CHAPTER 4

Enabling Security Features

This chapter explains how to use the client utilities to enable the client adapter's security features. The following topics are covered in this chapter:

Overview of Security Features

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

The WEP keys used to encrypt and decrypt transmitted data can be statically associated with your adapter or dynamically created as part of the LEAP authentication process. The information in the "Static WEP Keys" and "Dynamic WEP Keys with LEAP" sections below can help you to decide which type of WEP keys you want to use. Dynamic WEP keys with LEAP 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 contain more information than 40-bit keys and, therefore, offer a greater level of security.

Note Refer to the "Additional WEP Key Security Features" section on page 4-4 for information on three security features that can make your WEP keys even more secure.

Static WEP Keys

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

Static WEP keys are write-only and temporary; therefore, they cannot be read back from the client adapter and they are lost when power to the adapter is removed or the Windows CE device is rebooted. Although the keys are temporary, you do not need to re-enter them each time the client adapter is inserted or the Windows CE device is rebooted. This is because the keys are stored (in an encrypted format for security reasons) in the registry of the Windows CE 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.

Note Prior versions of the client software for Windows CE permitted WEP keys to be stored in either Flash memory (persistent) or volatile memory (temporary). If your client adapter has WEP keys that are stored in Flash memory from a prior release, Client Encryption Manager (CEM) version 2.10 or greater allows you to store WEP keys only in volatile memory, and these keys are used instead of those stored in Flash memory.

The CEM utility enables you to view the current WEP key settings for the client adapter and then to assign new WEP keys or overwrite existing WEP keys, and the Aironet Client Utility (ACU) allows you to enable or disable static WEP. Refer to the "Using Static WEP" section on page 4-6 for instructions.

Dynamic WEP Keys with LEAP

The new 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 Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network.

The 802.1X authentication type that is available on Windows CE devices is *EAP-Cisco Wireless*, or *LEAP*. Support for LEAP is provided not in the Windows CE operating system but in your client adapter's firmware and the Cisco software that supports it. RADIUS servers that support LEAP include Cisco Secure ACS version 2.6 and greater, Cisco Access Registrar version 1.7 and greater, and Funk Steel-Belted RADIUS version 3.0 and greater.

LEAP is enabled in ACU, and a LEAP username and password are entered in the Wireless Login Module (WLM). The username and password are used by the client adapter to perform mutual authentication with the RADIUS server through the access point. The LEAP username and password are stored in the client adapter's volatile memory; therefore, they are temporary and need to be re-entered whenever power is removed from the adapter, typically due to the client adapter being ejected or the system powering down.

Note Prior versions of the client software for Windows CE stored the LEAP username and password in the client adapter's nonvolatile Flash memory, which was referred to as *device-level LEAP*. If a LEAP username and password are stored in your client adapter's Flash memory from a prior release, WLM version 2.10 or greater erases them before a new username and password are written to the adapter's volatile memory, thereby disabling device-level LEAP.

When you enable Network-EAP on your access point and LEAP on your client adapter, authentication to the network occurs in the following sequence:

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

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

2. Communicating through the access point, the client and RADIUS server complete a mutual authentication process, with the password being the shared secret for authentication. The password is never transmitted during the process.
3. If mutual 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 that travel between them.

Refer to the "Using LEAP" section on page 4-11 for instructions on enabling or disabling LEAP and entering the LEAP username and password.

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

Additional WEP Key Security Features

Client adapter firmware version 4.25.23 and greater and Windows CE driver version 2.2x and greater support three new security features designed to prevent sophisticated attacks on your wireless network's WEP keys. These features (MIC, TKIP, and broadcast key rotation) do not need to be enabled on the client adapter; they are supported automatically in the driver and firmware versions listed above. However, they must be enabled on the access point.

