CHAPTER 5

Creating Profiles

This chapter explains how to use ACAU to create profiles that are saved to a configuration file and installed by the Install Wizard when a user installs the client adapter software.

The following topics are covered in this chapter:

Overview of the Profile Management Tab

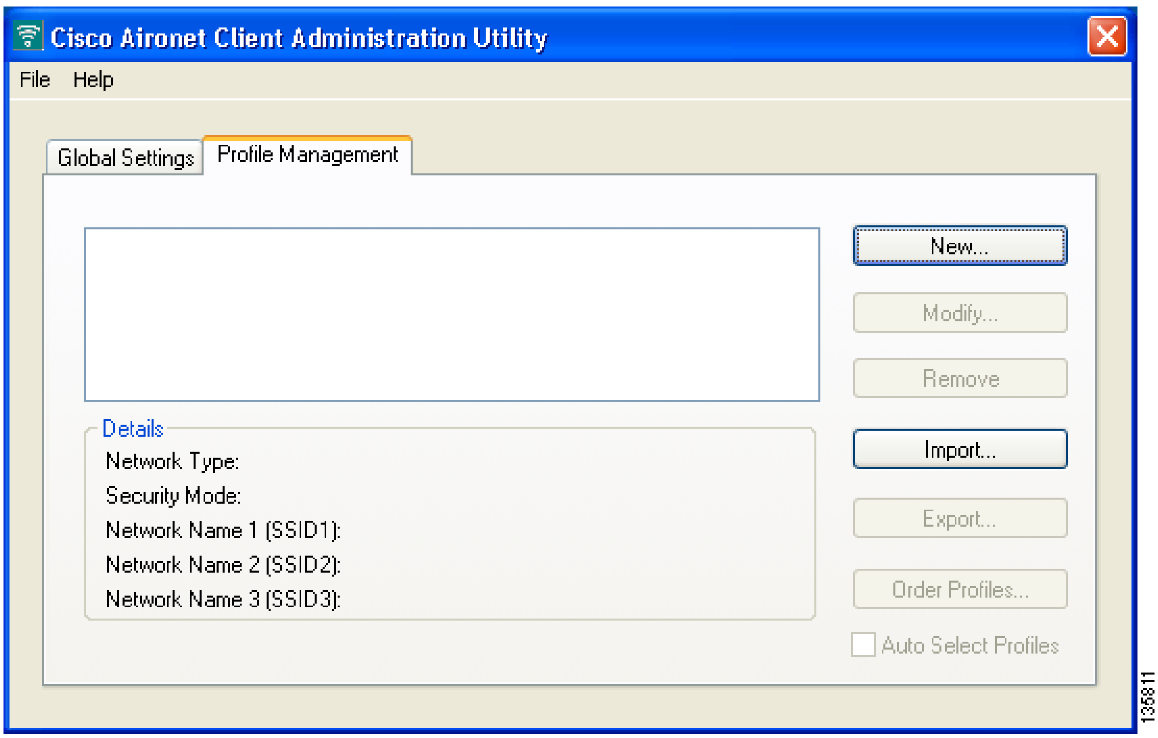
ACAU's Profile Management tab enables you to create or modify up to 16 *profiles* (saved configurations) for users' client adapters. The parameters that you set for each profile govern the operation of the adapters. After you create the profiles, you must save them to an ACAU configuration file where they are stored until the Install Wizard installs them during the installation of the client adapter software.

Note In addition to creating profiles, you can also use the Profile Management tab to remove, import, export, or auto-select profiles. See the "Managing Profiles" section on page 3-7 for more information.

Opening the Profile Manager

To open ACAU's profile manager, click the **Profile Management** tab. The Profile Management window appears (see Figure 5-1).

Figure 5-1 Profile Management Window



When you choose to create a new profile or modify an existing profile, the Profile Editor windows appear. These windows enable you to set the configuration parameters for that profile.

Each of the Profile Editor windows (listed below) contains parameters that affect a specific aspect of the client adapter:

- **General**—Prepares the client adapter for use in a wireless network
- **Advanced**—Controls how the client adapter operates within an infrastructure or ad hoc network
- **Security**—Controls how a client adapter associates to an access point, authenticates to the wireless network, and encrypts and decrypts data

Table 5-1 enables you to quickly locate instructions for setting each Profile Editor window's parameters.

Table 5-1 Locating Configuration Instructions

Parameter Category	Page Number
General	page 5-3
Advanced	page 5-6
Security	page 5-14

Setting General Parameters

The Profile Editor (General) window (see Figure 5-2) enables you to set parameters that prepare the client adapter for use in a wireless network. This window appears after you select the Profile Management tab and click **New** or **Modify** on the Profile Management window.

Figure 5-2 Profile Editor (General) Window

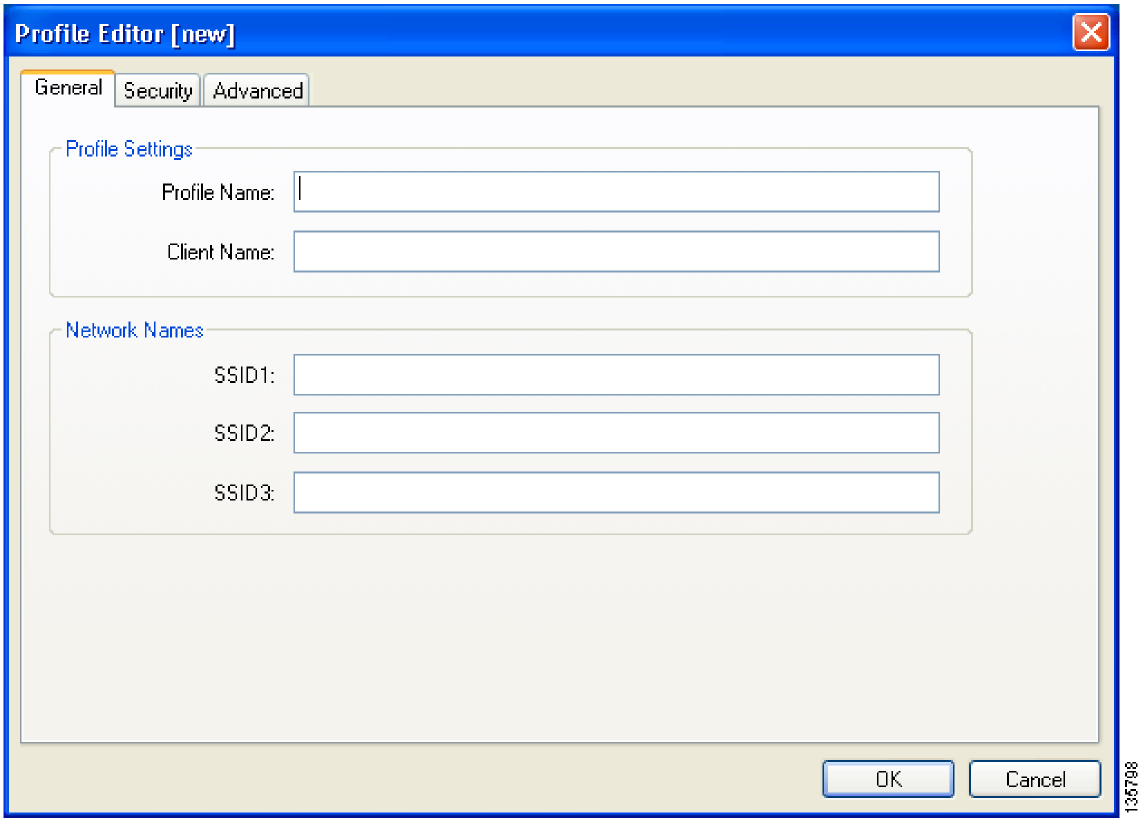


Table 5-2 lists and describes the profile's general parameters. Follow the instructions in the table to change any parameters.

Table 5-2 General Parameters

Parameter	Description
Profile Name	The name assigned to the configuration profile. **Range:** Up to 32 ASCII characters **Default:** A blank field
Client Name	A logical workstation name. It enables an administrator to determine which devices are connected to the access point without having to memorize every MAC address. This name is included in the access point's list of connected devices. The client name is filled in automatically but can be changed. **Range:** Up to 16 ASCII characters **Default:** The computer name **Note** Each computer on the network should have a unique client name.

Table 5-2 General Parameters (continued)

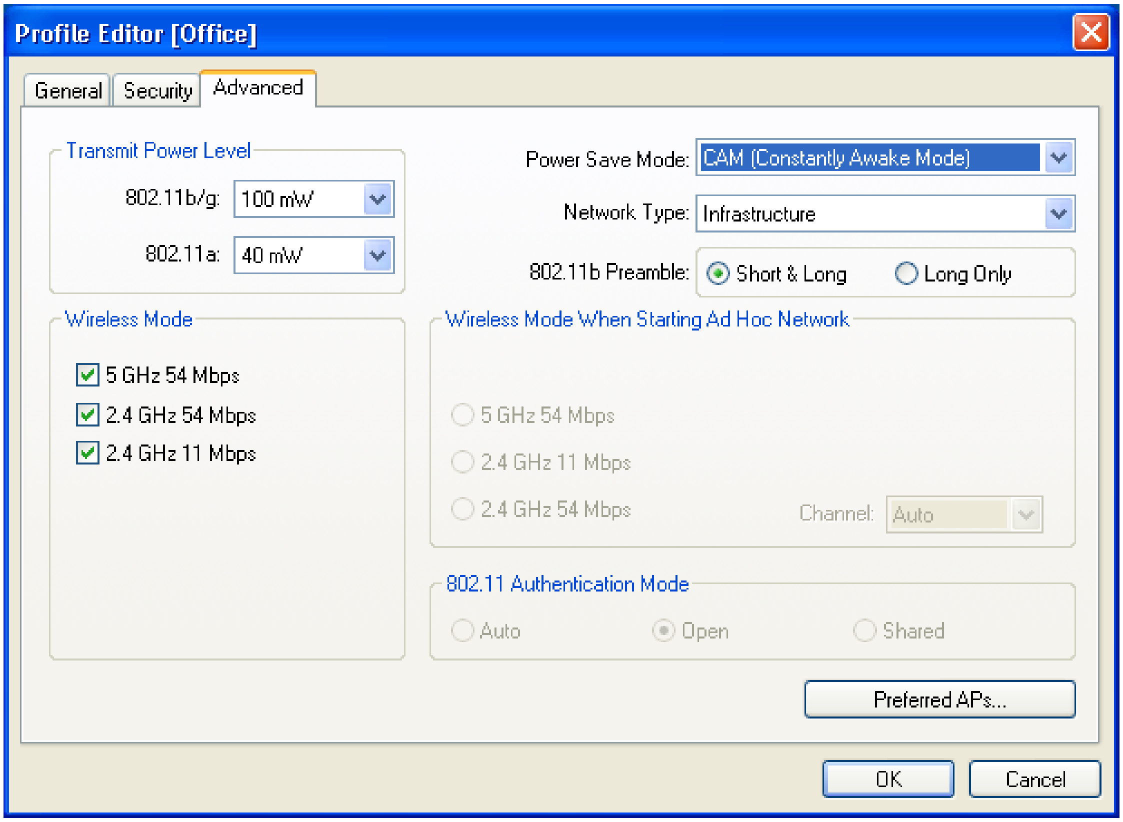
Parameter	Description
SSID1	The service set identifier (SSID) identifies the specific wireless network that you want the client adapter to access. **Range:** Up to 32 ASCII characters (case sensitive) **Default:** A blank field **Note** If you leave this parameter blank, the client adapter can associate to any access point on the network that is configured to allow broadcast SSIDs. If the access point with which the client adapter is to communicate is not configured to allow broadcast SSIDs, the value of this parameter must match the SSID of the access point. Otherwise, the client adapter is unable to access the network. **Note** If you leave this parameter blank, the profile cannot be added to the auto profile selection list. **Note** This parameter must contain a value if the profile is set for ad hoc mode. If the parameter is blank, you are prompted to enter a network name or reset the network type to *infrastructure*.
SSID2 and SSID3	An optional SSID that identifies a second or third distinct wireless network and enables the client adapter to roam to that network without having to be reconfigured. **Range:** Up to 32 ASCII characters (case sensitive) **Default:** A blank field **Note** If a profile specifies more than one SSID, it cannot be included in auto profile selection, used with WPA/WPA2 passphrase, or set for ad hoc mode.

Go to the next section to set additional parameters or click **OK** to return to the Profile Management window.

Setting Advanced Parameters

The Profile Editor (Advanced) window (see Figure 5-3) enables you to set parameters that control how the client adapter operates within an infrastructure or ad hoc network. To open this window, click the **Advanced** tab from any Profile Editor window.

Figure 5-3 Profile Editor (Advanced) Window



135790

Table 5-3 lists and describes the profile's advanced parameters. Follow the instructions in the table to change any parameters.

Table 5-3 Advanced Parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Transmit Power Level</td><td>Specifies the preferred power level at which the client adapter transmits. Although the adapter supports up to 100 mW, the transmit power level actually used is limited to the maximum value allowed by your country's regulatory agency (FCC in the U.S., DOC in Canada, ETSI in Europe, TELEC in Japan, etc.).

Options: Dependent on the radio band used and the power table programmed into the client adapter; see the table below

Default: The maximum power level programmed into the client adapter and allowed by your country's regulatory agency

<table>
<tr><th>Radio Band</th><th>Transmit Power Level</th></tr>
<tr><td>802.11b/g</td><td>10, 20, 32, 50, 63, or 100 mW</td></tr>
<tr><td>802.11a</td><td>10, 13, 20, 25, or 40 mW</td></tr>
</table>
Note When the client adapter operates in 802.11g mode, the maximum transmit power may be capped at a lower level than when operating in the 802.11b mode. This is due to 802.11g-specific regulatory limitations in some countries.

Note Reducing the transmit power level conserves battery power but decreases radio range.</td></tr>
</table>

Table 5-3 Advanced Parameters (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Power Save Mode</td><td>Sets the client adapter to its optimum power consumption setting.

