Managing Profiles

This chapter explains how to use the ACAU to create and save profiles used by the Install Wizard when a user installs the client adapter drivers and ADU.

The following topics are covered in this chapter:

Profile Management Tab

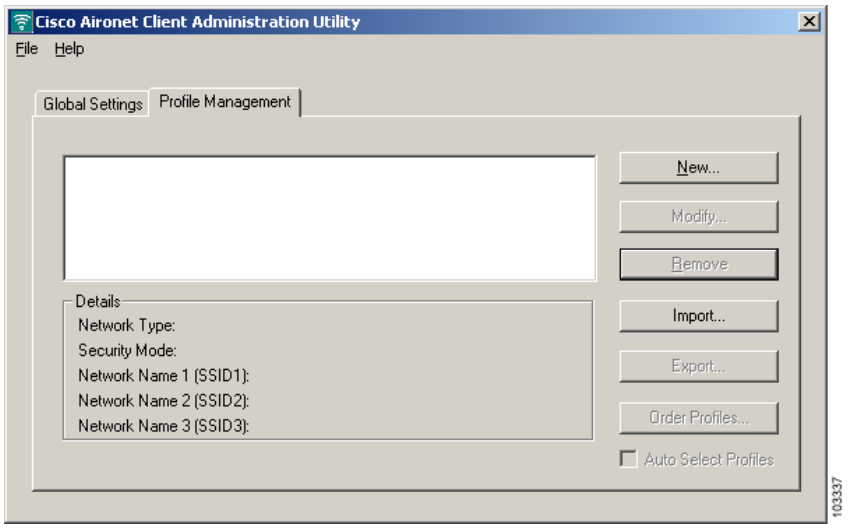
ACAU's profile management tab enables you to create and manage up to 16 *profiles* for the client adapter. These profiles enable you to configure user client adapters in different locations, each of which requires different configuration settings. For example, you may want to set up profiles for users who work in different environments such as at the office, at home, and in public areas such as airports. Once the profiles are created, you save them to the *ciscoadminconfig.dat* file where they are used when the drivers and ADU are installed.

Opening Profile Manager

To open ACAU's profile manager, double-click the **Aironet Client Administrator Utility (ACAU)** icon on your desktop to open ACAU. Then click the **Profile Management** tab. The Cisco Aironet Client Administration Utility (Profile Management) window appears

Figure 4-1 shows the beginning Profile Management window.

Figure 4-1 Profile Management Window



The Profile Management window enables you to perform the following profile management tasks:

- Create a new profile
- Modify an existing profile
- Remove a profile
- Import a profile
- Export a profile
- Order profiles
- Auto select profiles

Selecting the **New** or **Modify** command button enables you to open the Profile Management windows (listed below). These windows contain 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 4-1 enables you to quickly locate instructions for setting each Profile Management window's parameters.

Table 4-1 Locating Configuration Instructions

Parameter Category	Page Number
General	page 4-3
Advanced	page 4-5
Security	page 4-13

Setting General Parameters

The Profile Management (General) window (see Figure 4-2) 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 ACAU Profile Management window.

Figure 4-2 Profile Management (General) Window

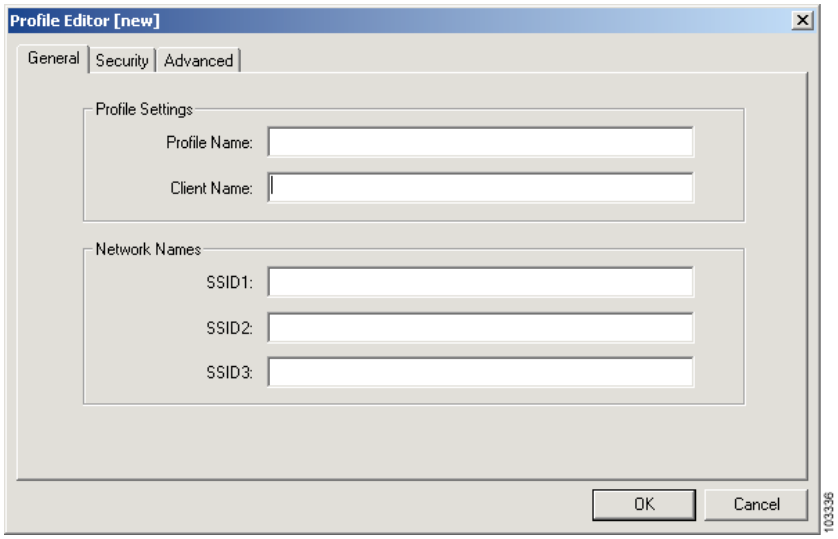


Table 4-2 lists and describes the client adapter's general parameters. Follow the instructions in the table to change any parameter.

Table 4-2 Profile Management General Parameters

Parameter	Description
Profile Name	The name assigned to the configuration profile. **Range:** Up to 32 ASCII characters
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 filled in automatically, but can be changed. **Range:** Up to 16 ASCII characters **Default:** The name of your computer **Note** Each computer on the network should have a unique client name.
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** In ad hoc mode, the SSID 1 field must contain a value. If it is blank, you are prompted to enter a network name or reset the network type to *infrastructure*.
SSID2 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 this field is blank or specifies more than one SSID, it cannot be included in auto profile selection. **Note** This field is unavailable for any profiles that are included in auto profile selection or configured for use in an ad hoc network. If these fields are populated, a warning appears specifying that they will be removed when the ad hoc mode is selected.

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

Setting Advanced Parameters

The Profile Management (Advanced) window (see Figure 4-3) enables you to set parameters that control how the client adapter operates within an infrastructure or ad hoc network. To open this window, select the **Advanced** tab from the Profile Management window.