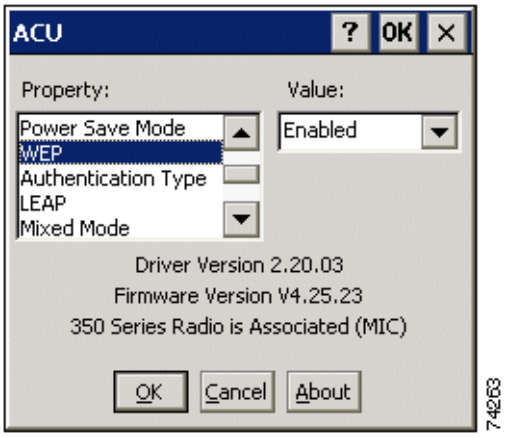
Note Access point firmware version 11.10T or greater is required to enable these security features. Refer to the *Cisco Aironet Access Point Software Configuration Guide* for instructions on enabling these security features on the access point.

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 ACU screen displays the word "(MIC)" next to the current status if MIC is supported by the client adapter's driver and firmware and is enabled on the access point. See Figure 4-1.

Figure 4-1 ACU Screen



Note If you enable MIC on the access point, your client adapter's driver must support MIC; otherwise, the client cannot associate.

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 If you enable TKIP on the access point, your client adapter's firmware must support TKIP; otherwise, the client cannot associate.

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. When you enable this feature, only wireless client devices using LEAP or EAP-TLS authentication can associate to the access point. Client devices using static WEP (with open, shared key, or EAP-MD5 authentication) cannot associate.

Synchronizing Security Features

In order to use any of the security features discussed in this section, both your client adapter and the access point to which it will associate must be set appropriately. Table 4-1 indicates the client and access point settings required for each security feature. This chapter provides specific instructions for enabling the security features on your client adapter. Refer to the *Cisco Aironet Access Point Software Configuration Guide* for instructions on enabling the features on the access point.

Table 4-1 Client and Access Point Security Settings

Security Feature	Client Setting	Access Point Setting
Static WEP with open authentication	Create a WEP key and enable Use Static WEP Keys and Open Authentication	Set up and enable WEP and enable Open Authentication
Static WEP with shared key authentication	Create a WEP key and enable Use Static WEP Keys and Shared Key Authentication	Set up and enable WEP and enable Shared Key Authentication
LEAP authentication	Enable LEAP	Set up and enable WEP and enable Network-EAP
MIC	Use driver version 2.2x or greater	Set up and enable WEP with full encryption, set MIC to MMH, and set Use Aironet Extensions to Yes
TKIP	Use firmware version 4.25.23 or greater	Set up and enable WEP, set TKIP to Cisco, and set Use Aironet Extensions to Yes
Broadcast key rotation	Use firmware version 4.25.23 or greater and enable LEAP	Set up and enable WEP and set Broadcast WEP Key Rotation Interval to any value other than zero (0)

Using Static WEP

This section provides instructions for entering new static WEP keys or overwriting existing static WEP keys. Follow the procedures in the order listed below:

1. Open CEM; see below
2. View the client adapter's current static WEP key settings; see page 4-7
3. Perform one of the following:
   - Enter a new static WEP key and enable WEP; see page 4-7
   - Overwrite an existing static WEP key; see page 4-9
4. Change the CEM password (optional); see page 4-10

Opening CEM

Follow the steps below to open CEM.

Step 1 Double-click the **Cisco CEM icon** or select **Start > Programs > Cisco > Client Encryption Manager**. The Enter Password screen appears (see Figure 4-2), provided a client adapter is installed in the Windows CE device and is running.

Figure 4-2 Enter Password Screen

Step 2 Enter the correct password in the Password field and click **OK**.

Passwords are case sensitive and can contain up to 256 alphanumeric characters. The default password is **Cisco** (uppercase *C* followed by lowercase *isco*). For security reasons, the characters you enter are displayed as asterisks.

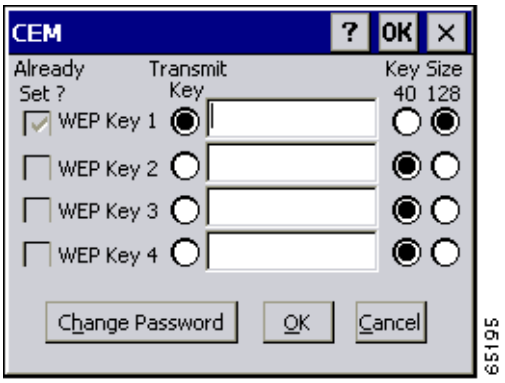
Note Refer to the "Changing the CEM Password" section on page 4-10 for instructions on changing the default password.