Options: CAM (Constantly Awake Mode), Fast PSP (Power Save Mode), or Max PSP (Max Power Saving)

Default: CAM (Constantly Awake Mode)
<table>
<tr><th>Power Save Mode</th><th>Description</th></tr>
<tr><td>CAM (Constantly Awake Mode)</td><td>Keeps the client adapter powered up continuously so there is little lag in message response time.

Consumes the most power but offers the highest throughput. Is recommended for desktop computers and devices that use AC power.

Note This is the only mode available in an ad hoc network.</td></tr>
<tr><td>Fast PSP (Power Save Mode)</td><td>Switches between PSP mode and CAM mode, depending on network traffic. This mode switches to CAM when retrieving a large number of packets and switches back to PSP after the packets have been retrieved.

Is recommended when power consumption is a concern but you need greater throughput than that allowed by Max PSP.

Note This mode is not available in an ad hoc network.</td></tr>
<tr><td>Max PSP (Max Power Saving)</td><td>Causes the access point to buffer incoming messages for the client adapter, which wakes up periodically and polls the access point to see if any buffered messages are waiting for it. The adapter can request each message and then go back to sleep.

Conserves the most power but offers the lowest throughput. Is recommended for devices for which power consumption is the ultimate concern (such as small battery-powered devices).

Note This mode is not available in an ad hoc network.</td></tr>
</table></td></tr>
</table>

Table 5-3 Advanced Parameters (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Network Type</td><td>Specifies the type of network in which the client adapter is installed.
Options: Infrastructure or Ad Hoc
Default: Infrastructure
<table>
<tr><th>Network Type</th><th>Description</th></tr>
<tr><td>Ad Hoc</td><td>Often referred to as peer to peer. Indicates that the wireless network consists of a few wireless devices that are not connected to a wired Ethernet network through an access point. For example, an ad hoc network could be set up between computers in a conference room so that users can share information in a meeting.</td></tr>
<tr><td>Infrastructure</td><td>Indicates that the wireless network is connected to a wired Ethernet network through an access point.</td></tr>
</table></td></tr>
<tr><td>802.11b Preamble</td><td>Determines whether the client adapter will use both short and long radio headers or only long radio headers. The adapter can use short radio headers only if the access point is also configured to support them and is using them. If any clients associated to an access point are using long headers, then all clients in that cell must also use long headers, even if both this client and the access point have short radio headers enabled.

Short radio headers improve throughput performance; long radio headers ensure compatibility with clients and access points that do not support short radio headers.

Options: Short & Long or Long Only
Default: Short & Long

Note This parameter is disabled if the Wireless Mode parameter does not include the 2.4 GHz 11 Mbps option.</td></tr>
</table>

Table 5-3 Advanced Parameters (continued)

Parameter	Description
Wireless Mode	Specifies the frequency and rate at which the client adapter should transmit packets to or receive packets from access points. **Options:**5 GHz 54 Mbps, 2.4 GHz 54 Mbps, and 2.4 GHz 11 Mbps **Default:** All options selected **Note** When more than one option is selected, the client adapter attempts to use the wireless modes in this order: 5 GHz 54 Mbps, 2.4 GHz 54 Mbps, 2.4 GHz 11 Mbps. **Note** If you choose 2.4 GHz 11 Mbps, the client adapter can associate to access points containing an 802.11b or 802.11g radio at 802.11b data rates. If you choose 2.4 GHz 54 Mbps, the client adapter can associate to access points containing an 802.11b radio at 802.11b data rates or to access points containing an 802.11g radio at 802.11b or 802.11g data rates. **Note** When you enable auto profile selection, the client adapter ignores the selected profile's wireless mode setting and scans the wireless modes specified by all the profiles in the auto profile selection list for an available network. Using this method, the client does not need to disassociate nor change the current profile while looking for networks in other profiles. **Note** The client adapter's wireless mode must match that of the access points with which it is to communicate. Otherwise, the client adapter may not be able to associate to them.
Wireless Mode When Starting Ad Hoc Network	Specifies the frequency and rate at which the client adapter should transmit packets to or receive packets from other clients (in ad hoc mode). **Options:**5 GHz 54 Mbps, 2.4 GHz 11 Mbps, or 2.4 GHz 54 Mbps **Default:** 5 GHz 54 Mbps **Note** The client scans the band(s) specified by the Wireless Mode parameter before creating a new ad hoc cell based on the band specified by the Wireless Mode When Starting Ad Hoc Network parameter. **Note** The client adapter's wireless mode must match that of the other clients with which it is to communicate. Otherwise, the client adapter may not be able to associate to them. **Note** The 2.4 GHz 54 Mbps wireless mode may not be functional on some vendors' products. In this case, the client adapter uses the 2.4 GHz 11 Mbps wireless mode.

Table 5-3 Advanced Parameters (continued)

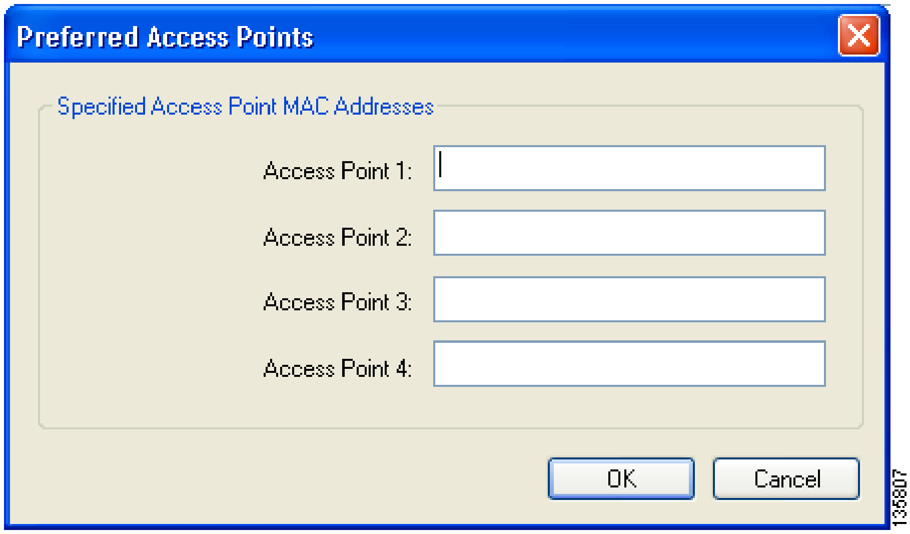
Parameter	Description
Channel	Specifies the channel that the client adapter uses for communications in a 2.4-GHz ad hoc network. The available channels conform to the IEEE 802.11 Standard for your regulatory domain. The channel of the client adapter must be set to match the channel used by the other clients in the wireless network. If the client adapter does not find any other ad hoc clients, this parameter specifies the channel with which the adapter will start its cell. **Range:** Dependent on regulatory domain **Example:** 1 to 11 (2412 to 2462 MHz) in North America **Default:** Auto (the client automatically determines the channel on which to start communications) **Note** This parameter is available only when 2.4 GHz 11 Mbps or 2.4 GHz 54 Mbps is selected for the Wireless Mode When Starting Ad Hoc Network parameter. When 5 GHz 54 Mbps is selected, the Channel parameter is set to Auto automatically. **Note** Refer to Appendix B for a list of channel identifiers, channel center frequencies, and regulatory domains for each channel.

Table 5-3 Advanced Parameters (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>802.11 Authentication Mode</td><td>
Specifies how the client adapter attempts to authenticate to an access point. Open and shared authentication do not rely on a RADIUS server on the user’s network.
Options: Auto, Open, or Shared
Default: Open
<table>
<tr><th>802.11 Authentication Mode</th><th>Description</th></tr>
<tr><td>Auto</td><td>Causes the client adapter to attempt to authenticate using shared authentication. If it fails, the client adapter then attempts to authenticate using open authentication.</td></tr>
<tr><td>Open</td><td>Enables the 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.</td></tr>
<tr><td>Shared</td><td> Enables the client adapter to authenticate and communicate only with access points that have the same WEP key. During shared key authentication, the access point sends an encrypted challenge packet to the client adapter, which encrypts the packet and sends it back to the access point. The access point attempts to decrypt the encrypted packet and sends an authentication response packet indicating the success or failure of the decryption back to the client adapter. If the packet is successfully encrypted/decrypted, the user is considered to be authenticated. </td></tr>
</table>
Note Cisco recommends that Auto and Shared not be used because they present a security risk.
Note The client adapter’s 802.11 authentication mode setting must match that of the access points with which it is to communicate. Otherwise, the client adapter may not be able to authenticate to them.
Note If this profile is configured for use in an adhoc network or is not configured to use static WEP, this parameter is unavailable, and Open authentication is used.
</td></tr>
</table>

If this profile is configured for use in an infrastructure network and you want to specify up to four access points to which the client adapter should attempt to associate, click **Preferred APs**. The Preferred Access Points window appears (see Figure 5-4).

Figure 5-4 Preferred Access Points Window



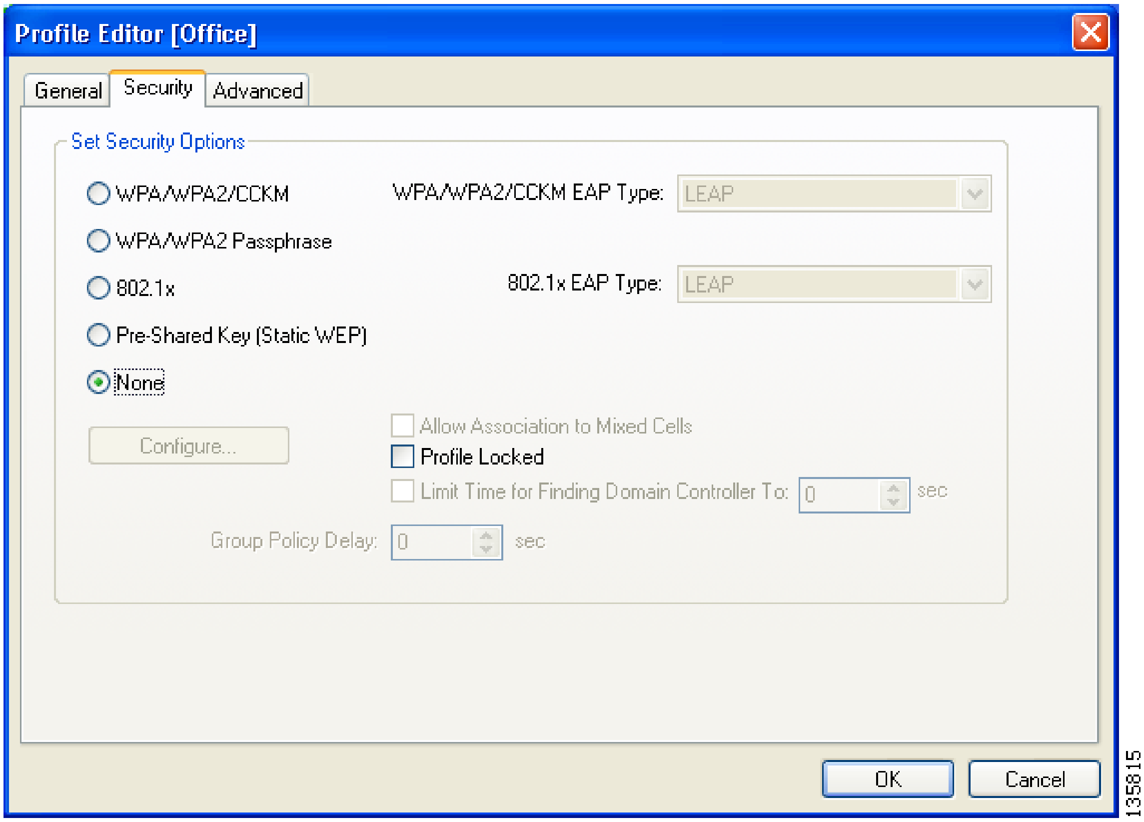
Leave the Access Point 1-4 fields blank or enter the MAC addresses of up to four preferred access points to which the client adapter can associate; then click **OK**. (The MAC address should consist of 12 hexadecimal characters.) If the specified access points are not found or the client adapter roams out of range, the adapter may associate to another access point.

Go to the next section to set security parameters or click **OK** to return to the Profile Management window.

Setting Security Parameters

The Profile Editor (Security) window (see Figure 5-5) enables you to set parameters that control how the client adapter associates to an access point, authenticates to the wireless network, and encrypts and decrypts data. To open this window, click the **Security** tab from any Profile Editor window.

Figure 5-5 Profile Editor (Security) Window



This window is different from the other Profile Editor windows in that it includes many security features, each of which involves a number of steps. In addition, the security features themselves are complex and need to be understood before they are implemented. Therefore, this section provides an overview of the security features as well as procedures for enabling them. Before moving on, however, you must decide whether to lock this particular profile. See the section below for more information.

Limiting Time for Finding a Domain Controller

If you want to limit the amount of time that is spent searching for a domain controller during the authentication process, check the **Limit Time for Finding Domain Controller To** check box. Then in the edit box, enter the amount of time (in seconds) to which you want to limit the search for the domain controller. A timeout value of 0 causes the authentication process to bypass the “Finding Domain Controller” step altogether.

Range of timeout value: 0 to 300 seconds

Default: Unchecked; 0 seconds

Locking a Profile

As an added security measure, ACAU gives you the option of locking individual profiles, which prevents users from being able to modify or remove these profiles. This feature ensures a high level of security and consistent configurations. It is especially useful if you want to create a standard profile for the corporate network, distribute it to each user, and ensure that it cannot be modified or removed.

The following rules apply to locked profiles:

- Locked profiles can be created only by an administrator using ACAU.
- A profile can be individually locked or unlocked; however, a user's ability to modify profiles (through ACAU's Global Settings - User Settings parameters) takes precedence. For example, if a user is not permitted to modify a profile, he or she is also unable to modify an unlocked profile.
- A locked profile cannot be overwritten, either by import or from the conversion of a 350 or CB20A profile through the profile migration tool.
- When a locked profile is exported and then imported onto another machine, the profile remains locked.
- All fields in a locked profile are read-only except password fields, which can be edited.

