备可用于侧面安装有 PC 卡插槽的台式计算机或膝上型计算机, 该插槽可确保用户或周围的人与天线至少相距 0.394 英寸 (1 厘米)。使用超薄膝上型计算机时, 可能需要特别注意在操作过程中与天线保持一定距离。本设备不能与手持式 PDA (个人数字助理) 一起使用。在其他配置中使用本设备可能无法确保符合 FCC RF 辐射暴露限制规定。禁止将本设备及其天线与任何其他天线或发射器安装在一起或同时使用。

**警告** この機器は既にテスト済みで、一般的なラップトップ コンピュータの構成における米国 FCC (連邦通信委員会) の無線周波 (RF) 照射 (SAR) 制限値に準拠しています。この機器は、デスクトップ コンピュータもしくは本体側面に PC カード スロットを備えたラップトップ コンピュータでの使用が可能です。いずれのコンピュータの場合も、アンテナと人体との間に、最低 1 cm の距離があることが前提です。薄型のラップトップ コンピュータの場合は、操作中アンテナとのスペースを維持するため、特別な注意が必要になることがあります。この機器は、ハンドヘルド式の PDA (携帯情報端末) には使用できません。他の配置構成での使用は、FCC の無線周波照射に関するガイドラインに準拠しない場合があります。この機器およびアンテナは、他のアンテナもしくはトランスミッタと同一の場所に配置したり、同時に使用してはなりません。



## Declarations of Conformity and Regulatory Information

---

This appendix provides declarations of conformity and regulatory information for the Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters.

The following topics are covered in this appendix:

- [Manufacturer's Federal Communication Commission Declaration of Conformity Statement, page C-38](#)
- [Department of Communications – Canada, page C-39](#)
- [European Community, Switzerland, Norway, Iceland, and Liechtenstein, page C-39](#)
- [Declaration of Conformity for RF Exposure, page C-43](#)
- [Guidelines for Operating Cisco Aironet Wireless LAN Client Adapters in Japan, page C-43](#)
- [Administrative Rules for Cisco Aironet Wireless LAN Client Adapters in Taiwan, page C-44](#)
- [Brazil/Anatel Approval, page C-45](#)

# Manufacturer's Federal Communication Commission Declaration of Conformity Statement



**Models:** AIR-CB21AG-A-K9, AIR-PI21AG-A-K9

**FCC Certification Number:** LDK102050 (CB21AG)  
LDK102051 (PI21AG)

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

This device complies with Part 15 rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

The CB21AG client adapter has been tested and complies with FCC RF Exposure (SAR) limits in typical laptop computer configurations, and this device can be used in laptop computers with side-mounted PCMCIA slots which can provide 0.394 in (1 cm) separation distance from the antenna to the body of the user or a nearby person. Thin laptop computers may need special attention to maintain antenna spacing while operating.

The PI21AG client adapter has been tested and complies with FCC RF Exposure (SAR) limits in typical desktop computer configurations. A separation distance of 7.9 in (20 cm) must be maintained between this device's antenna and the body of the user or a nearby person.

These devices cannot be used with handheld personal digital assistants (PDAs). Use in other configurations may not ensure compliance with FCC RF exposure guidelines. These devices and their antennas must not be co-located or operated in conjunction with any other antenna or transmitter.



**Caution**

---

The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using integrated antennas. Any changes or modification to the product not expressly approved by Cisco could void the user's authority to operate this device.

---



**Caution**

---

Within the 5.15-to-5.25-GHz band, UNII devices are restricted to indoor operations to reduce any potential for harmful interference to co-channel Mobile Satellite Systems (MSS) operations.

---

# Department of Communications – Canada

## Canadian Compliance Statement

This Class B Digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte les exigences du Règlement sur le matériel brouilleur du Canada.

This device complies with Class B Limits of Industry Canada. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters are certified to the requirements of RSS-210 for 2.4-GHz and 5-GHz devices. The use of these devices in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

## European Community, Switzerland, Norway, Iceland, and Liechtenstein

### Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC

English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Deutsch:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Dansk:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Español:	Este equipo cumple con los requisitos esenciales así como con otras disposiciones de la Directiva 1999/5/EC.
Ελληνικά:	Αυτός ο εξοπλισμός συμμορφώνεται με τις ουσιώδεις απαιτήσεις και τις λοιπές διατάξεις της Οδηγίας 1999/5/EK.
Français:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska:	Þessi búnaður samrýmist lögboðnum kröfum og öðrum ákvæðum tilskipunar 1999/5/ESB.
Italiano:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/EC.

Nederlands:	Deze apparatuur voldoet aan de belangrijkste eisen en andere voorzieningen van richtlijn 1999/5/EC.
Norsk:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EC.
Português:	Este equipamento satisfaz os requisitos essenciais e outras provisões da Directiva 1999/5/EC.
Suomalainen:	Tämä laite täyttää direktiivin 1999/5/EY oleelliset vaatimukset ja on siinä asetettujen muidenkin ehtojen mukainen.
Svenska:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

The Declaration of Conformity related to this product can be found at the following URL:

<http://www.ciscofax.com>

The following standards were applied:

- Radio: EN 300.328-1, EN 300.328-2 (2.4-GHz operation);  
EN 301.893 (5-GHz operation)
- EMC: EN 301.489-1, EN 301.489-17
- Safety: EN 60950

The following CE mark is affixed to the Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters:



**Note**

This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. For more details, contact your customer service representative.

# Declaration of Conformity Statement

## Cisco Aironet CB21AG Wireless LAN Client Adapter



### DECLARATION OF CONFORMITY with regard to the R&TTE Directive 1999/5/EC according to EN 45014

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

Declare under our sole responsibility that the product,

*AIR-CB21AG-E-K9 / Cisco Aironet 802.11a/b/g Wireless CardBus Adapter*

Fulfills the essential requirements of the Directive 1999/5/EC.

The following standards were applied:

<b>EMC</b>	<b>EN 301.489-1 v1.4.1: 2002-08; EN 301.489-17 v1.2.1: 2002-04</b>
<b>Health &amp; Safety</b>	<b>EN60950: 2000</b>
<b>Radio</b>	<b>EN 300 328 v1.4.1: 2003-04 EN 301.893 v1.2.3: 2003-08</b>

The conformity assessment procedure referred to in Article 10.4 and Annex III of Directive 1999/5/EC has been followed.

The product carries the CE Mark:



Date & Place of Issue: 1 January 2004, San Jose

Signature:

A handwritten signature in black ink that reads "Tony Youssef".

**Tony Youssef**  
Director Corporate Compliance  
125 West Tasman Drive  
San Jose, CA 95134 - USA

*DofC 340347*



**Cisco Aironet PI21AG Wireless LAN Client Adapter**

**DECLARATION OF CONFORMITY**  
 with regard to the R&TTE Directive 1999/5/EC  
 according to EN 45014

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

Declare under our sole responsibility that the product,

*AIR-PI21AG-E-K9 / Cisco Aironet 802.11a/b/g Wireless PCI Adapter*

Fulfills the essential requirements of the Directive 1999/5/EC.

The following standards were applied:

**EMC**                    **EN 301.489-1 v1.4.1: 2002-08; EN 301.489-17 v1.2.1: 2002-04**

**Health & Safety**   **EN60950: 2000**

**Radio**                **EN 300 328 v1.4.1: 2003-04**  
                              **EN 301.893 v1.2.3: 2003-08**

The conformity assessment procedure referred to in Article 10.4 and Annex III of Directive 1999/5/EC has been followed.

The product carries the CE Mark:



Date & Place of Issue:        1 January 2004, San Jose

Signature:

A handwritten signature in black ink that reads "Tony Youssef".

**Tony Youssef**  
 Director Corporate Compliance  
 125 West Tasman Drive  
 San Jose, CA 95134 - USA

*DofC 340350*

# Declaration of Conformity for RF Exposure

The radio module has been evaluated under FCC Bulletin OET 65C and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices.

## Guidelines for Operating Cisco Aironet Wireless LAN Client Adapters in Japan

This section provides guidelines for avoiding interference when operating Cisco Aironet Wireless LAN Client Adapters in Japan. These guidelines are provided in both Japanese and English.



Note

The use of 5-GHz devices is limited to indoor use in Japan.

### Japanese Translation

この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。

- 1 この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。
- 2 万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先にご連絡頂き、混信回避のための処置等(例えば、パーティションの設置など)についてご相談して下さい。
- 3 その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。

連絡先 : 03-5549-6500

43768

### English Translation

This equipment operates in the same frequency bandwidth as industrial, scientific, and medical devices such as microwave ovens and mobile object identification (RF-ID) systems (licensed premises radio stations and unlicensed specified low-power radio stations) used in factory production lines.

1. Before using this equipment, make sure that no premises radio stations or specified low-power radio stations of RF-ID are used in the vicinity.
2. If this equipment causes RF interference to a premises radio station of RF-ID, promptly change the frequency or stop using the device; contact the number below and ask for recommendations on avoiding radio interference, such as setting partitions.
3. If this equipment causes RF interference to a specified low-power radio station of RF-ID, contact the number below.

Contact Number: 03-5549-6500

# Administrative Rules for Cisco Aironet Wireless LAN Client Adapters in Taiwan

This section provides administrative rules for operating Cisco Aironet Wireless LAN Client Adapters in Taiwan. The rules are provided in both Chinese and English.

## 2.4- and 5-GHz Client Adapters

### Chinese Translation

#### 低功率電波輻射性電機管理辦法

第十四條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十七條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

117710

### English Translation

Administrative Rules for Low-power Radio-Frequency Devices

Article 14

For those low-power radio-frequency devices that have already received a type-approval, companies, business units or users should not change its frequencies, increase its power or change its original features and functions.

Article 17

The operation of the low-power radio-frequency devices is subject to the conditions that no harmful interference is caused to aviation safety and authorized radio station; and if interference is caused, the user must stop operating the device immediately and can't re-operate it until the harmful interference is clear.

The authorized radio station means a radio-communication service operating in accordance with COMMUNICATION ACT.

The operation of the low-power radio-frequency devices is subject to the interference caused by the operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator.

## 5-GHz Client Adapters

### Chinese Translation

本設備限於室內使用<sup>117711</sup>

### English Translation

This equipment is limited for indoor use.

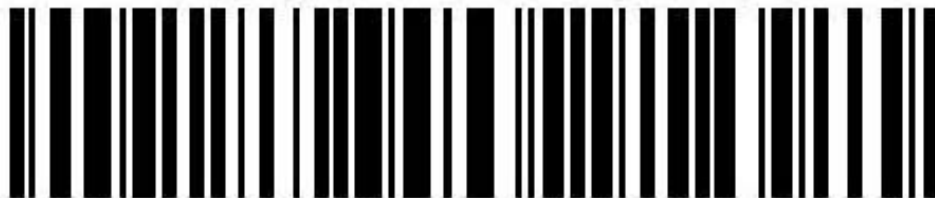
## Brazil/Anatel Approval

The following approval marks apply to the Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters.

### AIR-CB21AG-W-K9



1051-05-1086



(01)07898362231452

"Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário."

**AIR-PI21AG-W-K9**

1052-05-1086

**(01)07898362231469**

"Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário."



## Channels, Power Levels, and Antenna Gains

---

This appendix lists the IEEE 802.11a, b, and g channels supported by the world's regulatory domains as well as the maximum power levels and antenna gains allowed per data rate.

The following topics are covered in this appendix:

- [Channels, page D-48](#)
- [Maximum Power Levels and Antenna Gains, page D-50](#)

# Channels

## IEEE 802.11a

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11a 20-MHz-wide channel are shown in [Table D-1](#).

**Table D-1** Channels for IEEE 802.11a

Channel Identifier	Frequency (in MHz)	Regulatory Domains				
		America (-A)	EMEA (-E)	Japan (-J)	Japan (-P)	Rest of World (-W)
34	5170	—	—	X	X	—
36	5180	X	X	—	X	X
38	5190	—	—	X	X	—
40	5200	X	X	—	X	X
42	5210	—	—	X	X	—
44	5220	X	X	—	X	X
46	5230	—	—	X	X	—
48	5240	X	X	—	X	X
52	5260	X	X	—	X	X
56	5280	X	X	—	X	X
60	5300	X	X	—	X	X
64	5320	X	X	—	X	X
100	5500	X	X	—	—	X
104	5520	X	X	—	—	X
108	5540	X	X	—	—	X
112	5560	X	X	—	—	X
116	5580	X	X	—	—	X
120	5600	X	X	—	—	X
124	5620	X	X	—	—	X
128	5640	X	X	—	—	X
132	5660	X	X	—	—	X
136	5680	X	X	—	—	X
140	5700	X	X	—	—	X
149	5745	X	—	—	—	X
153	5765	X	—	—	—	X
157	5785	X	—	—	—	X
161	5805	X	—	—	—	X

**Note**

All channel sets are restricted to indoor usage except America (-A), which allows for indoor and outdoor use on channels 52 through 161 in the United States.

**Note**

The Japan (-J) channels apply only to AIR-CB21AG-J-K9 and AIR-PI21AG-J-K9 client adapters, and the Japan (-P) channels apply only to AIR-CB21AG-P-K9 and AIR-PI21AG-P-K9 client adapters.

## IEEE 802.11b/g

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11b/g 22-MHz-wide channel are shown in [Table D-2](#).

**Table D-2 Channels for IEEE 802.11b/g**

Channel Identifier	Frequency (in MHz)	Regulatory Domains			
		America (-A)	EMEA (-E)	Japan (-J)	Rest of World (-W)
1	2412	X	X	X	X
2	2417	X	X	X	X
3	2422	X	X	X	X
4	2427	X	X	X	X
5	2432	X	X	X	X
6	2437	X	X	X	X
7	2442	X	X	X	X
8	2447	X	X	X	X
9	2452	X	X	X	X
10	2457	X	X	X	X
11	2462	X	X	X	X
12	2467	–	X	X	X
13	2472	–	X	X	X
14	2484	–	–	X	–

**Note**

Mexico is included in the Rest of World regulatory domain; however, channels 1 through 8 are for indoor use only while channels 9 through 11 can be used indoors and outdoors. Users are responsible for ensuring that the channel set configuration is in compliance with the regulatory standards of Mexico.

**Note**

In Japan, channel 14 is not supported for 802.11g mode.



# Maximum Power Levels and Antenna Gains

## IEEE 802.11a

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. [Table D-3](#) indicates the maximum EIRP allowed for each data rate in the IEEE 802.11a regulatory domains.

**Table D-3** Maximum EIRP for IEEE 802.11a

Data Rate	Maximum EIRP for PC-Cardbus Card with 0-dBi Antenna Gain and PCI Card with 1-dBi Antenna Gain	
	mW	dBm
6 Mbps	40	16
9 Mbps	40	16
12 Mbps	40	16
18 Mbps	40	16
24 Mbps	40	16
36 Mbps	25.1	14
48 Mbps	20	13
54 Mbps	20	13

## IEEE 802.11b

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. [Table D-4](#) indicates the maximum EIRP allowed for each data rate in the IEEE 802.11b regulatory domains.

**Table D-4** Maximum EIRP for IEEE 802.11b

Data Rate	Maximum EIRP for PC-Cardbus Card with 0-dBi Antenna Gain and PCI Card with 1-dBi Antenna Gain	
	mW	dBm
1 Mbps	100	20
2 Mbps	100	20
5.5 Mbps	100	20
11 Mbps	100	20

## IEEE 802.11g

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. [Table D-5](#) indicates the maximum EIRP allowed for each data rate in the IEEE 802.11g regulatory domains.

**Table D-5** Maximum EIRP for IEEE 802.11g

Data Rate	Maximum EIRP for PC-Cardbus Card with 0-dBi Antenna Gain and PCI Card with 1-dBi Antenna Gain	
	mW	dBm
6 Mbps	50	17
9 Mbps	50	17
12 Mbps	50	17
18 Mbps	50	17
24 Mbps	50	17
36 Mbps	40	16
48 Mbps	31.6	15
54 Mbps	20	13





## Configuring the Client Adapter through the Windows XP Operating System

---

This appendix explains how to configure and use the client adapter with Windows XP.

The following topics are covered in this appendix:

- [Overview, page E-54](#)
- [Configuring the Client Adapter, page E-57](#)
- [Associating to an Access Point Using Windows XP, page E-70](#)
- [Viewing the Current Status of Your Client Adapter, page E-70](#)

# Overview

This appendix provides instructions for minimally configuring the client adapter through the Microsoft Wireless Configuration Manager in Windows XP (instead of through ADU) as well as for enabling the security options that are available for use with this operating system. The “[Overview of Security Features](#)” section below describes each of these options so that you can make an informed decision before you begin the configuration process.

In addition, this appendix also provides basic information on using Windows XP to specify the networks to which the client adapter associates and to view the current status of your client adapter.

**Note**

---

If you require more information about configuring or using your client adapter with Windows XP, refer to Microsoft’s documentation for Windows XP.

---

## Overview of Security Features

When you use your client adapter with Windows XP, you can protect your data as it is transmitted through your wireless network by encrypting it through the use of wired equivalent privacy (WEP) encryption keys. With WEP encryption, the transmitting device encrypts each packet with a WEP key, and the receiving device uses that same key to decrypt each packet.

The WEP keys used to encrypt and decrypt transmitted data can be statically associated with your adapter or dynamically created as part of the EAP authentication process. The information in the “[Static WEP Keys](#)” and “[EAP \(with Dynamic WEP Keys\)](#)” sections below can help you to decide which type of WEP keys you want to use. Dynamic WEP keys with EAP offer a higher degree of security than static WEP keys.

WEP keys, whether static or dynamic, are either 40 or 128 bits in length. 128-bit WEP keys offer a greater level of security than 40-bit WEP keys.

## Static WEP Keys

Each device within your wireless network can be assigned up to four static WEP keys. If a device receives a packet that is not encrypted with the appropriate key (as the WEP keys of all devices that are to communicate with each other must match), the device discards the packet and never delivers it to the intended receiver.

You do not need to re-enter static WEP keys each time the client adapter is inserted or the Windows device is rebooted because the keys are stored (in an encrypted format for security reasons) in the registry of the Windows device. When the driver loads and reads the client adapter’s registry parameters, it also finds the static WEP keys, unencrypts them, and stores them in volatile memory on the adapter.

## EAP (with Dynamic WEP Keys)

The standard for wireless LAN security, as defined by IEEE, is called *802.1X for 802.11*, or simply *802.1X*. An access point that supports 802.1X and its protocol, Extensible Authentication Protocol (EAP), acts as the interface between a wireless client and an authentication server, such as a RADIUS server, to which the access point communicates over the wired network.

Two 802.1X authentication types are available when configuring your client adapter through Windows XP:

- **EAP-TLS**—This authentication type uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It uses a client certificate for authentication. RADIUS servers that support EAP-TLS include Cisco Secure ACS release 3.0 or later and Cisco Access Registrar release 1.8 or later.
- **Protected EAP (or PEAP)**—One of the following PEAP authentication types are available, depending on the software that is installed on your computer:

- **PEAP (EAP-MSCHAP V2)**—This PEAP authentication type is available if Cisco's PEAP security module (included in the Install Wizard file for Cisco Aironet 340, 350, and CB20A client adapters) was not previously installed on your computer or was installed prior to Service Pack 1 for Windows XP.

PEAP (EAP-MSCHAP V2) authentication is based on EAP-TLS authentication but uses a password instead of a client certificate for authentication. PEAP (EAP-MSCHAP V2) uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data.

RADIUS servers that support PEAP (EAP-MSCHAP V2) authentication include Cisco Secure ACS release 3.2 or later.

- **PEAP (EAP-GTC)**—Although this authentication type is not officially supported for CB21AG and PI21AG client adapters, you may be able to use it successfully if Cisco's PEAP security module (included in the Install Wizard file for Cisco Aironet 340, 350, and CB20A client adapters) was previously installed on your computer and installed after Service Pack 1 for Windows XP.

PEAP (EAP-GTC) authentication is designed to support One-Time Password (OTP), Windows NT or 2000 domain, and LDAP user databases over a wireless LAN. It is based on EAP-TLS authentication but uses a password or PIN instead of a client certificate for authentication. PEAP (EAP-GTC) uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. If your network uses an OTP user database, PEAP (EAP-GTC) requires you to enter either a hardware token password or a software token PIN to start the EAP authentication process and gain access to the network. If your network uses a Windows NT or 2000 domain user database or an LDAP user database (such as NDS), PEAP (EAP-GTC) requires you to enter your username, password, and domain name in order to start the authentication process.

RADIUS servers that support PEAP (EAP-GTC) authentication include Cisco Secure ACS release 3.1 or later and Cisco Access Registrar release 3.5 or later.

When you enable EAP on your access point and configure your client adapter for EAP-TLS or PEAP using Windows XP, authentication to the network occurs in the following sequence:

1. The client adapter associates to an access point and begins the authentication process.



---

**Note** The client does not gain full access to the network until authentication between the client and the RADIUS server is successful.

---

2. Communicating through the access point, the client and RADIUS server complete the authentication process, with the password (PEAP) or certificate (EAP-TLS) being the shared secret for authentication. The password is never transmitted during the process.
3. If authentication is successful, the client and RADIUS server derive a dynamic, session-based WEP key that is unique to the client.
4. The RADIUS server transmits the key to the access point using a secure channel on the wired LAN.
5. For the length of a session, or time period, the access point and the client use this key to encrypt or decrypt all unicast packets (and broadcast packets if the access point is set up to do so) that travel between them.



**Note**

---

Refer to the IEEE 802.11 Standard for more information on 802.1X authentication and to the following URL for additional information on RADIUS servers:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products\\_configuration\\_guide\\_chapter09186a00800ca7ab.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7ab.html)

---

## WPA

Wi-Fi Protected Access (WPA) is a standards-based security solution from the Wi-Fi Alliance that provides data protection and access control for wireless LAN systems. It is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification. WPA uses Temporal Key Integrity Protocol (TKIP) and message integrity check (MIC) for data protection and 802.1X for authenticated key management.

WPA supports two mutually exclusive key management types: WPA and WPA passphrase (also known as *WPA pre-shared key* or *WPA-PSK*). Using WPA, clients and the authentication server authenticate to each other using an EAP authentication method, and the client and server generate a pairwise master key (PMK). The server generates the PMK dynamically and passes it to the access point. Using WPA passphrase, however, you configure a passphrase (or pre-shared key) on both the client and the access point, and that passphrase is used as the PMK.

In order to use WPA, your computer must be running Windows XP Service Pack 2.



**Note**

---

WPA must also be enabled on the access point. Access points must use Cisco IOS Release 12.2(11)JA or later to enable WPA. Refer to the documentation for your access point for instructions on enabling this feature.

---

# Configuring the Client Adapter

Follow the steps below to configure your client adapter using Windows XP.

**Note**

These instructions assume you are using the Windows XP classic view rather than the category view. Otherwise, the windows you see will look different than those shown in this section.

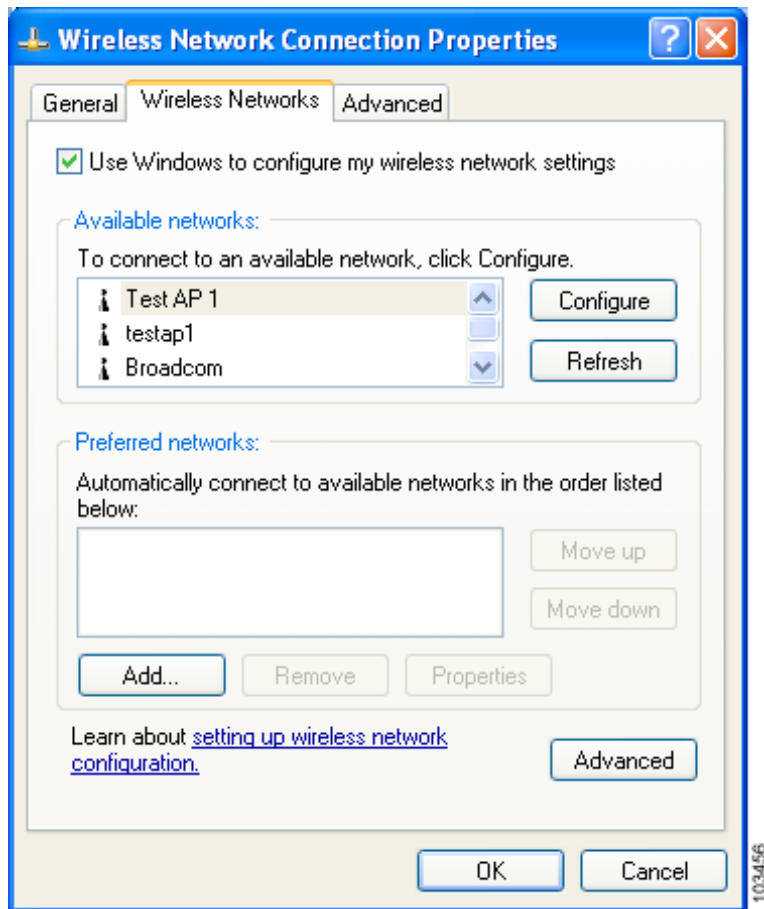
**Note**

The appropriate certificates must be installed on your computer if you are planning to enable EAP-TLS or PEAP authentication. EAP-TLS requires both a Certificate Authority (CA) certificate and a user certificate while PEAP requires only a CA certificate. Contact your system administrator if you need help obtaining and importing the necessary certificates.

- 
- Step 1** Make sure the client adapter's driver has been installed and the client adapter is inserted in the Windows XP device.
- Step 2** Double-click **My Computer**, **Control Panel**, and **Network Connections**.
- Step 3** Right-click **Wireless Network Connection**.
- Step 4** Click **Properties**. The Wireless Network Connection Properties window appears.
- Step 5** Click the **Wireless Networks** tab. The following window appears (see [Figure E-1](#)).