Viewing the Client Adapter's Current Static WEP Key Settings

Follow the steps below to view the client adapter's current static WEP key settings.

Step 1 If you entered the password correctly in the Enter Password screen, the CEM screen appears (see Figure 4-3).

Figure 4-3 CEM Screen



A checkmark appears in the Already Set? box for all existing static WEP keys.

Note For security reasons, the codes for existing static WEP keys do not appear on the screen.

Step 2 Perform one of the following:

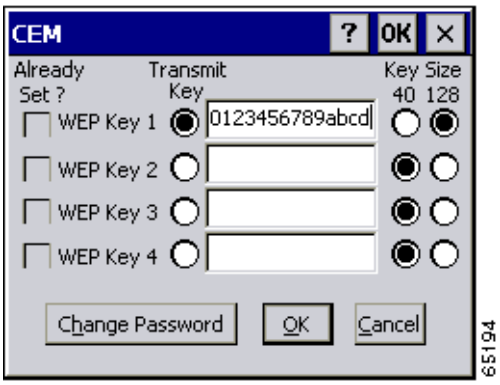
- If no static WEP keys have been set, go to the "Entering a New Static WEP Key and Enabling Static WEP" section on page 4-7 to set up one or more static WEP keys.
- If you want to use an existing static WEP key, make sure the **Transmit Key** button to the left of the key is selected and click **OK**. This is the key that will be used to transmit packets. Then open ACU and make sure WEP is enabled.
- If you want to overwrite an existing static WEP key, go to the "Overwriting an Existing Static WEP Key" section on page 4-9.

Entering a New Static WEP Key and Enabling Static WEP

Follow the steps below to enter a new static WEP key for your client adapter.

Step 1 If you entered the password correctly in the Enter Password screen, the CEM screen appears (see Figure 4-4).

Figure 4-4 CEM Screen



This screen allows you to create up to four static WEP keys.

Step 2 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 screen. 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 grayed out, and you are unable to select it.

Step 3 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 can consist of the following hexadecimal characters: 0-9, A-F, and a-f.
- WEP keys must contain the following number of characters:
  - 10 hexadecimal characters for 40-bit keys
    Example: 12345abcde
  - 26 hexadecimal characters for 128-bit keys
    Example: AB34CD78EFab01cd23ef456789
- Your client adapter's WEP key must match the WEP key used by the access point (in infrastructure mode) or clients (in ad hoc mode) with which you are planning to communicate.
- 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.

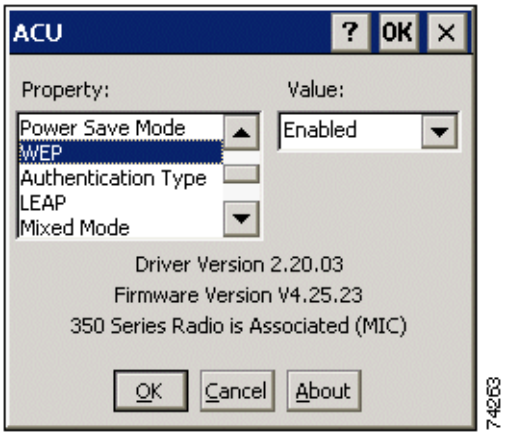
Note After you enter a WEP key, you can write over it, but you cannot edit or delete it.

Step 4 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 5 Click **OK** to write your WEP key(s) to the client adapter's volatile memory and the Windows CE registry and to exit the utility or click **Cancel** to exit the utility without updating the keys.

Step 6 Double-click the **Cisco ACU icon** or select **Start > Programs > Cisco > Aironet Client Utility**. The ACU screen appears (see Figure 4-5).

Figure 4-5 ACU Screen



Step 7 Select **WEP** under Property. Select **Enabled** from the list of options in the Value box to enable static WEP.