Perform one of the following:

- If you want to prevent users from being able to modify or remove this profile, check the **Profile Locked** check box.
- If you want to allow users to modify or remove this profile, uncheck the **Profile Locked** check box. This is the default setting.

Overview of Security Features

You can protect the user's data as it is transmitted through the 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 the 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 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.

Note Refer to the "Additional WEP Key Security Features" section on page 5-21 for information on three security features that can make WEP keys even more secure.

Static WEP Keys

Each device (or profile) within the 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.

The user does 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.

The Configure Pre-Shared Keys (Static WEP) window enables you to view the WEP key settings for a particular profile and to assign new WEP keys or overwrite existing WEP keys. Refer to the "Enabling Static WEP" section on page 5-25 for instructions.

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.

Five 802.1X authentication types are available in ACAU for use with Windows 2000 or XP:

- **EAP-Cisco Wireless** (or **LEAP**)—This authentication type leverages Cisco Key Integrity Protocol (CKIP) and MMH message integrity check (MIC) for data protection. ACAU offers a variety of LEAP configuration options, including how a username and password are entered to begin the authentication process.

  The username and password are used by the client adapter to perform mutual authentication with the RADIUS server through the access point. The username and password need to be re-entered each time the client adapter is inserted or the Windows device is rebooted unless the client adapter is using a profile with saved LEAP credentials.

  RADIUS servers that support LEAP include Cisco Secure ACS release 2.6 or later, Cisco Access Registrar release 1.7 or later, Funk Software's Steel-Belted RADIUS release 4.1 or later, and Meetinghouse Data Communications' AEGIS release 1.1 or later.

- **EAP-FAST**—This authentication type (Flexible Authentication via Secure Tunneling) uses a three-phased tunneled authentication process to provide advanced 802.1X EAP mutual authentication.
  - Phase 0 enables the client to dynamically provision a protected access credentials (PAC) when necessary. During this phase, a PAC is generated securely between the user and the network.
  - Phase 1 uses the PAC to establish a mutually authenticated and secure tunnel between the client and the RADIUS server. RADIUS servers that support EAP-FAST include Cisco Secure ACS version 3.2.3 and later.
  - Phase 2 performs client authentication in the established tunnel.

  ACAU offers a variety of EAP-FAST configuration options, including how and when a username and password are entered to begin the authentication process and whether automatic or manual PAC provisioning is used.

The client adapter uses the username, password, and PAC to perform mutual authentication with the RADIUS server through the access point. The username and password need to be re-entered each time the client adapter is inserted or the Windows device is rebooted unless the client adapter is using a profile with saved EAP-FAST credentials.

PACs are created by Cisco Secure ACS 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. When manual PAC provisioning is enabled, the PAC is manually copied from the server and imported onto the client device. The following rules govern PAC storage:

- PACs are stored as encrypted data files in either the global or private store on the user's computer.
  - Global PACs can be accessed and used by any user at any logon stage. They are available before or during logon or after the user is logged off if the profile is not configured with the No Network Connection Unless User Is Logged In option.
  - Private PACs can be accessed and used only by the user who provisioned them or the system administrator.

  Note Global PACs are stored on C:\Document and Settings\All Users\Application Data\Cisco\cscostore, and private PACs are stored on C:\Document and Settings*user*\ Application Data\Cisco\cscostore.

- If automatic PAC provisioning is enabled and it occurs after the user is logged on, the PAC is stored in the private store of the currently logged-on user. Otherwise, the PAC is stored in the global store.
- PAC files can be added or overwritten using the import feature.
- PAC files can be removed using the delete feature. They are also deleted when the client adapter software is uninstalled.
- PAC files are tied to the machine, so they cannot be used if copied to another machine.

EAP-FAST authentication is designed to support the following user databases over a wireless LAN:

- Cisco Secure ACS internal user database
- Cisco Secure ACS ODBC user database
- Windows NT/2000/2003 domain user database
- LDAP user database

LDAP user databases (such as NDS) support only manual PAC provisioning while the other three user databases support both automatic and manual PAC provisioning.

- **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.

- **PEAP (EAP-GTC)**—This PEAP authentication type 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 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 the user's network uses an OTP user database, PEAP (EAP-GTC) requires the user to enter a hardware or software token password to start the EAP authentication process and gain access to the network. If the user's network uses a Windows NT or 2000 domain user database or an LDAP user database (such as NDS), PEAP (EAP-GTC) requires the user to enter a 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.
- **PEAP (EAP-MSCHAP V2)**—This PEAP authentication type is based on EAP-TLS authentication but uses a password or 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.

When the access point is configured as indicated in Table 5-4 on page 5-21 and the client adapter is configured for LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2), authentication to the network occurs in the following sequence:

1. The client 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 (LEAP and PEAP), PAC (EAP-FAST), or certificate (EAP-TLS and PEAP) being the shared secret for authentication. The password and PAC are 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.

Refer to the following pages for instructions on enabling these EAP types:

- LEAP, page 5-28
- EAP-FAST, page 5-32
- EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2), page 5-44

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/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt2/scrad.htm

WPA and WPA2

Wi-Fi Protected Access (WPA) and WPA2 are standards-based security solutions from the Wi-Fi Alliance that provide data protection and access control for wireless LAN systems. WPA is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification; WPA2 is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard.

WPA uses Temporal Key Integrity Protocol (TKIP) and message integrity check (MIC) for data protection while WPA2 uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). Both WPA and WPA2 use 802.1X for authenticated key management.

Both WPA and WPA2 support two mutually exclusive key management types: WPA/WPA2 and WPA/WPA2 passphrase (also known as *WPA pre-shared key* or *WPA-PSK*). Using WPA or WPA2, 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 or WPA2 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.

Refer to the following pages for instructions on enabling these WPA variations:

- WPA/WPA2 passphrase, page 5-27
- LEAP with WPA/WPA2, page 5-28
- EAP-FAST with WPA/WPA2, page 5-19
- EAP-TLS with WPA/WPA2, page 5-45
- PEAP (EAP-GTC) with WPA/WPA2, page 5-48
- PEAP (EAP-MSCHAP V2) with WPA/WPA2, page 5-52

Note WPA must also be enabled on the access point. To use WPA, access points must use Cisco IOS Release 12.2(11)JA or later. To use WPA2, access points must use Cisco IOS Release 12.3(2)JA or later. Refer to the documentation for your access point for instructions on enabling this feature.

CCKM Fast Secure Roaming

Some applications that run on a client device may require fast roaming between access points. Voice applications, for example, require it to prevent delays and gaps in conversation. CCKM fast secure roaming is enabled automatically for CB21AG and PI21AG clients using WPA/WPA2/CCKM with LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2). However, this feature must be enabled on the access point.

During normal operation, EAP-enabled clients mutually authenticate with a new access point by performing a complete EAP authentication, including communication with the main RADIUS server. However, when you configure your wireless LAN for CCKM fast secure roaming, EAP-enabled clients securely roam from one access point to another without the need to reauthenticate with the RADIUS server. Using Cisco Centralized Key Management (CCKM), an access point that is configured for wireless domain services (WDS) uses a fast rekeying technique that enables Cisco client devices to roam from one access point to another typically in under 150 milliseconds (ms). CCKM fast secure roaming ensures that there is no perceptible delay in time-sensitive applications such as wireless Voice over IP (VoIP), enterprise resource planning (ERP), or Citrix-based solutions.

Note If you want to enable CCKM fast secure roaming on the client adapter, you must choose the WPA/WPA2/CCKM security option on the Profile Editor (Security) window, regardless of whether you want the adapter to use WPA or WPA2. The configuration of the access point to which the client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.

Note Access points must use Cisco IOS Release 12.2(11)JA or later to enable CCKM fast secure roaming. Refer to the documentation for your access point for instructions on enabling this feature.

Note The Microsoft Wireless Configuration Manager and the Microsoft 802.1X supplicant, if installed on the user's computer, must be disabled in order for CCKM fast secure roaming to operate correctly. If the computer is running Windows XP and the user chooses to configure the client adapter using ADU during installation, these features should already be disabled. Similarly, if the computer is running Windows 2000, the Microsoft 802.1X supplicant, if installed, should already be disabled.

Reporting Access Points that Fail LEAP Authentication

The CB21AG and PI21AG client adapters and the following access point firmware versions support a feature that is designed to detect access points that fail LEAP authentication:

- 12.00T or later (access points running VxWorks)
- Cisco IOS Release 12.2(4)JA or later (1100 series access points)
- Cisco IOS Release 12.2(8)JA or later (1200 series access points)
- Cisco IOS Release 12.2(13)JA or later (350 series access points)

An access point running one of these firmware versions records a message in the system log when the client discovers and reports another access point in the wireless network that has failed LEAP authentication.

The process takes place as follows:

1. A client with a LEAP profile attempts to associate to access point A.
2. Access point A does not handle LEAP authentication successfully, perhaps because the access point does not understand LEAP or cannot communicate to a trusted LEAP authentication server.
3. The client records the MAC address for access point A and the reason why the association failed.
4. The client associates successfully to access point B.
5. The client sends the MAC address of access point A and the reason code for the failure to access point B.
6. Access point B logs the failure in the system log.

Note This feature does not need to be enabled on the client adapter or access point; it is supported automatically by both devices. However, the access points must use the specified firmware versions or later.

Additional WEP Key Security Features

The three security features discussed in this section (MIC, TKIP, and broadcast key rotation) are designed to prevent sophisticated attacks on your wireless network's WEP keys. These features do not need to be enabled on the client adapter; they are supported automatically in the client adapter software. However, they must be enabled on the access point.

Note Refer to the documentation for your access point for instructions on enabling these security features.

Message Integrity Check (MIC)

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 MIC adds a few bytes to each packet to make the packets tamper-proof.

Temporal Key Integrity Protocol (TKIP)

This feature, also referred to as *WEP key hashing*, 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. It protects both unicast and broadcast WEP keys.

Note TKIP is enabled automatically when WPA is enabled, and it is disabled when WPA is disabled.

Broadcast Key Rotation

When you enable broadcast WEP key rotation, the access point provides a dynamic broadcast WEP key and changes it at the interval you select.

Synchronizing Security Features

In order to use any of the security features discussed in this section, both the client adapter and the access point to which it will associate must be set appropriately. Table 5-4 indicates the client and access point settings required for each security feature. This chapter provides specific instructions for enabling the security features on the client adapter. Refer to the documentation for your access point for instructions on enabling any of these features on the access point.

Table 5-4 Client and Access Point Security Settings

Security Feature	Client Setting	Access Point Setting
Static WEP with open authentication	Choose Open authentication and Pre-Shared Key (Static WEP) and create a WEP key	Set up and enable WEP and enable Open Authentication for the SSID
Static WEP with shared key authentication	Choose Shared authentication and Pre-Shared Key (Static WEP) and create a WEP key	Set up and enable WEP and enable Shared Key Authentication for the SSID

Table 5-4 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
WPA or WPA2 passphrase (or WPA or WPA2 pre-shared key)	Choose WPA/WPA2 Passphrase and enter the passphrase	Choose a cipher suite, enable Open Authentication and WPA for the SSID, and enter a WPA pre-shared key **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.
LEAP authentication	Choose 802.1x and LEAP; then set LEAP settings	Set up and enable WEP and enable Network-EAP Authentication for the SSID
LEAP authentication with WPA or WPA2	Choose WPA/WPA2/CCKM and LEAP; then set LEAP settings	For WPA, choose a cipher suite that includes TKIP and enable Network-EAP and Open with EAP Authentication and WPA for the SSID For WPA2, choose a cipher suite that includes AES-CCMP and enable Network-EAP and Open with EAP Authentication and WPA for the SSID **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.
EAP-FAST authentication	Choose 802.1x and EAP-FAST, set EAP-FAST settings, and enable automatic provisioning or import a PAC file	Set up and enable WEP and enable both Network-EAP and Open with EAP Authentication for the SSID
EAP-FAST authentication with WPA or WPA2	Choose WPA/WPA2/CCKM and EAP-FAST, set EAP-FAST settings, and enable automatic provisioning or import a PAC file	For WPA, choose a cipher suite that includes TKIP and enable both Network-EAP and Open with EAP Authentication as well as WPA for the SSID For WPA2, choose a cipher suite that includes AES-CCMP and enable both Network-EAP and Open with EAP Authentication as well as WPA for the SSID **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.

Table 5-4 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
EAP-TLS authentication	Choose 802.1x and EAP-TLS; then set EAP-TLS settings	Set up and enable WEP and enable Open with EAP Authentication for the SSID
EAP-TLS authentication with WPA or WPA2	Choose WPA/WPA2/CCKM and EAP-TLS; then set EAP-TLS settings	For WPA, choose a cipher suite that includes TKIP; then enable WPA and Open with EAP Authentication for the SSID For WPA2, choose a cipher suite that includes AES-CCMP; then enable WPA and Open with EAP Authentication for the SSID **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.
PEAP authentication	Choose 802.1x and PEAP (EAP-GTC) or PEAP (EAP-MSCHAP V2); then set PEAP settings	Set up and enable WEP and enable Open with EAP Authentication for the SSID
PEAP authentication with WPA or WPA2	Choose WPA/WPA2/CCKM and PEAP (EAP-GTC) or PEAP (EAP-MSCHAP V2); then set PEAP settings	For WPA, choose a cipher suite that includes TKIP; then enable WPA and Open with EAP Authentication for the SSID For WPA2, choose a cipher suite that includes AES-CCMP; then enable WPA and Open with EAP Authentication for the SSID **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.