Figure E-1 Wireless Network Connection Properties Window (Wireless Networks Tab)



**Step 6** Make sure that the **Use Windows to configure my wireless network settings** check box is checked.

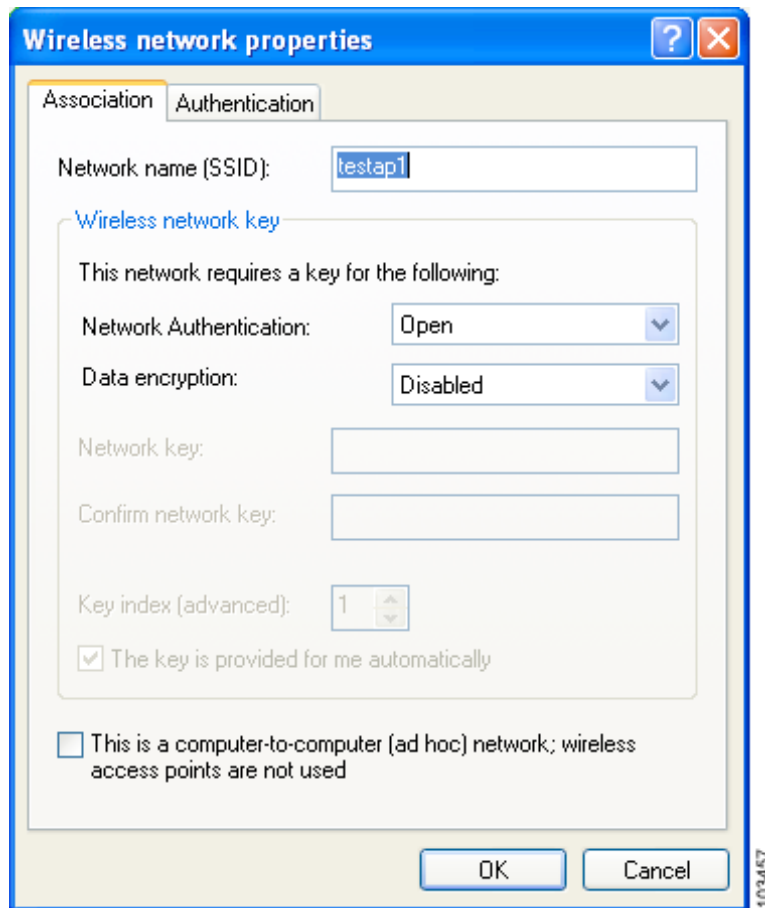
**Step 7** Choose the SSID of the access point to which you want the client adapter to associate from the list of available networks and click **Configure**. If the SSID of the access point you want to use is not listed or you are planning to operate the client adapter in an *ad hoc network* (a computer-to-computer network without access points), click **Add**.



**Note** The Allow Broadcast SSID to Associate option on the access point must be enabled for the SSID to appear in the list of available networks.

The Wireless Network Properties window appears (see [Figure E-2](#)).

**Figure E-2** Wireless Network Properties Window (Association Tab)



**Step 8** Perform one of the following:

- If you chose an SSID from the list of available networks, make sure the SSID appears in the Network name (SSID) field.
- If you clicked Add, enter the case-sensitive SSID of the access point or the ad hoc network to which you want the client adapter to associate in the Network name (SSID) field.

**Step 9** Check the **This is a computer-to-computer (ad hoc mode) network; wireless access points are not used** check box at the bottom of the window if you are planning to operate the client adapter in an ad hoc network.

**Step 10** Choose one of the following options from the Network Authentication drop-down list:

- **Open**—Enables your client adapter, regardless of its WEP settings, to authenticate and attempt to communicate with an access point. However, communication can occur only if the adapter's WEP key matches that of the access point. If your adapter is not using WEP, it will not attempt to authenticate to an access point that is using WEP and vice versa. This option is recommended if you want to use static WEP or EAP authentication without WPA.
- **Shared**—Enables your client adapter to authenticate and communicate only with access points that have the same WEP key. Cisco recommends that shared key authentication not be used because it presents a security risk.




---

**Note** Your client adapter's network authentication setting must match that of the access points with which it is to communicate. Otherwise, your client adapter may not be able to authenticate to them.

---




---

**Note** EAP-TLS does not work with shared key authentication because shared key authentication requires the use of a WEP key, and a WEP key is not set for EAP-TLS until after the completion of EAP authentication.

---

- **WPA**—Enables WPA, which enables your client adapter to associate to access points using WPA.
- **WPA-PSK**—Enables WPA pre-shared key (WPA-PSK), which enables your client adapter to associate to access points using WPA-PSK.




---

**Note** The WPA-None option is not supported for use with the CB21AG or PI21AG client adapter.

---




---

**Note** Refer to the [“WPA” section on page E-56](#) for more information on WPA and WPA-PSK.

---

**Step 11** Choose one of the following options from the Data encryption drop-down list:

- **Disabled**—Disables data encryption for your client adapter. This option is available only when Open or Shared has been selected for Network Authentication.
- **WEP**—Enables static or dynamic WEP for your client adapter. This option is recommended for use with open authentication.
- **TKIP**—Enables Temporal Key Integrity Protocol (TKIP) for your client adapter. This option is recommended for use with WPA and WPA-PSK unless the access point to which your client adapter will associate supports AES.
- **AES**—Enables the Advanced Encryption Standard (AES) encryption algorithm for your client adapter. This option provides a stronger encryption mechanism than TKIP and is therefore recommended for use with WPA and WPA-PSK, provided the access point to which your client adapter will associate supports AES.

**Step 12** Follow the steps below to enter a static WEP key if you are planning to use static WEP.



**Note** If you are planning to use EAP-TLS or PEAP authentication, which uses dynamic WEP, go to [Step 13](#).

- a. Make sure the **The key is provided for me automatically** check box is unchecked.
- b. Obtain the WEP key for the access point (in an infrastructure network) or other clients (in an ad hoc network) from your system administrator and enter it in both the Network key and Confirm network key fields. Follow the guidelines below to enter a new static WEP key:

- WEP keys must contain the following number of characters:

–10 hexadecimal characters or 5 ASCII text characters for 40-bit keys

**Example:** 5A5A313859 (hexadecimal) or ZZ18Y (ASCII)

–26 hexadecimal characters or 13 ASCII text characters for 128-bit keys

**Example:** 5A583135333554595549333534 (hexadecimal) or ZX1535TYUI354 (ASCII)



**Note** ASCII text WEP keys are not supported on Cisco Aironet 1200 Series Access Points, so you must enter hexadecimal characters if your client adapter will be used with these access points.

- Your client adapter's WEP key must match the WEP key used by the access point (in infrastructure mode) or clients (in ad hoc mode) with which you are planning to communicate.
- c. In the Key index (advanced) field, choose the number of the WEP key you are creating (**1, 2, 3, or 4**).



**Note** The WEP key must be assigned to the same number on both the client adapter and the access point (in an infrastructure network) or other clients (in an ad hoc network).

- d. Click **OK** to save your settings and to add this SSID to the list of preferred networks (see [Figure E-1](#)). The configuration is complete for static WEP. The client adapter automatically attempts to associate to the network(s) in the order in which they are listed.

**Step 13** If you enabled WPA-PSK, obtain the pre-shared key for the access point from your system administrator and enter it in both the Network key and Confirm network key fields. Follow the guidelines below to enter a pre-shared key:

- Pre-shared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.
- Your client adapter's pre-shared key must match the pre-shared key used by the access point with which you are planning to communicate.

**Step 14** Check the **The key is provided for me automatically** check box if you are planning to use EAP-TLS or PEAP, which uses dynamic WEP keys.



**Note** This parameter is not available if you enabled WPA or WPA-PSK.

**Step 15** Perform one of the following if you are planning to use EAP authentication:

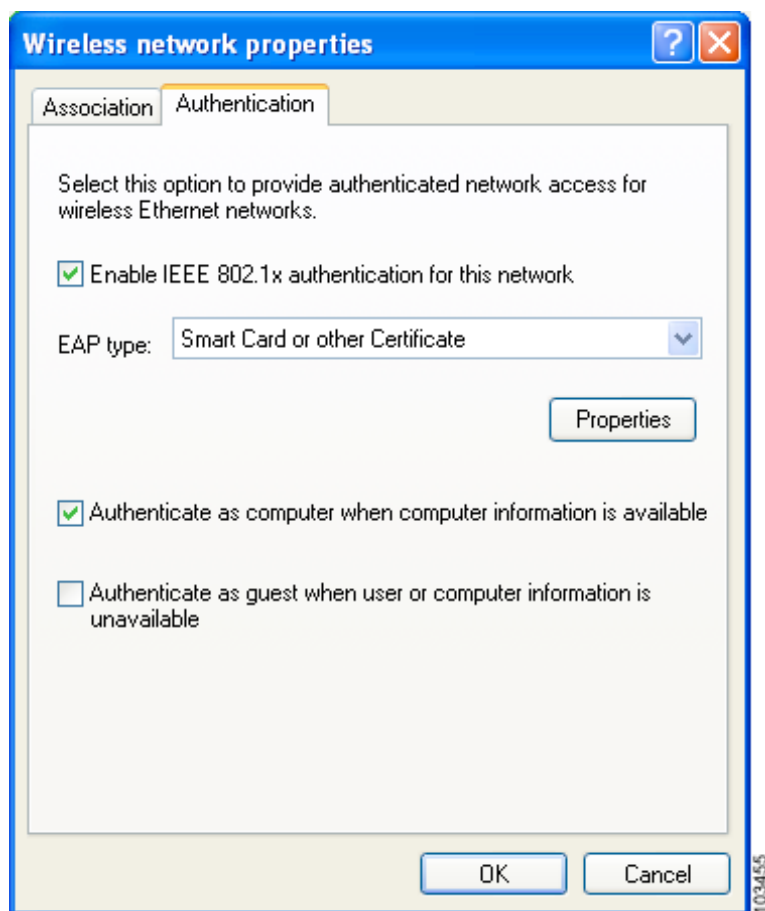
- If you are planning to use EAP-TLS authentication, follow the instructions in the “[Enabling EAP-TLS Authentication](#)” section on page E-62.
- If you are planning to use PEAP authentication, follow the instructions in the “[Enabling PEAP Authentication](#)” section on page E-65.

## Enabling EAP-TLS Authentication

Follow the steps below to prepare the client adapter to use EAP-TLS authentication, provided you have completed the initial configuration.

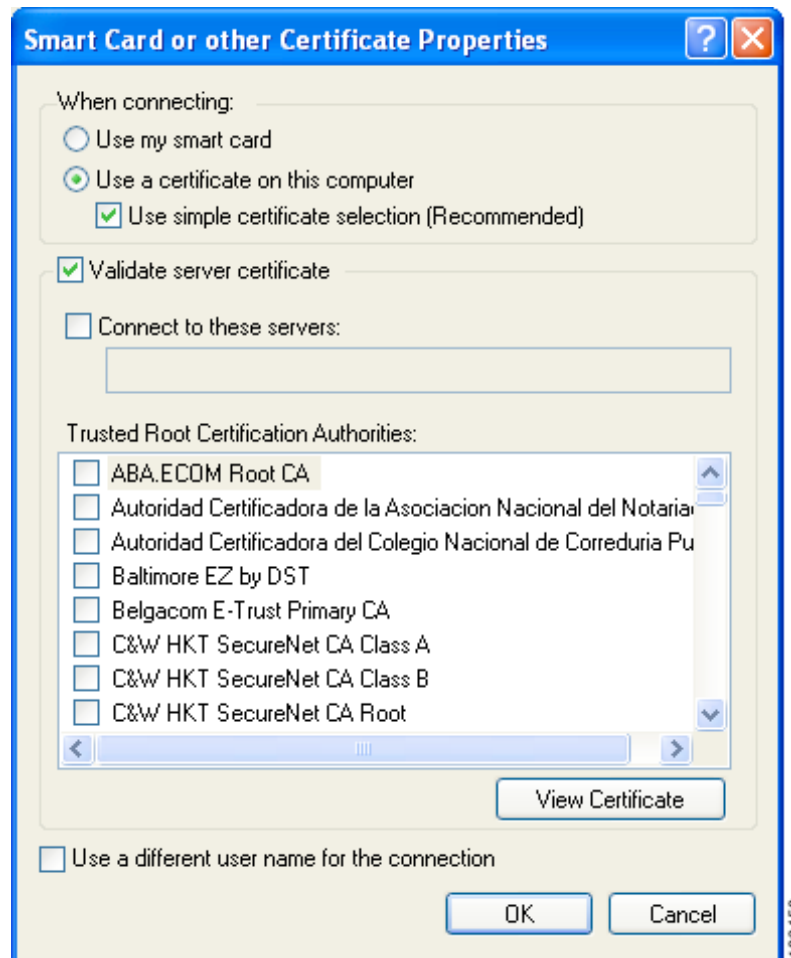
**Step 1** Click the **Authentication** tab on the Wireless Network Properties window. The following window appears (see [Figure E-3](#)).

**Figure E-3** Wireless Network Properties Window (Authentication Tab)



- Step 2** Check the **Enable IEEE 802.1x authentication for this network** check box if you did not enable WPA on the Association window.
- Step 3** For EAP type, choose **Smart Card or other Certificate**.
- Step 4** Click **Properties**. The Smart Card or other Certificate Properties window appears (see [Figure E-4](#)).

**Figure E-4** Smart Card or other Certificate Properties Window



- Step 5** Choose the **Use a certificate on this computer** option.
- Step 6** Check the **Use simple certificate selection (Recommended)** check box.
- Step 7** Check the **Validate server certificate** check box if server certificate validation is required.

- Step 8** If you want to specify the name of the server to connect to, check the **Connect to these servers** check box and enter the server name in the field below.



**Note** If you enter a server name and the client adapter connects to a server that does not match the name you entered, you are prompted to accept or cancel the connection during the authentication process.



**Note** If you leave this field blank, the server name is not verified, and a connection is established as long as the certificate is valid.

- Step 9** In the Trusted Root Certification Authorities field, check the check box beside the name of the certificate authority from which the server certificate was downloaded.



**Note** If you leave all check boxes unchecked, you are prompted to accept a connection to the root certification authority during the authentication process.

- Step 10** Click **OK** in each window to save your settings. The configuration is complete.

- Step 11** If a pop-up message appears above the system tray informing you that you need to accept a certificate to begin the EAP authentication process, click the message and follow the instructions provided to accept the certificate.



**Note** You should not be prompted to accept a certificate for future authentication attempts. After you accept one, the same certificate is used subsequently.

- Step 12** If a message appears indicating the root certification authority for the server's certificate, and it is the correct certification authority, click **OK** to accept the connection. Otherwise, click **Cancel**.

- Step 13** If a message appears indicating the server to which your client adapter is connected, and it is the correct server to connect to, click **OK** to accept the connection. Otherwise, click **Cancel**.

The client adapter should now EAP authenticate.



**Note** Whenever the computer reboots and you enter your Windows username and password, the EAP authentication process begins automatically and the client adapter should EAP authenticate.

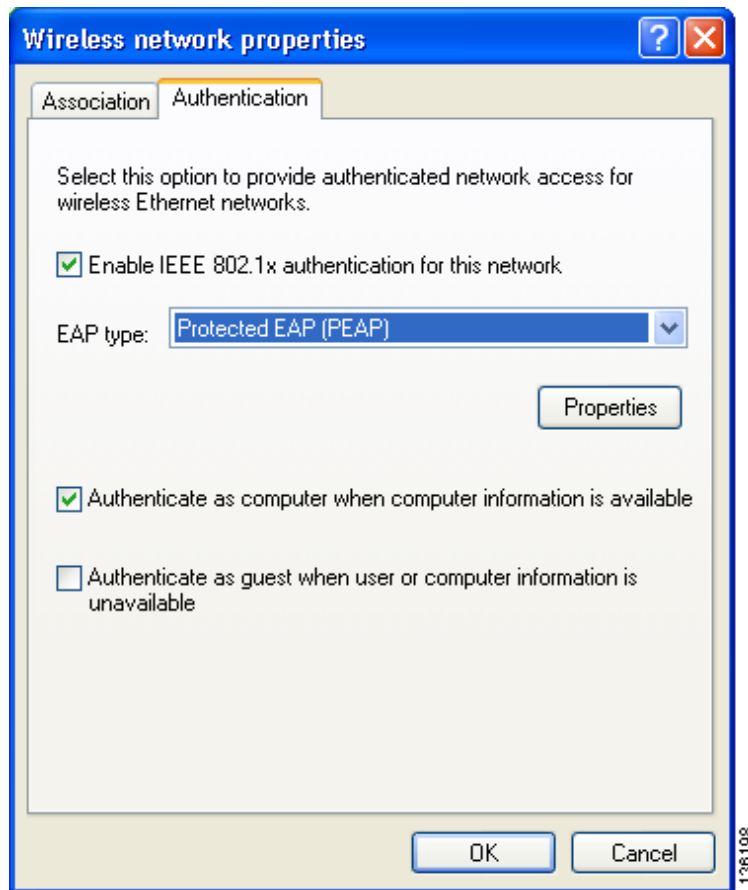
- Step 14** To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. The status appears to the right of your Wireless Network Connection. Click **View** and **Refresh** to obtain the current status. If the client adapter is authenticated, the status reads *Authentication succeeded*.

## Enabling PEAP Authentication

Follow the steps below to prepare the client adapter to use PEAP authentication, provided you have completed the initial configuration.

- Step 1** Click the **Authentication** tab on the Wireless Network Properties window. The following window appears (see [Figure E-5](#)).

**Figure E-5** Wireless Network Properties Window (Authentication Tab)



- Step 2** Check the **Enable IEEE 802.1x authentication for this network** check box if you did not enable WPA on the Association window.
- Step 3** For EAP type, choose one of the following, depending on the software that is installed on your computer:
- **Protected EAP (PEAP)**—This option appears for PEAP (EAP-MSCHAP V2).
  - **PEAP**—This option appears for PEAP (EAP-GTC).



**Note** PEAP (EAP-GTC) is not officially supported for CB21AG and PI21AG client adapters, but you may be able to use it successfully if Cisco's PEAP security module (included in the Install Wizard file for Cisco Aironet 340, 350, and CB20A client adapters) was previously installed on your computer and installed after Service Pack 1 for Windows XP.



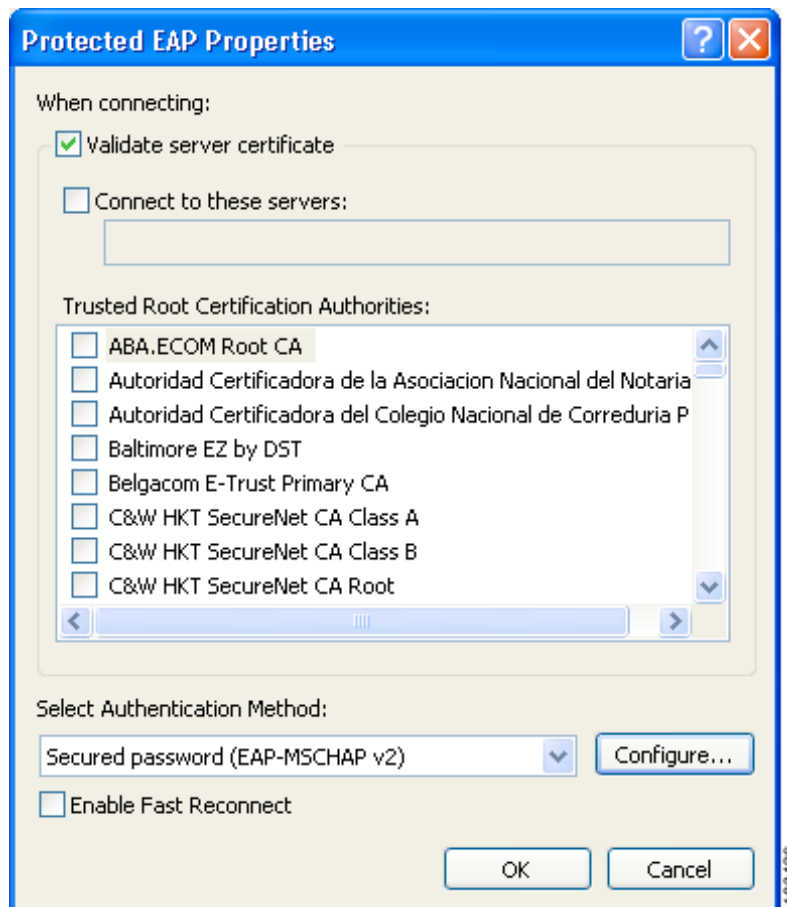
- Step 4** Perform one of the following:
- If you chose Protected EAP (PEAP), follow the instructions in the “[Enabling PEAP \(EAP-MSCHAP V2\)](#)” section below.
  - If you chose PEAP, follow the instructions in the “[Enabling PEAP \(EAP-GTC\)](#)” section on [page E-68](#).

## Enabling PEAP (EAP-MSCHAP V2)

Follow the steps below to enable PEAP (EAP-MSCHAP V2).

- Step 1** Click **Properties**. The Protected EAP Properties window appears (see [Figure E-8](#)).

**Figure E-6** Protected EAP Properties Window



- Step 2** Check the **Validate server certificate** check box if server certificate validation is required (recommended).

**Step 3** If you want to specify the name of the server to connect to, check the **Connect to these servers** check box and enter the appropriate server name in the field below.



**Note** If you enter a server name and the client adapter connects to a server that does not match the name you entered, you are prompted to accept or cancel the connection during the authentication process.



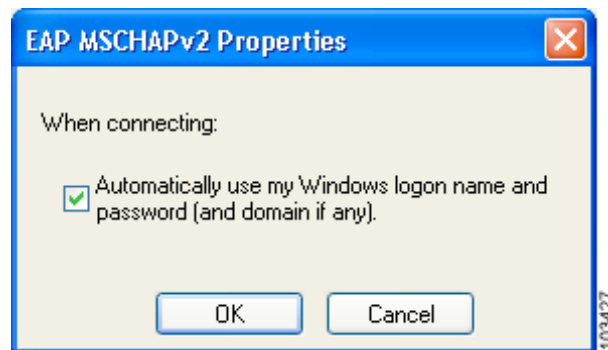
**Note** If you leave this field blank, the server name is not verified, and a connection is established as long as the certificate is valid.

**Step 4** In the Trusted Root Certification Authorities field, choose the certificate authority from which the server certificate was downloaded.

**Step 5** In the Select Authentication Method drop-down box, choose **Secured password (EAP-MSCHAP v2)**.

**Step 6** Click **Configure**. The EAP MSCHAPv2 Properties window appears (see [Figure E-7](#)).

**Figure E-7** EAP MSCHAPv2 Properties Window



**Step 7** Make sure the **Automatically use my Windows logon name and password (and domain if any)** check box is checked.

**Step 8** Click **OK** in each window to save your settings. The configuration is complete.

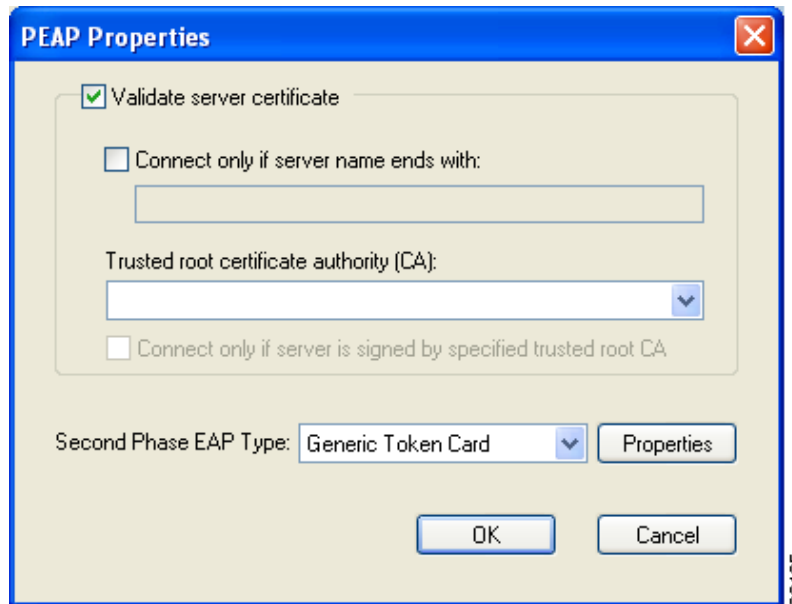
**Step 9** The EAP authentication process begins automatically, and the client adapter should EAP authenticate using your Windows credentials. To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. The status appears to the right of your Wireless Network Connection. Click **View** and **Refresh** to obtain the current status. If the client adapter is authenticated, the status reads *Authentication succeeded*.

## Enabling PEAP (EAP-GTC)

Follow the steps below to enable PEAP (EAP-GTC).

- Step 1** Click **Properties**. The PEAP Properties window appears (see [Figure E-8](#)).

**Figure E-8** PEAP Properties Window



- Step 2** Check the **Validate server certificate** check box if server certificate validation is required (recommended).
- Step 3** If you want to specify the name of the server to connect to, check the **Connect only if server name ends with** check box and enter the appropriate server name suffix in the field below.



**Note** If you enter a server name and the client adapter connects to a server that does not match the name you entered, you are prompted to accept or cancel the connection during the authentication process.



**Note** If you leave this field blank, the server name is not verified, and a connection is established as long as the certificate is valid.