Figure 4-3 Profile Management (Advanced) Window

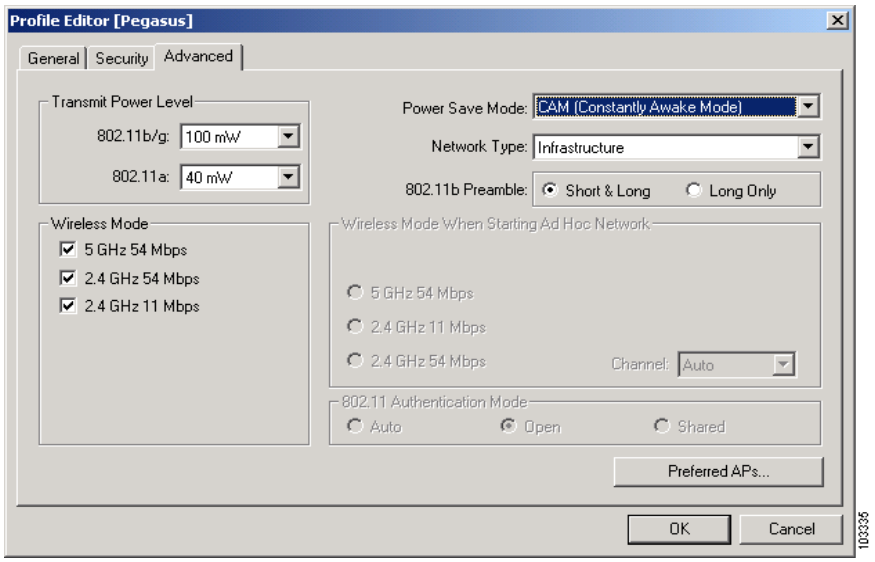


Table 4-3 lists and describes the client adapter's advanced parameters. Follow the instructions in the table to change any parameters.

Table 4-3 Profile Management Advanced Parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Transmit Power Level</td><td>Defines the power level at which your client adapter transmits. Although the adapter supports up to 100 mW, the maximum 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, 30, 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 4-3 Profile Management Advanced Parameters (continued)

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td>Power Save Mode</td><td colspan="2">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)</td></tr>
<tr><td></td><td>Power Save Mode</td><td>Description</td></tr>
<tr><td></td><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.
This mode is the only mode available in an ad hoc network.</td></tr>
<tr><td></td><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.
This mode is not available in an ad hoc network.</td></tr>
<tr><td></td><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).
This mode is not available in an ad hoc network.</td></tr>
</table>

Table 4-3 Profile Management 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 your 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 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 is set to 5 GHz 54 Mbps only.</td></tr>
</table>

Table 4-3 Profile Management Advanced Parameters (continued)

Parameter	Description
Wireless Mode	Specifies the frequency and rate at which the client adapter transmits or receives packets to or from access points. **Options:**5 GHz 54 Mbps, 2.4 GHz 11 Mbps, and 2.4 GHz 54 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: 2.4 GHz 54 Mbps, 5 GHz 54 Mbps, 2.4 GHz 11 Mbps. **Note** If you select 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 select 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** 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 transmits or receives packets to or from other clients (in ad hoc mode). **Options:**5 GHz 54 Mbps or 2.4 GHz 54/11 Mbps **Default:** 5 GHz 54 Mbps **Note** The client scans the band(s) specified by the Wireless Mode parameter before **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.

Table 4-3 Profile Management 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 adapters, 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 54/11 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 A for a list of channel identifiers, channel center frequencies, and regulatory domains for each channel.

Table 4-3 Profile Management 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 your 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. If the user’s adapter is not using WEP, it will not attempt to communicate to an access point that is using WEP and vice versa.</td></tr>
<tr><td>Shared</td><td>Enables the client adapter to 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 user’s 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.

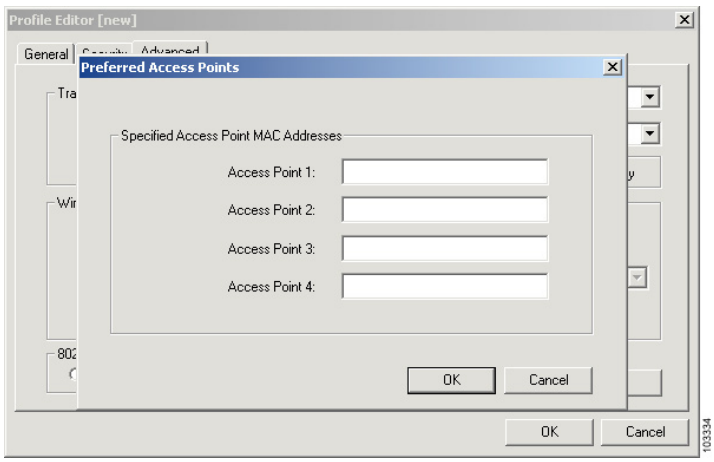
Note If this profile is configured for use in an adhoc network or is not configured to use static WEP, this parameter is unavailable, and Open authentication is used.</td></tr>
</table>

Table 4-3 Profile Management Advanced Parameters (continued)

Parameter	Description
Channel	Specifies the channel that the client adapter will use for communications in a 2.4-GHz ad hoc network. The available channels conform to the IEEE 802.11 Standard for your regulatory domain. **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** 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 adapters, this parameter specifies the channel with which the adapter will start its cell. **Note** This parameter is available only when 2.4 GHz 54/11 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 A for a list of channel identifiers, channel center frequencies, and regulatory domains for each channel.

If your client adapter is being 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 4-4).

Figure 4-4 Preferred Access Points Window



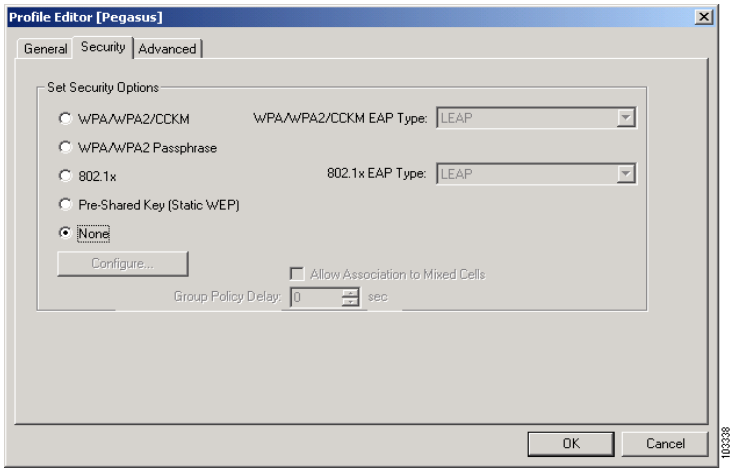
Leave the Access Point 1-4 fields blank or enter the MAC addresses of up to four preferred access points to which the client adapter can associate; then click **OK**. (The MAC address should consist of 12 hexadecimal characters.) If the specified access points are not found or the client adapter roams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

Setting Security Parameters

The Profile Management (Security) window (see Figure 4-5) 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 access this window, select the **Security** tab from any Profile Management window.