Table 5-4 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
CCKM fast secure roaming	Choose WPA/WPA2/CCKM and LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP MSCHAP V2); then set the EAP authentication settings **Note** If you want to enable CCKM, you must choose WPA/WPA2/CCKM, regardless of whether you want the client adapter to use WPA or WPA2. The configuration of the access point to which the client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.	Use Cisco IOS Release 12.2(11)JA or later, choose a cipher suite that is compatible with CCKM, enable both Network-EAP and Open with EAP Authentication and CCKM for the SSID, and configure for participation in wireless domain services (WDS) **Note** To allow both 802.1X clients and non-802.1X clients to use the SSID, enable optional CCKM.
Reporting access points that fail LEAP authentication	No settings required; automatically enabled	No settings required; automatically enabled in the firmware versions listed on page 5-20.
MIC	No settings required; automatically enabled	Set up and enable WEP with full encryption, set MIC to MMH or check the Enable MIC check box, and set Use Aironet Extensions to Yes
TKIP	No settings required; automatically enabled	Set up and enable WEP, set TKIP to Cisco or check the Enable Per Packet Keying check box, and set Use Aironet Extensions to Yes
Broadcast key rotation	Enable LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2)	Set up and enable WEP and set Broadcast WEP Key Rotation Interval to any value other than zero (0)

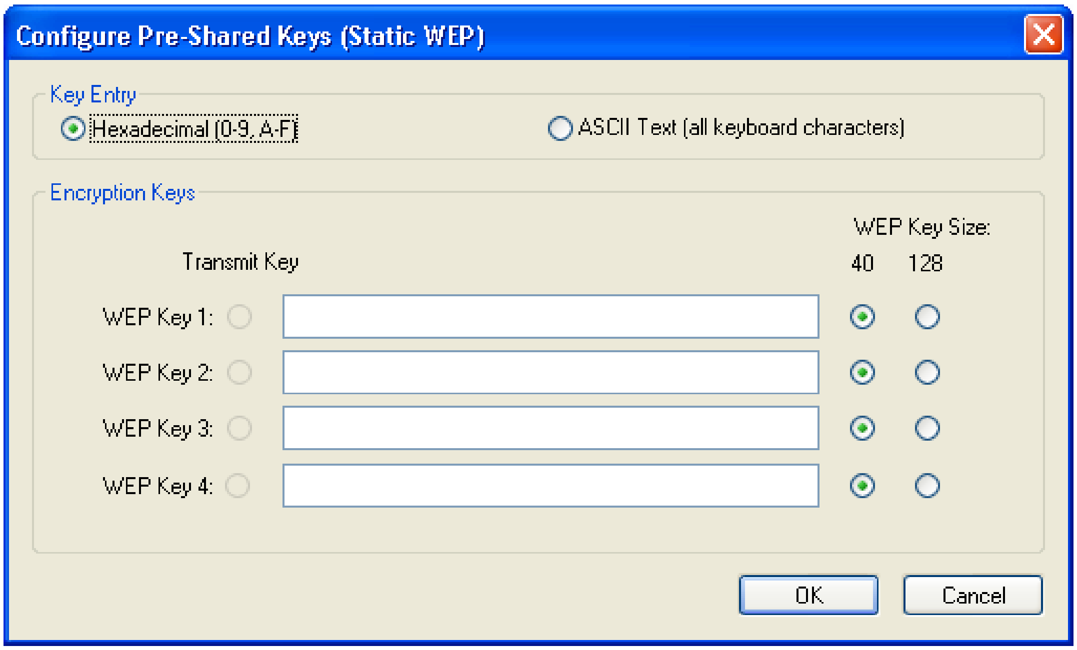
Enabling Static WEP

Follow the steps below to enable static WEP for this profile.

Step 1 Select **Pre-Shared Key (Static WEP)** on the Profile Editor (Security) window.

Step 2 Click **Configure**. The Configure Pre-Shared Keys (Static WEP) window appears (see Figure 5-6).

Figure 5-6 Configure Pre-Shared Keys (Static WEP) Window



135809

Step 3 Choose one of the following WEP key entry methods:

- **Hexadecimal (0-9, A-F)**—Specifies that the WEP key will be entered in hexadecimal characters, which include 0-9, A-F, and a-f.
- **ASCII Text (all keyboard characters)**—Specifies that the WEP key will be entered in ASCII text, which includes alpha characters, numbers, and punctuation marks.

Note ASCII text WEP keys are not supported on the Cisco Aironet 1200 Series Access Points, so you must choose the Hexadecimal (0-9, A-F) option if the client adapter may be used with these access points.

Step 4 For the static WEP key that you are entering (1, 2, 3, or 4), select a WEP key size of 40 or 128 on the right side of the window. 128-bit client adapters can use 40- or 128-bit keys, but 40-bit adapters can use only 40-bit keys. If 128 bit is not supported by the client adapter, this option is unavailable.

Step 5 Enter the static WEP key in the blank field for the key you are creating. 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 You must enter hexadecimal characters if the client adapter may be used with Cisco Aironet 1200 Series Access Points.

- The client adapter's WEP key must match the WEP key used by the access point (in infrastructure mode) or clients (in ad hoc mode).
- When setting more than one WEP key, the keys must be assigned to the same WEP key numbers for all devices. For example, WEP key 2 must be WEP key number 2 on all devices. When multiple WEP keys are set, they must be in the same order on all devices.

Note All existing static WEP keys are displayed as bullets for security reasons. If you need to modify a WEP key, simply click in the WEP key field, delete the bullets, and enter a new key.

Step 6 Click the **Transmit Key** button to the left of the key you want to use to transmit packets. Only one WEP key can be selected as the transmit key.

Step 7 Click **OK** to save your changes and return to the Profile Editor (Security) window.

Step 8 Perform one of the following to set the Allow Association to Mixed Cells parameter, which indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) has WEP set to Optional. Otherwise, the client is unable to establish a connection with the access point.
- Uncheck the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) does not have WEP set to Optional. This is the default setting.

Note For security reasons, Cisco recommends that WEP-enabled and WEP-disabled clients not be allowed in the same cell because broadcast packets are sent unencrypted, even to clients running WEP. However, you can enable VLANs on the access point to separate WEP-enabled and WEP-disabled clients.

Step 9 Click **OK** to save your settings and return to the Profile Management window.

Enabling WPA/WPA2 Passphrase

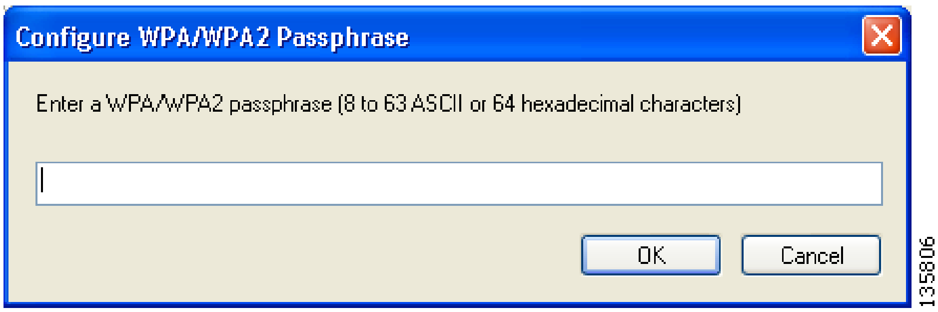
Follow the steps below to enable WPA/WPA2 passphrase (also known as *WPA/WPA2 pre-shared key*) for this profile.

Note To use WPA passphrase, access points must use Cisco IOS Release 12.2(11)JA or later. To use WPA2 passphrase, access points must use Cisco IOS Release 12.3(2)JA or later.

Step 1 Select **WPA/WPA2 Passphrase** on the Profile Editor (Security) window.

Step 2 Click **Configure**. The Configure WPA/WPA2 Passphrase window appears (see Figure 5-7).

Figure 5-7 Configure WPA/WPA2 Passphrase Window



Step 3 Enter the WPA/WPA2 passphrase for the access point (in an infrastructure network) or other clients (in an ad hoc network) in the WPA/WPA2 passphrase field. Follow the guidelines below to enter a passphrase:

- WPA/WPA2 passphrases must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.
- The client adapter's WPA/WPA2 passphrase must match the passphrase used by the access point.

Step 4 Click **OK** to save the passphrase and return to the Profile Editor (Security) window.

Step 5 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the user's computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000 or computers running Windows XP without Service Pack 2 or later. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section in Chapter 3 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for information on obtaining and installing the hot fix.

Step 6 Click **OK** to save your settings and return to the Profile Management window.

Enabling LEAP

In order to use LEAP authentication, the devices on the user's network must meet the following requirements:

- Access points to which the client adapter may attempt to authenticate must use the following firmware versions or later: 11.23T (access points running VxWorks), Cisco IOS Release 12.2(4)JA (1100 series access points), Cisco IOS Release 12.2(8)JA (1200 series access points), or Cisco IOS Release 12.2(13)JA (350 series access points).

  Note To use WPA or CCKM, access points must use Cisco IOS Release 12.2(11)JA or later. To use WPA2, access points must use Cisco IOS Release 12.3(2)JA or later. To use the Reporting Access Points That Fail LEAP Authentication feature, access points must use the firmware versions listed on page 5-21.

- All necessary infrastructure devices (for example, access points, servers, etc.) must be properly configured for LEAP authentication.

Follow the steps below to enable LEAP authentication for this profile.

Step 1 Perform one of the following on the Profile Editor (Security) window:

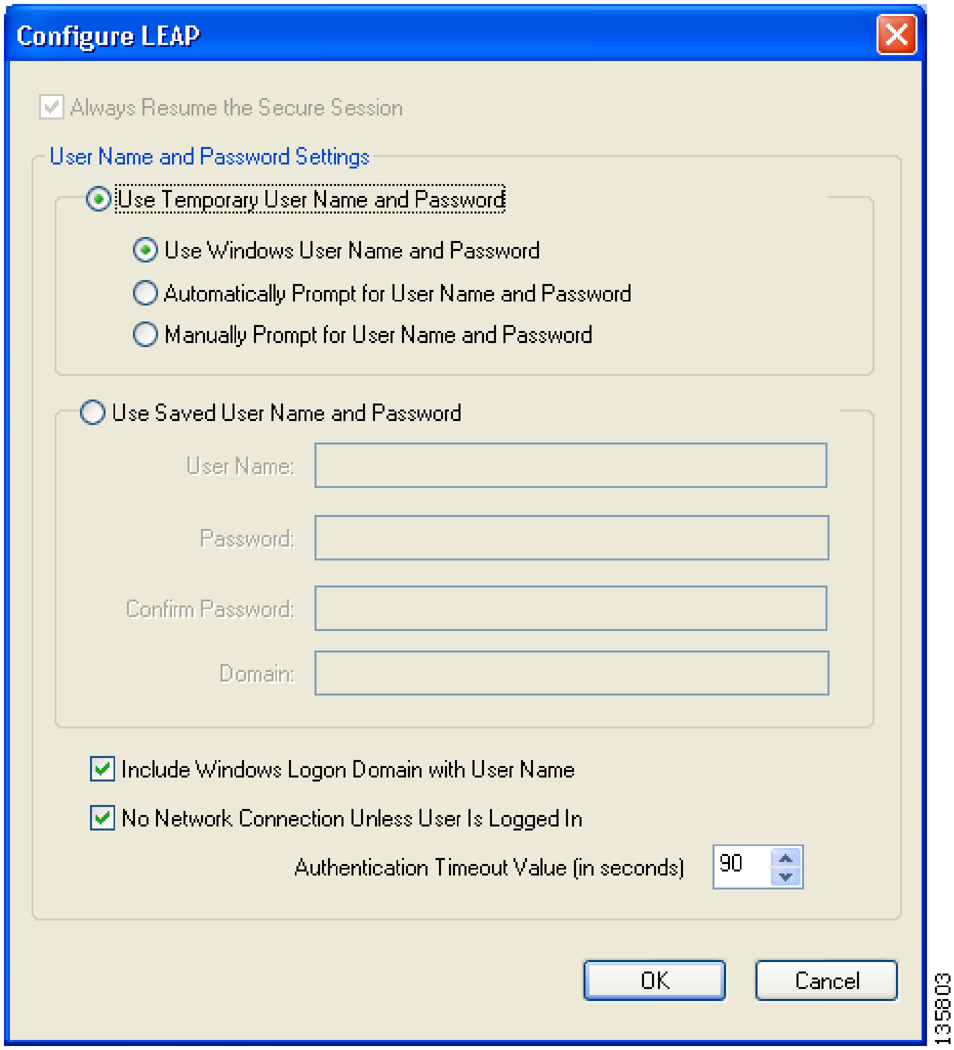
- If you want to enable LEAP without WPA or WPA2, choose **802.1x** under Set Security Options and **LEAP** in the 802.1x EAP Type drop-down box.
- If you want to enable LEAP with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **LEAP** in the WPA/WPA2/CCKM EAP Type drop-down box.

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

Note Refer to the "WPA and WPA2" section on page 5-19 for additional information.

Step 2 Click **Configure**. The Configure LEAP window appears (see Figure 5-8).

Figure 5-8 Configure LEAP Window



Step 3 Choose one of the following LEAP username and password setting options:

- **Use Temporary User Name and Password**—Requires the user to enter the LEAP username and password each time the computer reboots in order to authenticate and gain access to the network.
- **Use Saved User Name and Password**—Does not require the user to enter a LEAP username and password each time the computer reboots. Authentication occurs automatically as needed using a saved username and password (which are registered with the RADIUS server).

Step 4 Perform one of the following:

- If you selected Use Temporary User Name and Password in Step 3, select one of the following options:
  - **Use Windows User Name and Password**—Causes the user's Windows username and password to also serve as the LEAP username and password, giving the user only one set of credentials to remember. After the user logs in, the LEAP authentication process begins automatically. This option is the default setting.
  - **Automatically Prompt for User Name and Password**—Requires the user to enter a separate LEAP username and password (which are registered with the RADIUS server) in addition to the regular Windows login in order to start the LEAP authentication process.
  - **Manually Prompt for User Name and Password**—Requires the user to manually invoke the LEAP authentication process as needed using the Manual Login option in the ADU Action drop-down menu or ASTU. The user is not prompted to enter a LEAP username and password during the Windows login. This option might be used to support a software token one-time password system or other systems that require additional software that is not available at login.
- If you chose Use Saved User Name and Password in Step 3, follow these steps:
  - **a.** Enter a username and password in the appropriate fields.
  - **b.** Re-enter the password in the Confirm Password field.
  - **c.** If you wish to specify a domain name that is passed to the RADIUS server along with the username, enter it in the Domain field.