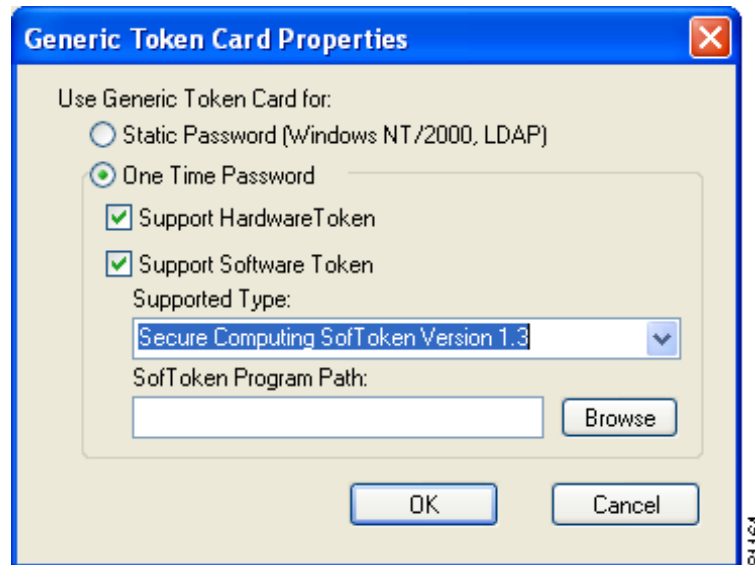
- Step 4** Make sure that the name of the certificate authority from which the server certificate was downloaded appears in the Trusted root certificate authority (CA) field. If necessary, click the arrow on the drop-down menu and choose the appropriate name.



**Note** If you leave this field blank, you are prompted to accept a connection to the root certification authority during the authentication process.

- Step 5** Check the **Connect only if server is signed by specified trusted root CA** check box if you want to ensure that the certificate server uses the trusted root certificate specified in the field above. This prevents the client from establishing connections to rogue access points.
- Step 6** Currently Generic Token Card is the only second phase EAP type available. Click **Properties**. The Generic Token Card Properties window appears (see [Figure E-9](#)).

**Figure E-9** Generic Token Card Properties Window



- Step 7** Choose either the **Static Password (Windows NT/2000, LDAP)** or the **One Time Password** option, depending on your user database.
- Step 8** Perform one of the following:
- If you chose the **Static Password (Windows NT/2000, LDAP)** option in [Step 7](#), go to [Step 9](#).
  - If you chose the **One Time Password** option in [Step 7](#), check one or both of the following check boxes to specify the type of tokens that will be supported for one-time passwords:
    - **Support Hardware Token**—A hardware token device obtains the one-time password. You must use your hardware token device to obtain the one-time password and enter the password when prompted for your user credentials.
    - **Support Software Token**—The PEAP supplicant works with a software token program to retrieve the one-time password. You have to enter only the PIN, not the one-time password. If you check this check box, you must also choose from the Supported Type drop-down box the software token software that is installed on the client (such as Secure Computing SofToken Version 2.1, Secure Computing SofToken II 2.0, or RSA SecurID Software Token 2.5), and if Secure Computing SofToken Version 2.1 is selected, you must find the software program path using the Browse button.



**Note** The SofToken Program Path field is unavailable if a software token program other than Secure Computing SofToken Version 2.1 is selected.

- Step 9** Click **OK** in each window to save your settings. The configuration is complete.
- Step 10** Refer to [Chapter 6](#) of the *Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows* (OL-1394-07 or later) for instructions on authenticating using PEAP (EAP-GTC).

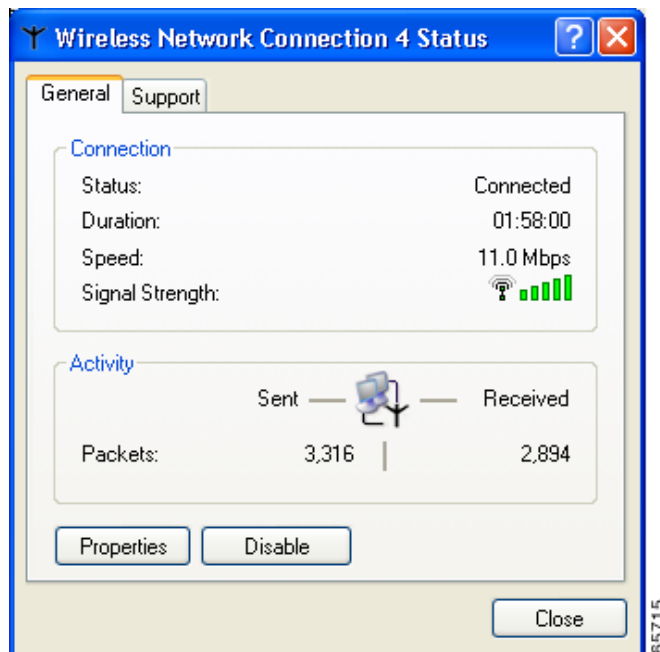
## Associating to an Access Point Using Windows XP

Windows XP causes the client adapter's driver to automatically attempt to associate to the first network in the list of preferred networks (see [Figure E-1](#)). If the adapter fails to associate or loses association, it automatically switches to the next network in the list of preferred networks. The adapter does not switch networks as long as it remains associated to the access point. To force the client adapter to associate to a different access point, you must choose a different network from the list of available networks (and click **Configure** and **OK**).

## Viewing the Current Status of Your Client Adapter

To view the status of your client adapter, click the icon of the two connected computers in the Windows system tray. The Wireless Network Connection Status window appears (see [Figure E-10](#)).

**Figure E-10** Wireless Network Connection Status Window





## Performing a Site Survey

---

This appendix explains how the site survey utility can be used when conducting a site survey.

The following topics are covered in this appendix:

- [Overview, page F-72](#)
- [Opening the Site Survey Utility, page F-73](#)
- [Selecting the Client Adapter, page F-73](#)
- [Using the Associated AP Status Tab, page F-74](#)
- [Using the AP Scan List Tab, page F-78](#)
- [Using the Proximity Beeper, page F-88](#)
- [Using Thresholds, page F-90](#)
- [Using AP Scanning, page F-96](#)
- [Viewing the Status Bar, page F-102](#)
- [Finding the Version of the Site Survey Utility, page F-103](#)
- [Accessing Online Help, page F-103](#)
- [Exiting the Site Survey Utility, page F-104](#)
- [Uninstalling the Site Survey Utility, page F-104](#)

# Overview

**Note**

---

This appendix applies only to people who are responsible for conducting a site survey to determine the best placement of infrastructure devices within a wireless network.

---

The site survey utility can assist you in conducting a site survey. The utility operates at the RF level and is used to determine the best placement and coverage (overlap) for your network's infrastructure devices. During a site survey, the current status of the network is read from the client adapter, and the status display is updated four times per second so you can accurately gauge network performance. The feedback that you receive can help you to eliminate areas of low RF signal levels that can result in a loss of connection between the client adapter and its associated access point (or other infrastructure device).

The site survey utility operates in a passive mode. That is, it does not initiate any RF network traffic; it simply listens to the traffic that the client adapter hears and displays the results.

## Guidelines

Keep the following guidelines in mind when preparing to perform a site survey:

- Perform the site survey when the RF link is functioning with all other systems and noise sources operational.
- Execute the site survey entirely from the mobile station.

## Additional Information

Also consider the following operating and environmental conditions when performing a site survey:

- **Data rates**—Sensitivity and range are inversely proportional to data bit rates. Therefore, the maximum radio range is achieved at the lowest workable data rate, and a decrease in receiver threshold sensitivity occurs as the radio data increases.
- **Antenna type and placement**—Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, range increases in proportion to antenna height.
- **Physical environment**—Clear or open areas provide better radio range than closed or filled areas. Also, the less cluttered the work environment, the greater the range.
- **Obstructions**—A physical obstruction such as metal shelving or a steel pillar can hinder the performance of wireless devices. Avoid placing these devices in a location where a metal barrier is between the sending and receiving antennas.
- **Building materials**—Radio penetration is greatly influenced by the building material used in construction. For example, drywall construction allows greater range than concrete blocks, and metal or steel construction is a barrier to radio signals.

**Note**

---

Refer to the hardware installation guide for your infrastructure device for additional information on factors affecting placement.

---

## Opening the Site Survey Utility

To open the site survey utility, choose **Start > Programs > Cisco Aironet > Aironet Site Survey Utility**.



**Note**

If you specified a different program folder during installation, you must access the site survey utility from that folder.



**Note**

The site survey utility is installed on your computer only if you checked the Install Site Survey Utility check box during the installation of the client adapter software. If you did not check this check box and want to use the site survey utility, uninstall the client adapter software and reinstall it, making sure to check the site survey check box.

## Selecting the Client Adapter



**Note**

The site survey utility can be used only with CB21AG and PI21AG client adapters.

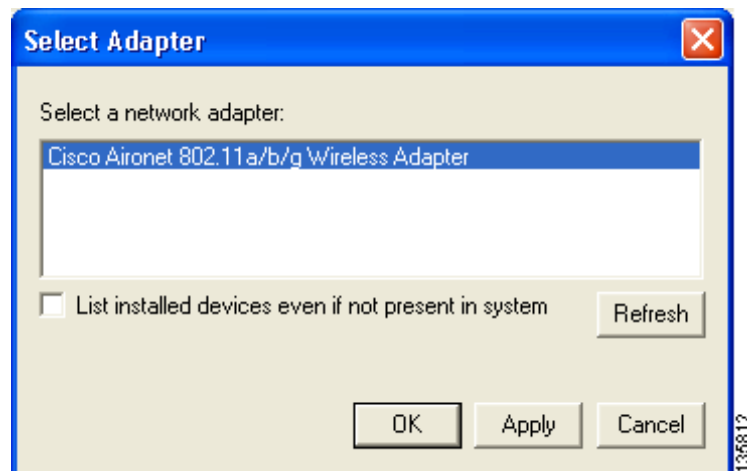
When the site survey utility starts, it scans for client adapters. If only one adapter is detected, it is selected automatically. However, if the utility detects multiple adapters or no adapters, the Select Adapter window appears (see [Figure F-1](#)).



**Note**

You can manually open this window at any time to select a different client adapter. Simply choose **Select Adapter** from the site survey utility's Action drop-down menu.

**Figure F-1** Site Survey Utility - Select Adapter Window





Follow these steps to select the desired client adapter.

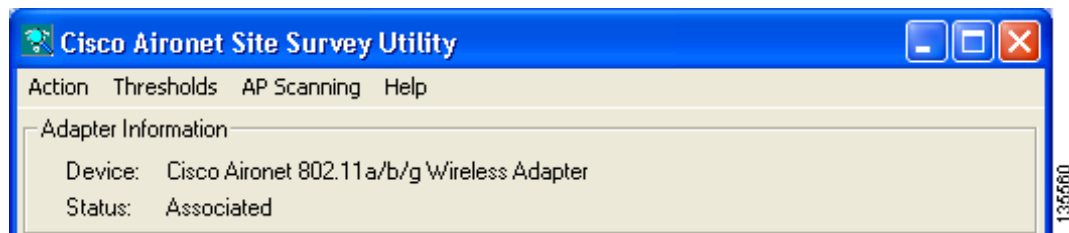
- Step 1** If you want to be able to choose client adapters that are installed but not physically present in your computer, check the **List installed devices even if not present in system** check box.
- Step 2** From the Select a Network Adapter list, select the client adapter that you want to use with the site survey utility.



**Note** Click **Refresh** to update the list of available client adapters (for instance, after an adapter has been ejected or inserted).

- Step 3** Click **OK** to save your selection and exit the Select Adapter window. The top of the site survey utility's main window (see [Figure F-2](#)) shows the client adapter that is being used with the utility and its current association status (Associated, Not Associated, Device Not Present, or Not a Wireless Adapter).

**Figure F-2 Site Survey Utility - Top of Main Window**



## Using the Associated AP Status Tab

You can perform these functions from the Associated AP Status tab:

- Specify display units, [F-74](#)
- View the access point's status, [F-75](#)

Follow the instructions on the pages indicated to perform these functions.

### Specifying Display Units

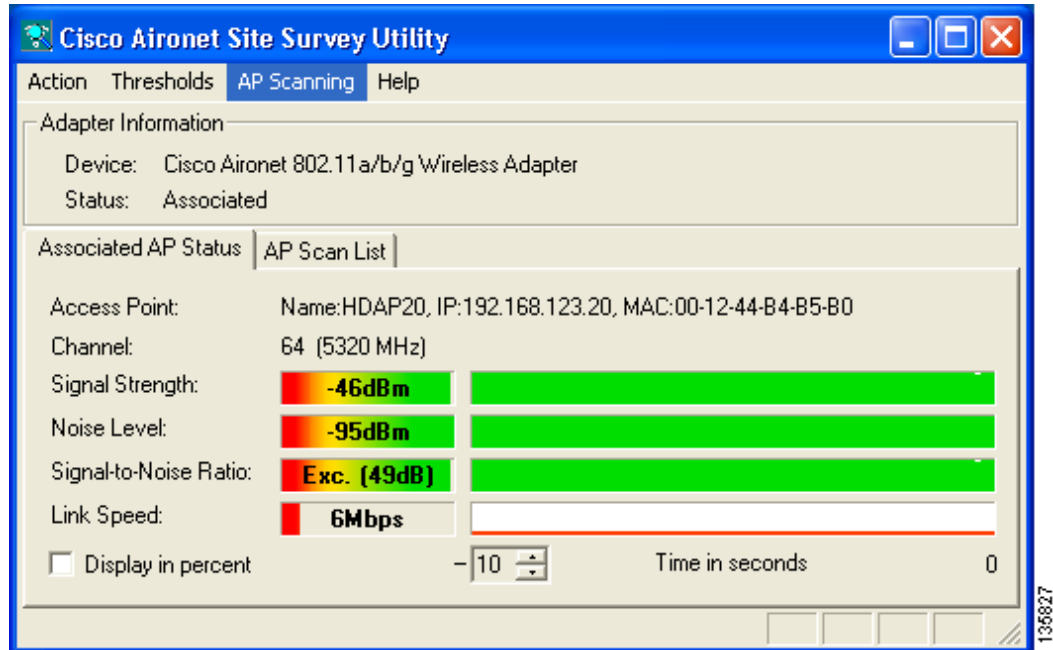
The **Display in percent** check box at the bottom of the Associated AP Status tab enables you to specify how display units are shown.

- Unchecking this check box causes the signal strength and noise level to be shown in decibels with respect to milliwatts (dBm) and the signal-to-noise ratio to be shown in decibels (db). This option, which is the default value, provides a more accurate representation of the data being presented than the percentage option.
- Checking this check box causes the signal strength, signal quality or beacons received, and overall link quality to be shown as a percentage.

## Viewing the Access Point's Status

The Associated AP Status tab shows the status of the access point to which your client adapter is associated. [Figure F-3](#) shows the tab with display units shown in dBm, and [Figure F-4](#) shows the tab with display units shown as a percentage.

**Figure F-3** Site Survey Utility - Associated AP Status Tab (with Display Units in dBm)



**Figure F-4** Site Survey Utility - Associated AP Status Tab (with Display Units as a Percentage)

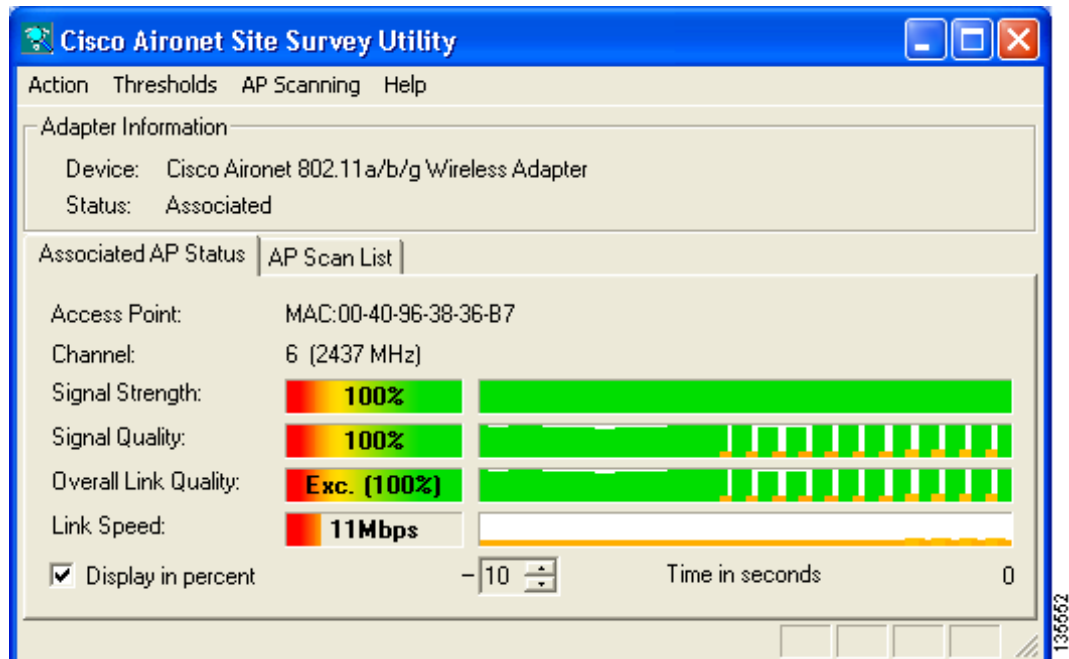


Table F-1 interprets the information that is displayed on the Associated AP Status tab.

**Note**

The trend graphs to the right of the smaller bar graphs provide a graphical representation of activity in the past 10 to 60 seconds. The height of an individual trend graph is proportional to the width of its corresponding bar graph. The time is displayed as a negative value to indicate that the data is older at the left edge of the graph than at the right. Use the up and down arrows to select the desired number of seconds from -10 through -60. The default value is -10.

**Table F-1 Site Survey Utility - Associated AP Status**

Associated AP Status Parameter	Description
Access Point	<p>The access point to which your client adapter is associated. This field may show the access point's name, IP address, and MAC address.</p> <p><b>Note</b> This information is shown only if the access point was configured with a name or IP address, Aironet Extensions are enabled (on access points running Cisco IOS release 12.2(4)JA or greater), and the access point transmits this information.</p> <p><b>Note</b> This field shows up to 15 characters for the access point name although the name may be longer.</p> <p><b>Note</b> If Aironet Extensions are disabled, the IP address of the associated access point is shown as 0.0.0.0.</p> <p><b>Note</b> This field displays the MAC address of the access point's Ethernet port (for access points that do not run Cisco IOS software) or the MAC address of the access point's radio (for access points that run Cisco IOS software). The MAC address of the Ethernet port on access points that run Cisco IOS software is printed on a label on the back of the device.</p>
Channel	<p>The channel and radio frequency (in MHz) that the access point is currently using for communications.</p> <p><b>Value:</b> Dependent on radio band and regulatory domain</p>
Signal Strength	<p>The signal strength of the most recently received packets. The higher the value and the wider the bar graph, the stronger the signal.</p> <p>The trend graph to the right of the bar graph provides a visual interpretation of the signal strength over time. Differences in signal strength are indicated by the following colors: green (strongest), yellow (middle of the range), and red (weakest).</p> <p><b>Range:</b> -95 to -45 dBm or 0 to 100%</p> <p><b>Note</b> The actual dBm reading could exceed the stated range.</p>

Table F-1 Site Survey Utility - Associated AP Status (continued)

Associated AP Status Parameter	Description
Noise Level	<p>The level of background radio frequency energy. The lower the value and the wider the bar graph, the less background noise present.</p> <p>The trend graph to the right of the bar graph provides a visual interpretation of the level of background noise over time. Differences in background noise level are indicated by the following colors: green (low noise), yellow (middle of the range), and red (high noise).</p> <p><b>Range:</b> -45 to -95 dBm</p> <p><b>Note</b> The actual reading could exceed the stated range.</p> <p><b>Note</b> This parameter appears only if the Display in Percent check box is unchecked.</p>
Signal Quality	<p>The signal quality of the most recently received packets. The higher the value and the wider the bar graph, the clearer the signal.</p> <p>The trend graph to the right of bar graph provides a visual interpretation of the signal quality over time. Differences in signal quality are indicated by the following colors: green (highest quality), yellow (average), and red (lowest quality).</p> <p><b>Range:</b> 0 to 100%</p> <p><b>Note</b> This parameter appears only if the Display in Percent check box is checked.</p>
Beacons Received	<p>The percentage of beacon packets received from the access point versus those expected to have been sent. The higher the value and the wider the bar graph, the clearer the signal.</p> <p>The trend graph to the right of bar graph provides a visual interpretation of the signal clarity over time. Differences in signal clarity are indicated by the following colors: green (highest quality), yellow (average), and red (lowest quality).</p> <p><b>Example:</b> The access point sends out 10 beacons per second, so you would expect the client adapter to receive 50 beacon packets in 5 seconds. If it receives only 40 packets, the percentage of beacons received would be 80%.</p> <p><b>Range:</b> 0 to 100%</p> <p><b>Note</b> This parameter appears only if the Display in Percent check box is checked and the client adapter does not provide a signal quality value.</p>

**Table F-1 Site Survey Utility - Associated AP Status (continued)**

Associated AP Status Parameter	Description
Signal-to-Noise Ratio	<p>The difference between the signal strength and the noise level. The higher the value and the wider the bar graph, the better the client adapter's ability to communicate with the access point.</p> <p>The trend graph to the right of the bar graph provides a visual interpretation of the signal-to-noise ratio over time. Differences in the client adapter's ability to communicate are indicated by the following colors: green (highest quality), yellow (average), and red (lowest quality).</p> <p><b>Range:</b> Poor, Fair, Good, Excellent; 0 to 50 dB</p> <p><b>Note</b> This parameter appears only if the Display in Percent check box is unchecked.</p>
Overall Link Quality	<p>A combination of signal strength and signal quality. The higher the value and the wider the bar graph, the better the client adapter's ability to communicate with the access point.</p> <p>The trend graph to the right of the bar graph provides a visual interpretation of the overall link quality over time. Differences in quality are indicated by the following colors: green (highest quality), yellow (average), and red (lowest quality).</p> <p><b>Value:</b> Poor, Fair, Good, Excellent; 0 to 100%</p> <p><b>Note</b> This parameter appears only if the Display as Percent check box is checked.</p>
Link Speed	<p>The site survey utility monitors transmitted network traffic, and the link speed reflects the current transmit rate of data packets.</p> <p>The trend graph provides a visual interpretation of the packet transmit rate over time. Differences in link speed are indicated by the following colors: green (fastest), yellow (middle of the range), and red (slowest).</p> <p><b>Value:</b> 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps, depending on radio band</p>

## Using the AP Scan List Tab

You can perform these functions from the AP Scan List tab:

- View the AP scan list, [F-79](#)
- Pause the AP scan list, [F-83](#)
- View AP details, [F-83](#)
- Generate an AP scan log file, [F-86](#)
- View an accumulation of access points, [F-88](#)

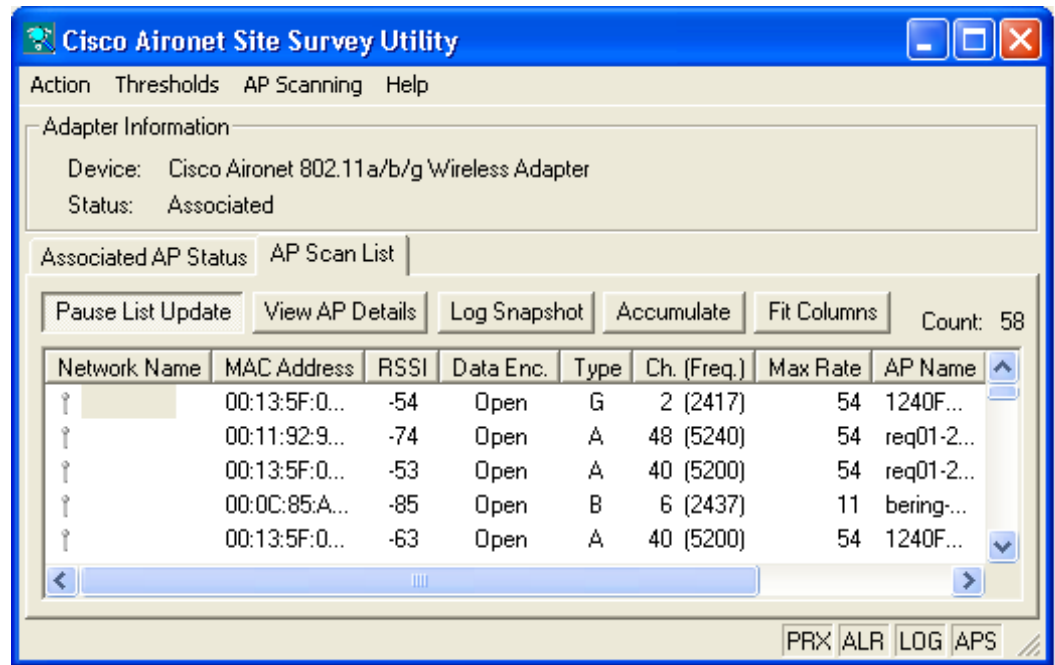
Follow the instructions on the pages indicated to perform these functions.

## Viewing the AP Scan List


Your client adapter can detect nearby access points by the beacon signals that the access points continually transmit. The AP scan list displays a continuously updated list of the access points detected by your client adapter as well as the information contained in their beacons.

To view the AP scan list, click the **AP Scan List** tab. The AP scan list appears (see [Figure F-5](#)).

**Figure F-5** Site Survey Utility - AP Scan List



To view the entire list of access points and all their information, perform one of the following:

- Click the resize tab in the lower right corner of the main window and drag it until the window reaches the desired size. 
- Use the vertical and horizontal scroll bars.
- Click the middle button in the top right corner of the window.



**Note**

Clicking **Fit Columns** resizes the columns on the AP scan list so that they are as wide as their widest text. This feature enables you to view the text in each column without it being truncated. However, you can also manually resize the columns by clicking on the edges of the column headers and dragging.

[Table F-2](#) interprets the information that is displayed in the AP scan list.



**Note**

The AP Detailed Information window provides details for many of the parameters listed in [Table F-2](#). See the “[Viewing AP Details](#)” section on [page F-83](#) for additional information.