Figure 4-5 Profile Management (Security) Window



This window is different from the other Profile Management windows in that it presents several 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 using them.

However, before you determine the appropriate security settings for profile, you must decide how to set the **Allow Association to Mixed Cells** parameter, which appears at the bottom of the Profile Management (Security) window and is not associated to any of the security features. See the "Setting the Allow Association to Mixed Cells Parameter" section below.

Setting the Allow Association to Mixed Cells Parameter

The Allow Association to Mixed Cells parameter indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations. Follow the steps below to set this parameter.

Note This parameter is unavailable if the WPA or WPA Passphrase security option is selected.

Step 1 Perform one of the following:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate has WEP set to Optional (or a VLAN to which the client will be assigned) and WEP is enabled on the client adapter. 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 does not have WEP set to Optional on a specific access point VLAN. 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.

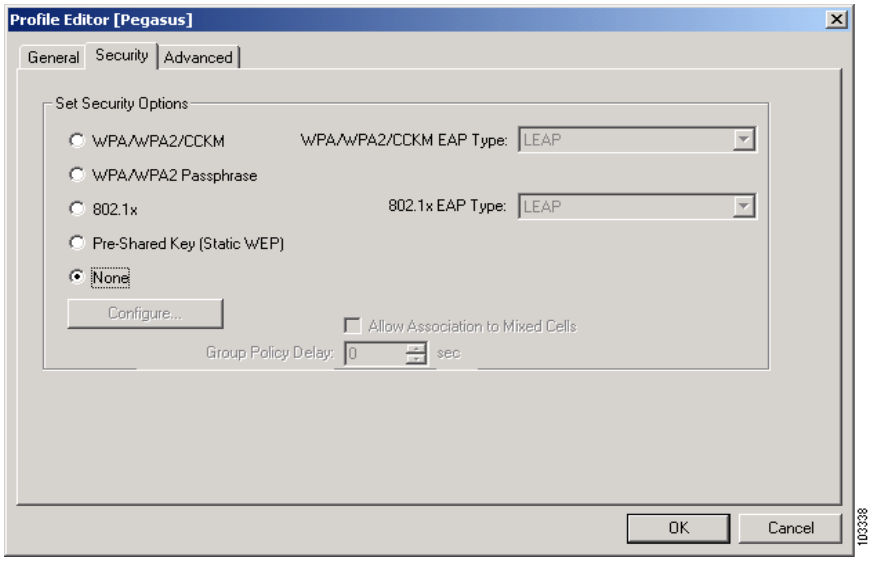
Step 2 Perform one of the following:

- If you do not want to change any other parameters on the Profile Management (Security) window, click **OK** to return to the ACAU (Profile Management) window.
- If you want to change some of the other parameters on the Profile Management (Security) window, go to the next section.

Setting Security Parameters

The Profile Management (Security) window (see Figure 4-5) 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, select the **Security** tab from any Profile Management window.

Figure 4-6 Profile Management (Security) Window



This window is different from the other Profile Management 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 using them.

However, before you determine the appropriate security settings for your configuration file, you must decide how to set the **Allow Association to Mixed Cells** parameter, which appears at the bottom of the Profile Management (Security) window and is not associated to any of the security features. See the "Setting the Allow Association to Mixed Cells Parameter" section below.

Setting the Allow Association to Mixed Cells Parameter

The Allow Association to Mixed Cells parameter indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations. Follow the steps below to set this parameter.

Note This parameter is unavailable if the WPA or WPA Passphrase security option is selected.

Step 1 Perform one of the following:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate has WEP set to Optional and static WEP is enabled on the client adapter. 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 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.

Step 2 Perform one of the following:

- If you do not want to change any other parameters on the Profile Management (Security) window, click **OK** to save your changes and return to the Cisco Aironet Client Administration Utility (Profile Management) window.
- If you want to change some of the other parameters on the Profile Management (Security) window, go to the next section.

Overview of Security Features

You can protect user 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 client 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 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 4-19 for information on three security features that can make WEP keys even more secure.

Static WEP Keys

Each device (or profile) within the user's 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 Define Pre-Shared Keys 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 4-22 for instructions.

EAP (with Dynamic WEP Keys)

The standard for wireless LAN security, as defined by the Institute of Electrical and Electronics Engineers (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.

Four 802.1X authentication types can be selected 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 adapter is configured to use saved LEAP credentials.

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

- **EAP-TLS**—This authentication type uses a dynamic session-based WEP key, which is 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 version 3.0 or later and Cisco Access Registrar version 1.8 or later.

  Note EAP-TLS requires the use of a certificate. Refer to Microsoft's documentation for information on downloading and installing the certificate.

- **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, which is 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 entering a hardware or software token password to start the EAP authentication process and gain access to the network. If the 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 version 3.1 or later.

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

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

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

Refer to the "Enabling LEAP" section on page 4-24 for instructions on enabling LEAP or to the "Enabling EAP-TLS or PEAP" section on page 4-26 for instructions on enabling EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2).

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

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) is a standards-based, interoperable security enhancement that provides data protection and access control for existing and future wireless LAN systems. It is derived from and is forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages Temporal Key Integrity Protocol (TKIP) and Michael message integrity check (MIC) for data protection and 802.1X for authenticated key management.

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

Refer to the "Enabling WPA Passphrase" section on page 4-23 for instructions on using a WPA passphrase, the "Enabling LEAP" section on page 4-24 for instructions on enabling LEAP with WPA, or the "Enabling EAP-TLS or PEAP" section on page 4-26 for instructions on enabling EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2) with WPA.

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

Fast Roaming (CCKM)

Some applications that run on a client device may require fast roaming between access points. Voice applications, for example, require fast roaming to prevent delays and gaps in conversation. Fast roaming is enabled automatically for LEAP-enabled CB21AG and PI21AG clients using WPA but must be enabled on the access point.