Step 5 If you chose Automatically Prompt for User Name and Password or Manually Prompt for User Name and Password in Step 4, perform one of the following:

- Check the **Always Resume the Secure Session** check box at the top of the window if you want the LEAP supplicant to always attempt to resume the previous session without prompting the user to re-enter his or her credentials whenever the client adapter becomes disassociated. Session resume occurs after the client temporarily loses connection to the access point (such as by roaming in and out of range) or wakes up from suspend or hibernate mode. This is the default setting.
- Uncheck the **Always Resume the Secure Session** check box if you want the user to be prompted to re-enter his or her LEAP username and password whenever the client adapter temporarily loses association by roaming out of range or wakes up from suspend or hibernate mode.

Note Checking this check box gives the user the convenience of not having to re-enter his or her username and password when the client adapter experiences momentary losses of association. However, if the user leaves the device unattended during the period of time when the LEAP session can be resumed without re-entering user credentials, be aware that someone can resume the user's LEAP session and access the network.

Note The Always Resume the Secure Session check box is disabled if you chose Use Windows User Name and Password or Use Saved User Name and Password in Step 4.

Step 6 If the user works in an environment with multiple domains and you want the Windows login domain to be passed to the RADIUS server along with the username, check the **Include Windows Logon Domain with User Name** check box. The default setting is checked.

Note If you chose to use a saved username and password but do not check the Include Windows Logon Domain with User Name check box, the saved domain name is not passed to the RADIUS server.

Step 7 If you want to force the client adapter to disassociate after the user logs off so that another user cannot gain access to the wireless network using the user's credentials, check the **No Network Connection Unless User Is Logged In** check box. The default setting is checked.

Step 8 In the Authentication Timeout Value field, choose the amount of time (in seconds) before a LEAP authentication attempt is considered to be failed and an error message appears.

Range: 30 to 300 seconds

Default: 90 seconds

Step 9 Click **OK** to save your changes and return to the Profile Editor (Security) window.

Step 10 Perform one of the following to set the Allow Association to Mixed Cells parameter, which indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) has WEP set to Optional. Otherwise, the client is unable to establish a connection with the access point.
- Uncheck the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) does not have WEP set to Optional. This is the default setting.

Note This parameter is available only if the 802.1x or Pre-Shared Keys (Static WEP) security option is selected.

Note For security reasons, Cisco recommends that WEP-enabled and WEP-disabled clients not be allowed in the same cell because broadcast packets are sent unencrypted, even to clients running WEP. However, you can enable VLANs on the access point to separate WEP-enabled and WEP-disabled clients.

Step 11 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the user's computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000 or computers running Windows XP without Service Pack 2 or later. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section in Chapter 3 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for information on obtaining and installing the hot fix.

Step 12 Click **OK** to save your settings and return to the Profile Management window.

Enabling EAP-FAST

Before you can enable EAP-FAST authentication, your network devices must meet the following requirements:

- Access points to which your client adapter may attempt to authenticate must use the following firmware versions or later: 11.23T (340 and 350 series access points), 11.54T (1200 series access points), Cisco IOS Release 12.3(4)JA (1130 series and BR 1310 series access points), Cisco IOS Release 12.3(7)JA (1240 series access points), or Cisco IOS Release 12.2(4)JA (1100 series access points).

  Note To use WPA or CCKM, access points must use Cisco IOS Release 12.2(11)JA or later. To use WPA2, access points must use Cisco IOS Release 12.3(2)JA or later. To use the Reporting Access Points That Fail LEAP or EAP-FAST Authentication feature, access points must use the firmware versions listed on page 5-20.

  Note The access point to which your client adapter will associate must be configured for open authentication.

- All necessary infrastructure devices (such as access points, servers, gateways and user databases) must be properly configured for EAP-FAST authentication.

Follow these steps to enable EAP-FAST authentication for this profile.

Step 1 Perform one of the following on the Profile Management (Security) window:

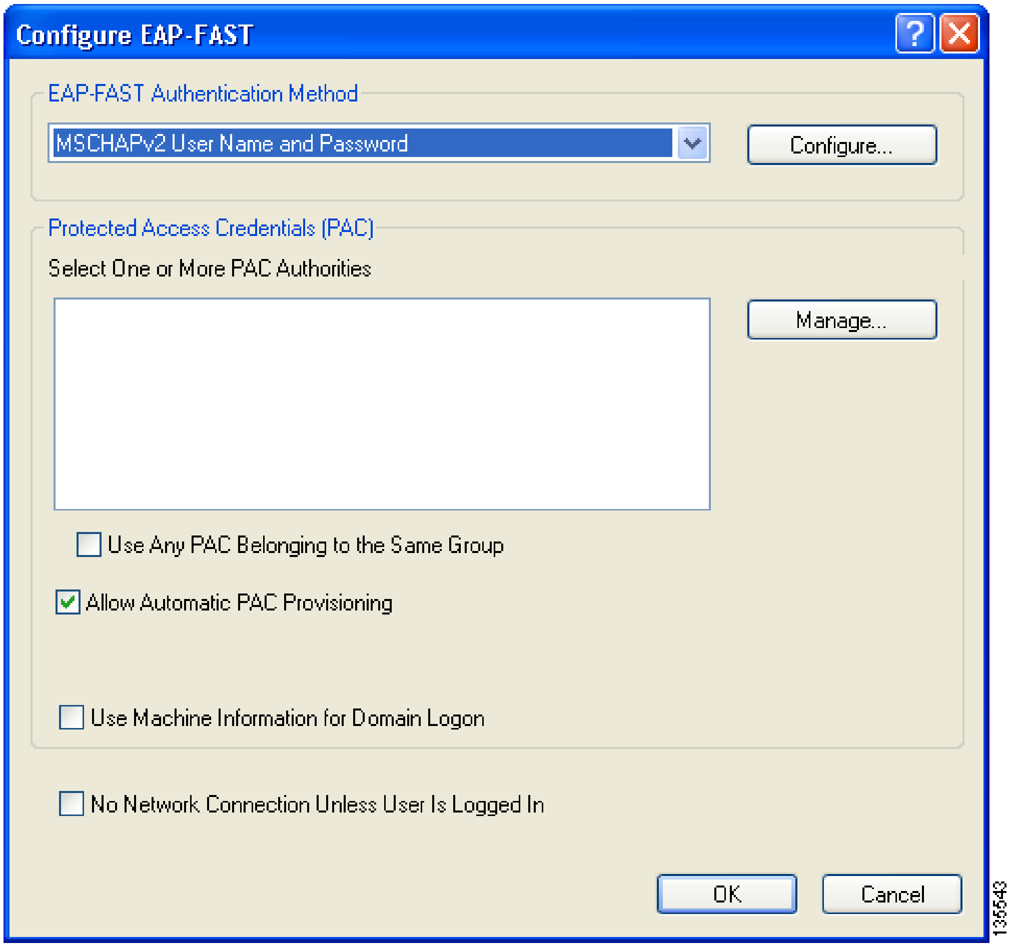
- If you want to enable EAP-FAST without WPA or WPA2, choose **802.1x** under Set Security Options and **EAP-FAST** in the 802.1x EAP Type drop-down box.
- If you want to enable EAP-FAST with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **EAP-FAST** in the WPA/WPA2/CCKM EAP Type drop-down box.

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

Note Refer to the "WPA and WPA2" section on page 5-19 for additional information.

Step 2 Click **Configure**. The Configure EAP-FAST window appears (see Figure 5-9).

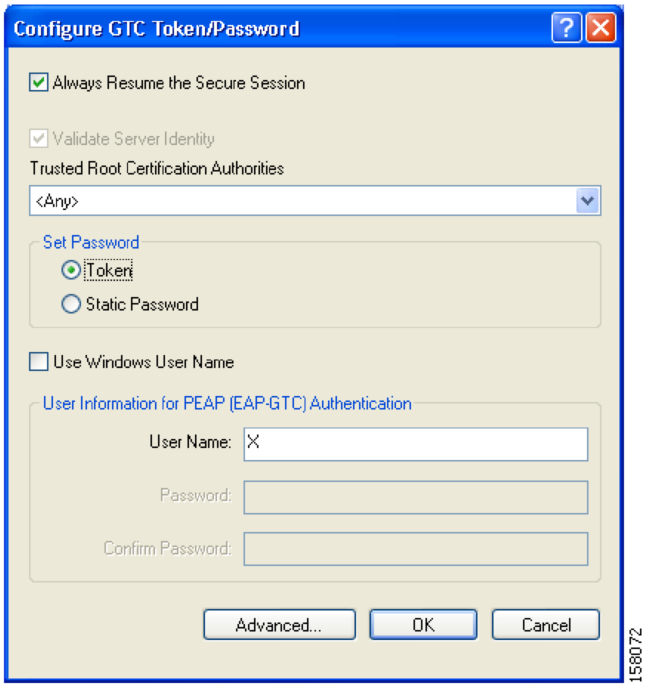
Figure 5-9 Configure EAP-FAST Window



Step 3 Choose an authentication method from the EAP-FAST Authentication Method drop-down list and click Configure.

Step 4 If you chose **GTC Token/Password** in Step 3, do the following in the Configure GTC Token/Password window (see Figure 5-10):

Figure 5-10 Configure GTC Token/Password Window



1. Check the **Always Resume the Secure Session** check box at the top of the window if you want the EAP-FAST supplicant to always attempt to resume the previous session without prompting you to re-enter your credentials whenever the client adapter becomes disassociated. The session resumes after the client temporarily loses connection to the access point (such as by roaming in and out of coverage) or wakes up from suspend or hibernate mode. This is the default setting.

   Uncheck the **Always Resume the Secure Session** check box if you want to be prompted to re-enter your EAP-FAST username and password whenever your client adapter temporarily loses association by roaming out of coverage or wakes up from suspend or hibernate mode.

Note Checking this check box gives you the convenience of not having to re-enter your network credentials when your client adapter experiences momentary losses of association. However, if you leave your device unattended during the period of time when the EAP-FAST session can be resumed without re-entering user credentials, be aware that someone can resume your EAP-FAST session and access the network.

Note The Always Resume the Secure Session check box is disabled if you chose **Static Password**.

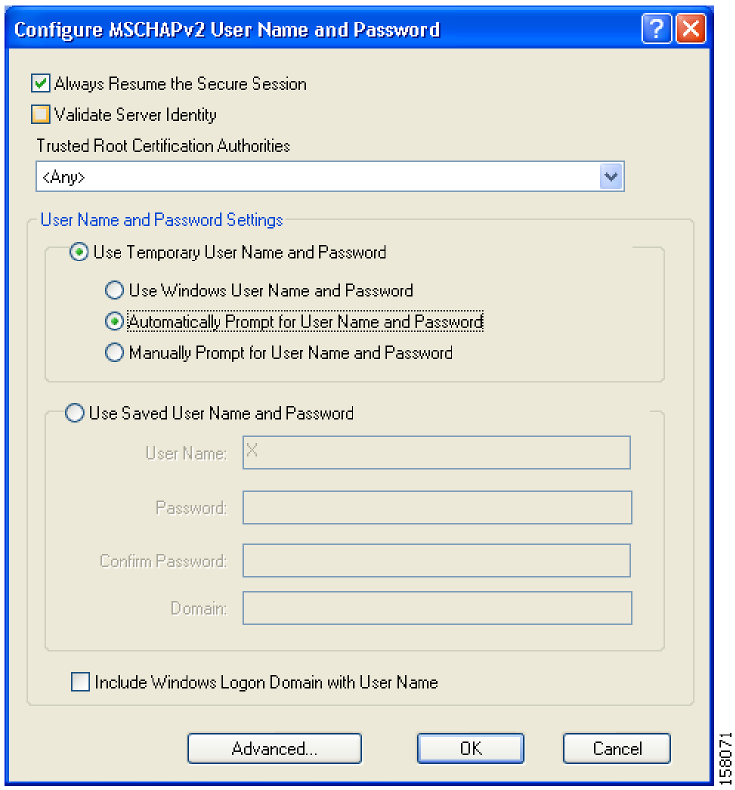
2. Check the **Validate Server Identity** check box to force the system to validate the identity of the server as an added level of security.

   If you uncheck this box, only user credentials will be validated.

3. To configure the remaining options in this window, refer to "Enabling PEAP (EAP-GTC)" section on page 5-48.
4. Click **OK** to save your settings and return to the Configure EAP-FAST window.

Step 5 If you chose **MSCHAPv2 User Name and Password** in Step 3, do the following in the Configure MSCHAPv2 User Name and Password window (see Figure 5-11):

Figure 5-11 Configure MSCHAPv2 User Name and Password Window



1. Check the **Always Resume the Secure Session** check box at the top of the window if you want the EAP-FAST supplicant to always attempt to resume the previous session without prompting you to re-enter your credentials whenever the client adapter becomes disassociated. The session resumes after the client temporarily loses connection to the access point (such as by roaming in and out of coverage) or wakes up from suspend or hibernate mode. This is the default setting.

   Uncheck the **Always Resume the Secure Session** check box if you want to be prompted to re-enter your EAP-FAST username and password whenever your client adapter temporarily loses association by roaming out of coverage or wakes up from suspend or hibernate mode.

   Note To check or uncheck the **Always Resume the Secure Session** check box, you must first choose **Automatically Prompt for User Name and Password** or **Manually Prompt for User Name and Password** under Use Temporary User Name and Password.

2. Check the **Validate Server Identity** check box to force the system to validate the identity of the server as an added level of security.

   If you uncheck this box, only user credentials will be validated.

3. Choose a certificate authority from which the server certificate was downloaded in the Trusted Root Certification Authorities drop-down box, or, if applicable, choose **<Any>**.

4. To use a temporary username and password, choose **Use Temporary User Name and Password**.

   This option requires you to enter the EAP-FAST username and password each time the computer reboots in order to authenticate and gain access to the network, unless you choose **Use Windows User Name and Password**.

   Choose one of the following options under Use Temporary User Name and Password:

   - **Use Windows User Name and Password—**Causes your Windows username and password to also serve as your EAP-FAST username and password, giving you only one set of credentials to remember. After you log in, the authentication process begins automatically. This option is the default setting.
   - **Automatically Prompt for User Name and Password**—Requires you to enter a separate EAP-FAST username and password (which are registered with the RADIUS server) in addition to your regular Windows login in order to start the authentication process.
   - **Manually Prompt for User Name and Password**—Requires you to manually invoke the EAP-FAST authentication process as needed using the Manual Login option in the Action drop-down menu or ASTU. You are not prompted to enter an EAP-FAST username and password during the Windows login. This option might be used to support a software token one-time password system or other systems that require additional software that is not available at login.