**Note**

The AP Scanning drop-down menu contains options that enable you to save and open the AP scan list. These two options are available only when the AP Scan List tab is selected. See the [“Using AP Scanning” section on page F-96](#) for more information.

**Table F-2 Site Survey Utility - AP Scan List**







AP Scan List Parameter	Description						
Count	The number of rows, or access points, in the scan list. <b>Note</b> This parameter appears above the AP scan list and to the right.						
Network Name	The network name, or service set identifier (SSID), indicates the name of an available wireless network. The icon to the left of the SSID provides information on link status.						
	<table border="1"> <thead> <tr> <th>Icon</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td></td> <td>An available wireless network.</td> </tr> <tr> <td></td> <td>The wireless network to which your client adapter is currently associated.</td> </tr> </tbody> </table>	Icon	Description		An available wireless network.		The wireless network to which your client adapter is currently associated.
Icon	Description						
	An available wireless network.						
	The wireless network to which your client adapter is currently associated.						
	<b>Note</b> The SSID of a Cisco IOS access point appears in the list of available networks only if a Guest Mode SSID is enabled or the Broadcast SSID in Beacon option is selected. Refer to the software configuration guide for your access point for additional information.						
MAC Address	The access point’s MAC address. <b>Note</b> This field displays the MAC address of the access point’s Ethernet port (for access points that do not run Cisco IOS software) or the MAC address of the access point’s radio (for access points that run Cisco IOS software). The MAC address of the Ethernet port on access points that run Cisco IOS software is printed on a label on the back of the device.						
RSSI	The received signal strength indicator (RSSI) is a measure of signal strength in decibels with respect to milliwatts (dBm).						
Time of Day	The date and time when the signal strength of each access point was at its maximum. They appear in this format: 2005-07-20 16:13:09. <b>Note</b> The time is based on a 24-hour clock. <b>Note</b> This field is visible only in Accumulate mode. See the <a href="#">“Viewing an Accumulation of Access Points” section on page F-88</a> for information on the Accumulate mode.						

Table F-2 Site Survey Utility - AP Scan List (continued)

AP Scan List Parameter	Description						
Data Encryption	Indicates whether the data exchanged with this access point is encrypted. <b>Value:</b> Secure or Open						
	<table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Secure</td> <td>The data exchanged with this access point is encrypted.</td> </tr> <tr> <td>Open</td> <td>The data exchanged with this access point is unencrypted.</td> </tr> </tbody> </table>	Value	Description	Secure	The data exchanged with this access point is encrypted.	Open	The data exchanged with this access point is unencrypted.
Value	Description						
Secure	The data exchanged with this access point is encrypted.						
Open	The data exchanged with this access point is unencrypted.						
Type	The IEEE 802.11 standard that describes the access point's radio band. <b>Value:</b> A, B, or G						
Channel (Frequency)	The channel and radio frequency (in MHz) that the access point is currently using for communications. <b>Value:</b> Dependent on radio band and regulatory domain						
Max Rate	The maximum rate at which the client adapter can transfer data with an access point. The supported rates of both the client adapter and the access point are examined, and the highest rate that they have in common is the one that is used.						
AP Name	The access point's name. It is shown only if the access point was configured with a name, Aironet Extensions are enabled (on access points running Cisco IOS Release 12.2(4)JA or later), and the access point transmits this information. <b>Note</b> This field shows up to 15 characters although the name of the access point may be longer.						
Load	The access point's channel utilization in terms of traffic and throughput. <b>Value:</b> 0 to 100% <b>Note</b> This parameter is shown only if the access point is using QoS Basis Service Set (QBSS) or call admission control (CAC). If neither is used, this field is left blank. If both are used, the value comes from the QBSS.						
CCX	The version of Cisco Compatible Extensions (CCX) supported by the access point. It is shown only if the access point transmits this information. <b>Value:</b> 1, 2, 3, or 4						



Table F-2 Site Survey Utility - AP Scan List (continued)

AP Scan List Parameter	Description																						
Other Information	<p>A list of miscellaneous values that may appear depending on the access point's current status and the information that it transmits.</p> <p><b>Values:</b> See table below.</p>																						
	<table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Ad-Hoc</td> <td>Indicates that the device is not an access point but another client adapter operating in ad hoc mode.</td> </tr> <tr> <td>CAC</td> <td>Indicates that the access point is using distributed call admission control (CAC).</td> </tr> <tr> <td>CEC</td> <td>Indicates that the access point is using Cisco extended capabilities (CEC).</td> </tr> <tr> <td>Power</td> <td>Indicates that the access point can limit the transmitting power of the client adapter. The power limit is shown in milliwatts (mW).</td> </tr> <tr> <td>Qos</td> <td>Indicates that the access point is using quality of service (QoS). QoS on wireless LANs (WLAN) provides prioritization of traffic from the access point over the WLAN based on traffic classification.</td> </tr> <tr> <td>RM-Normal RM-APScan RM-CliWlk</td> <td>Indicates that the access point is using radio management. RM-Normal indicates normal status, RM-APScan indicates AP radio scan, and RM-CliWlk indicates client walkabout. Any unrecognized value appears as RM-State?.</td> </tr> <tr> <td>Ssidl</td> <td>Indicates that the access point is using the SSID List feature. The number of hidden SSIDs is shown as a number (for example, Ssidl:2).</td> </tr> <tr> <td>WMM</td> <td>Indicates that the access point is using Wi-Fi Multimedia (WMM), a component of the IEEE 802.11e wireless LAN standard for quality of service (QoS).</td> </tr> <tr> <td>WPA</td> <td>Indicates that the access point is using Wi-Fi Protected Access (WPA), a standards-based security solution from the Wi-Fi Alliance that provides data protection and access control for wireless LAN systems. It is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification. WPA uses TKIP and MIC for data protection and 802.1X for authenticated key management.</td> </tr> <tr> <td>WPA2</td> <td>Indicates that the access point is using Wi-Fi Protected Access 2 (WPA2), the next generation of Wi-Fi security. It is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard. WPA2 uses AES-CCMP for data protection and 802.1X for authenticated key management.</td> </tr> </tbody> </table>	Value	Description	Ad-Hoc	Indicates that the device is not an access point but another client adapter operating in ad hoc mode.	CAC	Indicates that the access point is using distributed call admission control (CAC).	CEC	Indicates that the access point is using Cisco extended capabilities (CEC).	Power	Indicates that the access point can limit the transmitting power of the client adapter. The power limit is shown in milliwatts (mW).	Qos	Indicates that the access point is using quality of service (QoS). QoS on wireless LANs (WLAN) provides prioritization of traffic from the access point over the WLAN based on traffic classification.	RM-Normal RM-APScan RM-CliWlk	Indicates that the access point is using radio management. RM-Normal indicates normal status, RM-APScan indicates AP radio scan, and RM-CliWlk indicates client walkabout. Any unrecognized value appears as RM-State?.	Ssidl	Indicates that the access point is using the SSID List feature. The number of hidden SSIDs is shown as a number (for example, Ssidl:2).	WMM	Indicates that the access point is using Wi-Fi Multimedia (WMM), a component of the IEEE 802.11e wireless LAN standard for quality of service (QoS).	WPA	Indicates that the access point is using Wi-Fi Protected Access (WPA), a standards-based security solution from the Wi-Fi Alliance that provides data protection and access control for wireless LAN systems. It is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification. WPA uses TKIP and MIC for data protection and 802.1X for authenticated key management.	WPA2	Indicates that the access point is using Wi-Fi Protected Access 2 (WPA2), the next generation of Wi-Fi security. It is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard. WPA2 uses AES-CCMP for data protection and 802.1X for authenticated key management.
Value	Description																						
Ad-Hoc	Indicates that the device is not an access point but another client adapter operating in ad hoc mode.																						
CAC	Indicates that the access point is using distributed call admission control (CAC).																						
CEC	Indicates that the access point is using Cisco extended capabilities (CEC).																						
Power	Indicates that the access point can limit the transmitting power of the client adapter. The power limit is shown in milliwatts (mW).																						
Qos	Indicates that the access point is using quality of service (QoS). QoS on wireless LANs (WLAN) provides prioritization of traffic from the access point over the WLAN based on traffic classification.																						
RM-Normal RM-APScan RM-CliWlk	Indicates that the access point is using radio management. RM-Normal indicates normal status, RM-APScan indicates AP radio scan, and RM-CliWlk indicates client walkabout. Any unrecognized value appears as RM-State?.																						
Ssidl	Indicates that the access point is using the SSID List feature. The number of hidden SSIDs is shown as a number (for example, Ssidl:2).																						
WMM	Indicates that the access point is using Wi-Fi Multimedia (WMM), a component of the IEEE 802.11e wireless LAN standard for quality of service (QoS).																						
WPA	Indicates that the access point is using Wi-Fi Protected Access (WPA), a standards-based security solution from the Wi-Fi Alliance that provides data protection and access control for wireless LAN systems. It is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification. WPA uses TKIP and MIC for data protection and 802.1X for authenticated key management.																						
WPA2	Indicates that the access point is using Wi-Fi Protected Access 2 (WPA2), the next generation of Wi-Fi security. It is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard. WPA2 uses AES-CCMP for data protection and 802.1X for authenticated key management.																						

## Pausing the AP Scan List

The AP scan list is updated continually. To pause the current list, click **Pause List Update** above the AP scan list.



**Note**

AP scanning continues to occur in the background when the Pause List Update button is depressed. For example, the threshold based on the AP scan list count continues to function.



**Note**

Clicking this button again resumes the list update.

## Viewing AP Details

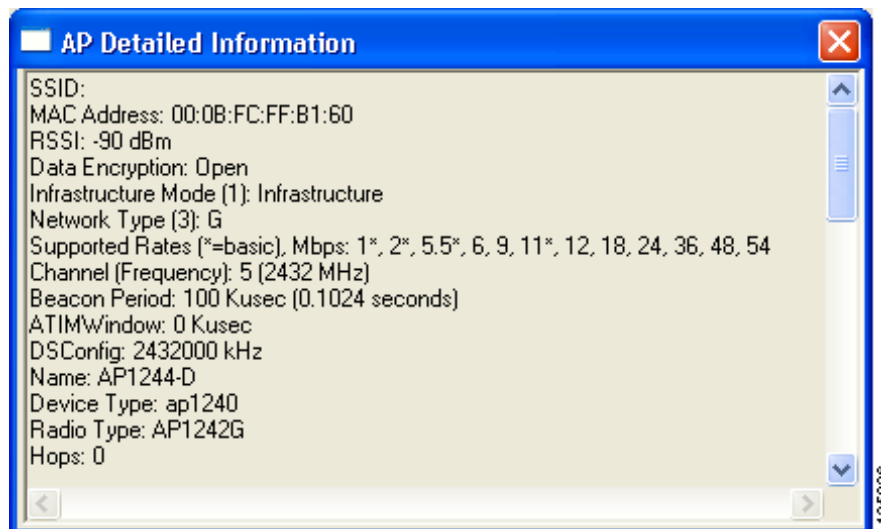
To view details for a particular access point in the AP scan list, select the desired network name in the scan list and click **View AP Details**. The AP Detailed Information window appears (see [Figure F-6](#)).



**Note**

You can also open the AP Detailed Information window by double-clicking in the first column of the desired row.

**Figure F-6** Site Survey Utility - AP Detailed Information Window



[Table F-3](#) interprets the information that is displayed in the AP Detailed Information window.



**Note**

The AP Detailed Information window contains text summaries of all the information elements present in the access point's beacon or probe response. As a result, the window may contain different information than that described in [Table F-3](#).

**Note**

If you also want the AP Detailed Information window to display debugging information, including a hexadecimal debug-style dump of raw access point scan data, choose **Options** from the site survey utility's Action drop-down menu and check the **Enable Expert Mode for AP Detailed Information** check box. The debug information appears at the bottom of the AP Detailed Information window under the "Expert Mode (Debug Dump)" heading.

**Table F-3 Site Survey Utility - AP Detailed Information**

Detailed Information Parameter	Description
SSID	The network name, or service set identifier (SSID), indicates the name of the access point's wireless network.
MAC Address	The access point's MAC address. <b>Note</b> This field displays the MAC address of the access point's Ethernet port (for access points that do not run Cisco IOS software) or the MAC address of the access point's radio (for access points that run Cisco IOS software). The MAC address of the Ethernet port on access points that run Cisco IOS software is printed on a label on the back of the device.
RSSI	The received signal strength indicator (RSSI) is a measure of signal strength in decibels with respect to milliwatts (dBm).
Data Encryption	Indicates whether the data exchanged with this access point is encrypted. <b>Value:</b> Secure or Open
Infrastructure Mode	Indicates whether the device is an access point operating in infrastructure mode or another client adapter operating in ad hoc mode. <b>Value:</b> Infrastructure or Ad-Hoc
Network Type	The IEEE 802.11 standard that describes the access point's radio band. <b>Value:</b> A, B, or G
Supported Rates	The rates at which the access point is capable of transmitting and receiving data packets. <b>Value:</b> 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps
Channel (Frequency)	The channel and radio frequency that the access point is currently using for communications. <b>Value:</b> Dependent on radio band and regulatory domain
Beacon Period	The amount of time between access point beacons in Kilomicroseconds (K $\mu$ sec). <b>Note</b> One K $\mu$ sec equals 1,024 microseconds.
ATIMWindow	Announcement traffic information message (ATIM) window. The brief time period immediately following the transmission of each beacon in an ad hoc network. This value is expressed in Kilomicroseconds (K $\mu$ sec). <b>Note</b> One K $\mu$ sec equals 1,024 microseconds. <b>Note</b> This parameter's value is 0 when the device is operating in infrastructure mode.

**Table F-3 Site Survey Utility - AP Detailed Information (continued)**

Detailed Information Parameter	Description
DSConfig	The frequency of the selected channel. <b>Range:</b> 2,412,000 to 2,484,000 kHz (802.11b/g); 5,000,000 to 6,000,000 kHz (802.11a)
Name	The access point's name. It is shown only if the access point was configured with a name, Aironet Extensions are enabled (on access points running Cisco IOS Release 12.2(4)JA or later), and the access point transmits this information. <b>Note</b> This field shows up to 15 characters although the name of the access point may be longer.
Device Type	The access point's model number.
Radio Type	The type of radio used in the access point.
Hops	The number of hops that the packets must take to get to the root. For example, if there is a repeater between your client adapter and the access point to which it is associated, the number of hops is 1.
Load	The access point's channel utilization in terms of traffic and throughput. <b>Note</b> This parameter is shown only if the access point is using QoS Basis Service Set (QBSS) or call admission control (CAC). If neither is used, this field is left blank. If both are used, the value comes from the QBSS.
CWmin	The minimum value used by the access point to calculate a contention window (CW). <b>Note</b> Contention occurs when two or more radios in the same area try to transmit at the same time. When this occurs, the radios wait for a certain amount of time before trying again. Because contention can occur more than once, the radios use a series of progressively longer wait periods, or "windows," each time they encounter contention for a given packet.
CWmax	The maximum value used by the access point to calculate a contention window (CW). <b>Note</b> Contention occurs when two or more radios in the same area try to transmit at the same time. When this occurs, the radios wait for a certain amount of time before trying again. Because contention can occur more than once, the radios use a series of progressively longer wait periods, or "windows," each time they encounter contention for a given packet.
Associations	The number of associations currently being maintained by the access point.
CCX Version	The version of Cisco Compatible Extensions (CCX) supported by the access point.

**Table F-3 Site Survey Utility - AP Detailed Information (continued)**

Detailed Information Parameter	Description
Power Limit	The power limit that the access point has set for the client adapter. It is shown in milliwatts (mW).
RM-Normal RM-APScan RM-CliWlk	Indicates that the access point is using radio management. RM-Normal indicates normal status, RM-APScan indicates AP radio scan, and RM-CliWlk indicates client walkabout. Any unrecognized value appears as RM-State?.

## Generating an AP Scan Log File

To enter the current contents of the AP scan list into a log file, click **Log Snapshot**. The “Logged current AP Scan List” message appears below the scan list, and the log file is saved. The default filename is SST\_APScanLog.txt, and the default location is the directory where the site survey utility is installed.



### Note

If desired, you can change the filename and its location using the AP Scan List Logging Configuration window. See the “[Configuring AP Scan Logging](#)” section on page F-96 for more information.

If the AP scan list is paused when you click Log Snapshot, the currently displayed data (not the latest available data) is added to the log. Each time you click **Log Snapshot**, the new scan list is written at the end of the existing log file.

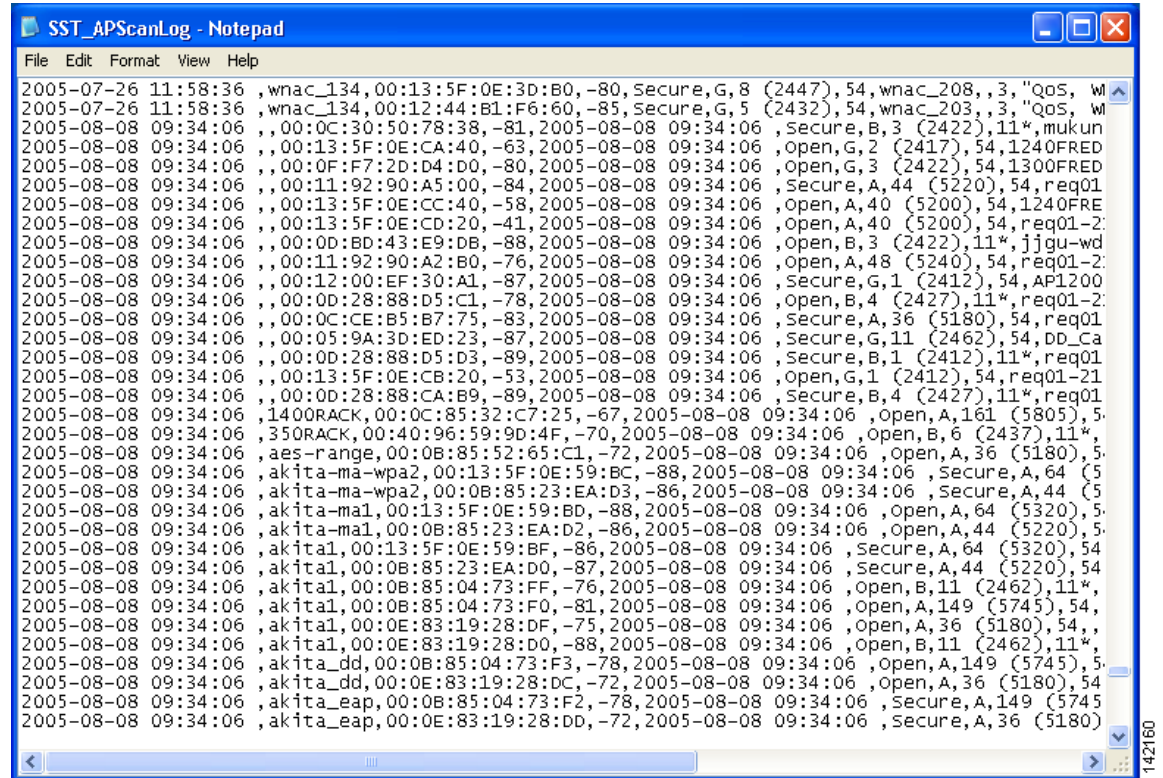
To view the log file, choose **View AP Scan Log** from the AP Scanning drop-down menu. The log file opens in the configured viewer (see [Figure F-7](#)).



### Note

The log file can be viewed in Notepad or any other viewer. However, because it is written in a comma-separated values (CSV) format, it can also be opened by a spreadsheet or database program (such as Microsoft Excel). If the file is renamed with a .csv extension, Microsoft Excel would automatically place the values in separate columns.

Figure F-7 Site Survey Utility - AP Scan Log File



```

2005-07-26 11:58:36 ,wnac_134,00:13:5F:0E:3D:B0,-80,Secure,G,8 (2447),54,wnac_208,,3,"QoS, W
2005-07-26 11:58:36 ,wnac_134,00:12:44:B1:F6:60,-85,Secure,G,5 (2432),54,wnac_203,,3,"QoS, W
2005-08-08 09:34:06 ,,00:0C:30:50:78:38,-81,2005-08-08 09:34:06 ,secure,B,3 (2422),11*,mukun
2005-08-08 09:34:06 ,,00:13:5F:0E:CA:40,-63,2005-08-08 09:34:06 ,open,G,2 (2417),54,1240FRED
2005-08-08 09:34:06 ,,00:0F:F7:2D:D4:D0,-80,2005-08-08 09:34:06 ,open,G,3 (2422),54,1300FRED
2005-08-08 09:34:06 ,,00:11:92:90:A5:00,-84,2005-08-08 09:34:06 ,secure,A,44 (5220),54,req01
2005-08-08 09:34:06 ,,00:13:5F:0E:CC:40,-58,2005-08-08 09:34:06 ,open,A,40 (5200),54,1240FRE
2005-08-08 09:34:06 ,,00:13:5F:0E:CD:20,-41,2005-08-08 09:34:06 ,open,A,40 (5200),54,req01-2
2005-08-08 09:34:06 ,,00:0D:BD:43:E9:DB,-88,2005-08-08 09:34:06 ,open,B,3 (2422),11*,jjgu-wd
2005-08-08 09:34:06 ,,00:11:92:90:A2:B0,-76,2005-08-08 09:34:06 ,open,A,48 (5240),54,req01-2
2005-08-08 09:34:06 ,,00:12:00:EF:30:A1,-87,2005-08-08 09:34:06 ,secure,G,1 (2412),54,AP1200
2005-08-08 09:34:06 ,,00:0D:28:88:D5:C1,-78,2005-08-08 09:34:06 ,open,B,4 (2427),11*,req01-2
2005-08-08 09:34:06 ,,00:0C:CE:B5:B7:75,-83,2005-08-08 09:34:06 ,secure,A,36 (5180),54,req01
2005-08-08 09:34:06 ,,00:05:9A:3D:ED:23,-87,2005-08-08 09:34:06 ,secure,G,11 (2462),54,DD_Ca
2005-08-08 09:34:06 ,,00:0D:28:88:D5:D3,-89,2005-08-08 09:34:06 ,secure,B,1 (2412),11*,req01
2005-08-08 09:34:06 ,,00:13:5F:0E:CB:20,-53,2005-08-08 09:34:06 ,open,G,1 (2412),54,req01-21
2005-08-08 09:34:06 ,,00:0D:28:88:CA:B9,-89,2005-08-08 09:34:06 ,secure,B,4 (2427),11*,req01
2005-08-08 09:34:06 ,1400RACK,00:0C:85:32:C7:25,-67,2005-08-08 09:34:06 ,open,A,161 (5805),5
2005-08-08 09:34:06 ,350RACK,00:40:96:59:9D:4F,-70,2005-08-08 09:34:06 ,open,B,6 (2437),11*,
2005-08-08 09:34:06 ,aes-range,00:0B:85:52:65:C1,-72,2005-08-08 09:34:06 ,open,A,36 (5180),5
2005-08-08 09:34:06 ,akita-ma-wpa2,00:13:5F:0E:59:BC,-88,2005-08-08 09:34:06 ,secure,A,64 (5
2005-08-08 09:34:06 ,akita-ma-wpa2,00:0B:85:23:EA:D3,-86,2005-08-08 09:34:06 ,secure,A,44 (5
2005-08-08 09:34:06 ,akita-ma1,00:13:5F:0E:59:BD,-88,2005-08-08 09:34:06 ,open,A,64 (5320),5
2005-08-08 09:34:06 ,akita-ma1,00:0B:85:23:EA:D2,-86,2005-08-08 09:34:06 ,open,A,44 (5220),5
2005-08-08 09:34:06 ,akita1,00:13:5F:0E:59:BF,-86,2005-08-08 09:34:06 ,secure,A,64 (5320),54
2005-08-08 09:34:06 ,akita1,00:0B:85:23:EA:D0,-87,2005-08-08 09:34:06 ,secure,A,44 (5220),54
2005-08-08 09:34:06 ,akita1,00:0B:85:04:73:FF,-76,2005-08-08 09:34:06 ,open,B,11 (2462),11*,
2005-08-08 09:34:06 ,akita1,00:0B:85:04:73:F0,-81,2005-08-08 09:34:06 ,open,A,149 (5745),54
2005-08-08 09:34:06 ,akita1,00:0E:83:19:28:DF,-75,2005-08-08 09:34:06 ,open,A,36 (5180),54,,
2005-08-08 09:34:06 ,akita1,00:0E:83:19:28:D0,-88,2005-08-08 09:34:06 ,open,B,11 (2462),11*,
2005-08-08 09:34:06 ,akita_dd,00:0B:85:04:73:F3,-78,2005-08-08 09:34:06 ,open,A,149 (5745),5
2005-08-08 09:34:06 ,akita_dd,00:0E:83:19:28:DC,-72,2005-08-08 09:34:06 ,open,A,36 (5180),54
2005-08-08 09:34:06 ,akita_eap,00:0B:85:04:73:F2,-78,2005-08-08 09:34:06 ,secure,A,149 (5745
2005-08-08 09:34:06 ,akita_eap,00:0E:83:19:28:DD,-72,2005-08-08 09:34:06 ,secure,A,36 (5180)

```

The log entries are time-stamped and appear in ASCII text. Each line typically represents a different access point.



**Note**

If the Accumulate button is depressed when you click Log Snapshot, two timestamps appear on each line. The timestamp in column one of the log file is the time when the log entry is made. The second timestamp, which appears only when the Accumulate button is depressed, is the Time of Day. This value indicates the date and time when the signal strength of each access point was at its maximum. Both timestamps appear in this format: 2005-07-20 16:13:09. The time is based on a 24-hour clock. For example, the first two lines in Figure F-7 show only one timestamp while the remaining lines show both timestamps.