During normal operation, LEAP-enabled clients mutually authenticate with a new access point by performing a complete LEAP authentication, including communication with the main RADIUS server. However, when you configure your wireless LAN for fast roaming, LEAP-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 client devices to roam from one access point to another typically in under 150 milliseconds (ms). Fast 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 The Microsoft Wireless Configuration Manager and the Microsoft 802.1X supplicant, if installed on the user's computer, must be disabled in order for fast roaming to operate correctly. Refer to Chapter 10 of the *Cisco Aironet 802.11a/b/g/ Wireless Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* if you need additional information.

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

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 greater (access points running VxWorks)
- Cisco IOS Release 12.2(4)JA or greater (1100 series access points)
- Cisco IOS Release 12.2(8)JA or greater (1200 series access points)
- Cisco IOS Release 12.2(13)JA or greater (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 need not 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 versions.

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 the user's wireless network's WEP keys. These features need not 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.

The Advanced Status window indicates if MIC is being used, and the Advanced Statistics window provides MIC statistics.

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 whenever WPA is enabled, and it is disabled whenever WPA is disabled.

Broadcast Key Rotation

EAP authentication provides dynamic unicast WEP keys for client devices but uses static broadcast, or multicast, keys. 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 access point to which it associates must be set appropriately. Table 4-4 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 4-4 Client and Access Point Security Settings

Security Feature	Client Setting	Access Point Setting
Static WEP with open authentication	Select 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	Select 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
WPA Passphrase (or WPA Pre-Shared Key)	Select WPA Passphrase and enter the passphrase	Select 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	Select 802.1x and LEAP; then set LEAP settings	Set up and enable WEP and enable Network-EAP for the SSID

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

Security Feature	Client Setting	Access Point Setting
LEAP authentication with WPA	Select WPA and LEAP; then set LEAP settings	Select a cipher suite that includes TKIP and enable Network-EAP and WPA for the SSID **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.
EAP-TLS authentication without WPA	Select 802.1x and EAP-TLS; then set EAP-TLS settings	Set up and enable WEP and enable Open Authentication for the SSID and specify the use of EAP
EAP-TLS authentication with WPA	Select WPA and EAP-TLS; then set EAP-TLS settings	Select a cipher suite that includes TKIP; set up and enable WEP; and enable WPA and Open Authentication for the SSID and specify the use of EAP **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.
PEAP authentication without WPA	Select 802.1x and PEAP (EAP-GTC) or PEAP (EAP-MSCHAP V2); then set PEAP settings	Set up and enable WEP and enable Open Authentication for the SSID and specify the use of EAP
PEAP authentication with WPA	Select WPA and PEAP (EAP-GTC) or PEAP (EAP-MSCHAP V2); then set PEAP settings	Select a cipher suite that includes TKIP; set up and enable WEP; and enable WPA and Open Authentication for the SSID and specify the use of EAP **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.
Fast roaming (CCKM)	Select 802.1x and LEAP; then set LEAP settings	Use firmware version 12.2(11)JA or later, select a cipher suite that is compatible with CCKM, and enable Network-EAP and CCKM for the SSID 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 4-19.

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

Security Feature	Client Setting	Access Point Setting
MIC	No settings required; automatically enabled	Set up and enable WEP with full encryption, set MIC to MMH or select 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 select Enable Per Packet Keying check box, and set Use Aironet Extensions to Yes
Broadcast key rotation	Enable LEAP, EAP-TLS, or PEAP	Set up and enable WEP and set Broadcast WEP Key Rotation Interval to any value other than zero (0)

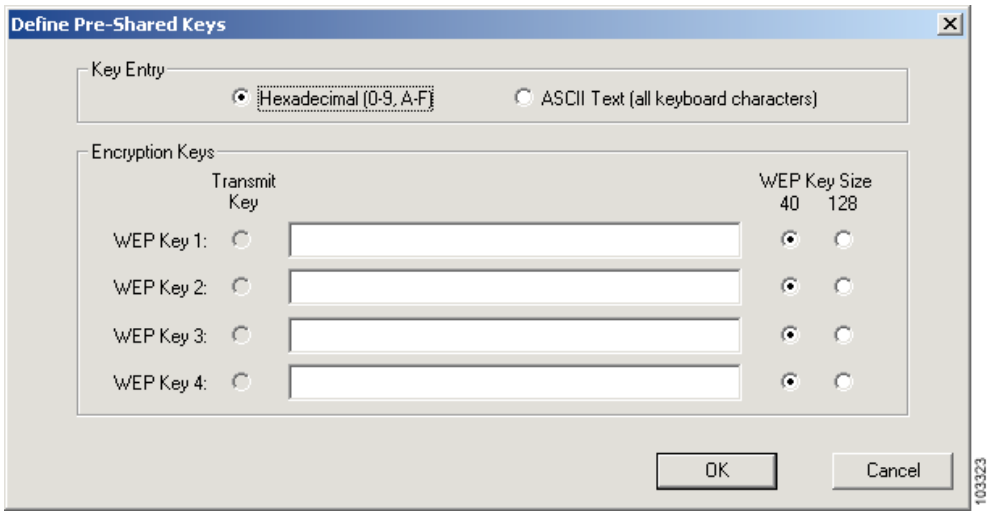
Enabling Static WEP

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

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

Step 2 Click **Configure**. The Define Pre-Shared Keys window appears (see Figure 4-7).

Figure 4-7 Define Pre-Shared Keys Window



Step 3 Select 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 select the Hexadecimal (0-9, A-F) option if you are planning to use your client adapter 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 Obtain the static WEP key from your system administrator and enter it 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 user's client adapter is used with Cisco Aironet 1200 Series Access Points.

- The user's client adapter's WEP key must match the WEP key used by the access point (in infrastructure mode) or clients (in ad hoc mode) with which you are planning to communicate.
- 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. If you modify a WEP key be sure to save the configuration file to make the modification effective.

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** twice to save your changes and return to the Cisco Aironet Administration Utility (Profile Management) window.