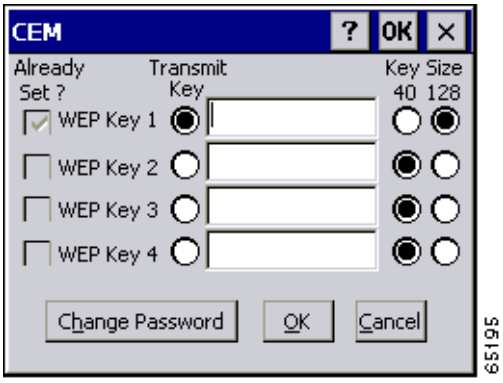
Step 8 Click **OK** to save your changes and to exit the utility.

Overwriting an Existing Static WEP Key

Follow the steps below to overwrite an existing static WEP key.

Step 1 If you entered the password correctly in the Enter Password screen, the CEM screen appears (see Figure 4-6).

Figure 4-6 CEM Screen



A checkmark appears in the Already Set? box for all existing static WEP keys.

Note For security reasons, the codes for existing static WEP keys do not appear on the screen. Also, you can write over existing keys, but you cannot edit or delete them.

Step 2 Decide which existing static WEP key you want to overwrite.

Step 3 Click within the blank field of that key.

Step 4 Enter a new key, following the guidelines outlined in Step 3 of the "Entering a New Static WEP Key and Enabling Static WEP" section on page 4-7.

Step 5 Make sure the **Transmit Key** button to the left of your key is selected, if you want this key to be used to transmit packets.

Step 6 Click **OK** to write your new static WEP key to the client adapter's volatile memory and the Windows CE registry and to exit the utility or click **Cancel** to exit the utility without overwriting any keys.

Step 7 Open ACU and make sure WEP is enabled.

Changing the CEM Password

Follow the steps below if you want to change the password that allows you to access CEM.

Note For security reasons, Cisco recommends that you change the default password.

Step 1 Double-click the **Cisco CEM icon** or select **Start > Programs > Cisco > Client Encryption Manager**.

Step 2 Enter the correct password in the Enter Password screen (see Figure 4-2) and click **OK**. The CEM screen appears (see Figure 4-6).

Step 3 Click the **Change Password** button. The Change Password screen appears (see Figure 4-7).

Figure 4-7 Change Password Screen

Step 4 Enter the current password in the Existing Password field.

Step 5 Enter a new password in the New Password field.

Note Passwords are case sensitive and can contain up to 256 alphanumeric characters.

Step 6 Re-enter the new password in the Confirm New Password field.

Step 7 Click **OK** to save your new password or click **Cancel** to exit the screen without changing the password. If your password is accepted, the following message appears, "Password Successfully Changed."

Step 8 Click **OK** to exit the utility.

Disabling Static WEP

Follow the steps below if you ever need to disable static WEP.

Step 1 Double-click the **Cisco ACU icon** or select **Start > Programs > Cisco > Aironet Client Utility**. The ACU screen appears (see Figure 4-5).

Step 2 Select **WEP** under Property. Select **Disabled** from the list of options in the Value box to disable WEP.

Step 3 Click **OK** to save your changes and to exit the utility.

Using LEAP

This section provides instructions for enabling LEAP and entering the LEAP username and password.

Note LEAP is supported only on client adapters that support WEP and use firmware version 4.13 or greater.

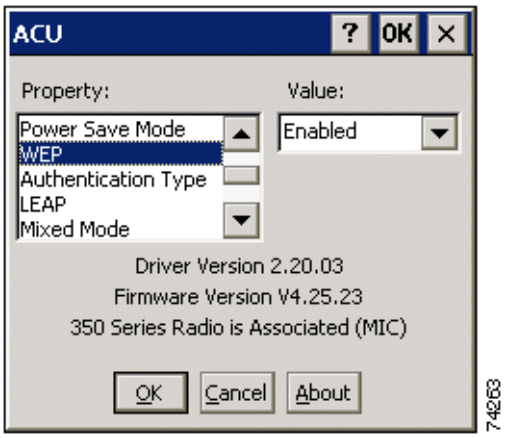
Note In order to use LEAP authentication, your client adapter and access point firmware must have matching 802.1X draft standards. That is, if the access point uses draft 8 firmware (prior to 11.06) or has draft 8 selected, the client adapter must use draft 8 firmware (prior to 4.25.x). Similarly, if the access point uses draft 10 firmware (11.06 or later) and has draft 10 selected, the client adapter must use draft 10 firmware (4.25.x or later).