**Note**

As an alternative to using the Log Snapshot button, you can configure the site survey utility to automatically copy the contents of the AP scan list to a log file using the AP Scanning drop-down menu options. See the “Using AP Scanning” section on page F-96 for more information.

## Viewing an Accumulation of Access Points

Clicking the **Accumulate** button changes the behavior of the AP scan list. Instead of displaying only the current AP scan list, the list includes all of the access points (based on MAC address) that have appeared in the scan list since the Accumulate button was last clicked.

After a scan line is added to the list, it is never removed nor updated with new scan information unless the signal strength (RSSI) of the latest scan is greater than or equal to any detected previously from that access point. The Time of Day field, which appears only in Accumulate mode, indicates the date and time when the signal strength of each access point was at its maximum.

The Accumulate mode provides a convenient way to list all access points within a facility, not just those that may be visible at one time from a particular location. By using the information in the Time of Day field with a site map and a wristwatch, you may be able to determine the approximate location of each access point in the list.

**Note**

---

Clicking the Accumulate button again deactivates the Accumulate mode and returns the current AP scan list.

---

**Note**

---

You can use the Save AP Scan List and Open AP Scan List options in the AP Scanning drop-down menu to save and reload accumulated scan lists back into the application at a later time.

---

## Using the Proximity Beeper

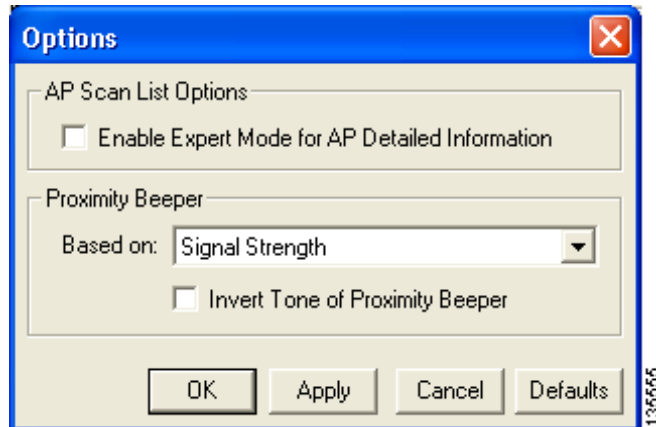
You can use the site survey utility's proximity beeper to identify areas where wireless coverage is good or weak based on the client adapter's proximity to access points within a particular area. The beeper can be set to sound as the client adapter approaches or moves farther away from an access point.

## Configuring the Proximity Beeper

Follow these steps to configure the proximity beeper.

- 
- Step 1** Choose **Options** from the site survey utility's Action drop-down menu. The Options window appears (see [Figure F-8](#)).

Figure F-8 Site Survey Utility - Options Window



**Step 2** Choose one of these options on which the proximity beeper will be based:

Proximity Beeper Option	Description
Signal Strength	The beeper sounds as an access point's signal becomes stronger. <b>Note</b> This is the default value.
Noise Level/Signal Quality	The beeper sounds as the level of background radio frequency energy decreases or the signal quality of the most recently received packets improves.
Signal-to-Noise Ratio/ Overall Link Quality	The beeper sounds as the client adapter's ability to communicate with an access point improves.
Link Speed	The beeper sounds as the transmit rate of data packets between the client adapter and an access point becomes faster.

**Step 3** Perform one of the following to set the tone of the proximity beeper:

- Uncheck the **Invert Tone of Proximity Beeper** check box if you want the beeper's rate and pitch to increase in response to the option selected in [Step 2](#). The beeps become more alarming as the client adapter moves closer to an access point, enabling you to identify areas of good coverage. This is the default setting.
- Check the **Invert Tone of Proximity Beeper** check box if you want the beeper's rate and pitch to decrease in response to the option selected in [Step 2](#). The beeps become more alarming as the client adapter approaches areas of weaker coverage.

**Step 4** Click **OK** to save your changes.

**Step 5** Follow the instructions in the [“Enabling the Proximity Beeper”](#) section below to enable the proximity beeper.



## Enabling the Proximity Beeper

To enable the proximity beeper, choose **Enable Proximity Beeper** from the Action drop-down menu or press **F6**. When the beeper is enabled, a check mark appears next to the Enable Proximity Beeper menu option, and PRX appears in the site survey utility's status bar.

**Note**

---

To disable the proximity beeper, choose the **Enable Proximity Beeper** menu option again so that the check mark disappears or re-press **F6**.

---

## Using Thresholds

You can perform these threshold-related functions:

- Configure threshold values, [F-90](#)
- Enable threshold triggers, [F-93](#)
- Enter a comment in the threshold log file, [F-94](#)
- View the threshold log file, [F-94](#)
- Delete the threshold log file, [F-95](#)

Follow the instructions on the pages indicated to perform these functions.

## Configuring Threshold Values

Follow these steps to configure threshold values that trigger audible alerts, entries in the threshold log file, or both.

- 
- Step 1** Choose **Configure Thresholds** from the site survey utility's Thresholds drop-down menu. The Threshold Logging Configuration window appears (see [Figure F-9](#)).

Figure F-9 Site Survey Utility - Threshold Logging Configuration Window

- Step 2** Check the check box for each condition below for which you want to trigger audible alerts, text entries in the threshold log file, or both. You can check as many as you like.

Condition	Description
A change in the client adapter's association status	Triggers audible alerts, log file entries, or both when the client adapter's association status changes. <b>Default:</b> Unchecked
Connectivity with this URL or IP Address	Triggers audible alerts, log file entries, or both when the client adapter is able to successfully access the specified URL or IP address after associating to an access point. When the client adapter associates to an access point, the connectivity test transmits ping requests to the specified URL or IP address at a rate of 4 per second for up to 10 seconds or until a ping reply is received. If a reply is received within that time, the test ends successfully. Otherwise, the test fails, and no triggers are generated. No further ping requests are sent until the client adapter loses association and reassociates. If you check this check box, be sure to also enter the URL or IP address that invokes the triggers. <b>Default:</b> Unchecked

Condition	Description
Signal Strength	<p>Triggers audible alerts, log file entries, or both when the Signal Strength value reaches or crosses over the specified threshold value. If you check this check box, be sure to also choose a threshold value.</p> <p><b>Threshold Value Range:</b> –95 to –45 dBm or 0 to 100%</p> <p><b>Default:</b> Unchecked; –75 dBm or 40%</p> <p><b>Note</b> The actual dBm reading could exceed the stated threshold value range.</p> <p><b>Note</b> The Display in percent check box on the Associated AP Status tab determines which threshold value units are used.</p>
Noise Level/Signal Quality	<p>Triggers audible alerts, log file entries, or both when the Noise Level or Signal Quality value reaches or crosses over the specified threshold value. If you check this check box, be sure to also choose a threshold value.</p> <p><b>Threshold Value Range:</b> –45 to –95 dBm or 0 to 100%</p> <p><b>Default:</b> Unchecked; –65 dBm or 40%</p> <p><b>Note</b> The actual dBm reading could exceed the stated threshold value range.</p> <p><b>Note</b> The Display in percent check box on the Associated AP Status tab determines which condition and threshold value units are used.</p>
Signal-to-Noise Ratio/Link Quality	<p>Triggers audible alerts, log file entries, or both when the Signal-to-Noise Ratio or Link Quality value reaches or crosses over the specified threshold value. If you check this check box, be sure to also choose a threshold value.</p> <p><b>Threshold Value Range:</b> 0 to 50 dBm or 0 to 100%</p> <p><b>Default:</b> Unchecked; 20 dBm or 40%</p> <p><b>Note</b> The actual dBm reading could exceed the stated threshold value range.</p> <p><b>Note</b> The Display in percent check box on the Associated AP Status tab determines which condition and threshold value units are used.</p>
Link Speed	<p>Triggers audible alerts, log file entries, or both when the Link Speed value reaches or crosses over the specified threshold value. If you check this check box, be sure to also choose a threshold value.</p> <p><b>Threshold Value Range:</b> 0 to the maximum rate of the current connection</p> <p><b>Default:</b> Unchecked; 11 Mbps</p>



**Note** When a value reaches a threshold and stays there, continuous triggers are not generated. After a value reaches a threshold, it must become not equal to the threshold value before another trigger is generated.

**Step 3** If you want to specify the length of time that the above conditions must exist before triggering audible alerts, log file entries, or both, check the **Hysteresis** check box and choose a value in seconds.

**Range:** 1 to 10 seconds

**Default:** Checked; 3 seconds



**Note** The Hysteresis setting does not apply to the connectivity test. Connectivity is achieved if just one ping response is returned.

**Step 4** The Filename field specifies the name and location of the threshold log file. If you want to change the name of the log file, enter a new name in the Filename field. If you want to change the location of the log file, click **Browse**, navigate to the desired location, and click **OK**.

**Default Name:** SST\_ThreshLog.txt

**Default Location:** The directory where the site survey utility is installed

**Step 5** The Viewer field specifies the name and location of the program that is used to view the threshold log file. (To view the log file, choose **View Threshold Log** from the Thresholds drop-down menu.) If you want a different program to be used, click **Browse**, navigate to the location of the desired program, and click **OK**.

**Default Program:** Notepad.exe

**Step 6** Click **OK** to save your changes.

**Step 7** Follow the instructions in the “[Enabling Threshold Triggers](#)” section below to enable the threshold triggers.

## Enabling Threshold Triggers

In the previous section, you specified the conditions under which threshold triggers are generated, provided those triggers are enabled.

To enable audible alerts when a threshold condition occurs, choose **Enable Threshold Alerts** from the Thresholds drop-down menu or press **F7**. When threshold alerts are enabled, a check mark appears next to the Enable Threshold Alerts menu option, and ALR appears in the site survey utility’s status bar.

To enable the logging of text messages to the threshold log file when a threshold condition occurs, choose **Enable Threshold Logging** from the Thresholds drop-down menu or press **F8**. When threshold logging is enabled, a check mark appears next to the Enable Threshold Logging menu option, and LOG appears in the site survey utility’s status bar.



**Note** You can enable one or both triggers.



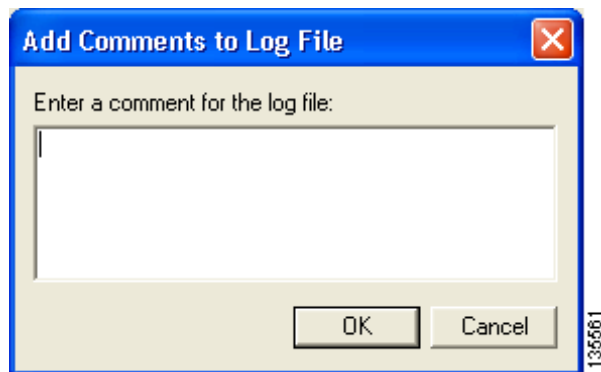
**Note** To disable the threshold triggers, choose the **Enable Threshold Alerts** and **Enable Threshold Logging** menu options again so that the check mark disappears or re-press **F7** and **F8**.

## Entering a Comment in the Threshold Log File

Follow these steps if you want to enter a comment in the threshold log file.

- Step 1** Choose **Add User Comment** from the Thresholds drop-down menu. The Add Comments to Log File window appears (see [Figure F-10](#)).

**Figure F-10** Site Survey Utility - Add Comments to Log File Window



- Step 2** Type one or more lines of text or paste text copied from another application.
- Step 3** Click **OK** to have your comments entered into the threshold log file.



**Note** User comments are entered in the threshold log file even if threshold logging is not currently enabled.

## Viewing the Threshold Log File

Follow these steps to view the threshold log file from within the site survey utility.



**Note**

You can also open the threshold log file from Windows Explorer.

- Step 1** Choose **View Threshold Log** from the Thresholds drop-down menu. The log file opens in the configured viewer (see [Figure F-11](#)).



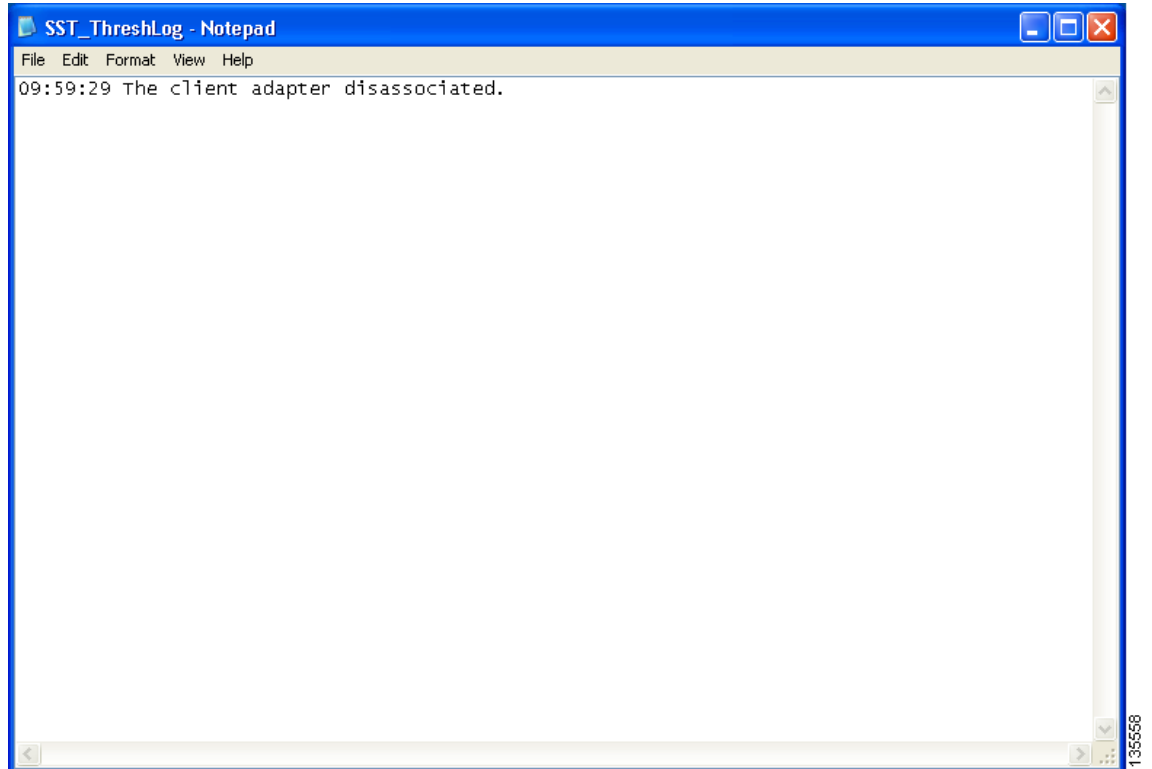
**Note**

The View Threshold Log menu option is disabled if the log file does not exist.



**Note**

[Figure F-11](#) shows the threshold log file in Notepad, but other viewers can be used.

**Figure F-11 Site Survey Utility - Threshold Log File Window**

- Step 2** Click the **X** in the upper right-hand corner of the window to close the window.
- 

## Deleting the Threshold Log File

Follow these steps to delete the threshold log file.

---

- Step 1** Choose **Delete Threshold Log** from the Thresholds drop-down menu.



**Note** The Delete Threshold Log menu option is disabled if the log file does not exist.

---

- Step 2** Click **Yes** when asked to confirm your decision.
-

## Using AP Scanning

You can perform these functions related to AP scanning:

- Configure AP scan logging, [F-96](#)
- Enable AP scan logging, [F-98](#)
- View the AP scan log, [F-98](#)
- Delete the AP scan log, [F-100](#)
- Save the AP scan list, [F-100](#)
- Open the AP scan list, [F-101](#)

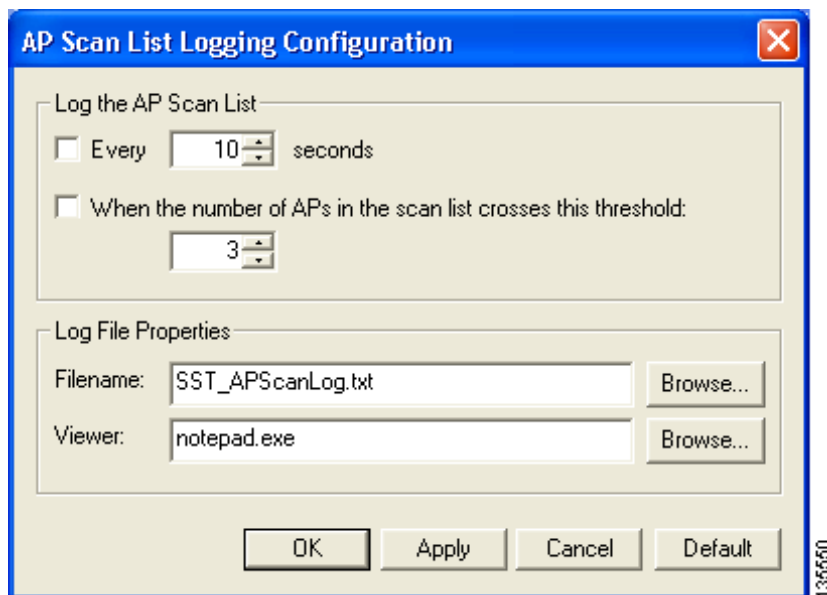
Follow the instructions on the pages indicated to perform these functions.

## Configuring AP Scan Logging

Follow these steps to configure the site survey utility to automatically copy the contents of the AP scan list to a log file.

- Step 1** Choose **Configure AP Scan Logging** from the AP Scanning drop-down menu. The AP Scan List Logging Configuration window appears (see [Figure F-12](#)).

**Figure F-12 Site Survey Utility - AP Scan List Logging Configuration Window**



- Step 2** Check the check box and select a numerical value for each condition below that you want to cause the contents of the AP scan list to be automatically copied to a log file. You can check one or both.

Condition	Description
Every XXX seconds	Causes the contents of the AP scan list to be copied to a log file after a specified amount of time elapses. For example, if you set the value to 60, the AP scan list is logged to a file every 60 seconds.  <b>Default:</b> Unchecked; 10 seconds
When the number of APs in the scan list crosses this threshold	Causes the contents of the AP scan list to be copied to a log file whenever the number of access points in the scan list reaches or crosses over the specified threshold value. For example, if you set the value to 5, the AP scan list is logged to a file each time the number of access points in the scan list rises to or above 5 or falls to or below 5. However, if the number of access points in the scan list stays at 5, continuous triggers are not generated.  <b>Default:</b> Unchecked; 3  <b>Note</b> If threshold alerts are enabled (on the Thresholds drop-down menu), an audible alert sounds whenever the number of access points in the scan list reaches or crosses over the specified threshold value. Likewise, if threshold logging is enabled, a text entry is made to the threshold log file whenever this condition is met.

- Step 3** The Filename field specifies the name and location of the AP scan log file. If you want to change the name of the log file, enter a new name in the Filename field. If you want to change the location of the log file, click **Browse**, navigate to the desired location, and click **OK**.

**Default Name:** SST\_APScanLog.txt

**Default Location:** The directory in which the site survey utility is installed



**Note** The filename and location that you choose here also applies to the log file that is created when you click the Log Snapshot button on the AP Scan List tab.

- Step 4** The Viewer field specifies the name and location of the program that is used to view the AP scan log file. (To view the log file, choose **View AP Scan Log** from the AP Scanning drop-down menu.) If you want a different program to be used, click **Browse**, navigate to the location of the desired program, and click **OK**.

**Default Program:** Notepad.exe



**Note** The log file can be viewed in Notepad or any other viewer. However, because it is written in a comma-separated values (CSV) format, it can also be opened by a spreadsheet or database program (such as Microsoft Excel). If the file is renamed with a .csv extension, Microsoft Excel would automatically place the values in separate columns.

- Step 5** Click **OK** to save your changes.

- Step 6** Follow the instructions in the [“Enabling AP Scan Logging”](#) section below to enable AP scan logging.



## Enabling AP Scan Logging

To enable the site survey utility to automatically copy the contents of the AP scan list to a log file under the conditions specified above, choose **Enable AP Scan Logging** from the AP Scanning drop-down menu or press **F9**. When AP scan logging is enabled, a check mark appears next to the Enable AP Scan Logging menu option, and APS appears in the site survey utility's status bar.

**Note**

When AP scan logging is enabled, log entries are made even when the AP Scan List tab is not visible and when it is visible with updates paused.

**Note**

To disable AP scan logging, choose the **Enable AP Scan Logging** menu option again so that the check mark disappears or re-press **F9**.

## Viewing the AP Scan Log

Follow these steps to view the AP scan log file from within the site survey utility.

**Note**

You can also open the AP scan log file from Windows Explorer.

**Step 1**

Choose **View AP Scan Log** from the AP Scanning drop-down menu. The log file opens in the configured viewer (see [Figure F-13](#)).

**Note**

The View AP Scan Log menu option is disabled if the log file does not exist.

**Note**

[Figure F-13](#) shows the AP scan log file in Notepad, but other viewers can be used.

Figure F-13 Site Survey Utility - AP Scan Log File

```

SST_APScanLog - Notepad
File Edit Format View Help
2005-07-26 11:58:36 ,wnac_134,00:13:5F:0E:3D:B0,-80,Secure,G,8 (2447),54,wnac_208,,3,"QoS, W
2005-07-26 11:58:36 ,wnac_134,00:12:44:B1:F6:60,-85,Secure,G,5 (2432),54,wnac_203,,3,"QoS, W
2005-08-08 09:34:06 ,,00:0C:30:50:78:38,-81,2005-08-08 09:34:06 ,secure,B,3 (2422),11*,mukun
2005-08-08 09:34:06 ,,00:13:5F:0E:CA:40,-63,2005-08-08 09:34:06 ,open,G,2 (2417),54,1240FRED
2005-08-08 09:34:06 ,,00:0F:F7:2D:D4:D0,-80,2005-08-08 09:34:06 ,open,G,3 (2422),54,1300FRED
2005-08-08 09:34:06 ,,00:11:92:90:A5:00,-84,2005-08-08 09:34:06 ,secure,A,44 (5220),54,req01
2005-08-08 09:34:06 ,,00:13:5F:0E:CC:40,-58,2005-08-08 09:34:06 ,open,A,40 (5200),54,1240FRE
2005-08-08 09:34:06 ,,00:13:5F:0E:CD:20,-41,2005-08-08 09:34:06 ,open,A,40 (5200),54,req01-2
2005-08-08 09:34:06 ,,00:0D:BD:43:E9:DB,-88,2005-08-08 09:34:06 ,open,B,3 (2422),11*,jjgu-wd
2005-08-08 09:34:06 ,,00:11:92:90:A2:B0,-76,2005-08-08 09:34:06 ,open,A,48 (5240),54,req01-2
2005-08-08 09:34:06 ,,00:12:00:EF:30:A1,-87,2005-08-08 09:34:06 ,secure,G,1 (2412),54,AP1200
2005-08-08 09:34:06 ,,00:0D:28:88:D5:C1,-78,2005-08-08 09:34:06 ,open,B,4 (2427),11*,req01-2
2005-08-08 09:34:06 ,,00:0C:CE:B5:B7:75,-83,2005-08-08 09:34:06 ,secure,A,36 (5180),54,req01
2005-08-08 09:34:06 ,,00:05:9A:3D:ED:23,-87,2005-08-08 09:34:06 ,secure,G,11 (2462),54,DD_ca
2005-08-08 09:34:06 ,,00:0D:28:88:D5:D3,-89,2005-08-08 09:34:06 ,secure,B,1 (2412),11*,req01
2005-08-08 09:34:06 ,,00:13:5F:0E:CB:20,-53,2005-08-08 09:34:06 ,open,G,1 (2412),54,req01-21
2005-08-08 09:34:06 ,,00:0D:28:88:CA:B9,-89,2005-08-08 09:34:06 ,secure,B,4 (2427),11*,req01
2005-08-08 09:34:06 ,1400RACK,00:0C:85:32:C7:25,-67,2005-08-08 09:34:06 ,open,A,161 (5805),5
2005-08-08 09:34:06 ,350RACK,00:40:96:59:9D:4F,-70,2005-08-08 09:34:06 ,open,B,6 (2437),11*,
2005-08-08 09:34:06 ,aes-range,00:0B:85:52:65:C1,-72,2005-08-08 09:34:06 ,open,A,36 (5180),5
2005-08-08 09:34:06 ,akita-ma-wpa2,00:13:5F:0E:59:BC,-88,2005-08-08 09:34:06 ,secure,A,64 (5
2005-08-08 09:34:06 ,akita-ma-wpa2,00:0B:85:23:EA:D3,-86,2005-08-08 09:34:06 ,secure,A,44 (5
2005-08-08 09:34:06 ,akita-ma1,00:13:5F:0E:59:BD,-88,2005-08-08 09:34:06 ,open,A,64 (5320),5
2005-08-08 09:34:06 ,akita-ma1,00:0B:85:23:EA:D2,-86,2005-08-08 09:34:06 ,open,A,44 (5220),5
2005-08-08 09:34:06 ,akita1,00:13:5F:0E:59:BF,-86,2005-08-08 09:34:06 ,secure,A,64 (5320),54
2005-08-08 09:34:06 ,akita1,00:0B:85:23:EA:D0,-87,2005-08-08 09:34:06 ,secure,A,44 (5220),54
2005-08-08 09:34:06 ,akita1,00:0B:85:04:73:FF,-76,2005-08-08 09:34:06 ,open,B,11 (2462),11*,
2005-08-08 09:34:06 ,akita1,00:0B:85:04:73:F0,-81,2005-08-08 09:34:06 ,open,A,149 (5745),54,
2005-08-08 09:34:06 ,akita1,00:0E:83:19:28:DF,-75,2005-08-08 09:34:06 ,open,A,36 (5180),54,,
2005-08-08 09:34:06 ,akita1,00:0E:83:19:28:D0,-88,2005-08-08 09:34:06 ,open,B,11 (2462),11*,
2005-08-08 09:34:06 ,akita_dd,00:0B:85:04:73:F3,-78,2005-08-08 09:34:06 ,open,A,149 (5745),5
2005-08-08 09:34:06 ,akita_dd,00:0E:83:19:28:DC,-72,2005-08-08 09:34:06 ,open,A,36 (5180),54
2005-08-08 09:34:06 ,akita_eap,00:0B:85:04:73:F2,-78,2005-08-08 09:34:06 ,secure,A,149 (5745
2005-08-08 09:34:06 ,akita_eap,00:0E:83:19:28:DD,-72,2005-08-08 09:34:06 ,secure,A,36 (5180)

```

The log entries are time-stamped and appear in ASCII text. Each line typically represents a different access point.