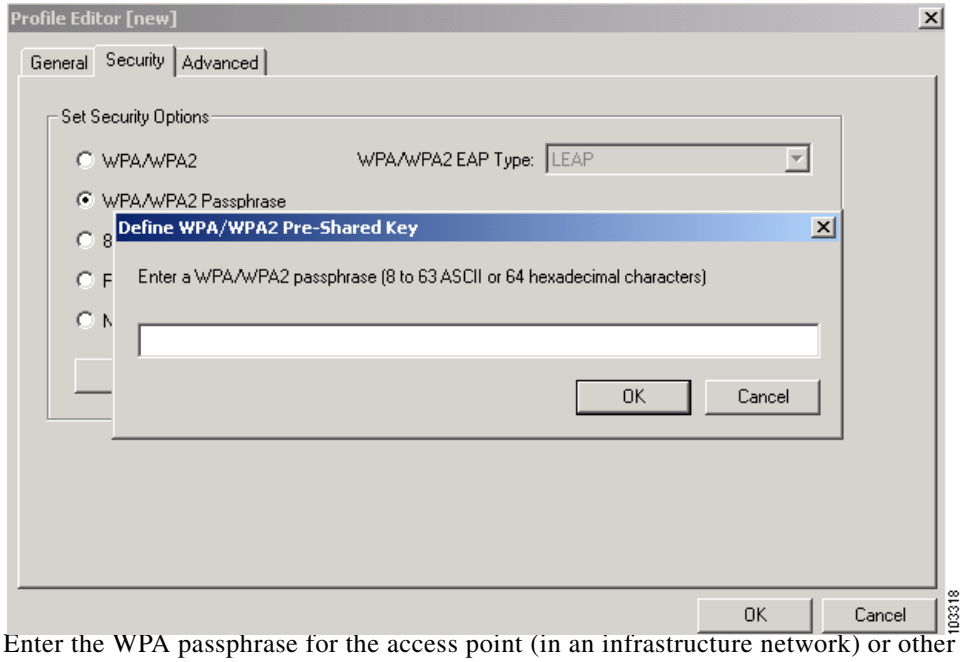
Enabling WPA Passphrase

Follow the steps below to enable WPA passphrase (also known as *WPA Pre-Shared Key*) for this profile.

Step 1 Select **WPA Passphrase** on the Profile Management (Security) window.

Step 2 Click **Configure**. The Define WPA Pre-Shared Key window appears (see Figure 4-8).

Figure 4-8 Define WPA Pre-Shared Key Window



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

- WPA passphrases must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.
- The client adapter's WPA passphrase must match the passphrase used by the access point with which you are planning to communicate.

Step 4 Click **OK** twice to save your changes and return to the Cisco Aironet Client Administration Utility (Profile Management) window.

Enabling LEAP

Before you can enable LEAP authentication, your network devices must meet the following requirements:

- Access points to which the user's client adapter may attempt to authenticate must use the following firmware versions or greater: 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 fast roaming, access points must use Cisco IOS Release 12.2(11)JA or later. To use the Reporting Access Points That Fail LEAP Authentication feature, access points must use the firmware versions listed on page 4-20.

- 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.

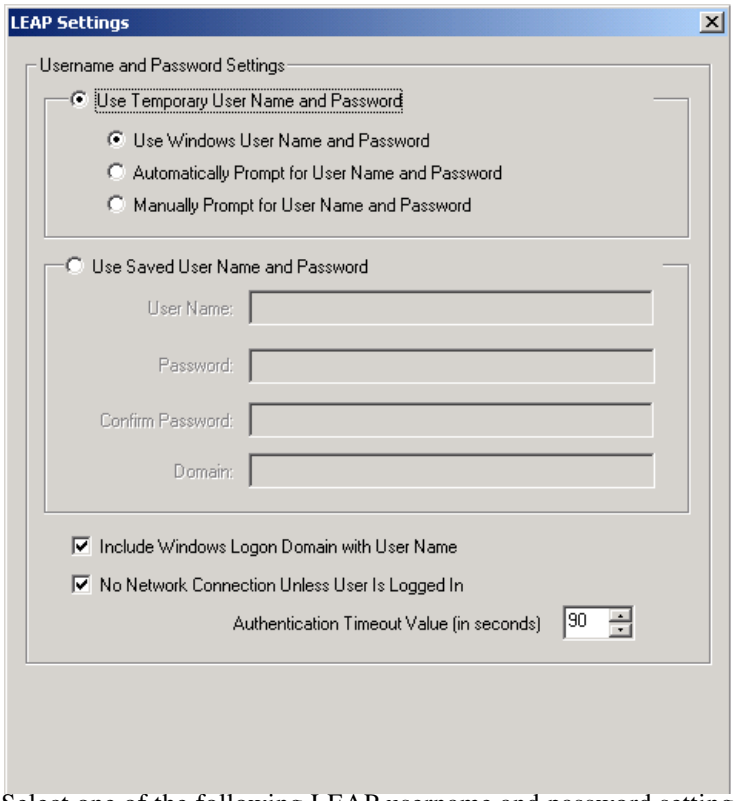
Step 1 Perform one of the following on the Profile Management (Security) window:

- If you want to enable LEAP without WPA, select **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, select **WPA** under Set Security Options and **LEAP** in the WPA EAP Type drop-down box.

Note Refer to the "Wi-Fi Protected Access (WPA)" section on page 4-18 for additional information on WPA.

Step 2 Click **Configure**. The LEAP Settings window appears (see Figure 4-9).

Figure 4-9 LEAP Settings Window



Step 3 Select 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.
- **Manually Prompt for LEAP User Name and Password**—Requires the user to manually invoke the LEAP authentication process as needed using the Manual LEAP Login option in the 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 selected Use Saved User Name and Password in Step 3, follow the steps below:
  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 the user will work in an environment with multiple domains and therefore 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.

Step 6 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 7 In the LEAP Authentication Timeout Value field, select the amount of time (in seconds) before a LEAP authentication is considered to be failed and an error message appears.

Range: 30 to 500 seconds

Default: 90 seconds

Step 8 Click **OK** twice to save your changes and return to the Cisco Aironet Client Administration Utility (Profile Management) window.

Step 9 Refer to "Enabling LEAP" section on page 4-24 for instructions on authenticating using LEAP.