Enabling LEAP

Follow the steps below to enable LEAP for your client adapter.

Step 1 Double-click the **Cisco ACU icon** or select **Start > Programs > Cisco > Aironet Client Utility**. The ACU screen appears (see Figure 4-8).

Figure 4-8 ACU Screen



Step 2 Select **LEAP** under Property.

Step 3 Select **Enabled** in the Value box.

Step 4 Click **OK** to enable LEAP and exit the utility. When LEAP is enabled, the following parameters in the ACU screen are changed automatically:

- WEP is set to Enabled.
- Authentication Type is set to Open.

Entering the LEAP Username and Password

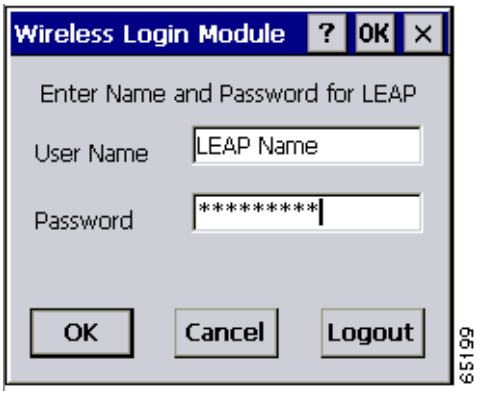
Follow the steps below to enter the LEAP username and password.

Step 1 WLM starts automatically whenever you start ACU with a client adapter inserted, change the LEAP parameter from Disabled to Enabled, and click **OK**. If LEAP is already enabled, WLM starts automatically whenever you insert the client adapter, reboot or reset the Windows CE device, or load new firmware.

Note You can also start WLM by selecting **Start > Programs > Cisco > Wireless Login Module**. You may want to do this if you inadvertently exited WLM after it started or if you roam to a different part of the network where a different login is required.

When WLM starts, the Wireless Login Module screen appears (see Figure 4-9).

Figure 4-9 Wireless Login Module Screen



Step 2 Obtain the username and password for your RADIUS server account from your system administrator.

Note The password is optional because not all host accounts on the RADIUS server are set up with a password.

Step 3 Enter the username in the User Name field.

Note Usernames and passwords are case sensitive and can contain up to 32 alphanumeric characters.

Note If your device is running Windows CE 3.0 version 2002 and your RADIUS server account specifies a domain, enter the domain name before the username and separate the two with a forward slash (e.g., *domain/username*).

Step 4 Enter the password in the Password field if the RADIUS server account for the Windows CE device was set up with a password.

Note For security reasons, the characters entered for the password are displayed as asterisks.

Step 5 Click **OK**. If the username and password were entered correctly, they are written to volatile memory on the client adapter. The username and password remain on the client adapter until power is removed from the adapter, typically due to the client adapter being ejected or the system powering down.

Note If a username and password are stored in the client adapter's Flash memory from a prior release, they are erased before the new username and password are written to the adapter's volatile memory, thereby disabling device-level LEAP.

Step 6 One of three scenarios occurs:

1. The client adapter authenticates to the RADIUS server using your username and password and receives a dynamic, session-based WEP key. The bottom of the ACU screen indicates that your client adapter is authenticated to an access point.
2. If you enter the username and password incorrectly or enter ones that are not valid for the RADIUS server on the network, the Wireless Login Module screen reappears with a message indicating that your login was incorrect. You are able to retry immediately by re-entering the username and password.
3. The client adapter times out while trying to authenticate, possibly because it is out of range of an access point. After 60 seconds, a message appears indicating that the first attempt to authenticate failed and that the client adapter will continue trying.

Note During the 60 seconds before the timeout occurs, WLM is running in the background. It is hidden and does not appear as a running program. If you try to start WLM during this time, nothing happens because it is already running.

Disabling LEAP

Follow the steps below if you ever need to disable LEAP.

Step 1 Double-click the **Cisco ACU icon** or select **Start > Programs > Cisco > Aironet Client Utility**. The ACU screen appears (see Figure 4-8).

Step 2 Select **LEAP** under Property.

Step 3 Select **Disabled** in the Value box.

Step 4 Click **OK** to disable LEAP and to exit the utility.