**Note** The log file can be viewed in Notepad or any other viewer. However, because it is written in a comma-separated values (CSV) format, it can also be opened by a spreadsheet or database program (such as Microsoft Excel). If the file is renamed with a .csv extension, Microsoft Excel would automatically place the values in separate columns.



**Note** If the Accumulate button was depressed when you saved the AP scan log, two timestamps appear on each line. The timestamp in column one of the log file is the time when the log entry is made. The second timestamp, which appears only when the Accumulate button is depressed, is the Time of Day. This value indicates the date and time when the signal strength of each access point was at its maximum. Both timestamps appear in this format: 2005-07-20 16:13:09. The time is based on a 24-hour clock. For example, the first two lines in [Figure F-13](#) show only one timestamp while the remaining lines show both timestamps.

**Step 2** Click the **X** in the upper right-hand corner of the window to close the window.

## Deleting the AP Scan Log

Follow these steps to delete the AP scan log file.

- Step 1** Choose **Delete AP Scan Log** from the AP Scanning drop-down menu.



**Note** The Delete AP Scan Log menu option is disabled if the log file does not exist.

- Step 2** Click **Yes** when asked to confirm your decision.

## Saving the AP Scan List

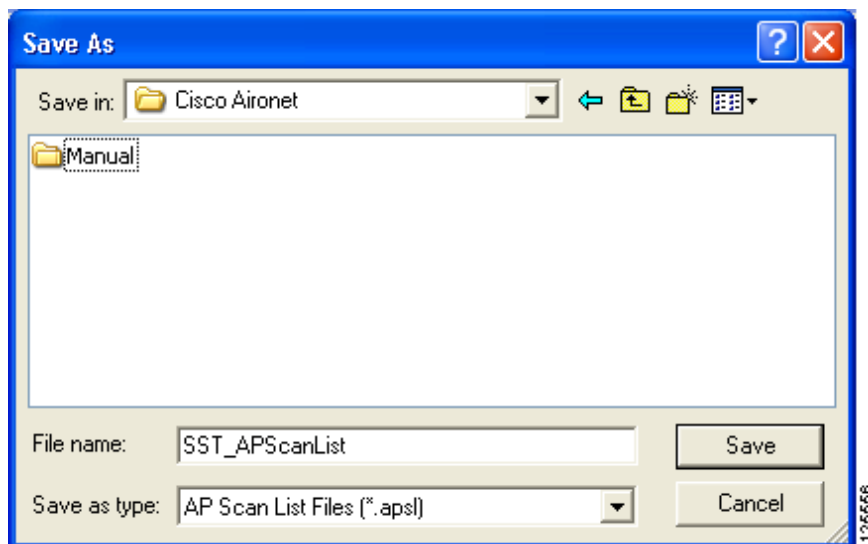
Follow these steps to save the current contents of the AP scan list to a file.

- Step 1** Choose **Save AP Scan List** from the AP Scanning drop-down menu. The Save As window appears (see [Figure F-14](#)).



**Note** The Save AP Scan List option is available only if the AP Scan List tab is selected.

**Figure F-14** Site Survey Utility - Save As Window



- Step 2** From the Save in drop-down box, choose the location where you want to save the AP scan list file.



**Note** The initial default location is the directory where the site survey utility is installed. However, after you save the AP scan list file the first time, the default directory becomes the one that was last used to open or save the AP scan list file.

- Step 3** The default filename (SST\_APScanList.apsl) appears in the File name box at the bottom of the window. If desired, type in a new filename.
- Step 4** Click **Save**.

## Opening the AP Scan List

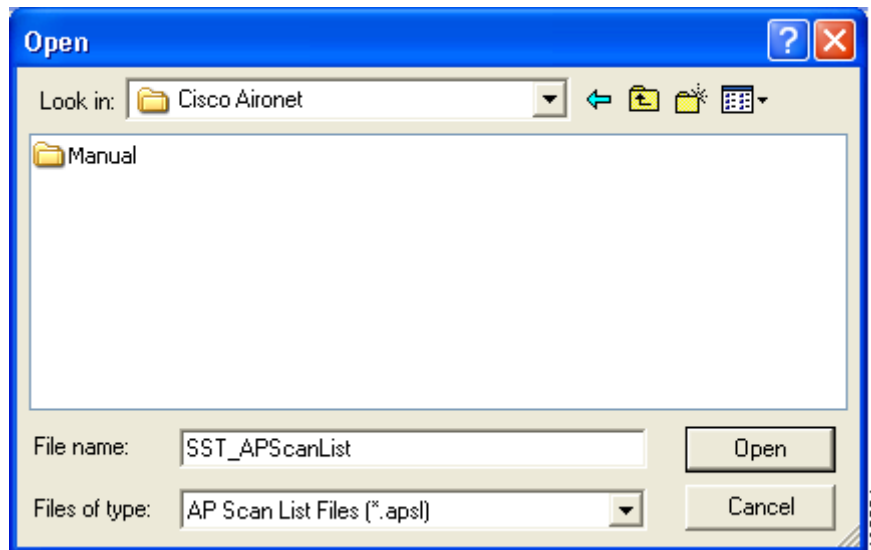
Follow these steps to open a saved AP scan list file.

- Step 1** Choose **Open AP Scan List** from the AP Scanning drop-down menu. The Open window appears (see [Figure F-15](#)).



**Note** The Open AP Scan List option is available only if the AP Scan List tab is selected.

**Figure F-15** Site Survey Utility - Open Window



- Step 2** From the Look in drop-down box, find the AP scan list file.



**Note** The default directory is the one that was last used to open or save the AP scan list file.

- Step 3** Click the AP scan list file (SST\_APScanList.apsl) so that it appears in the File name box at the bottom of the window.

- Step 4** Click **Open**. The contents of the AP scan list file appear in the AP scan list window.

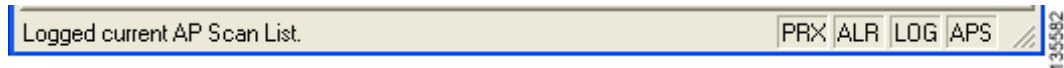


**Note** Updating of the AP scan list is paused automatically.

## Viewing the Status Bar

The site survey utility's status bar runs along the bottom of the window (see [Figure F-16](#)).

**Figure F-16 Site Survey Utility - Status Bar**



It consists of three sections:

- A message area
- Four indicators
- A resize handle

## Status Messages

The left side of the status bar displays status messages from the site survey utility. [Table F-4](#) lists and explains the messages that may appear.



**Note**

The messages disappear after a short period of time.

**Table F-4 Site Survey Utility - Status Messages**

Status Message	Description
“Added remarks to log file”	The comments you entered in the Add Comments to Log File window have been added to the threshold log file.
“The client adapter associated (<access point string as shown on main screen>)”	Your client adapter is associated to the specified access point.
“The client adapter disassociated”	Your client adapter has lost its connection to the access point.
“Connectivity test succeeded (<user’s URL or IP address setting>)”	Your client adapter successfully accessed the specified URL or IP address after associating to an access point.
“Logged current AP Scan List”	The current contents of the AP scan list were logged to a file.
Threshold crossing notifications of the form: <status-parameter> (<value><units>) rose above or to the threshold value of (<value>)	<ul style="list-style-type: none"> <li>• &lt;status-parameter&gt;—Can be any value that appears on the Associated AP Status tab</li> <li>• &lt;value&gt;—A number in the range appropriate for the parameter</li> <li>• &lt;units&gt;—The scientific units of the parameter</li> </ul> <p><b>Note</b> “Rose above or to” is replaced by “fell below or to” depending on the direction of crossing.</p>

## Indicators

The right side of the status bar can show up to four indicators:

- PRX—The proximity beeper is enabled.
- ALR—Threshold alerts are enabled.
- LOG—Threshold logging is enabled.
- APS—Automatic AP scan list logging is enabled.

**Note**

The indicators do not appear when their corresponding features are disabled.

## Resize Tab

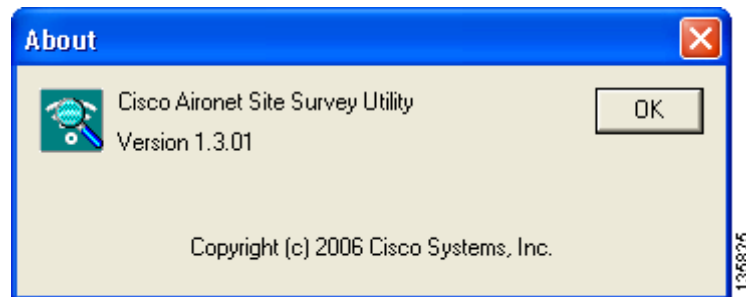
The resize tab in the right corner of the status bar can be used to change the size of the site survey utility's main window. Simply click the resize tab and drag it until the window reaches the desired size.



## Finding the Version of the Site Survey Utility

To find the current version of the site survey utility, choose **About** from the Help drop-down menu. The About window appears (see [Figure F-17](#)).

*Figure F-17 Site Survey Utility - About Window*



## Accessing Online Help

To access the site survey utility's online help, choose **Contents** from the Help drop-down menu.

## Exiting the Site Survey Utility

To exit the site survey utility, perform one of the following:

- Click the **X** in the top right corner of the main window.
- Choose **Exit** from the Action drop-down menu.

## Uninstalling the Site Survey Utility

Uninstalling the client adapter software also uninstalls the site survey utility. Refer to the [“Uninstalling the Client Adapter Software”](#) section on page 9-6 for instructions.



## Using the Profile Migration Tool

---

This appendix explains how to use the profile migration tool to migrate Cisco Aironet 350 series and CB20A wireless LAN client adapter profiles to profiles that can be used with Cisco Aironet CB21AG and PI21AG client adapters.

The following topics are covered in this appendix:

- [Overview of the Profile Migration Tool, page G-106](#)
- [Rules Governing Profile Migration, page G-106](#)
- [Installing the Profile Migration Tool, page G-107](#)
- [Running the Profile Migration Tool, page G-108](#)
- [Command Line Options, page G-109](#)
- [Uninstalling the Profile Migration Tool, page G-111](#)



# Overview of the Profile Migration Tool

The profile migration tool is designed to migrate Cisco Aironet 350 series and CB20A wireless LAN client adapter profiles to profiles that can be used with Cisco Aironet CB21AG and PI21AG client adapters. The tool is meant to migrate profiles with minimal modification, but its behavior can be altered by command line options. The legacy 350 and CB20A profiles are not deleted or modified in any way.

Cisco expects the profile migration tool to be executed once, most likely immediately after installing or updating the CB21AG/PI21AG client adapter software. Upon completion, the profile migration tool may be removed from your computer.

**Note**

Profile migration tool 1.0 can be used only with Install Wizard 2.5. To find the current version number of the profile migration tool, find the PMT.exe file in the directory where ADU is installed, right-click the file, and click **Properties** and the **Version** tab.

## Rules Governing Profile Migration

These rules govern the operation of the profile migration tool:

- Legacy profiles that are configured for host-based EAP are not migrated.
- Passwords that are stored in LEAP and EAP-FAST profiles may or may not be migrated, depending on the encryption method used for those passwords. Passwords that are not migrated must be re-entered after the migration.
- The PAC files for EAP-FAST profiles are not migrated. They must be reprovisioned after the migration.
- A profile's auto profile selection properties are migrated only if auto profile selection is enabled.
- Legacy profiles that were created using older versions of ACU may experience problems during migration. In such cases, the profile migration tool migrates the information that it can and ignores any additional information.
- If multiple instances of the same profile name exist, the names are mangled unless overridden by command line options. The default name-mangling scheme causes subsequent profiles with the same name to have an *\_a* or *\_b* appended to the end of the name, indicating whether the profile migrated from an 802.11a (CB20A) or 802.11b (350) radio. A third instance would have an *\_aa* or *\_bb* appended and so on (for example, *Office*, *Office\_a*, *Office\_aa*).

**Note**

If the original name is too long to be appended, it is shortened by truncating as necessary.

- CB21AG and PI21AG client adapters have a limit of 16 profiles, so the total number of profiles that can be migrated is 16 minus the number of existing CB21AG and PI21AG profiles. If the number of profiles to migrate is greater than the number of profiles that can be migrated, some legacy profiles are not migrated. In this case, the client adapter priority is as follows, unless overridden by command line options:

1. 350 PCMCIA
2. 350 PCI
3. 350 mini PCI
4. CB20A

For each client adapter, profiles are migrated in this order:

1. Default profiles
  2. Auto-selectable profiles
  3. Any current profiles for inserted legacy client adapters that have not already been migrated
  4. Any remaining profiles
- Profile names that existed before the migration are preserved unless the **-replace** command is executed.

## Installing the Profile Migration Tool

When you install the client adapter software, the Install Wizard automatically installs the profile migration tool, unless your system administrator used an administrative tool to prevent its installation. It is saved in the same directory as ADU.



### Note

---

The name of the PMT installation log is migrate.log. It is saved at the root level of your hard drive (C:\).

---

# Running the Profile Migration Tool

Follow these steps to run the profile migration tool to migrate your 350 and CB20A profiles to CB21AG/PI21AG profiles.


**Note**

The best time to run the profile migration tool is immediately after the Install Wizard has installed the client adapter software.


**Note**

The following conditions must be true before the profile migration tool can be run successfully:

- Your computer must contain the 350 and CB20A profiles that you want to migrate.
- ADU must be installed on the same computer but must not be running during the profile migration.
- A CB21AG or PI21AG client adapter must be inserted into your computer.

**Step 1** Perform one of the following:

- If the profile migration tool runs automatically after the Install Wizard installs the client adapter software, go to [Step 4](#).
- If you want to manually activate the profile migration tool, open the Windows Command Prompt from **Start > Programs > Accessories**. Go to [Step 2](#).

**Step 2** Use MS-DOS commands to access the directory where the profile migration tool (PMT.exe) is located on your computer.

**Step 3** Type **PMT** and press **Enter**. The profile migration tool runs and displays the results.


**Note**

See the “[Command Line Options](#)” section below if you want to alter the behavior of the profile migration tool before running it.

**Step 4** Restart your computer.

**Step 5** Open ADU. Your migrated 350 and CB20A profiles now appear as CB21AG/PI21AG profiles on the Profile Management window and are ready for use.

**Step 6** Re-enter the WEP keys in ADU.

**Step 7** If desired, you can view the log file generated by the profile migration tool. This file shows the profiles that were processed, their status, and the reason why any profiles were not migrated.


**Note**

Unless you changed the default name and location of the log file using the **-logfile** command, you can find the log file at C:\migrate.log.

**Step 8** If desired, you can remove the profile migration tool from your computer.

# Command Line Options

These command line options can be used to alter the behavior of the profile migration tool. The correct format is **PMT -command**.



**Note**

---

Leave a space between multiple commands (such as **-command -command**).

---

- **-AllowReRun**—Enables the profile migration tool to be run multiple times. When you rerun the tool, it migrates all the existing profiles, even the ones that were already migrated. If you have modified any of the previously migrated profiles, the modifications are lost.

**Example:** PMT -AllowReRun



**Note**

---

If you do not use this command, you can run the profile migration tool only once. If you attempt to run it again, a message appears indicating that the profiles have already been migrated and that the tool does not need to be run again.

---

- **-CardOrder <cardtype> <cardtype>...**—Specifies the order in which profiles are migrated when multiple client adapters are selected.

**Example:** PMT -CardOrder -pci350 -pcmcia350

- **-CB20A**—Selects only CB20A profiles for migration. This command can be used alone or in conjunction with the **-CardOrder <cardtype> <cardtype>...** command to specify the order in which client adapter profiles are migrated.

**Examples:** PMT -CB20A  
PMT -CardOrder -CB20A -pcmcia350

- **-ConfigFile <filename> <filename>...**—Enables you to run the profile migration tool using multiple command lines that are specified within one or more configuration files. You can create the configuration file(s) using a text editor such as Notepad. To do so, simply type the desired commands (such as **-miniPCI -replace**) in the text editor and save the file. (Do not include **PMT** when typing the commands in the text editor.) After you have created the configuration file(s), use the **-ConfigFile** command with the file(s) you created.

**Examples:** PMT -ConfigFile filename1.txt  
PMT -ConfigFile filename1.txt filename2.txt



**Note**

---

If more than one file is specified, the profile migration tool performs all its functions for each file. It ignores all other command line options and executes only the options in the file(s) in order to prevent confusion regarding command priority.

---

- **-logfile <logfile name>**—Enables you to change the name and location of the log file, which identifies the migrated and unmigrated profiles after you run the profile migration tool. The default name is *migrate.log*, and its default location is the system drive root (for example, C:).

**Examples:** PMT -logfile logfile.log  
PMT -logfile C:\Cisco Aironet\migrate.log




---

**Note** If you specify a new location for the log file, that location must already exist. Otherwise, the file is saved to the system drive root (for example, C:).

---




---

**Note** If the **-logfile** command is used without the **<logfile name>** parameter, a log file is not generated.

---

- **-miniPCI**—Selects only 350 mini PCI profiles for migration. This command can be used alone or in conjunction with the **-CardOrder <cardtype> <cardtype>...** command to specify the order in which client adapter profiles are migrated.

**Examples:** PMT -miniPCI  
PMT -CardOrder -CB20A -miniPCI -pci350

- **-pci350**—Selects only 350 PCI profiles for migration. This command can be used alone or in conjunction with the **-CardOrder <cardtype> <cardtype>...** command to specify the order in which client adapter profiles are migrated.

**Examples:** PMT -pci350  
PMT -CardOrder -miniPCI -pci350

- **-pcmcia350**—Selects only 350 PCMCIA profiles for migration. This command can be used alone or in conjunction with the **-CardOrder <cardtype> <cardtype>...** command to specify the order in which client adapter profiles are migrated.

**Examples:** PMT -pcmcia350  
PMT -CardOrder -pcmcia350 -pci350

- **-replace**—Causes legacy profiles with the same name as existing CB21AG/PI21AG profiles to replace the existing profiles. This command is intended to minimize the number of similarly named profiles on your system.

For example, if both a 350 PCI legacy profile and a CB21AG profile have the same name (such as *Office*), the legacy profile replaces the CB21AG profile, resulting in only one *Office* profile. If this command is not used, you have two profiles after migration: *Office* and *Office\_b*.

**Example:** PMT -replace




---

**Note** If you have multiple legacy profiles with the same name (such as *Home*), only one *Home* profile is available after migration.

---

## Uninstalling the Profile Migration Tool

The profile migration tool is uninstalled automatically when the client adapter software is uninstalled. If you want to uninstall only the profile migration tool, find the PMT.exe file in the directory where ADU is installed and delete it.





- 16-QAM** Quadrature amplitude modulation. A modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 24 and 36 Mbps.
- 64-QAM** Quadrature amplitude modulation. A modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 48 and 54 Mbps.
- 802.1X** Also called *802.1X for 802.11*. 802.1X is the standard for wireless LAN security, as defined by the Institute of Electrical and Electronics Engineers (IEEE). An access point that supports 802.1X and its protocol, Extensible Authentication Protocol (EAP), acts as the interface between a wireless client and an authentication server, such as a Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network.
- 802.11** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 1- and 2-megabit-per-second (Mbps) wireless LANs operating in the 2.4-GHz band.
- 802.11a** The IEEE standard that governs the deployment of 5-GHz OFDM systems. It specifies the implementation of the physical layer for wireless UNII bands (see [UNII](#), [UNII 1](#), and [UNII 2](#)) and provides four channels per 100 MHz of bandwidth.
- 802.11b** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5- and 11-Mbps 2.4-GHz wireless LANs.
- 802.11g** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 54-Mbps 2.4-GHz wireless LANs.
- 802.11i** The IEEE standard that defines security standards for wireless LANs. It specifies encryption, authentication, and key management strategies for wireless data and system security. It includes the TKIP and AES-CCMP data-confidentiality protocols.

---

## A

- access point** A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations.
- ad hoc network** A wireless network composed of stations without access points.
- AES-CCMP** Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES-CCMP is the encryption protocol in the 802.11i standard.
- alphanumeric** A set of characters that contains both letters and numbers.
- associated** A station is configured properly to enable it to wirelessly communicate with an access point.



---

**B**

- bandwidth** Specifies the amount of the frequency spectrum that is usable for data transfer. It identifies the maximum data rate that a signal can attain on the medium without encountering significant power loss.
- BPSK** Binary phase shift keying. A modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 1 Mbps.
- broadcast key rotation** A security feature for use with dynamic WEP keys. If your client adapter uses LEAP, EAP-FAST, EAP-TLS, or PEAP authentication and you enable this feature, the access point changes the dynamic broadcast WEP key that it provides at the interval you select.

---

**C**

- CCK** Complementary code keying. A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 5.5 and 11 Mbps.
- CCKM** Cisco Centralized Key Management. Using CCKM, authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network provides wireless domain services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS access point's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point.
- CKIP** Cisco Key Integrity Protocol. Cisco's WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group.
- client adapter** A radio device that uses the services of an access point to communicate wirelessly with other devices on a local area network.
- CSMA** Carrier sense multiple access. A wireless LAN media access method specified by the IEEE 802.11 specification.
- CRC** Cyclic redundancy check. A method of checking for errors in a received packet.

---

**D**

- data rates** The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).
- dBi** A ratio of decibels to an isotropic antenna that is commonly used to measure antenna gain. The greater the dBi value, the higher the gain and the more acute the angle of coverage.
- DHCP** Dynamic Host Configuration Protocol. A protocol available with many operating systems that automatically issues IP addresses within a specified range to devices on the network. The device retains the assigned address for a specific administrator-defined period.

**DSSS** Direct-sequence spread spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.

**duplicate packets** Packets that were received twice because an acknowledgement got lost and the sender retransmitted the packet.

---

## E

**EAP** Extensible Authentication Protocol. EAP is the protocol for the optional IEEE 802.1X wireless LAN security feature. An access point that supports 802.1X and EAP acts as the interface between a wireless client and an authentication server, such as a Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network.

**EAP-FAST** Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling. An 802.1X authentication type that is available for use with Windows 2000 and XP. With EAP-FAST, a username, password, and PAC are used by the client adapter to perform mutual authentication with the RADIUS server through an access point.

**Ethernet** The most widely used wired local area network. Ethernet uses carrier sense multiple access (CSMA) to enable computers to share a network and operates at 10, 100, or 1000 megabits per second (Mbps), depending on the physical layer used.

---

## F

**file server** A repository for files so that a local area network can share files, mail, and programs.

**fragmentation threshold** The size at which packets are fragmented and transmitted a piece at a time instead of all at once. The setting must be within the range of 64 to 2312 bytes.

**full duplex** A means of communication whereby each node receives and transmits simultaneously (two-way). See also [half duplex](#).

---

## G

**gateway** A device that connects two otherwise incompatible networks together.

**GHz** Gigahertz. One billion cycles per second. A unit of measure for frequency.

---

## H

**half duplex** A means of communication whereby each node receives and transmits in turn (one-way). See also [full duplex](#).

**hexadecimal** A set of characters consisting of ten numbers and six letters (0-9, A-F, and a-f).

---

**I**

<b>IEEE</b>	Institute of Electrical and Electronics Engineers. A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.
<b>infrastructure</b>	The wired Ethernet network.
<b>infrastructure device</b>	A device (such as an access point, bridge, or base station) that connects client adapters to a wired LAN.
<b>IP address</b>	The Internet Protocol address of a station.
<b>IP subnet mask</b>	The number used to identify the IP subnetwork, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway.
<b>IPX</b>	Internetwork Packet Exchange. The NetWare network layer protocol used for transferring data from servers to workstations.

---

**L**

<b>LEAP</b>	LEAP, or <i>EAP-Cisco Wireless</i> , is an 802.1X authentication type. With LEAP, a username and password are used by the client adapter to perform mutual authentication with the RADIUS server through an access point.
-------------	---

---

**M**

<b>MAC address</b>	The Media Access Control (MAC) address is a unique serial number assigned to a networking device by the manufacturer.
<b>MIC</b>	Message integrity check. MIC prevents bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The client adapter's driver must support MIC functionality, and MIC must be enabled on the access point.
<b>modulation</b>	Any of several techniques for combining user information with a transmitter's carrier signal.
<b>multicast packets</b>	Packets transmitted to multiple stations.
<b>multipath</b>	The echoes created as a radio signal bounces off of physical objects.

---

**O**

<b>OFDM</b>	Orthogonal frequency division multiplexing. A multicarrier modulation method for broadband wireless communications.
<b>overrun packets</b>	Packets that were discarded because the access point had a temporary overload of packets to handle.

---

**P**

**PAC** Protected access credentials. Credentials that are either automatically or manually provisioned and used to perform mutual authentication with the RADIUS server during EAP-FAST authentication. PACs are created by the Cisco Secure ACS server and are identified by an ID. The user obtains his or her own copy of the PAC from the server, and the ID links the PAC to the profile created in ADU. When manual PAC provisioning is enabled, the PAC file is manually copied from the server and imported onto the client device.

**packet** A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error detection information.

---

**Q**

**QoS** Quality of service. QoS on wireless LANs provides prioritization of traffic from the access point over the WLAN based on traffic classification. The benefits of QoS become more obvious as the load on the wireless LAN increases, keeping the latency, jitter, and loss for selected traffic types within an acceptable range.