Enabling EAP-TLS or PEAP

Before you can enable EAP-TLS or PEAP authentication, the user's network devices 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 your computer. EAP-TLS requires both a Certificate Authority (CA) certificate and a user certificate while PEAP requires only a CA certificate.
- Access points to which the user's client adapter may attempt to authenticate must use the following firmware versions or greater: 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 fast roaming, access points must use Cisco IOS Release 12.2(11)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 4-27
- Enabling PEAP (EAP-GTC), page 4-28
- Enabling PEAP (EAP-MSCHAP V2), page 4-30

Enabling EAP-TLS

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

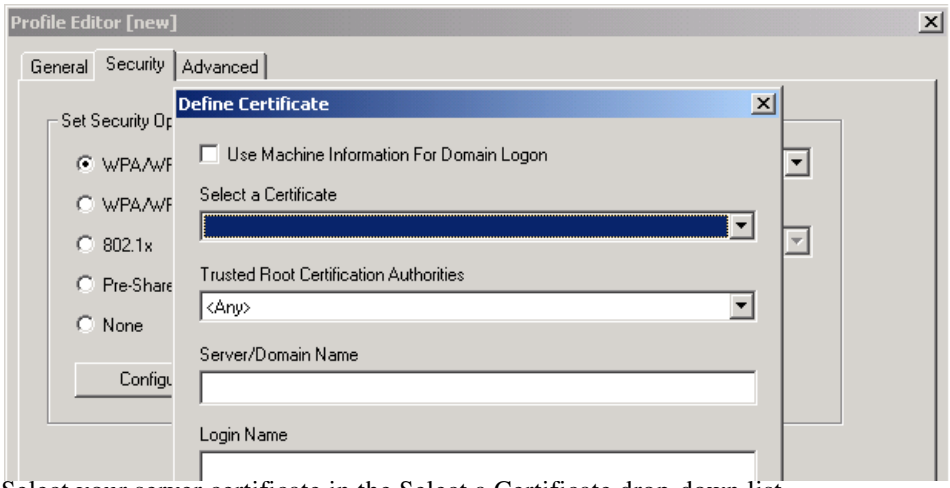
Step 1 Perform one of the following on the Profile Management (Security) window:

- If you want to enable EAP-TLS without WPA, select **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, select **WPA** under Set Security Options and **EAP-TLS** in the WPA EAP Type drop-down box.

Note Refer to the "Wi-Fi Protected Access (WPA)" section on page 4-18 for additional information on WPA.

Step 2 Click **Configure**. The Define Certificate window appears (see Figure 4-10).

Figure 4-10 Define Certificate Window



Step 3 Select your server certificate in the Select a Certificate drop-down list.

Step 4 Select the certificate authority from which the server certificate was downloaded in the Server Properties drop-down list.

Step 5 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 Server Properties drop-down list. This is the recommended option.

- Enter the fully qualified domain name of the specific server from which you want the client to accept a certificate. For example: cert.server.cisco.com.

Step 6 The Login Name is filled in automatically with the subject alternative name of the user certificate but can be changed.

Step 7 Click **OK** twice to save your changes and return to the Cisco Aironet Client Administration Utility (Profile Management) window.

Step 8 Refer to "Enabling EAP-TLS or PEAP" section on page 4-26 for instructions on authenticating using EAP-TLS.

Enabling PEAP (EAP-GTC)

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

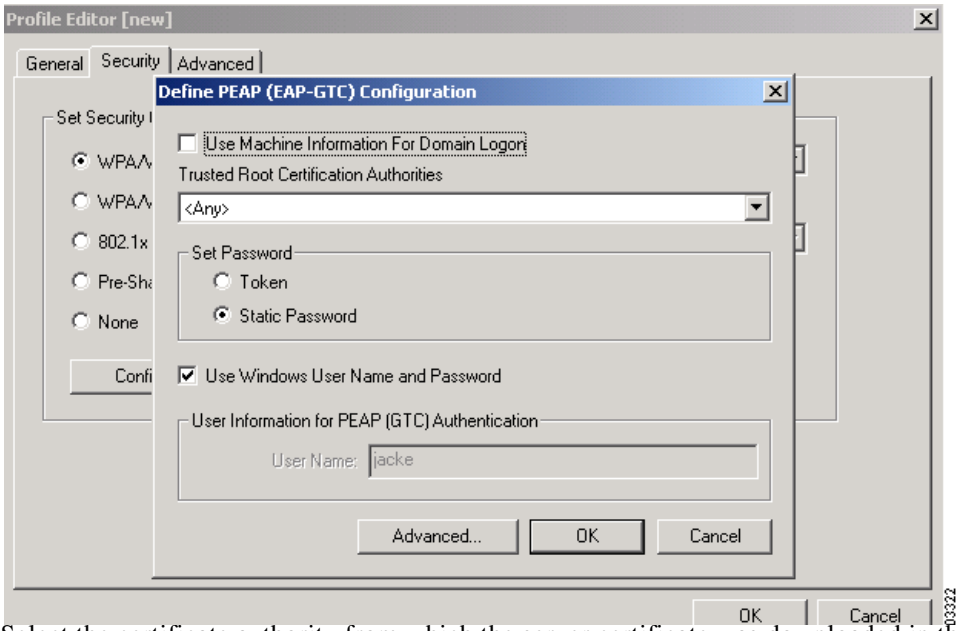
Step 1 Perform one of the following:

- If you want to enable PEAP (EAP-GTC) without WPA, select **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, select **WPA** under Set Security Options and **PEAP (EAP-GTC)** in the WPA EAP Type drop-down box.

Note Refer to the "Wi-Fi Protected Access (WPA)" section on page 4-18 for additional information on WPA.

Step 2 Click **Configure**. The Define PEAP (EAP-GTC) Configuration window appears (see Figure 4-11).

Figure 4-11 Define PEAP (EAP-GTC) Configuration Window



Step 3 Select the certificate authority from which the server certificate was downloaded in the Network Certificate Authority drop-down list.