5. To use a saved username and password, choose **Use Saved User Name and Password**.

   This option does not require you to enter an EAP-FAST username and password each time the computer reboots. Authentication occurs automatically as needed using a saved username and password (which are registered with the RADIUS server).

   Follow these steps to specify the username and password to use for EAP-FAST authentication:

   a. Enter a username and password in the appropriate fields.

   b. Re-enter the password in the Confirm Password field.

   c. If you wish to specify a domain name that will be passed to the RADIUS server along with your username, enter it in the Domain field.

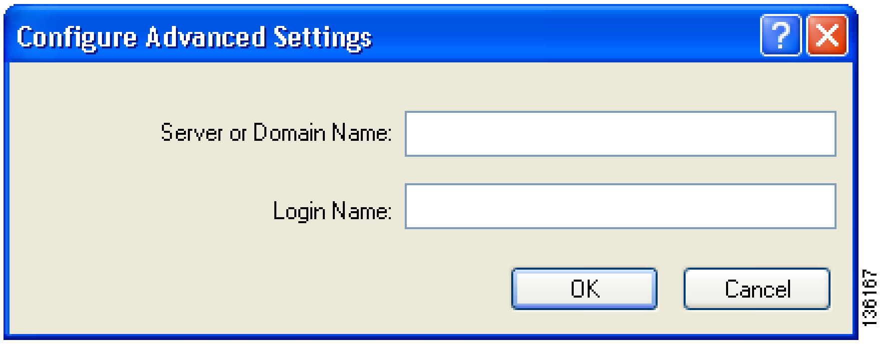
6. If you work in an environment with multiple domains and therefore want your Windows login domain to be passed to the RADIUS server along with your username, check the **Include Windows Logon Domain with User Name** check box. The default setting is checked.

Note If you chose to use a saved username and password but do not check the Include Windows Logon Domain with User Name check box, the saved domain name is not passed to the RADIUS server.

Step 6 If the Use Windows User Name and Password check box is unchecked and you want to implement added security, follow these steps:

a. Click **Advanced**. The Configure Advanced Settings window appears (see Figure 5-19).

Figure 5-12 Configure Advanced Settings Window



b. Leave the Specific Server or Domain field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the selected certificate authority or enter the domain name of the server from which the client will accept a certificate.

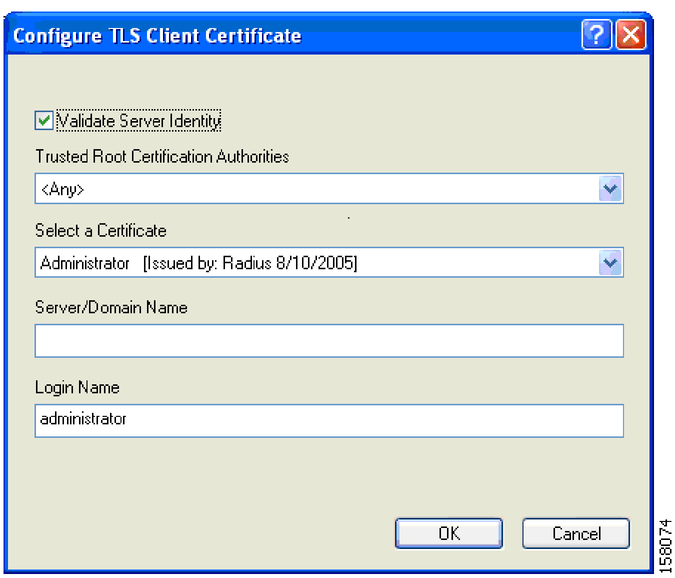
c. If the Login Name field is not filled in automatically, enter the username with nothing after it (for example, jsmith).

d. Click **OK** to save your settings.

Step 7 Click **OK** to save your settings and return to the Configure EAP-FAST window.

Step 8 If you chose **TLS Client Certificate** in Step 3, refer to "Enabling EAP-TLS" section on page 5-45 (Step 5 to Step 10) to configure the options in the Configure TLS Client Certificate window (Figure 5-13).

Figure 5-13 Configure TLS Client Certificate Window



Step 9 In the Select One or More PAC Authorities list, select the PAC authorities and PAC authority groups that are associated with the network defined by the profile's SSID. The list contains the names of all the authentication servers from which you have previously provisioned a PAC.

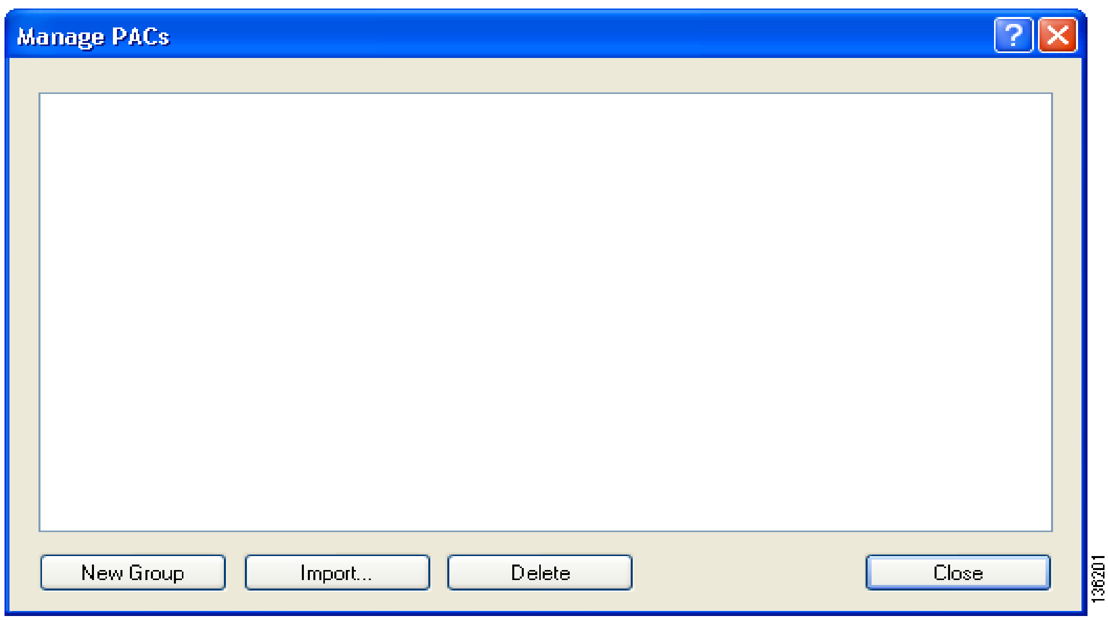
If the Select One or More PAC Authorities list is empty or does not contain the name of a desired PAC authority, go to Step 10 to import a PAC file.

Note This step is required for manual PAC provisioning but optional for automatic PAC provisioning. If automatic provisioning is enabled, automatic provisioning will be initiated during the authentication process of the EAP-FAST profile if no PAC authority was selected, the PAC could not be found, or the specified PAC does not match the server ID.

Step 10 If necessary, follow these steps to import or modify the grouping of PAC files:

a. Click **Manage**. The Manage PACs window appears (see Figure 5-14).

Figure 5-14 Manage PACs Window

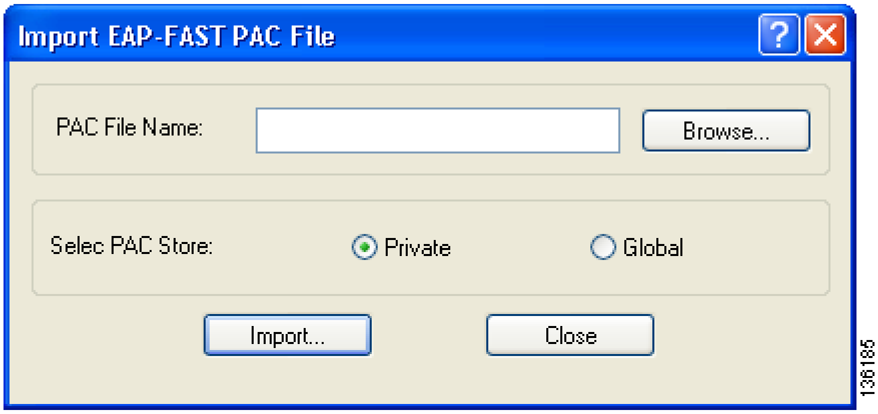


b. To create a new group, click **New Group**.

c. To move a PAC from one group to another, just drag it to the destination group.

d. Click **Import**. The Import EAP-FAST PAC File window appears (see Figure 5-15).

Figure 5-15 Import EAP-FAST PAC File Window



e. Find the location of the PAC file (*.pac) in the Look in box. The default location is C:\Program Files\Cisco Aironet.

Note The filename and extension of a PAC file is determined by the PAC authority that issues it, but the standard file extension is *pac*.

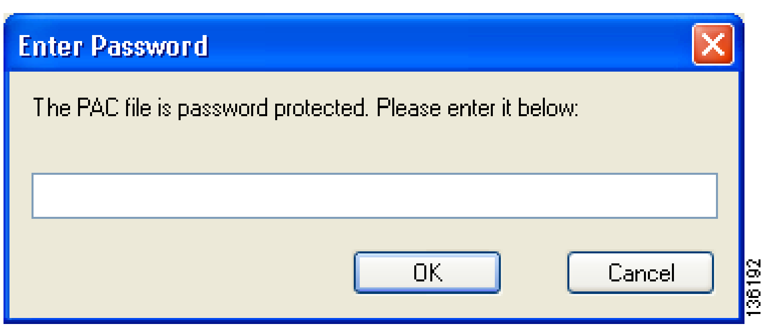
f. Choose one of these PAC store options to determine where the imported PAC file will be stored and to whom it will be accessible:

- **Global**—PACs that are stored in the global PAC store can be accessed and used by any user at any logon stage. Global PACs are available before or during logon or after the user is logged off if the profile is not configured with the No Network Connection Unless User Is Logged In option.
- **Private**—PACs that are stored in the private store can be accessed and used only by the user who provisioned them or the system administrator. They are not accessible until the user is logged onto the local system. This is the default option.

g. Click **Import**.

h. If the Enter Password window appears (see Figure 5-16), enter the PAC file password, which can be obtained from your system administrator, and click **OK**.

Figure 5-16 Enter Password Window



Note PAC file passwords are optional. The PAC authority determines whether to issue PAC files that require user-supplied passwords. Nevertheless, all PAC files (even those without passwords) are encrypted and protected. PAC file passwords are different from EAP-FAST passwords and need to be entered only once, at the time a PAC is imported.

i. If you try to import a PAC file with the same PAC ID as a previously imported PAC file, you are asked if you want to update the existing PAC. If you click **Yes**, the existing PAC is replaced by the new one from the imported file.

j. If the PAC file was imported successfully, the following message appears: "The EAP-FAST PAC file was imported and is ready for use." Click **OK** to return to the Manage PACs window.

k. The imported PAC now appears in the PAC tree on the Manage PACs window.

l. To delete a group or manually provisioned PAC file from storage, select the item and click **Delete**. When a message appears asking you to confirm your decision, click **Yes**. The PAC file is removed from the tree.

m. Click **Close** to return to the Configure EAP-FAST window.

n. The name of the PAC authority that issued the PAC now appears in the PAC authority list on the Configure EAP-FAST window. Select the desired PAC authorities or groups from the list.

Step 11 Check the **Use Any PAC Belonging to the Same Group** check box to use any PAC authority in the selected groups for PAC provisioning.

Step 12 Perform one of the following to configure PAC provisioning:

- If you want to enable automatic PAC provisioning, make sure the **Allow Automatic PAC Provisioning** check box is checked. A protected access credentials (PAC) is automatically obtained as needed (for example, when a PAC expires, when the client adapter accesses a different server or when the EAP-FAST username cannot be matched to a previously provisioned PAC).
- If you want to enable manual PAC provisioning, uncheck the **Allow Automatic PAC Provisioning** check box. This option requires you to choose a PAC authority or manually import a PAC file.

Note LDAP user databases support only manual PAC provisioning while Cisco Secure ACS internal, Cisco Secure ODBC, and Windows NT/2000/2003 domain user databases support both automatic and manual PAC provisioning.

Note Provisioning occurs only upon initial negotiation of the PAC or upon PAC expiration. After the PAC is provisioned, it serves as the per-user key by which authentication transactions are secured.

Step 13 Check the **Use Machine Information for Domain Logon** check box if you want the client to attempt to log into a domain using machine authentication with a machine certificate and machine credentials rather than user authentication. Doing so enables your computer to connect to the network prior to user logon. The default setting is unchecked.

Note If you do not check the Use Machine Information for Domain Logon check box, machine authentication is not performed. Authentication does not occur until you log on.

Step 14 If you want to force the client adapter to disassociate after you log off so that another user cannot gain access to the wireless network using your credentials, check the **No Network Connection Unless User Is Logged In** check box. The default setting is checked.

Step 15 Click **OK** to save your settings and return to the Profile Management (Security) window.

> **Note** If you selected a private PAC and the No Network Connection Unless User Is Logged In check box is unchecked, a message appears indicating that the PAC may not be accessible during the domain logon process or when you are logged off. 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**; then click **OK** when a message appears indicating that you may need to later reconfigure your profile to use a global PAC if you experience wireless connection problems during domain logon or when you are not logged on.

Step 16 Perform one of the following to set the Allow Association to Mixed Cells parameter, which indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) has WEP set to Optional. Otherwise, the client is unable to establish a connection with the access point.
- Uncheck the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) does not have WEP set to Optional. This is the default setting.

> **Note** This parameter is available only if the 802.1x security option is selected.

> **Note** For security reasons, Cisco recommends that WEP-enabled and WEP-disabled clients not be allowed in the same cell because broadcast packets are sent unencrypted, even to clients running WEP. However, you can enable VLANs on the access point to separate WEP-enabled and WEP-disabled clients.