**QPSK** Quadruple phase shift keying. A modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 2 Mbps.

---

**R**

**radio channel** The frequency at which a radio operates.

**range** A linear measure of the distance that a transmitter can send a signal.

**receiver sensitivity** A measurement of the weakest signal a receiver can receive and still correctly translate it into data.

**RF** Radio frequency. A generic term for radio-based technology.

**roaming** A feature of some access points that enables users to move through a facility while maintaining an unbroken connection to the LAN.

**RTS threshold** The packet size at which an access point issues a request to send (RTS) before sending the packet.

---

**S**

**spread spectrum** A radio transmission technology that spreads data over a much wider bandwidth than otherwise required in order to gain benefits such as improved interference tolerance and unlicensed operation.

**SSID** Service set identifier. A unique identifier that stations must use to be able to communicate with an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

---

**T**

- TKIP** Temporal Key Integrity Protocol. Also referred to as *WEP key hashing*. A security feature that defends against an attack on WEP in which the intruder uses the initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs.
- transmit power** The power level of radio transmission.

---

**U**

- unicast packets** Packets transmitted in point-to-point communication.
- UNII** Unlicensed National Information Infrastructure. An FCC regulatory domain for 5-GHz wireless devices. UNII bands are 100 MHz wide and divided into four channels when using 802.11a OFDM modulation.
- UNII 1** A UNII band dedicated to in-building wireless LAN applications. UNII 1 is located at 5.15 to 5.25 GHz and allows for a maximum transmit power of 40 mW (or 16 dBm) with an antenna up to 6 dBi. UNII 1 regulations require a nonremovable, integrated antenna.
- UNII 2** A UNII band dedicated to in-building wireless LAN applications. UNII 2 is located at 5.25 to 5.35 GHz and allows for a maximum transmit power of 200 mW (or 23 dBm) with an antenna up to 6 dBi. UNII 2 regulations allow for an auxiliary, user-installable antenna.
- UNII 3** A UNII band dedicated to wireless LAN applications. UNII 3 is located at 5.725 to 5.825 GHz and allows for a maximum transmit power of 1 Watt (or 30 dBm) with an antenna up to 6 dBi. UNII 3 regulations allow for an auxiliary, user-installable antenna.

---

**V**

- VLAN** A switched network that is logically segmented, by functions, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN regardless of their physical connections to the network or the fact that they might be intermingled with other teams. You use VLANs to reconfigure the network through software rather than physically unplugging and moving devices or wires.
- A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment such as LAN switches that operate bridging protocols between them with a separate group for each VLAN.

---

**W**

- WDS** Wireless domain services (WDS). An access point providing WDS on your wireless LAN maintains a cache of credentials for CCKM-capable client devices on your wireless LAN. When a CCKM-capable client roams from one access point to another, the WDS access point forwards the client's credentials to the new access point with the multicast key. Only two packets pass between the client and the new access point, greatly shortening the reassociation time.
- WEP** Wired equivalent privacy. An optional security mechanism defined within the 802.11 standard designed to protect your data as it is transmitted through your wireless network by encrypting it through the use of encryption keys.
- WMM** Wi-Fi Multimedia. WMM is a component of the IEEE 802.11e wireless LAN standard for quality of service (QoS). It specifically supports priority tagging and queuing.
- workstation** A computing device with an installed client adapter.
- WPA** Wi-Fi Protected Access. A standards-based security solution from the Wi-Fi Alliance that provides data protection and access control for wireless LAN systems. It is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification. WPA uses TKIP and MIC for data protection and 802.1X for authenticated key management.
- WPA2** Wi-Fi Protected Access 2. The next generation of Wi-Fi security. It is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard. WPA2 uses AES-CCMP for data protection and 802.1X for authenticated key management.





---

## Numerics

- 802.11 Authentication Mode parameter [5-12](#)
- 802.11b preamble, status of [7-10](#)
- 802.11b Preamble parameter [5-9](#)
- 802.11 mode, in ASTU [8-5](#)
- 802.1X
  - authentication types
    - in ADU [5-15 to 5-19](#)
    - in Windows XP [55](#)
  - defined [5-15, 55](#)
- 802.1x EAP Type parameter [5-29, 5-34, 5-45, 5-48, 5-52, 5-56](#)
- 802.1x option [5-29, 5-34, 5-45, 5-48, 5-52, 5-56](#)

---

## A

- About Aironet Desktop Utility, ADU menu option [9-9](#)
- About window
  - in ADU [9-9](#)
  - in site survey utility [103](#)
- access point
  - CCX version supported [81, 85](#)
  - channel, in site survey utility [76, 81, 84](#)
  - currently associated to [7-9, 8-11](#)
  - data rates, in site survey utility [84](#)
  - frequency, in site survey utility [76, 81, 84](#)
  - in wireless infrastructure [1-6](#)
  - IP address
    - in ADU [7-9](#)
    - in ASTU [8-11](#)
    - in site survey utility [76](#)
  - load, in site survey utility [81, 85](#)
  - MAC address

- in ADU [7-9](#)
- in site survey utility [76, 80, 84](#)
- maximum transmit data rate, in site survey utility [81](#)
- mismatches [7-14](#)
- model number [85](#)
- name
  - in ADU [7-9](#)
  - in ASTU [8-11](#)
  - in site survey utility [76, 81, 85](#)
- number of associations [85](#)
- problems associating to [10-10](#)
- radio [85](#)
- radio band, in site survey utility [81, 84](#)
- role in wireless network [1-5](#)
- security settings [5-22 to 5-25](#)
- Access Point 1 through 4 parameters [5-13](#)
- access points
  - associating to in Windows XP [70](#)
  - number displayed in site survey utility [80](#)
  - preferred, setting [5-13](#)
  - reporting those that fail LEAP authentication [5-20 to 5-21, 5-25](#)
  - viewing an accumulation of [88](#)
  - viewing details in site survey utility [83 to 86](#)
  - viewing status in site survey utility [75 to 78](#)
- Accumulate button, in site survey utility [87, 88](#)
- ACK frames [7-14](#)
- Action drop-down menu
  - in ADU [6-10, 9-8](#)
  - in site survey utility [73, 90, 104](#)
- Activate button [4-6, 4-10](#)
- Adapter Information
  - button [9-10](#)



- window [9-10](#)
- Add Comments to Log File window (site survey utility) [94](#)
- Add User Comment, site survey utility menu option [94](#)
- ad hoc mode, in site survey utility [82](#)
- ad hoc network
  - defined [58](#)
  - selecting in ADU [5-9](#)
  - selecting in Windows XP [59](#)
  - setting wireless mode [5-10](#)
  - wireless LAN configuration [1-5](#)
- ADU
  - See Aironet Desktop Utility (ADU)
- Advanced button [7-7](#)
- advanced parameters
  - described [5-2](#)
  - setting [5-6 to 5-13](#)
- Advanced Statistics
  - button [7-13](#)
  - window [7-13](#)
- Advanced Status window [7-7](#)
- AES, status of [7-6, 7-7](#)
- AES-CCMP, with WPA2 [5-19](#)
- AES option, in Windows XP [60](#)
- Aironet Desktop Utility (ADU)
  - accessing help [9-10](#)
  - described [1-4](#)
  - exiting [9-8](#)
  - feature comparison to Windows XP [3-17 to 3-18](#)
  - finding version [9-9](#)
  - icon [9-8](#)
  - opening [9-8](#)
  - Profile Management windows, overview [5-2](#)
  - status and statistics tools
    - overview [7-2](#)
    - setting parameters [7-2 to 7-3](#)
    - using [7-4 to 7-15](#)
- Aironet Desktop Utility Help, ADU menu option [9-10](#)
- Aironet System Tray Utility (ASTU)
  - accessing help [8-5](#)
  - described [1-4](#)
  - exiting [8-6](#)
  - icon [8-2 to 8-3, 9-8](#)
  - opening [8-6](#)
  - overview [8-2](#)
  - pop-up menu [8-5 to 8-11](#)
  - selecting the active profile [8-8 to 8-9](#)
  - setting preferences [8-6 to 8-7](#)
  - specifying pop-up menu options [8-7](#)
  - Tool Tip window [8-3 to 8-5](#)
  - using [8-1 to 8-11](#)
  - using to open ADU [8-6](#)
  - using to open troubleshooting utility [8-6](#)
- Aironet System Tray Utility Preferences window [8-6](#)
- Allow Association to Mixed Cells parameter
  - setting with EAP-FAST [5-42 to 5-43](#)
  - setting with EAP-TLS [5-47](#)
  - setting with LEAP [5-32](#)
  - setting with PEAP (EAP-GTC) [5-51](#)
  - setting with PEAP (EAP-MSCHAP V2) [5-55](#)
  - setting with static WEP [5-27](#)
- Allow Automatic PAC Provisioning for this Profile parameter [5-42](#)
- AllowReRun, profile migration tool command line option [109](#)
- ALR, in site survey utility [103](#)
- Always Resume the Secure Session parameter
  - for LEAP [5-31](#)
  - for PEAP (EAP-GTC) [5-50](#)
- antenna
  - assembling [3-5 to 3-6](#)
  - described [1-3](#)
  - gains
    - IEEE 802.11a [50](#)
    - IEEE 802.11b [50](#)
    - IEEE 802.11g [51](#)
  - mounting [3-6 to 3-8](#)
  - placement [72](#)

- rotating [3-8](#)
  - specifications [29](#)
  - antenna base, mounting [3-6 to 3-8](#)
  - AP detailed information parameters (site survey utility) [84 to 86](#)
  - AP Detailed Information window (site survey utility) [83](#)
  - APS, in site survey utility [103](#)
  - AP scan list, in site survey utility
    - displayed [79](#)
    - opening [101](#)
    - parameters [80 to 82](#)
    - pausing [83](#)
    - saving [100 to 101](#)
    - viewing [79 to 82](#)
  - AP Scan List Logging Configuration window (site survey utility) [96](#)
  - AP Scan List tab (site survey utility), using [78 to 88](#)
  - AP scan log, in site survey utility
    - deleting [100](#)
    - viewing [98 to 99](#)
  - AP scan log file, in site survey utility
    - displayed [87, 99](#)
    - generating [86 to 87](#)
    - name and location [97](#)
  - AP scan logging, in site survey utility
    - configuring [96 to 97](#)
    - disabling [98](#)
    - enabling [98](#)
  - AP scanning, using in site survey utility [96 to 101](#)
  - associated AP status parameters (site survey utility) [76 to 78](#)
  - Associated AP Status tab (site survey utility)
    - units as a percentage [75](#)
    - units in dBm [75](#)
    - using [74 to 78](#)
  - association
    - rejections [7-15](#)
    - time-outs [7-15](#)
  - associations, in site survey utility [85](#)
  - ASTU
    - See Aironet System Tray Utility (ASTU)
  - ATIM Window, in site survey utility [84](#)
  - audience of document [xii](#)
  - authentication
    - process [5-17, 56](#)
    - rejections [7-15](#)
    - time-outs [7-15](#)
    - type
      - setting [5-12](#)
      - status of [7-8](#)
  - Authentication Timeout Value parameter
    - for LEAP [5-32](#)
  - Automatically Prompt for User Name and Password option
    - for EAP-FAST [5-38](#)
    - for LEAP [5-31](#)
  - auto profile selection
    - enabling [4-10](#)
    - including a profile in [4-8 to 4-9](#)
    - prioritizing profiles [4-9](#)
    - removing a profile from [4-9](#)
    - restrictions [4-9](#)
    - status of [8-10](#)
    - using [8-8](#)
  - Auto Profile Selection Management window [4-8](#)
  - Auto Select Profiles parameter [4-10](#)
  - Available Infrastructure and Ad Hoc Networks window [4-4](#)
- 
- ## B
- beacon period, in site survey utility [84](#)
  - beacons received
    - in ADU [7-14](#)
    - in site survey utility [77](#)
  - broadcast key rotation
    - described [5-21](#)
    - setting on client and access point [5-25](#)
  - broadcast packets
    - number received [7-13](#)

number transmitted [7-13](#)  
 broadcast SSIDs [5-4, 58](#)  
 BSS Aging Interval parameter (Windows Control Panel) [5-64](#)  
 bytes  
 number received [7-13](#)  
 number transmitted [7-13](#)

## C

call admission control (CAC), in site survey utility [82](#)  
 CAM  
 See Constantly Awake Mode (CAM)  
 Canadian compliance statement [39](#)  
 card name [9-10](#)  
 -CardOrder, profile migration tool command line option [109](#)  
 caution, defined [xiii](#)  
 -CB20A, profile migration tool command line option [109](#)  
 CCKM fast secure roaming  
 described [5-20](#)  
 enabling with EAP-FAST [5-34](#)  
 enabling with EAP-TLS [5-45](#)  
 enabling with LEAP [5-29](#)  
 enabling with PEAP (EAP-GTC) [5-48](#)  
 enabling with PEAP (EAP-MSCHAP V2) [5-52](#)  
 setting on client and access point [5-25](#)  
 CCX, version supported by access point [81, 85](#)  
 certificates, required for EAP-TLS and PEAP authentication [5-44](#)  
 channel of access point  
 in ADU [4-6](#)  
 in site survey utility [76, 81, 84](#)  
 channel of client adapter [7-6, 7-10](#)  
 Channel parameter [5-11](#)  
 channels, supported by regulatory domains  
 IEEE 802.11a [48](#)  
 IEEE 802.11b/g [49](#)

channel set, for which client adapter is configured [7-11](#)  
 Choose Destination Location window (Install Wizard) [3-14](#)  
 Cisco Aironet 802.11a/b/g Wireless Adapter Properties window [5-63](#)  
 Cisco Aironet Desktop Utility (Diagnostics) window [7-12](#)  
 Cisco Aironet Desktop Utility (Profile Management) window [4-2](#)  
 Cisco Aironet Installation Program window (Install Wizard) [3-11](#)  
 Cisco Centralized Key Management (CCKM)  
 See CCKM fast secure roaming  
 Cisco extended capabilities (CEC), in site survey utility [82](#)  
 Cisco Key Integrity Protocol (CKIP)  
 statistics [7-15](#)  
 status of [7-6](#)  
 with LEAP [5-15](#)  
 client adapter  
 association status in site survey utility [74](#)  
 selecting in site survey utility [73 to 74](#)  
 client name [9-10](#)  
 Client Name parameter [5-4](#)  
 client utilities  
 See Aironet Desktop Utility (ADU) and Aironet System Tray Utility (ASTU)  
 command line options, for profile migration tool [109 to 110](#)  
 -ConfigFile, profile migration tool command line option [109](#)  
 Configuration Settings window  
 for PEAP (EAP-MSCHAP V2) [5-54](#)  
 Configure AP Scan Logging, site survey utility menu option [96](#)  
 Configure Scan List Columns window [4-5](#)  
 Configure Thresholds, site survey utility menu option [90](#)  
 configuring AP scan logging in site survey utility [96 to 97](#)  
 configuring client adapter  
 deciding between ADU and Windows XP [3-17 to 3-18](#)  
 in ADU [5-1 to 5-58](#)  
 in Windows XP [57 to 62](#)

configuring scan list columns [4-5](#)  
 configuring threshold values in site survey utility [90 to 93](#)  
 connection status [8-4, 8-10](#)  
 Connection Status window (ASTU) [8-9](#)  
 Constantly Awake Mode (CAM) [5-8](#)  
 Contents, site survey utility menu option [103](#)  
 conventions of document [xiii to xiv](#)  
 CRC errors [7-14](#)  
 CTS frames [7-14](#)  
 Current Status window [7-4](#)  
 CWmax, in site survey utility [85](#)  
 CWmin, in site survey utility [85](#)

---

## D

Data Display parameter [7-3, 7-12](#)  
 data encryption  
     in ADU [7-7](#)  
     in site survey utility [81, 84](#)  
 data frames [7-14](#)  
 data rate  
     in ADU [7-5](#)  
     mismatches [7-14](#)  
     of access point, in site survey utility [84](#)  
     setting [5-10](#)  
     specifications [27](#)  
     when performing a site survey [72](#)  
 debugging information, in site survey utility [84](#)  
 declarations of conformity  
     European community, Switzerland, Norway, Iceland,  
         and Liechtenstein [39 to 43](#)  
     FCC [38](#)  
     RF exposure [43](#)  
 default values, using [5-2](#)  
 Define Certificate window [5-46](#)  
 Define PEAP (EAP-GTC) Configuration window [5-49](#)  
 Define PEAP (EAP-MSCHAP V2) Configuration  
     window [5-53](#)  
 Define Pre-Shared Keys window [5-26](#)  
 Define WPA/WPA2 Pre-Shared Key window [5-28](#)  
 Delete AP Scan Log, site survey utility menu option [100](#)  
 Delete Threshold Log, site survey utility menu option [95](#)  
 diagnosing client adapter operation [10-4 to 10-6](#)  
 Diagnostics window [7-12](#)  
 Disable Radio  
     ADU menu option [9-11](#)  
     ASTU menu option [8-7](#)  
 Display in Percent parameter (site survey utility) [74](#)  
 Display Settings  
     ADU menu option [7-2](#)  
     window [7-2](#)  
 display units, specifying in site survey utility [74](#)  
 diversity antenna [1-3](#)  
 document  
     audience [xii](#)  
     conventions [xiii to xiv](#)  
     organization [xii to xiii](#)  
     purpose [xii](#)  
 domain name  
     including in Windows login  
         for EAP-FAST [5-38](#)  
         for LEAP [5-32](#)  
     specifying for saved user name and password  
         for EAP-FAST [5-38](#)  
         for LEAP [5-31](#)  
 driver  
     current version [9-9, 9-10](#)  
     date [9-10](#)  
     described [1-4](#)  
     manually installing or upgrading [9-6](#)  
     name [9-10](#)  
 DSConfig, in site survey utility [85](#)  
 duplicate frames, number received [7-14](#)  
 dynamic WEP keys, overview [5-15 to 5-19, 55 to 56](#)

---

## E

EAP authentication

- described [56](#)
- overview [5-15 to 5-19, 6-2, 55 to 56](#)
- restarting [6-16](#)
- using [6-1 to 6-16](#)
- EAP-Cisco Wireless
  - See LEAP authentication
- EAP-FAST authentication
  - authenticating after a reboot/logon
    - with automatically prompted login [6-7](#)
    - with saved username and password [6-13](#)
    - with Windows username and password [6-4](#)
  - authenticating after a reboot/logon/card insertion, with manually prompted login [6-10 to 6-12](#)
  - authenticating after EAP-FAST password expires
    - with automatically prompted login [6-8](#)
    - with manually prompted login [6-12](#)
    - with saved username and password [6-14](#)
    - with Windows username and password [6-5](#)
  - authenticating after profile activation, with manually prompted login [6-9 to 6-10](#)
  - authenticating after profile activation/card insertion
    - with automatically prompted login [6-6](#)
    - with saved username and password [6-13](#)
    - with Windows username and password [6-3 to 6-4](#)
  - described [5-16 to 5-19](#)
  - disabling [5-58](#)
  - enabling [5-34](#)
  - overview [6-2 to 6-3](#)
  - RADIUS servers supported [5-16](#)
  - requirements [5-34](#)
  - setting on client and access point [5-23](#)
  - stages of [6-3](#)
  - user databases supported [5-17](#)
- EAP-FAST Authentication Status window
  - displayed [6-2](#)
  - minimizing [6-3](#)
- EAP-FAST option [5-34](#)
- EAP-FAST Settings window [5-35, 5-36](#)
- EAP MSCHAPv2 Properties window - Windows XP [67](#)
- EAP-TLS authentication
  - authenticating after profile activation/card insertion/reboot/logon [6-14](#)
  - described [5-17 to 5-19, 55, 56](#)
  - disabling [5-58](#)
  - enabling
    - in ADU [5-44 to 5-47](#)
    - in Windows XP [62 to 64](#)
  - RADIUS servers supported [5-17, 55](#)
  - requirements [5-44](#)
  - setting on client and access point [5-23](#)
- EAP-TLS machine authentication with machine credentials
  - requirements [5-44](#)
  - setting [5-42, 5-46](#)
- EAP-TLS option [5-45](#)
- EIRP, maximum supported by regulatory domains
  - IEEE 802.11a [50](#)
  - IEEE 802.11b [50](#)
  - IEEE 802.11g [51](#)
- Enable AP Scan Logging, site survey utility menu option [98](#)
- Enable Expert Mode for AP Detailed Information parameter (site survey utility) [84](#)
- Enable Radio
  - ADU menu option [9-11](#)
  - ASTU menu option [8-7](#)
- Enable Threshold Alerts, site survey utility menu option [93](#)
- Enable Threshold Logging, site survey utility menu option [93](#)
- Enable Tray Icon, ADU menu option [8-6](#)
- encryption errors [7-14](#)
- Enter Password window [5-41](#)
- Enter Wireless Network Password window [6-6, 6-7, 6-9, 6-11](#)
- error messages [10-12 to 10-24](#)
- errors
  - CRC [7-14](#)
  - encryption [7-14](#)
  - MIC [7-15](#)

Exit menu option  
 in ADU [9-8](#)  
 in ASTU [8-6, 9-8](#)  
 in site survey utility [104](#)

Export button [4-13](#)  
 Export Profile window [4-13](#)

---

## F

Fast PSP [5-8](#)

FCC

declaration of conformity statement [38](#)  
 safety compliance statement [2-2](#)

finding domain controller timeout value

for EAP-FAST [5-43](#)  
 for LEAP [5-32](#)

Fit Columns parameter (site survey utility) [79](#)

frames

ACK [7-14](#)  
 CTS [7-14](#)  
 duplicate [7-14](#)  
 number dropped [7-14](#)  
 number received successfully [7-14](#)  
 number received with errors [7-14](#)  
 number retried [7-14](#)  
 number transmitted successfully [7-14](#)  
 RTS [7-14](#)

frequencies, supported by regulatory domains

IEEE 802.11a [48](#)  
 IEEE 802.11b/g [49](#)

frequency

in ADU [7-5, 7-11](#)  
 of access point, in site survey utility [81, 84](#)  
 setting [5-10](#)

---

## G

general parameters

described [5-2](#)  
 setting [5-3 to 5-5](#)

Generic Token Card Properties window - Windows XP [69](#)

global PACs [5-16, 5-41](#)

Group Policy, described [3-21](#)

Group Policy Delay parameter

installing hot fix for [3-21 to 3-22](#)  
 setting with EAP-FAST [5-44](#)  
 setting with EAP-TLS [5-47](#)  
 setting with LEAP [5-33](#)  
 setting with PEAP (EAP-GTC) [5-51](#)  
 setting with PEAP (EAP-MSCHAP V2) [5-55](#)  
 setting with PEAP (EAP-MSCHAP V2) machine authentication with machine credentials [5-56](#)  
 setting with WPA/WPA2 passphrase [5-28](#)

---

## H

hardware components of client adapter [1-3](#)

help

in ADU [9-10](#)  
 in ASTU [8-5](#)  
 in site survey utility [103](#)

hops, in site survey utility [85](#)

Host Based EAP option [5-56](#)

host devices [2-4](#)

Hysteresis parameter (site survey utility) [93](#)

---

## I

I/O range [10-9](#)

Import button [4-12](#)

Import EAP-FAST PAC File window [5-40](#)

Import Profile window [4-12](#)

Include Windows Logon Domain with User Name parameter

for EAP-FAST [5-38](#)  
 for LEAP [5-32](#)

- indicators, in site survey utility [103](#)
  - information about client adapter [9-10](#)
  - infrastructure device, defined [1-2](#)
  - infrastructure mode, in site survey utility [84](#)
  - infrastructure network
    - selecting in ADU [5-9](#)
    - wireless LAN configuration [1-6](#)
  - inserting client adapter [3-2 to 3-8](#)
  - Install Cisco Aironet Site Survey Utility window (Install Wizard) [3-13](#)
  - installing
    - client adapter software [3-9 to 3-20](#)
    - profile migration tool [107](#)
  - Install Wizard file
    - described [1-4](#)
    - installing [3-9 to 3-20](#)
    - name [3-9](#)
    - removing [9-7](#)
  - interference [2-5, 3-6](#)
  - interrupt request (IRQ) [10-9](#)
  - introduction to client adapters [1-2](#)
  - IP address
    - of access point
      - in ADU [7-9](#)
      - in ASTU [8-11](#)
      - in site survey utility [76](#)
    - of client adapter [7-6, 8-5, 8-11](#)
- 
- J**
- Japan, guidelines for operating client adapters [43](#)
- 
- K**
- key icon [4-6](#)
- 
- L**
- LEAP authentication
    - authenticating after a reboot/logon
      - with automatically prompted login [6-7](#)
      - with saved username and password [6-13](#)
      - with Windows username and password [6-4](#)
    - authenticating after a reboot/logon/card insertion, with manually prompted login [6-10 to 6-12](#)
    - authenticating after profile activation, with manually prompted login [6-9 to 6-10](#)
    - authenticating after profile activation/card insertion
      - with automatically prompted login [6-6](#)
      - with saved username and password [6-13](#)
      - with Windows username and password [6-3 to 6-4](#)
    - described [5-15 to 5-19](#)
    - disabling [5-58](#)
    - enabling [5-29 to 5-33](#)
    - overview [6-2 to 6-3](#)
    - RADIUS servers supported [5-15](#)
    - requirements [5-29](#)
    - setting on client and access point [5-22](#)
    - stages of [6-3](#)
    - timeout value [4-10, 8-8](#)
    - using with login scripts [4-10](#)
  - LEAP Authentication Status window
    - displayed [6-2](#)
    - minimizing [6-3](#)
  - LEAP option [5-29](#)
  - LEAP Settings window [5-30](#)
  - LEDs
    - described [1-3](#)
    - interpreting [10-2](#)
  - link quality
    - in ASTU [8-5, 8-11](#)
    - in site survey utility [78](#)
  - link speed
    - in ASTU [8-5](#)
    - in site survey utility [78](#)
  - List Installed Devices Even If Not Present in System parameter (site survey utility) [74](#)
  - load, in site survey utility [81, 85](#)
  - Locked Profile parameter [5-14](#)

locked profiles [5-14](#)  
 LOG, in site survey utility [103](#)  
 log file, generating in site survey utility [87](#)  
 -logfile, profile migration tool command line option [110](#)  
 login scripts, using with LEAP [4-10, 8-9](#)  
 Log Snapshot button, in site survey utility [86](#)  
 long radio headers  
   status of [7-10](#)  
   using [5-9](#)