Step 4 Perform one of the following to specify the username that is to be used for inner PEAP tunnel authentication:

- If you want your Windows username to also serve as your PEAP username, check the **Use Windows User Name** check box. This option gives you only one username to remember.
- If you want the user to enter a separate PEAP username (which is registered with the RADIUS server) in addition to your regular Windows username in order to start the PEAP authentication process, enter a PEAP username in the User Name field.

Note The user's Windows username is filled in automatically. Simply delete the Windows username and enter a separate PEAP username.

Step 5 Select either **Token** or **Static Password**, depending on the user' user database.

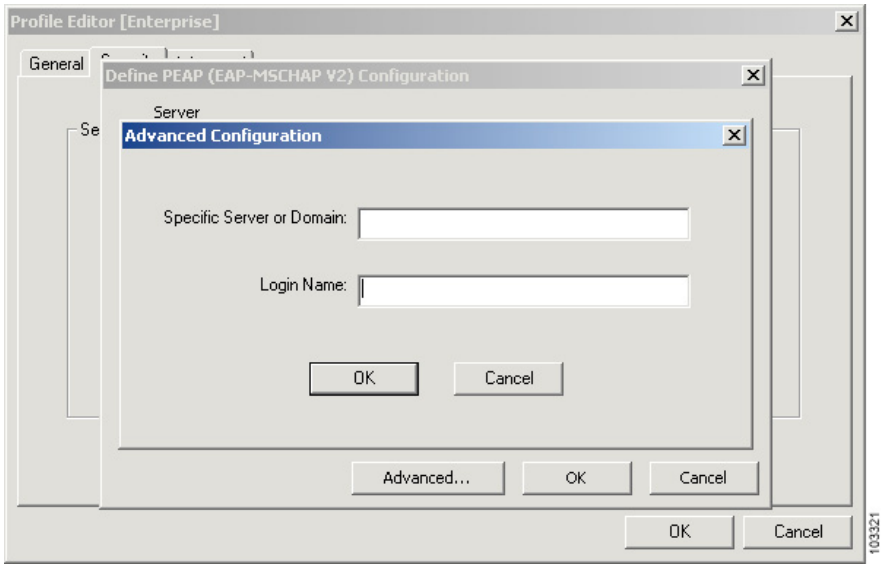
Note If you select Token, you must use a hardware token device or the Secure Computing SofToken program (version 1.3 or later) to obtain the one-time password and enter the password when prompted during the authentication process. Secure Computing PremierAccess version 3.1.1 or later is the only supported token server.

Step 6 Perform one of the following:

- If you are finished configuring PEAP (EAP-GTC) for this profile, go to Step 7.
- If 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 the steps below:

  a. Click **Advanced**. The Advanced Configuration window appears (see Figure 4-12).

Figure 4-12 Advanced Configuration Window



b. Perform one of the following:

- 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 certificate authority listed in the Network Certificate Authority drop-down list on the Define PEAP (EAP-GTC) Configuration window. This is the recommended option.
- Enter the fully qualified domain name of the specific server from which you want the client to accept a certificate. For example: cert.server.cisco.com.

c. The Login Name, which will used for outer PEAP tunnel authentication, is filled in automatically as follows: PEAP-*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is your computer's MAC address, but can be changed.

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

Step 7 Click **OK** twice to save your settings and return to the Cisco Aironet Administrator's Utility (Profile Management) window.

Step 8 Refer to "Enabling PEAP (EAP-GTC)" section on page 4-28 for instructions on authenticating using PEAP (EAP-GTC).

Enabling PEAP (EAP-MSCHAP V2)

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

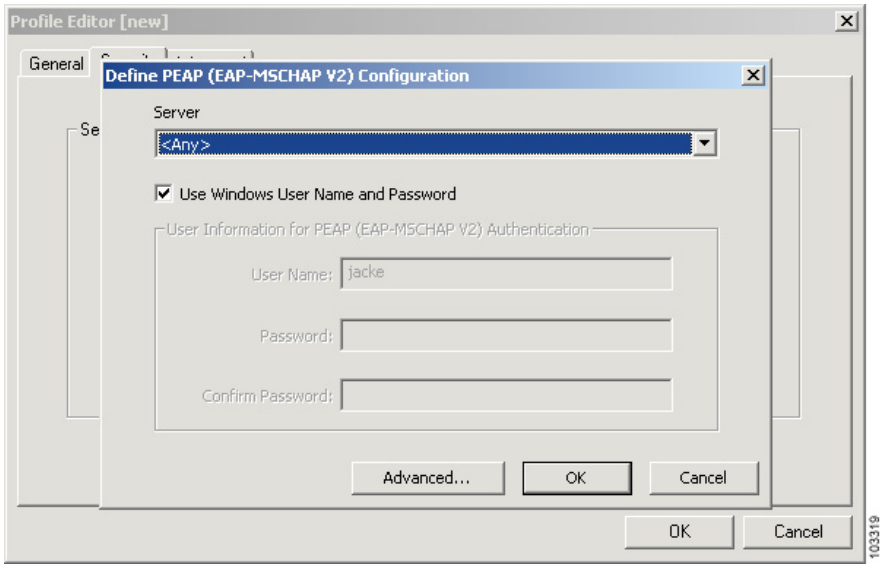
Step 1 Perform one of the following:

- If you want to enable PEAP (EAP-MSCHAP V2) without WPA, select **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, select **WPA** under Set Security Options and **PEAP (EAP-MSCHAP V2)** in the WPA EAP Type drop-down box.

Note Refer to the "Wi-Fi Protected Access (WPA)" section on page 4-18 for additional information on WPA.

Step 2 Click **Configure**. The Define PEAP (EAP-MSCHAP V2) Configuration window appears (see Figure 4-13).

Figure 4-13 Define PEAP (EAP-MSCHAP V2) Configuration Window



Step 3 Select the certificate authority from which the server certificate was downloaded in the Server drop-down list.

Step 4 Perform one of the following to specify the username and password that is to 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. This option gives the user only one set of credentials to remember. After the user logs in, the PEAP authentication process begins automatically.
- If you want the user to enter a separate PEAP username and password (which are registered with the RADIUS server) in addition to a regular Windows login in order to start the PEAP authentication process, follow the steps below:

  a. Enter the user's PEAP username and password in the corresponding fields.