Step 17 If you want to limit the amount of time that is spent searching for a domain controller during the authentication process, check the **Limit Time for Finding Domain Controller To** check box. Then in the edit box, enter the amount of time (in seconds) to which you want to limit the search for the domain controller. A timeout value of 0 causes the authentication process to bypass the “Finding Domain Controller” step altogether.

Range of timeout value: 0 to 300 seconds

Default: Unchecked; 0 seconds

Note When the "Finding Domain Controller" step is reached during the authentication process, a timer starts based on the number of seconds you specified for finding the domain controller. If either this value or the EAP-FAST authentication timeout value expires before the domain controller is found, the authentication process times out. For example, if the authentication timeout value is 60 seconds and the finding domain controller timeout value is 10 seconds, the client adapter has up to 60 seconds to complete the entire authentication process, up to 10 seconds of which is allocated for finding the domain controller. However, if authentication happens quickly, the software might reach the "Finding Domain Controller" step in 5 seconds. If the domain controller could not be found within 10 seconds, the authentication process would timeout in just 15 seconds.

Note The finding domain controller timeout value can never extend the authentication process beyond the EAP-FAST authentication timeout value, even if the finding domain controller timeout value is greater than the EAP-FAST authentication timeout value.

Note If you require domain services such as login scripts and roaming desktops, Cisco recommends that you uncheck the **Limit Time for Finding Domain Controller To** check box.

Note Regardless of whether the check box is checked or unchecked, the "Finding Domain Controller" step is bypassed once you are logged into Windows or if you log into the local machine and not into a domain.

Step 18 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000 or computers running Windows XP without Service Pack 2 or later. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section in Chapter 3 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for information on obtaining and installing the hot fix.

Step 19 Click **OK** to save your settings and return to the Profile Management window.

Enabling EAP-TLS or PEAP

In order to use EAP-TLS or PEAP authentication, the devices on the user's network must meet the following requirements:

- The user must have a valid Windows username and password, and the password cannot be blank.
- The appropriate certificates must be installed on the user's computer. EAP-TLS requires both a Certificate Authority (CA) certificate and a user certificate while PEAP requires only a CA certificate.
- To support EAP-TLS machine authentication with machine credentials:
  - A machine certificate must be obtained from the server, and client machine access must be enabled on the server.
  - Permissions for the MachineKeys folder, which stores the certificate pair keys for both the computer and users, must be set correctly. Refer to Microsoft knowledgebase article Q278381 for information on correctly setting up folder permissions:

    http://support.microsoft.com/default.aspx?scid=kb;en-us;Q278381

    Note If you ever change permissions on higher-level directories and those settings are applied to all subdirectories, you may need to reset the permissions for the MachineKeys folder.

- Access points to which the client adapter may attempt to authenticate must use the following firmware versions or later: 12.00T (access points running VxWorks), Cisco IOS Release 12.2(4)JA (1100 series access points), Cisco IOS Release 12.2(8)JA (1200 series access points), or Cisco IOS Release 12.2(13)JA (350 series access points).

  Note To use WPA or CCKM, access points must use Cisco IOS Release 12.2(11)JA or later. To use WPA2, access points must use Cisco IOS Release 12.3(2)JA or later.

- All necessary infrastructure devices (such as access points, servers, gateways, user databases, etc.) must be properly configured for the authentication type you plan to enable on the client.

Follow the instructions in one of the sections below to enable EAP-TLS or PEAP authentication for this profile:

- Enabling EAP-TLS, page 5-45
- Enabling PEAP (EAP-GTC), page 5-48
- Enabling PEAP (EAP-MSCHAP V2), page 5-52
- Enabling PEAP (EAP-MSCHAP V2) machine authentication with machine certificates, page 5-56

Enabling EAP-TLS

Follow the steps below to enable EAP-TLS authentication for this profile.

Step 1 Perform one of the following on the Profile Editor (Security) window:

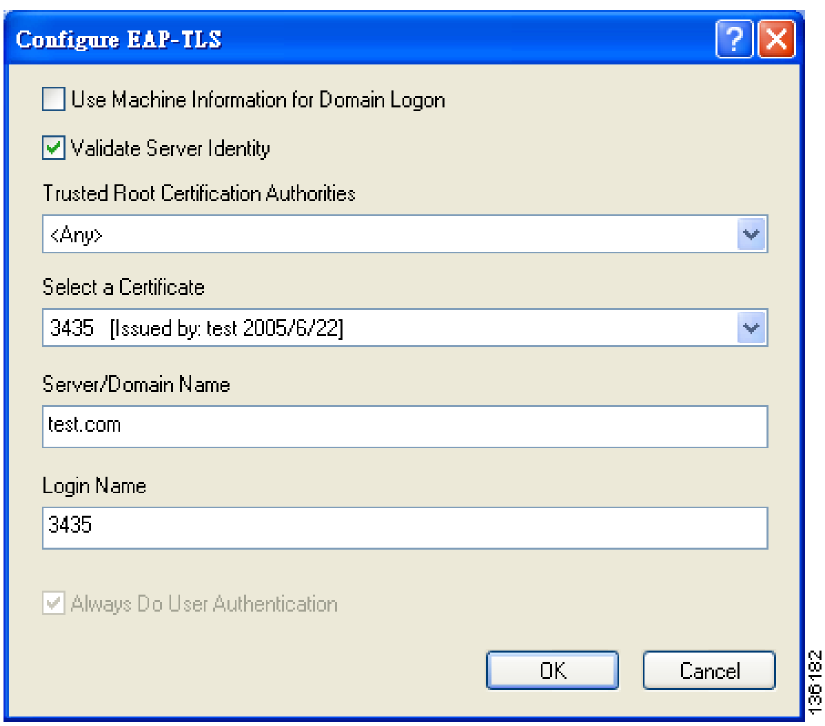
- If you want to enable EAP-TLS without WPA or WPA2, choose **802.1x** under Set Security Options and **EAP-TLS** in the 802.1x EAP Type drop-down box.
- If you want to enable EAP-TLS with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **EAP-TLS** in the WPA/WPA2/CCKM EAP Type drop-down box.

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

Note Refer to the "WPA and WPA2" section on page 5-19 for additional information.

Step 2 Click **Configure**. The Configure EAP-TLS window appears (see Figure 5-17).

Figure 5-17 Configure EAP-TLS Window



Step 3 Check the **Use Machine Information For Domain Logon** check box if you want the client to attempt to log into a domain using machine authentication with a machine certificate and machine credentials rather than user authentication. Doing so enables your computer to connect to the network prior to user logon. The default setting is unchecked.

Note If you do not check the Use Machine Information For Domain Logon check box, machine authentication is not performed. Authentication does not occur until you log on.

Step 4 If you checked the Use Machine Information For Domain Logon check box in the previous step, the Always Do User Authentication check box at the bottom of the window becomes active. Perform one of the following:

- Check the **Always Do User Authentication** check box if you want the client to switch from using machine authentication to using user authentication after you log on using your username and password. This is the default setting.
- Uncheck the **Always Do User Authentication** check box if you want the client to continue to use machine authentication after your computer logs into the domain.

Step 5 Check the **Validate Server Identity** check box to force the system to validate the identity of the server as an added level of security. If you uncheck this box, only user credentials will be validated.

Step 6 Choose the certificate authority from which the server certificate was downloaded in the Trusted Root Certification Authorities drop-down box.

Step 7 Choose your server certificate in the Select a Certificate drop-down box.

Step 8 Perform one of the following:

- Leave the Server/Domain Name field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the certificate authority listed in the Trusted Root Certification Authorities drop-down box. This is the recommended option.
- In the Server/Domain Name field, enter the domain name of the server from which the client will accept a certificate.

Step 9 If the Login Name field is not filled in automatically, enter your username in this format: *username@domain* (for example, jsmith@acs-test.cisco.com).

Step 10 Click **OK** to save your settings and return to the Profile Management (Security) window.

Step 11 Perform one of the following to set the Allow Association to Mixed Cells parameter, which indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) has WEP set to Optional. Otherwise, the client is unable to establish a connection with the access point.
- Uncheck the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) does not have WEP set to Optional. This is the default setting.

Note This parameter is available only if the 802.1x security option is selected.

Note For security reasons, Cisco recommends that WEP-enabled and WEP-disabled clients not be allowed in the same cell because broadcast packets are sent unencrypted, even to clients running WEP. However, you can enable VLANs on the access point to separate WEP-enabled and WEP-disabled clients.

Step 12 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the user's computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000 or computers running Windows XP without Service Pack 2 or later. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section in Chapter 3 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for information on obtaining and installing the hot fix.

Step 13 Click **OK** to save your settings and return to the Profile Management window.

Enabling PEAP (EAP-GTC)

Follow these steps to enable PEAP (EAP-GTC) authentication for this profile.

Step 1 Perform one of the following:

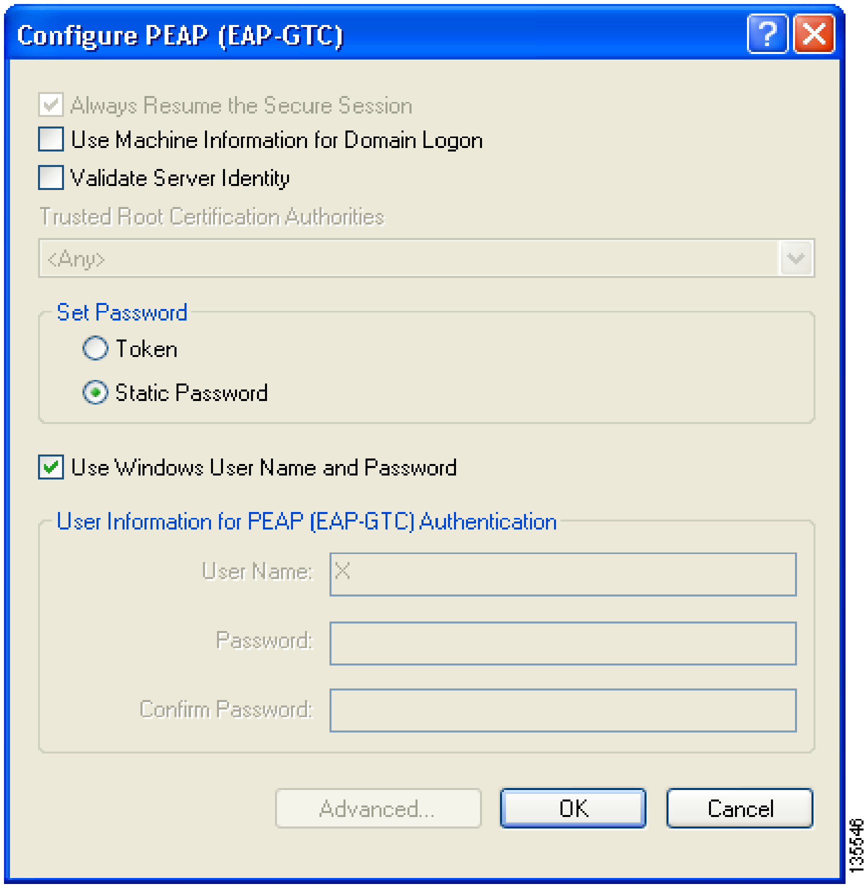
- If you want to enable PEAP (EAP-GTC) without WPA or WPA2, choose **802.1x** under Set Security Options and **PEAP (EAP-GTC)** in the 802.1x EAP Type drop-down box.
- If you want to enable PEAP (EAP-GTC) with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **PEAP (EAP-GTC)** in the WPA/WPA2/CCKM EAP Type drop-down box.

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

Note Refer to the "WPA and WPA2" section on page 5-19 for additional information.

Step 2 Click **Configure**. The Configure PEAP (EAP-GTC) window appears (see Figure 5-18).

Figure 5-18 Configure PEAP (EAP-GTC) Window



Step 3 Check the **Use Machine Information For Domain Logon** check box if you want the client to attempt to log into a domain using machine authentication with user credentials rather than user authentication. Doing so enables the computer to connect to the network prior to user logon. The default setting is checked.

Note If you do not check the Use Machine Information For Domain Logon check box, machine authentication is not performed. Authentication does not occur until the user logs on.

Step 4 Check the **Validate Server Identity** check box to force the system to validate the identity of the server as an added level of security. If you uncheck this box, only user credentials will be validated.

Step 5 Choose the certificate authority from which the server certificate was downloaded in the Trusted Root Certification Authorities drop-down box, or, if applicable, choose **<Any>**.

Step 6 Select either **Token** or **Static Password**, depending on the user's database.

Note If you choose Token, the user must use a hardware token device or the Secure Computing SofToken program (version 2.1 or later) to obtain the one-time password and enter the password when prompted during the authentication process. Secure Computing PremierAccess version 3.1.1 or later is the only supported token server.

Step 7 If you chose Token in Step 6, perform one of the following:

- Check the **Always Resume the Secure Session** check box at the top of the window if you want the PEAP (EAP-GTC) supplicant to always attempt to resume the previous session without prompting the user to re-enter his or her credentials whenever the client adapter becomes disassociated. The session resumes after the client temporarily loses connection to the access point (such as by roaming in and out of coverage) or wakes up from suspend or hibernate mode. This is the default setting.
- Uncheck the **Always Resume the Secure Session** check box if you want the user to be prompted to re-enter his or her PEAP (EAP-GTC) username and password whenever the client adapter temporarily loses association by roaming out of coverage or wakes up from suspend or hibernate mode.

Note Checking this check box gives the user the convenience of not having to re-enter his or her username and password when the client adapter experiences momentary losses of association. However, if the user leaves the device unattended during the period of time when the PEAP (EAP-GTC) session can be resumed without re-entering user credentials, be aware that someone can resume the user's PEAP (EAP-GTC) session and access the network.

Note The Always Resume the Secure Session check box is disabled if you chose Static Password in Step 6.

Step 8 Perform one of the following to specify the username that will be used for inner PEAP tunnel authentication:

- If you want the user's Windows username to also serve as the PEAP username, check the **Use Windows User Name** check box. This option gives the user only one username to remember.