## M

MAC address  
   of access point  
     in site survey utility [76, 80, 84](#)  
     specifying [5-13](#)  
     viewing [7-9](#)  
   of client adapter [9-10](#)  
 machine authentication with machine credentials  
   using EAP-TLS [5-42, 5-46](#)  
   using PEAP (EAP-MSCHAP V2) [5-55 to 5-57](#)  
 machine authentication with user credentials  
   using PEAP (EAP-GTC) [5-49](#)  
   using PEAP (EAP-MSCHAP V2) [5-53](#)  
 Manual Login  
   ADU menu option [5-31, 6-10](#)  
   ASTU menu option [8-8](#)  
 Manually Prompt for User Name and Password option  
   for EAP-FAST [5-38](#)  
   for LEAP [5-31](#)  
 Max PSP [5-8](#)  
 message integrity check (MIC)  
   described [5-21, 7-8](#)  
   errors [7-15](#)  
   setting on client and access point [5-25](#)  
   statistics [7-15](#)  
   status of [7-8](#)  
   types of [7-8](#)  
   with WPA [5-19](#)  
 Michael MIC, status of [7-8](#)  
 microcellular network [1-6](#)  
 Microsoft 802.1X supplicant, disabling [10-8](#)  
 Microsoft hot fix  
   installing [3-21 to 3-22](#)  
   required for Group Policy Delay parameter [3-21](#)  
 Microsoft Wireless Configuration Manager  
   disabling [10-8](#)  
   enabling in Install Wizard [3-17](#)  
   role in switching between host-based EAP and non-host-based EAP profiles [5-56, 5-57](#)  
 -miniPCI, profile migration tool command line option [110](#)  
 MMH MIC  
   status of [7-8](#)  
   with LEAP [5-15](#)  
 Modify button [4-11, 5-3](#)  
 multicast packets  
   number received [7-13](#)  
   number transmitted [7-13](#)

## N

network  
   configurations [1-5 to 1-6](#)  
   prioritizing connections [10-11](#)  
   problems connecting to [10-11](#)  
   type, current [4-3, 7-5](#)  
 network name  
   in ADU [5-4, 7-7](#)  
   in ASTU [8-3](#)  
   in site survey utility [80, 84](#)  
 Network Type parameter [5-9](#)  
 New button [4-4, 5-3](#)  
 noise level  
   in ADU [7-10](#)  
   in site survey utility [77](#)  
 No Network Connection Unless User Is Logged In parameter



for EAP-FAST [5-42, 6-13](#)  
 for LEAP [5-32, 6-13](#)  
 note, defined [xiii](#)

## O

online help  
 for ADU [9-10](#)  
 for ASTU [8-5](#)  
 for site survey utility [103](#)  
 Open Aironet Desktop Utility, ASTU menu option [8-6, 9-8](#)  
 Open AP Scan List, site survey utility menu option [101](#)  
 open authentication  
 setting [5-12, 60](#)  
 status of [7-8](#)  
 Open window (site survey utility) [101](#)  
 operating systems supported [xii, 2-4, 3-9](#)  
 Options, site survey utility menu option [84, 88](#)  
 Options window (site survey utility) [89](#)  
 Order Profiles button [4-8](#)  
 organization of document [xii to xiii](#)

## P

PAC authority, selecting [5-39, 5-41](#)  
 package contents [2-3](#)  
 packets  
 broadcast [7-13](#)  
 multicast [7-13](#)  
 unicast [7-13](#)  
 PAC provisioning  
 automatic [5-42](#)  
 manual [5-42](#)  
 PACs  
 copying from private store to global store [5-42](#)  
 described [5-16, 5-42](#)  
 entering password for [5-41](#)  
 importing [5-40 to 5-41](#)  
 rules for storage [5-16](#)  
 types of [5-16](#)  
 PAC stores  
 selecting [5-41](#)  
 types of [5-41](#)  
 Pause List Update button, in site survey utility [83](#)  
 PC-Cardbus card  
 antenna [1-3](#)  
 described [1-2](#)  
 inserting [3-2](#)  
 profiles tied to slot [4-7](#)  
 removing [9-2](#)  
 -pci350, profile migration tool command line option [110](#)  
 PCI card  
 antenna  
 assembling [3-5 to 3-6](#)  
 described [1-3](#)  
 mounting [3-6 to 3-8](#)  
 rotating [3-8](#)  
 changing bracket [3-3](#)  
 described [1-2](#)  
 inserting [3-3 to 3-8](#)  
 removing [9-2](#)  
 -pcmcia350, profile migration tool command line option [110](#)  
 PEAP (EAP-GTC) authentication  
 authenticating after profile activation/card insertion/reboot/logon [6-15](#)  
 described [5-17, 55, 56](#)  
 disabling [5-58](#)  
 enabling  
 in ADU [5-48 to 5-51](#)  
 in Windows XP [65 to 66, 68 to 70](#)  
 RADIUS servers supported [5-17, 55](#)  
 requirements [5-44](#)  
 setting on client and access point [5-24](#)  
 user databases supported [5-17](#)  
 PEAP (EAP-GTC) machine authentication with user credentials, setting [5-49](#)  
 PEAP (EAP-GTC) option [5-48](#)

- PEAP (EAP-MSCHAP V2) authentication
  - authenticating after profile activation/card insertion/reboot/logon [6-16](#)
  - Certificate option [5-53](#)
  - described [5-17 to 5-19](#), [55](#), [56](#)
  - disabling [5-58](#)
  - enabling
    - in ADU [5-52 to 5-55](#)
    - in Windows XP [65 to 67](#)
  - RADIUS servers supported [5-17](#), [55](#)
  - requirements [5-44](#)
  - setting on client and access point [5-24](#)
  - User Name and Password option [5-53](#)
- PEAP (EAP-MSCHAP V2) machine authentication with machine credentials, setting [5-55 to 5-57](#)
- PEAP (EAP-MSCHAP V2) machine authentication with user credentials, setting [5-53](#)
- PEAP (EAP-MSCHAP V2) option [5-52](#)
- PEAP Properties window - Windows XP [68](#)
- peer-to-peer network [1-5](#), [5-9](#)
- physical specifications [26](#)
- Please Change Password window [6-5](#), [6-8](#), [6-12](#), [6-14](#)
- power level, current [7-9](#)
- power levels, available [7-9](#)
- power save mode, currently being used [7-9](#)
- Power Save Mode parameter [5-8](#)
- power specifications [30](#)
- Preferences, ASTU menu option [8-6](#)
- Preferred Access Points window [5-13](#)
- Preparing Setup window (Install Wizard) [3-10](#), [9-3](#)
- Pre-Shared Key (Static WEP) option [5-26](#)
- Previous Installation Detected window (Install Wizard) [9-4](#)
- private PACs [5-16](#), [5-41](#)
- product model numbers [1-2](#)
- profile
  - active [4-10](#), [8-3](#), [8-10](#)
  - default [4-2](#)
  - described [4-2](#)
  - locked [5-14](#)
- Profile Management (Advanced) window [5-6](#)
- Profile Management (General) window [4-7](#)
- Profile Management (Security) window [5-14](#)
- Profile Management window [4-2](#)
- Profile Management windows, parameters missing [10-11](#)
- profile manager
  - auto profile selection feature [4-8 to 4-9](#)
  - creating a new profile [4-4 to 4-7](#)
  - deleting a profile [4-11](#)
  - editing a profile [4-11](#)
  - exporting a profile [4-12 to 4-13](#)
  - importing a profile [4-12](#)
  - opening [4-2 to 4-3](#)
  - parameters missing [4-3](#), [10-11](#)
  - selecting the active profile [4-10](#)
- profile migration tool
  - command line options [109 to 110](#)
  - compatibility with Install Wizard [106](#)
  - entering multiple commands [109](#)
  - finding version number [106](#)
  - installing [107](#)
  - name and location of generated log file [108](#), [110](#)
  - name mangling [106](#)
  - overview [106](#)
  - rules governing profile migration [106 to 107](#)
  - running [108](#)
  - running multiple times [109](#)
  - uninstalling [111](#)
  - using [105 to 111](#)
  - viewing generated log file [108](#)
- Profile Name parameter [5-4](#)
- profiles, losing [9-6](#)
- profiles submenu (ASTU) [8-8](#)
- Protected EAP
  - See PEAP (EAP-GTC) authentication and PEAP (EAP-MSCHAP V2) authentication
- Protected EAP Properties window - Windows XP [66](#)
- protocol driver, finding version [9-9](#)
- proximity beeper

configuring [88 to 89](#)  
 disabling [90](#)  
 enabling [90](#)  
 inverting the tone of [89](#)  
 using [88 to 90](#)  
 PRX, in site survey utility [103](#)  
 purpose of document [xii](#)

---

## Q

QoS  
     See quality of service  
 QoS Packet Scheduler  
     enabling on Windows 2000 [5-59 to 5-61](#)  
     enabling on Windows XP [5-62](#)  
 quality of service (QoS)  
     described [5-59](#)  
     in site survey utility [82](#)  
     status of [7-8](#)

---

## R

radio  
     described [1-3](#)  
     enabling or disabling [8-7, 9-11](#)  
     specifications [27 to 29](#)  
 radio band of access point, in site survey utility [81, 84](#)  
 RADIUS servers  
     additional information [5-19, 56](#)  
     defined [5-15, 55](#)  
     supported [5-15 to 5-19, 55](#)  
 range [5-7](#)  
 Reauthenticate menu option  
     in ADU [6-16](#)  
     in ASTU [6-16, 8-8](#)  
 receive rate [7-10, 8-11](#)  
 receive statistics [7-13, 7-14 to 7-15](#)  
 Refresh button [4-4](#)  
 Refresh Interval parameter [7-3, 7-12](#)  
 regulatory  
     domains  
         IEEE 802.11a [48](#)  
         IEEE 802.11b/g [49](#)  
     information [38 to 45](#)  
     specifications [30](#)  
 related publications [xv](#)  
 Remove button [4-11](#)  
 removing client adapter [9-2](#)  
 -replace, profile migration tool command line option [110](#)  
 resize tab, on site survey utility [103](#)  
 resource conflicts, resolving  
     in Windows 2000 [10-9](#)  
     in Windows XP [10-10](#)  
 Restrict Time Finding Domain Controller parameter  
     setting with EAP-FAST [5-43](#)  
     setting with LEAP [5-32 to 5-33](#)  
 RF obstructions [2-5, 3-6, 72](#)  
 RM-APScan, in site survey utility [82, 86](#)  
 RM-CliWlk, in site survey utility [82, 86](#)  
 RM-Normal, in site survey utility [82, 86](#)  
 roaming  
     described [1-6](#)  
     parameters, setting in the Windows Control Panel [5-63 to 5-64](#)  
     threshold [5-64](#)  
 RSSI, in site survey utility [80, 84](#)  
 RTS frames [7-14](#)  
 Run Test button, in troubleshooting utility [10-5](#)

---

## S

safety  
     information [2-2 to 2-3](#)  
     specifications [30](#)  
 Save AP Scan List, site survey utility menu option [100](#)  
 Save As window (site survey utility) [100](#)  
 saved username and password

- described
  - for LEAP [5-30](#)
- entering
  - for EAP-FAST [5-38](#)
  - for LEAP [5-31](#)
- Save Report, in troubleshooting utility
  - button [10-7](#)
  - window [10-7](#)
- Scan button [4-4](#)
- scan list columns, configuring [4-5](#)
- Scan List Settings, ADU menu option [4-4](#)
- Scan Valid Interval parameter (Windows Control Panel) [5-64](#)
- seamless roaming [1-6](#)
- security features
  - overview [5-14 to 5-21](#)
  - synchronizing [5-22 to 5-25](#)
- security mode [4-3](#)
- security parameters
  - described [5-2](#)
  - setting [5-14 to 5-57](#)
- Select Adapter
  - site survey utility menu option [73](#)
  - window (site survey utility) [73](#)
- Select Network Component Type window [5-61](#)
- Select Network Service window [5-61](#)
- Select Profile, ASTU menu option [8-8 to 8-9](#)
- sensitivity [28](#)
- serial number of client adapter [9-10](#)
- server-based authentication, currently being used [7-7](#)
- Setup Status window (Install Wizard) [9-5](#)
- Setup Type window (Install Wizard) [3-12](#)
- shared authentication
  - setting [5-12, 60](#)
  - status of [7-8](#)
- short radio headers
  - status of [7-10](#)
  - using [5-9](#)
- Show Connection Status, ASTU menu option [8-9](#)
- signal quality
  - in ADU [7-10](#)
  - in site survey utility [77](#)
- signal strength
  - as a percentage [7-3](#)
  - in ADU [7-6, 7-10](#)
  - in ASTU [8-5](#)
  - in dBm [7-3](#)
- Signal Strength Display Units parameter [7-3](#)
- signal-to-noise ratio (SNR)
  - as a percentage [7-3](#)
  - in ADU [4-6](#)
  - in dB [7-3](#)
  - in site survey utility [78](#)
- site requirements
  - for client devices [2-5](#)
  - for infrastructure devices [2-5](#)
- site survey
  - environmental considerations [72](#)
  - guidelines [72](#)
  - performing [71 to 104](#)
- site survey utility
  - About window [103](#)
  - accessing help [103](#)
  - Accumulate button [87, 88](#)
  - AP detailed information parameters [84 to 86](#)
  - AP Detailed Information window [83](#)
  - AP scan list
    - parameters [80 to 82](#)
    - pausing [83](#)
    - viewing [79 to 82](#)
  - associated AP status parameters [76 to 78](#)
  - client adapter association status [74](#)
  - configuring
    - AP scan logging [96 to 97](#)
    - proximity beeper [88 to 89](#)
    - threshold values [90 to 93](#)
  - debugging information [84](#)
  - deleting

- AP scan log [100](#)
- threshold log file [95](#)
- disabling
  - AP scan logging [98](#)
  - proximity beeper [90](#)
  - threshold triggers [93](#)
- enabling
  - AP scan logging [98](#)
  - proximity beeper [90](#)
  - threshold triggers [93](#)
- exiting [104](#)
- finding version of [103](#)
- Fit Columns parameter [79](#)
- generating AP scan log file [86 to 87](#)
- indicators [103](#)
- inverting tone of proximity beeper [89](#)
- log file [87](#)
- Log Snapshot button [86](#)
- opening [73](#)
- opening AP scan list [101](#)
- overview [72](#)
- Pause List Update button [83](#)
- resize tab [103](#)
- resizing columns [79](#)
- saving AP scan list [100 to 101](#)
- selecting client adapter [73 to 74](#)
- specifying
  - directory [3-13](#)
  - display units [74](#)
- status bar [102 to 103](#)
- status messages [102](#)
- top of main window [74](#)
- trend graph, explained [76](#)
- uninstalling [104](#)
- using
  - AP Scan List tab [78 to 88](#)
  - AP scanning [96 to 101](#)
  - thresholds [90 to 95](#)
- View AP Details button [83](#)
- viewing
  - access point details [83 to 86](#)
  - an accumulation of access points [88](#)
  - AP scan log [98 to 99](#)
  - status of access point [75 to 78](#)
  - threshold log file [94 to 95](#)
- Smart Card or other Certificate Properties window -  
Windows XP [63](#)
- software
  - compatibility with Cisco Aironet client adapters [3-9](#)
  - installing [3-9 to 3-20](#)
  - procedures [9-3 to 9-11](#)
  - uninstalling [9-6 to 9-7](#)
  - upgrading [9-3 to 9-5](#)
- software components
  - described [1-4](#)
  - finding versions [9-9](#)
- specifications
  - physical [26](#)
  - power [30](#)
  - radio [27 to 29](#)
  - regulatory compliance [30](#)
  - safety [30](#)
- spread spectrum [1-3](#)
- SSID
  - setting [5-4](#)
  - viewing
    - in ADU [4-3, 4-5, 7-7](#)
    - in ASTU [8-3, 8-11](#)
    - in site survey utility [80, 84, 89](#)
- SSID1 parameter [5-4](#)
- SSID2 parameter [5-5](#)
- SSID3 parameter [5-5](#)
- Ssidl, in site survey utility [82](#)
- Start Test button, in troubleshooting utility [10-5](#)
- static WEP
  - disabling [5-58](#)
  - enabling [5-26 to 5-27](#)

- with open authentication, setting on client and access point [5-22](#)
  - with shared key authentication, setting on client and access point [5-22](#)
  - static WEP keys
    - guidelines for entering
      - in ADU [5-27](#)
      - in Windows XP [61](#)
    - overview [5-15, 54](#)
    - selecting transmit key [5-27](#)
    - size of [5-26](#)
  - statistics
    - method of calculation [7-12](#)
    - receive [7-13, 7-14 to 7-15](#)
    - transmit [7-13, 7-14](#)
    - viewing [7-12 to 7-15](#)
  - status bar, in site survey utility [102 to 103](#)
  - status messages, in site survey utility [102](#)
  - status of client adapter
    - in ADU Advanced Status window [7-7 to 7-11](#)
    - in ADU Current Status window [7-4 to 7-6](#)
    - in ASTU Connection Status window [8-9 to 8-11](#)
    - in ASTU Tool Tip window [8-4](#)
    - in Windows XP [70](#)
  - Stop Test button, in troubleshooting utility [10-5](#)
  - supplicant, finding version [9-9](#)
  - system requirements [2-4](#)
- 
- T**
- Taiwan, administrative rules for client adapters [44 to 45](#)
  - Temporal Key Integrity Protocol (TKIP)
    - described [5-21](#)
    - setting on client and access point [5-25](#)
    - with WPA [5-19](#)
  - temporary username and password
    - automatically prompt for
      - for EAP-FAST [5-38](#)
      - for LEAP [5-31](#)
  - described
    - for EAP-FAST [5-37, 5-38](#)
    - for LEAP [5-30](#)
  - manually prompt for
    - for EAP-FAST [5-38](#)
    - for LEAP [5-31](#)
  - selecting options
    - for EAP-FAST [5-38](#)
    - for LEAP [5-31](#)
  - using Windows credentials
    - for LEAP [5-31](#)
  - third-party tool, enabling in Install Wizard [3-17](#)
  - threshold log file
    - adding a comment to [94](#)
    - deleting in site survey utility [95](#)
    - name and location [93](#)
    - viewing in site survey utility [94 to 95](#)
  - Threshold Log File window (site survey utility) [95](#)
  - Threshold Logging Configuration window (site survey utility) [91](#)
  - thresholds, using in site survey utility [90 to 95](#)
  - threshold triggers
    - disabling in site survey utility [93](#)
    - enabling in site survey utility [93](#)
  - throughput [5-8, 5-9](#)
  - time of day, in site survey utility [80, 87, 88](#)
  - TKIP
    - option in Windows XP [60](#)
    - status of [7-6](#)
  - Token Configuration window [6-15](#)
  - translated safety warnings [31 to 36](#)
  - transmit key [5-27](#)
  - transmit power, in site survey utility [82, 86](#)
  - Transmit Power Level parameter [5-7](#)
  - transmit rate [7-10, 8-11](#)
  - transmit statistics [7-13, 7-14](#)
  - Troubleshooting
    - ADU menu option [10-4](#)
    - ASTU menu option [8-6, 10-4](#)

- button [10-4](#)
- troubleshooting information, accessing [10-2](#)
- troubleshooting utility
  - saving detailed report to text file [10-7](#)
  - using [10-3 to 10-7](#)
- Troubleshooting Utility window
  - detailed report [10-6](#)
  - initial window [10-4](#)
  - with test results [10-5](#)

---

## U

- unicast packets
  - number received [7-13](#)
  - number transmitted [7-13](#)
- uninstalling
  - client adapter software [9-6 to 9-7](#)
  - profile migration tool [111](#)
- unpacking the client adapter [2-3](#)
- upgrading client adapter software [9-3 to 9-5](#)
- up time, status of [7-10](#)
- Use Auto Profile Selection, ASTU menu option [8-8](#)
- Use Machine Information For Domain Logon parameter
  - for EAP-TLS [5-42, 5-46](#)
  - for PEAP (EAP-GTC) [5-49](#)
  - for PEAP (EAP-MSCHAP V2) [5-53](#)
- Use Saved User Name and Password option
  - for EAP-FAST [5-38](#)
  - for LEAP [5-30](#)
- Use Temporary User Name and Password option
  - for EAP-FAST [5-37, 5-38](#)
  - for LEAP [5-30](#)
- Use Windows to Configure My Wireless Network Settings parameter - Windows XP [58](#)
- Use Windows User Name and Password option
  - for EAP-FAST [5-38](#)
  - for LEAP [5-30, 5-31, 5-38](#)

---

## V

- View AP Details button, in site survey utility [83](#)
- View AP Scan Log, site survey utility menu option [86, 98](#)
- viewer, name and location [93, 97](#)
- View Report button, in troubleshooting utility [10-6](#)
- View Threshold Log, site survey utility menu option [94](#)

---

## W

- warning
  - antenna [2-2, 33](#)
  - defined [xiii to xiv](#)
  - explosive device proximity [2-2, 32](#)
  - laptop users [2-3, 34 to 36](#)
- WEP
  - keys
    - additional security features [5-21](#)
    - defined [5-14, 54](#)
    - entry method [5-26](#)
    - size of [5-15, 54](#)
    - types of [5-15, 54](#)
    - status of [7-6](#)
  - WEP key hashing, described [5-21](#)
  - WEP option, in Windows XP [60](#)
- Wi-Fi Multimedia (WMM)
  - enabling [5-59 to 5-62](#)
  - in site survey utility [82](#)
  - status of [7-8](#)
- Wi-Fi Protected Access (WPA)
  - described [5-19, 56](#)
  - enabling in Windows XP [60](#)
  - enabling with EAP-FAST [5-34](#)
  - enabling with EAP-TLS [5-45](#)
  - enabling with LEAP [5-29](#)
  - enabling with PEAP (EAP-GTC) [5-48](#)
  - enabling with PEAP (EAP-MSCHAP V2) [5-52](#)
  - in site survey utility [82](#)
  - software required [56](#)

- Wi-Fi Protected Access 2 (WPA2)
  - described [5-19](#)
  - enabling with EAP-FAST [5-34](#)
  - enabling with EAP-TLS [5-45](#)
  - enabling with LEAP [5-29](#)
  - enabling with PEAP (EAP-GTC) [5-48](#)
  - enabling with PEAP (EAP-MSCHAP V2) [5-52](#)
  - in site survey utility [82](#)
- Windows 2000
  - disabling Microsoft 802.1X supplicant [10-8](#)
  - resolving resource conflicts [10-9](#)
- Windows Wireless Network Connection icon, shows unavailable connection [10-11](#)
- Windows XP
  - associating to an access point [70](#)
  - configuring client adapter through [57 to 62](#)
  - disabling Microsoft Wireless Configuration Manager [10-8](#)
  - enabling EAP-TLS authentication [62 to 64](#)
  - enabling PEAP authentication [65 to 70](#)
  - feature comparison to ADU [3-17 to 3-18](#)
  - making a configuration decision [3-17 to 3-18](#)
  - resolving resource conflicts [10-10](#)
  - security features [54 to 56](#)
  - viewing status of client adapter [70](#)
- Wireless Cisco Connection Properties window - Windows 2000 [5-60](#)
- wireless infrastructure [1-6](#)
- wireless mode, current [4-6, 7-5](#)
- Wireless Mode parameter [5-10](#)
- Wireless Mode When Starting Ad Hoc Network parameter [5-10](#)
- Wireless Network Connection Properties window (Wireless Networks Tab) - Windows XP [58](#)
- Wireless Network Connection Properties window - Windows XP [5-62](#)
- Wireless Network Connection Status window - Windows XP [70](#)
- Wireless Network Properties window (Association Tab) - Windows XP [59](#)
- Wireless Network Properties window (Authentication Tab) - Windows XP [62, 65](#)
- WMM
  - See Wi-Fi Multimedia (WMM)
- workstation
  - defined [1-2](#)
  - in wireless infrastructure [1-6](#)
- WPA
  - See Wi-Fi Protected Access (WPA)
- WPA/WPA2/CCKM EAP Type parameter
  - with EAP-FAST [5-34](#)
  - with EAP-TLS [5-45](#)
  - with LEAP [5-29](#)
  - with PEAP (EAP-GTC) [5-48](#)
  - with PEAP (EAP-MSCHAP V2) [5-52](#)
- WPA/WPA2/CCKM option
  - used to enable CCKM fast secure roaming [5-20](#)
  - with EAP-FAST [5-34](#)
  - with EAP-TLS [5-45](#)
  - with LEAP [5-29](#)
  - with PEAP (EAP-GTC) [5-48](#)
  - with PEAP (EAP-MSCHAP V2) [5-52](#)
- WPA/WPA2 Passphrase option [5-28](#)
- WPA2
  - See Wi-Fi Protected Access 2 (WPA2)
- WPA2 passphrase
  - described [5-19](#)
  - disabling [5-58](#)
  - enabling [5-28](#)
  - setting on client and access point [5-22](#)
- WPA option, in Windows XP [60](#)
- WPA passphrase
  - described [5-19, 56](#)
  - disabling [5-58](#)
  - enabling [5-28](#)
  - setting on client and access point [5-22](#)
- WPA Pre-Shared Key
  - See WPA passphrase or WPA2 passphrase
- WPA-PSK



described [5-19, 56](#)

option in Windows XP [60](#)