  Note The user's Windows username is filled in automatically. Simply delete the user's Windows username and enter a separate PEAP username.

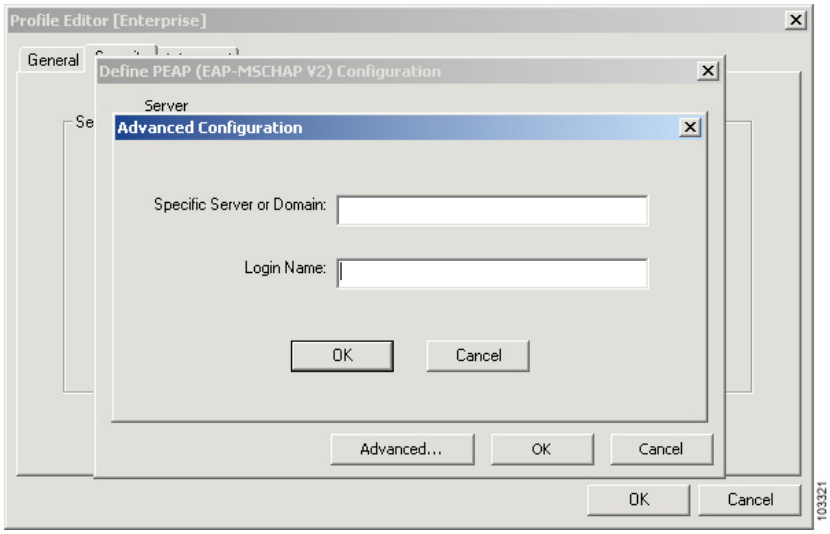
  b. Re-enter the user's password in the Confirm Password field.

Step 5 Perform one of the following:

- If you are finished configuring PEAP (EAP-MSCHAP V2) for this profile, go to Step 7.
- If 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 the steps below:

  a. Click **Advanced**. The Advanced Configuration window appears (see Figure 4-14).

Figure 4-14 Advanced Configuration Window



  b. Perform one of the following:

  - 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 certificate authority listed in the Server drop-down list on the Define PEAP (EAP-MSCHAP V2) Configuration window. This is the recommended option.
  - Enter the fully qualified domain name of the specific server from which you want the client to accept a certificate. For example: cert.server.cisco.com.

  c. The Login Name, which will used for outer PEAP tunnel authentication, is filled in automatically with the user's Windows username but can be changed.

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 Define PEAP (EAP-MSCHAP V2) Configuration window.

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

Step 6 Click **OK** twice to save your changes and return to the Cisco Aironet Client Administration Utility (Profile Management) window.

Step 7 Refer to "Enabling PEAP (EAP-MSCHAP V2)" section on page 4-30 for instructions on authenticating using PEAP (EAP-MSCHAP V2).

Including a Profile in Auto Profile Selection

After you have created profiles, you can choose to include them in the profile manager's auto profile selection feature. Then when auto profile selection is enabled, the client adapter automatically selects a profile from the list of profiles that were included in auto profile selection and uses it to establish a connection to the network.

Follow the steps below to include any of the profiles in auto profile selection and to establish the order in which the profiles are selected for use.

Step 1 Open ACAU. The utility opens and the Global Settings window appears.

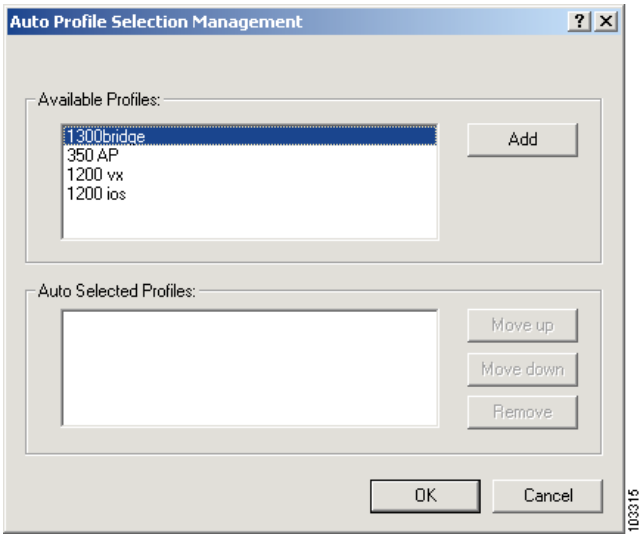
Step 2 On the File drop-down menu, click **Open** and browse to the folder where the *ciscoadminconfig.dat* file resides.

Step 3 Highlight the file and Click **Open**. The configuration file name appears on the ACAU window title bar.

Step 4 Click the **Profile Management** tab. The Profile Management window appears.

Step 5 Click **Order Profiles**. The Auto Profile Selection Management window appears (see Figure 4-15).

Figure 4-15 Auto Profile Selection Management Window



Step 6 All the profiles that you created are listed in the Available Profiles box. Highlight each one that you want to include in auto profile selection and click the **Add** button. The profiles appear in the Auto Selected Profiles box.

The following rules apply to auto profile selection:

- You must include at least two profiles in the Auto Selected Profiles box.
- The profiles must specify an SSID; otherwise, they do not appear in the Available Profiles box.
- Profiles cannot specify multiple SSIDs; otherwise, they do not appear in the Available Profiles box.

- Each profile that is included in auto profile selection must have a unique SSID. For example, if Profile A and Profile B both have "ABCD" as their SSID, only Profile A or Profile B (whichever one was created first) appears in the Available Profiles box and can be included in auto profile selection.

Note To remove a profile from auto profile selection, select the profile in the Auto Selected Profiles box and click **Remove**. The profile is removed from the Auto Selected Profiles box.

Step 7 The first profile in the Auto Selected Profiles box has the highest priority while the last profile has the lowest priority. To change the order (and priority) of your auto-selectable profiles, highlight the profile that you want to move and click **Move up** or **Move down** to move the profile up or down, respectively.

Step 8 Click **OK**.

When auto profile selection is enabled (see the section below for instructions), the client adapter scans for an available network. The profile with the highest priority and the same SSID as one of the found networks is the one that is used to connect to the network. If the connection fails, the client adapter tries the next highest priority profile that matches the SSID and so on.