  Note If you chose the Static Password option in Step 6, the check box reads *Use Windows User Name and Password*.

- If you want the user to enter a separate PEAP username (which is registered with the RADIUS server) in addition to his or her regular Windows username in order to start the PEAP authentication process, enter the PEAP username in the User Name field.

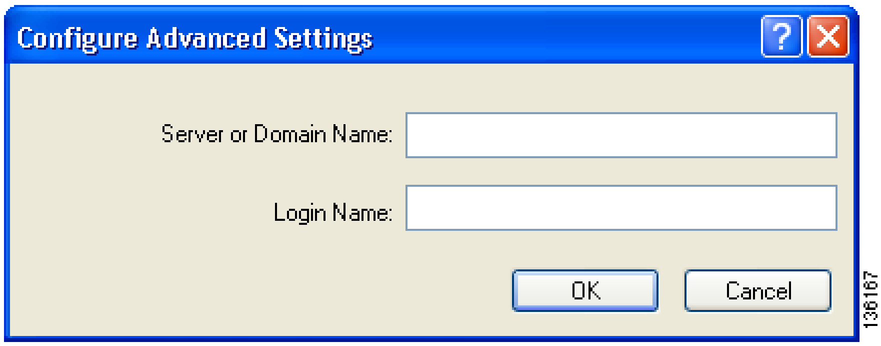
  Note Your Windows username is filled in automatically. Simply delete your Windows username and enter a separate PEAP username.

Step 9 If you entered a PEAP username in the previous step and chose the Static Password option in Step 6, enter your PEAP authentication password (which is registered with the RADIUS server) in both the Password and Confirm Password fields.

Step 10 If the Use Windows User Name and Password check box is unchecked and you want to implement added security by further refining the network certificate that will be accepted and controlling the string used to set up the outer PEAP tunnel, follow these steps:

a. Click **Advanced**. The Configure Advanced Settings window appears (see Figure 5-19).

Figure 5-19 Configure Advanced Settings Window



b. Leave the Specific Server or Domain field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the selected certificate authority or enter the domain name of the server from which the client will accept a certificate.

c. If the Login Name field is not filled in automatically, enter the username with nothing after it (for example, jsmith).

d. Click **OK** to save your settings.

Step 11 Click **OK** to save your settings and return to the Profile Editor (Security) window.

Step 12 Perform one of the following to set the Allow Association to Mixed Cells parameter, which indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) has WEP set to Optional. Otherwise, the client is unable to establish a connection with the access point.
- Uncheck the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) does not have WEP set to Optional. This is the default setting.

Note This parameter is available only if the 802.1x security option is selected.

Note For security reasons, Cisco recommends that WEP-enabled and WEP-disabled clients not be allowed in the same cell because broadcast packets are sent unencrypted, even to clients running WEP. However, you can enable VLANs on the access point to separate WEP-enabled and WEP-disabled clients.

Step 13 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the user's computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000 or computers running Windows XP without Service Pack 2 or later. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" in Chapter 3 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for information on obtaining and installing the hot fix.

Step 14 Click **OK** to save your settings and return to the Profile Management window.

Enabling PEAP (EAP-MSCHAP V2)

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

Step 1 Perform one of the following:

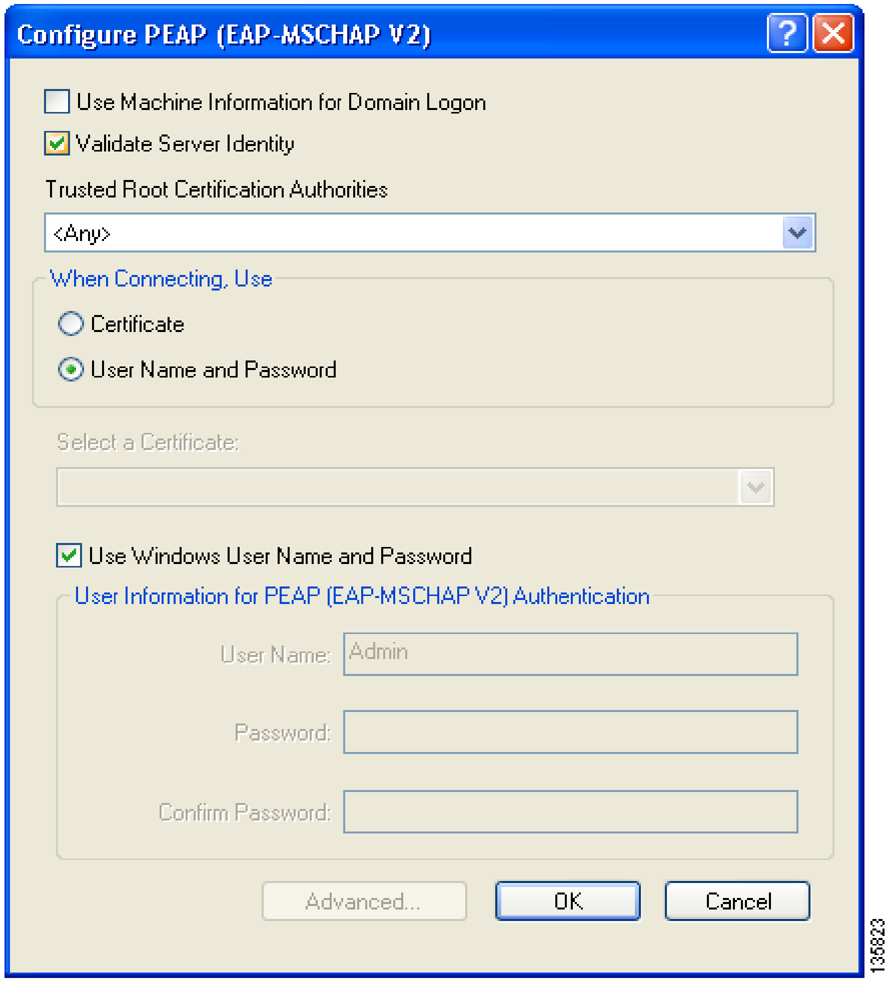
- If you want to enable PEAP (EAP-MSCHAP V2) without WPA or WPA2, choose **802.1x** under Set Security Options and **PEAP (EAP-MSCHAP V2)** in the 802.1x EAP Type drop-down box.
- If you want to enable PEAP (EAP-MSCHAP V2) with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **PEAP (EAP-MSCHAP V2)** in the WPA/WPA2/CCKM EAP Type drop-down box.

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

Note Refer to the "WPA and WPA2" section on page 5-19 for additional information.

Step 2 Click **Configure**. The Configure PEAP (EAP-MSCHAP V2) window appears (see Figure 5-20).

Figure 5-20 Configure PEAP (EAP-MSCHAP V2) Window



Step 3 Check the **Use Machine Information For Domain Logon** check box if you want the client to attempt to log into a domain using machine authentication with user credentials rather than user authentication. Doing so enables the computer to connect to the network prior to user logon. The default setting is checked.

> **Note** If you do not check the Use Machine Information For Domain Logon check box, machine authentication is not performed. Authentication does not occur until the user logs on.

Step 4 Check the **Validate Server Identity** check box to force the system to validate the identity of the server as an added level of security. If you uncheck this box, only user credentials will be validated.

Step 5 Choose the certificate authority from which the server certificate was downloaded in the Trusted Root Certification Authorities drop-down box, or, if applicable, choose **<Any>**.

Step 6 Perform one of the following to specify how you want the user to establish a network connection:

- If you want the user to connect using a username and password, choose **User Name and Password** and go to Step 7.
- If you want the user to connect using a user certificate installed on the user's computer, choose **Certificate**, select a certificate from the drop-down box, and go to Step 8.

Step 7 Perform one of the following to specify the username and password that will be used for inner PEAP tunnel authentication:

- If you want the user's Windows username and password to also serve as the PEAP username and password, check the **Use Windows User Name and Password** check box.
- If you want to use a distinct username and password (which are registered with the RADIUS server) to start the PEAP authentication process, follow these steps:

  a. Enter the PEAP username and password in the corresponding fields.

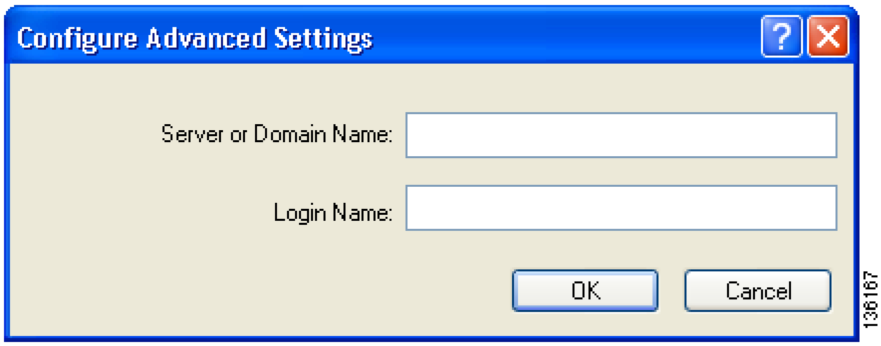
  > **Note** Your Windows username is filled in automatically. Simply delete your Windows username and enter the separate PEAP username.

  b. Re-enter the password in the Confirm Password field.

Step 8 If you selected a certificate or entered a distinct username and password and you want to implement added security by further refining the network certificate that will be accepted and controlling the string used to set up the outer PEAP tunnel, follow these steps:

a. Click **Advanced**. The Configure Advanced Settings window appears (see Figure 5-19).

Figure 5-21 Configure Advanced Settings Window



b. Leave the Specific Server or Domain field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the selected certificate authority or enter the domain name of the server from which the client will accept a certificate.

c. If the Login Name field is not filled in automatically, enter the username with nothing after it (for example, jsmith).

Note Some RADIUS servers require that the same name be entered for both the inner and outer PEAP tunnels. That is, the same name may need to be entered in both the Login Name field and the User Name field on the Configure PEAP (EAP-MSCHAP V2) window.

d. Click **OK** to save your settings.

Step 9 Click **OK** to save your settings and return to the Profile Editor (Security) window.

Step 10 Perform one of the following to set the Allow Association to Mixed Cells parameter, which indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) has WEP set to Optional. Otherwise, the client is unable to establish a connection with the access point.
- Uncheck the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) does not have WEP set to Optional. This is the default setting.

Note This parameter is available only if the 802.1x security option is selected.

Note For security reasons, Cisco recommends that WEP-enabled and WEP-disabled clients not be allowed in the same cell because broadcast packets are sent unencrypted, even to clients running WEP. However, you can enable VLANs on the access point to separate WEP-enabled and WEP-disabled clients.

Step 11 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the user's computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000 or computers running Windows XP without Service Pack 2 or later. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section in Chapter 3 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for information on obtaining and installing the hot fix.

Step 12 Click **OK** to save your settings and return to the Profile Management window.

Enabling PEAP (EAP-MSCHAP V2) Machine Authentication with Machine Credentials

The Host Based EAP option in the 802.1x EAP Type drop-down box on the Profile Editor (Security) window enables client adapters that are configured through ADU to attempt to log into a domain using PEAP (EAP-MSCHAP V2) machine authentication with machine credentials. Doing so enables the user's computer to connect to the network prior to user logon. Follow these steps to enable this authentication type.

Note This procedure enables the client adapter to use PEAP (EAP-MSCHAP V2) machine authentication with *machine* credentials. If you want to enable PEAP (EAP-MSCHAP V2) machine authentication with *user* credentials, follow the instructions in the "Enabling PEAP (EAP-MSCHAP V2)" section on page 5-52.

Note Because this feature requires the Microsoft Wireless Configuration Manager to start and stop as the user switches between host-based EAP and non-host-based EAP profiles, it works only for users with administrator or power-user privileges. An error message appears if you attempt to switch to or from a host-based EAP profile and you do not have the proper permissions.

Note To use this feature on a computer running Windows 2000, the computer must have the Microsoft 802.1X supplicant installed.

Note Host Based EAP is not included in the list of WPA/WPA2/CCKM EAP Type options on the Profile Editor (Security) window because this feature is not supported for use with WPA or WPA2.

Step 1 Choose **802.1x** under Set Security Options and **Host Based EAP** in the 802.1x EAP Type drop-down box.

Step 2 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the user's computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000 or computers running Windows XP without Service Pack 2 or later. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section in Chapter 3 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for information on obtaining and installing the hot fix.

Step 3 Click **OK** to save your settings. The remaining steps must be completed on the user's computer after the Install Wizard has been used to install the client adapter software and this profile from the ACAU configuration file.

Step 4 Activate this profile on the Profile Management window. The Microsoft Wireless Configuration Manager starts.

Step 5 Click **Start** > **Settings** > **Control Panel** > **Network and Dial-up Connections** or **Network Connections**.

Step 6 Right-click the wireless connection.

Step 7 Click **Properties**. The Connection Properties window appears.

Step 8 Perform one of the following:

- On Windows 2000, click the **Authentication** tab.
- On Windows XP, choose the **Wireless Networks** tab, make sure that the **Use Windows to configure my wireless network settings** check box is checked, click the SSID of the access point to which the client adapter is to associate from the list of available networks, click **Configure**, and choose the **Authentication** tab.

Step 9 For EAP type, choose **Protected EAP (PEAP)**.

Step 10 Configure any applicable settings on the Protected EAP Properties window and subwindows.

Step 11 After the configuration is finished, PEAP authentication should begin. Depending on the configuration settings selected, the user may be prompted for a PEAP username, password, and domain name. ADU may need to be minimized to access the pop-up window that prompts for user credentials.

Note Multiple host-based EAP profiles can exist in ADU, but the Microsoft Wireless Configuration Manager maintains only one configuration. To use different PEAP property settings for different host-based EAP profiles, the user must repeat the previous steps beginning with Step 4 every time he or she switches to a different host-based EAP profile.

Note When a host-based EAP profile is activated, the Microsoft Wireless Configuration Manager takes control of the client adapter's authentication attempt. However, when a non-host-based EAP profile is activated, ADU assumes this control.

Note If problems occur while using a host-based EAP profile, make sure that 802.1X authentication is disabled for any other network connection.